
Amazon Elastic Compute Cloud

User Guide for Linux Instances



Amazon Elastic Compute Cloud: User Guide for Linux Instances

Copyright © 2019 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon's trademarks and trade dress may not be used in connection with any product or service that is not Amazon's, in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits Amazon. All other trademarks not owned by Amazon are the property of their respective owners, who may or may not be affiliated with, connected to, or sponsored by Amazon.

Table of Contents

O que é o Amazon EC2?	1
Recursos do Amazon EC2	1
Conceitos básicos do Amazon EC2	1
Serviços relacionados	2
Acessando o Amazon EC2	3
Definição de preço do Amazon EC2	4
Conformidade do PCI DSS	4
Instâncias e AMIs	4
Instâncias	5
AMIs	6
Regiões e Zonas de disponibilidade	7
Conceitos sobre região e zona de disponibilidade	7
Regiões disponíveis	8
Regiões e endpoints	10
Descrição de regiões e zonas de disponibilidade	10
Especificação da região para um recurso	12
Execução de instâncias em uma zona de disponibilidade	14
Migração de uma instância para outra zona de disponibilidade	14
Volume do dispositivo raiz	15
Conceitos de armazenamento do dispositivo raiz	15
Escolha de uma AMI por tipo de dispositivo raiz	17
Determinação do tipo de dispositivo raiz da sua instância	18
Alteração do volume do dispositivo raiz para persistência	18
Configuração	21
Cadastre-se na AWS	21
Criar um usuário da IAM	21
Criar um par de chaves	23
Criar uma Virtual Private Cloud (VPC)	26
Criar um security group	26
Conceitos básicos	30
Visão geral	30
Pré-requisitos	31
Etapa 1: Executar uma instância	31
Etapa 2: Conecte-se à sua instância	32
Etapa 3: Limpar a instância	32
Próximas etapas	33
Melhores práticas	34
Tutoriais	36
Instalar um servidor LAMP (Amazon Linux 2)	36
Etapa 1: Preparar o servidor LAMP	36
Etapa 2: Testar o servidor LAMP	40
Etapa 3: proteger o servidor do banco de dados	41
Etapa 4: (opcional) instalar o phpMyAdmin	42
Solução de problemas	45
Tópicos relacionados	45
Instalar um servidor LAMP (Amazon Linux AMI)	46
Solução de problemas	45
Tópicos relacionados	45
Tutorial: Hospedagem de um blog do WordPress	56
Pré-requisitos	57
Instalar o WordPress	57
Próximas etapas	63
Ajuda! Meu nome DNS público mudou e agora meu blog quebrou	64
Tutorial: Configurar o servidor web Apache no Amazon Linux 2 para usar SSL/TLS	65

Pré-requisitos	65
Etapa 1: Habilitar SSL/TLS no servidor	66
Etapa 2: Obter um certificado assinado por uma CA	68
Etapa 3: Testar e intensificar a configuração de segurança	73
Solução de problemas	75
Apêndice: Let's Encrypt com o Certbot no Amazon Linux 2	76
Tutorial: Como aumentar a disponibilidade do seu aplicativo	80
Pré-requisitos	81
Dimensione e faça o load balancing do seu aplicativo	81
Teste seu load balancer	83
Tutorial: Gerenciar remotamente suas instâncias	84
Conceder o acesso à conta de usuário ao Systems Manager	84
Instalar o agente de SSM	85
Enviar um comando usando o console do EC2	85
Enviar um comando usando AWS Tools para Windows PowerShell	86
Enviar um comando usando a AWS CLI	87
Conteúdo relacionado	88
Imagens de máquina da Amazon	89
Como usar uma AMI	89
Como criar sua própria AMI	89
Como comprar, compartilhar e vender AMIs	90
Cancelamento do registro da sua AMI	90
Amazon Linux 2 e Amazon Linux AMI	90
Tipos de AMI	91
Permissões de execução	91
Armazenamento para o dispositivo raiz	91
Tipos de virtualização	94
Localizar uma AMI do Linux	95
Localizar AMI do Linux usando o console do Amazon EC2	95
Localizar uma AMI usando o AWS CLI	96
Encontrar uma AMI de início rápido	96
AMIs compartilhadas	97
Localização de AMIs compartilhadas	98
Transformação em AMI pública	100
Compartilhamento de uma AMI com contas específicas da AWS	101
Uso de favoritos	103
Diretrizes para AMIs em Linux compartilhadas	103
AMIs pagas	107
Como vender sua AMI	108
Como encontrar uma AMI paga	108
Comprar uma AMI paga	109
Como obter o código de produto para sua instância	110
Como usar suporte pago	110
Faturas para AMI pagas e compatíveis	111
Gerenciamento de suas assinaturas do AWS Marketplace	111
Criação de uma AMI do Linux com Amazon EBS	111
Visão geral da criação de AMIs com Amazon EBS	112
Criação de uma AMI do Linux de uma instância	112
Criação de uma AMI do Linux de um snapshot	114
Criação de uma AMI em Linux com armazenamento de instâncias	115
Visão geral do processo de criação para AMIs baseadas no armazenamento de instâncias	116
Pré-requisitos	116
Configuração das ferramentas de AMI	117
Criação de uma AMI com base em uma instância com armazenamento de instâncias	120
Conversão em AMI com Amazon EBS	127
Referência ferramentas de AMI	130
AMIs com snapshots criptografados	147

Cenários de AMIs que envolvem snapshots criptografados do EBS	148
Cópia de uma AMI	150
Permissões para copiar uma AMI com armazenamento de instâncias	151
Cópia da AMI de outra região	151
Cópia da AMI entre contas	152
Criptografia e cópia de AMI	153
Cópia de uma AMI	154
Parada de uma operação de cópia de AMI pendente	155
Cancelar o registro da AMI do Linux	156
Limpeza da sua AMI com Amazon EBS	156
Limpeza da sua AMI com armazenamento de instâncias	157
Amazon Linux	158
Conexão com uma instância do Amazon Linux	158
Identificação de imagens do Amazon Linux	159
Ferramentas de linha de comando da AWS	160
Repositório de pacotes	161
Biblioteca de extras (Amazon Linux 2)	163
Como acessar pacotes de origem para referência	163
cloud-init	163
Como assinar notificações do Amazon Linux	165
Execução do Amazon Linux 2 como uma máquina virtual local	166
Kernels fornecidos pelo usuário	169
AMIs HVM (GRUB)	170
AMIs paravirtuais (PV-GRUB)	171
Instâncias	176
Tipos de instância	176
Tipos de instância disponíveis	177
Especificações de hardware	178
Tipos de virtualização de AMI	179
Instâncias baseadas em Nitro	179
Recursos de redes e armazenamento	180
Limites das instâncias	182
Instâncias de uso geral	182
Instâncias otimizadas para computação	219
Instâncias otimizadas para memória	223
Instâncias otimizadas para armazenamento	231
Instâncias computacionais aceleradas	237
Alterar o tipo de instância	247
Opções de compra de instância	251
Determinação do ciclo de vida da instância	252
Instâncias reservadas	253
Instâncias programadas	289
Instâncias spot	293
Hosts dedicados	356
Instâncias dedicadas	371
Reservas de capacidade sob demanda	376
Ciclo de vida da instância	385
Execução da instância	386
Parada e início de instância (somente instâncias baseadas em Amazon EBS)	387
Hibernação de instância (somente instâncias baseadas em Amazon EBS)	387
Reinicialização da instância	388
Inativação da instância	388
Encerramento da instância	388
Diferenças entre reinicialização, parada, hibernação e encerramento	389
Executar	390
Conecte-se	439
Parar e iniciar	458

Hibernar	461
Reinicializar	467
Retirada	468
Encerrar	470
Recuperar	476
Configurar instâncias	477
Cenários de configuração comuns	477
Gerenciamento de software	478
Gerenciamento de usuários	483
Controle do estado do processador	485
Definição de horário	491
Otimizar opções de CPU	495
Alteração do nome do host	506
Configuração do DNS dinâmico	508
Execução de comandos na inicialização	510
Metadados da instância e dados do usuário	516
Identificar instâncias	531
Inspeção do documento de identidade da instância	532
Inspeção do UUID do sistema	532
Elastic Inference	534
Conceitos básicos de Amazon EI	534
Definição de preço do Amazon EI	535
Considerações sobre o Amazon EI	535
Escolha de uma instância e de um tipo de acelerador para seu modelo	536
Uso do Amazon Elastic Inference com Auto Scaling do EC2	536
Como trabalhar com o Amazon EI	537
Configuração	537
Modelos TensorFlow	542
Modelos MXNet	552
Uso das métricas do CloudWatch para monitorar o Amazon EI	557
Métricas e dimensões do Amazon EI	558
Criação de alarmes do CloudWatch para monitorar o Amazon EI	559
Solução de problemas	560
Problemas na execução de aceleradores	560
Resolver problemas de configuração	560
Resolução de problemas de conectividade	560
Como resolver problemas de status não íntegro	560
Parar e iniciar a instância	560
Solução de problemas de desempenho de modelos	561
Como enviar comentários	561
Monitoramento	562
Monitoramento automático e manual	563
Ferramentas de monitoramento automatizadas	563
Ferramentas de monitoramento manual	564
Melhores práticas de monitoramento	565
Monitoramento do status de suas instâncias	565
Verificações de status de instâncias	565
Eventos agendados	570
Monitoramento das suas instâncias usando o CloudWatch	575
Habilitar monitoramento detalhado	575
Listar métricas disponíveis	577
Obter estatísticas para métricas	586
Represente métricas em gráficos	594
Criar um alarme	594
Crie alarmes para parar, encerrar, reiniciar ou recuperar uma instância	595
Automatizar o Amazon EC2 com os Eventos do CloudWatch	604
Monitoramento das métricas de memória e disco	605

Novo agente do CloudWatch disponível	605
Scripts de monitoramento do CloudWatch	605
Registrar em log chamadas à API com o AWS CloudTrail	613
Informações sobre o Amazon EC2 e o Amazon EBS no CloudTrail	614
Noções básicas sobre as entradas no arquivos de log do Amazon EC2 e do Amazon EBS	614
Rede e segurança	616
Pares de chaves	616
Criação de um par de chaves usando o Amazon EC2	617
Importação da sua própria chave pública para o Amazon EC2	618
Recuperação da chave pública para seu par de chaves no Linux	619
Recuperação da chave pública para seu par de chaves no Windows	620
Recuperação da chave pública para seu par de chaves a partir da sua instância	620
Verificação da impressão digital do seu par de chaves	621
Excluir o par de chaves	621
Adição ou substituição de um par de chaves para sua instância	622
Conexão à sua instância do Linux se você perder sua chave privada	623
Grupos de segurança	626
Regras de security groups	627
Security groups padrão	629
Security groups personalizados	630
Como trabalhar com security groups	630
Referência de regras de security groups	634
Controlar o acesso	641
Acesso à rede para a instância	641
Atributos de permissões do Amazon EC2	641
IAM e Amazon EC2	642
Políticas do IAM	643
Funções do IAM	712
Acesso à rede	720
Endereçamento IP de instâncias	723
Endereços IPv4 privados e nomes de host DNS internos	723
Endereços IPv4 públicos e nomes de host DNS externos	724
Endereços IP elásticos (IPv4)	725
Servidor DNS da Amazon	725
Endereços IPv6	725
Como trabalhar com endereços IP para a instância	726
Vários endereços IP	730
Traga seus próprios endereços IP	738
Requisitos	739
Preparar-se para levar seu intervalo de endereços para sua conta da AWS	739
Provisionar o intervalo de endereços para uso com a AWS	740
Anunciar o intervalo de endereços por meio da AWS	741
Desprovisionar o intervalo de endereços	741
Endereços Elastic IP	742
Noções básicas sobre endereços IP elásticos	742
Como trabalhar com endereços IP elásticos	743
Como usar o DNS reverso para aplicativos de e-mail	747
Limite de endereços IP elásticos	747
Interfaces de rede	747
Informações básicas de interfaces de rede	748
Endereços IP por interface de rede por tipo de instância	749
Cenários para interfaces de rede	755
Práticas recomendadas para configurar interfaces de rede	757
Trabalho com interfaces de rede	758
Interfaces de rede gerenciadas pelo solicitante	767
Redes avançadas	768
Tipos de rede avançada	768

Como habilitar a rede avançada na instância	768
Redes avançadas: ENA	769
Rede avançada: Intel 82599 VF	780
Solução de problemas do ENA	786
Placement groups	793
Placement groups de cluster	793
Placement groups de partição	794
Placement groups de distribuição	795
Regras e limitações do placement group	795
Criação de um placement group	797
Execução de instâncias em um placement group	797
Descrever instâncias em um placement group	798
Como alterar o placement group de uma instância	799
Exclusão de um placement group	800
Conexão MTU	801
Frames jumbo (9001 MTU)	801
Path MTU Discovery	802
Verifique o MTU do caminho entre dois hosts	802
Verificar e definir o MTU na instância do Linux	803
Solução de problemas	803
Virtual Private Clouds	804
Documentação do Amazon VPC	804
EC2-Classic	804
Detecção de plataformas com suporte	804
Tipos de instância disponíveis no EC2-Classic	806
Diferenças entre instâncias no EC2-Classic e em uma VPC	806
Compartilhamento e acesso a recursos entre o EC2-Classic e uma VPC	811
ClassicLink	812
Migração do EC2-Classic para uma VPC	826
Armazenamento	838
Amazon EBS	839
Recursos do Amazon EBS	840
Volumes do EC2	841
Snapshots do EBS	896
Otimização do EBS	916
Criptografia do EBS	926
Volumes do EBS e NVMe	929
Desempenho do EBS	932
Eventos do EBS CloudWatch	950
Armazenamento de instâncias	958
Vida útil do armazenamento de instâncias	958
Volumes de armazenamento de instâncias	959
Adicionar volumes de armazenamento de instâncias	962
Volumes de armazenamento de instâncias SSD	965
Volumes de troca de armazenamento de instâncias	967
Como otimizar o desempenho dos discos	969
Armazenamento de arquivos	970
Amazon EFS	970
Amazon FSx	974
Amazon S3	974
Amazon S3 e Amazon EC2	975
Limites de volume de instância	976
Limites de volume específicos do Linux	976
Limites de volume específicos do Windows	977
Limites de tipo de instância	977
Largura de banda x capacidade	977
Nomenclatura de dispositivos	978

Nomes de dispositivos disponíveis	978
Considerações sobre nomes de dispositivos	979
Mapeamento de dispositivos de blocos	979
Conceitos de mapeamento de dispositivos de blocos	980
Mapeamento de dispositivos de blocos da AMI	983
Mapeamento de dispositivos de blocos da instância	985
Como usar bancos de dados públicos	989
Conceitos de bancos de dados públicos	989
Como localizar bancos de dados públicos	990
Como criar um volume de banco de dados público em um snapshot	990
Como anexar e montar o volume de banco de dados público	991
Recursos e tags	992
Locais de recursos	992
IDs de recursos	993
Como trabalhar com IDs mais longos	994
Controle do acesso a configurações de ID mais longo	998
Listagem e filtragem dos seus recursos	999
Pesquisa avançada	999
Listagem dos recursos usando o console	1000
Filtro dos recursos usando o console	1001
Listagem e filtragem com o uso de CLI e API	1002
Atribuição de tags aos seus recursos	1003
Conceitos básicos de tags	1003
Marcação dos seus recursos	1004
Restrições de tag	1007
Marcação dos seus recursos para faturamento	1007
Trabalho com tags usando o console	1008
Trabalho com tags usando a CLI ou a API	1011
Service Limits	1013
Visualizando seus limites atuais	1013
Como solicitar um aumento de limite	1014
Limites de e-mails enviados usando a porta 25	1015
Relatórios de uso do	1015
EC2Rescue para Linux	1016
Instalação do EC2Rescue para Linux	1016
(Opcional) Verifique a assinatura de EC2Rescue para Linux	1017
Instalar as ferramentas do GPG	1017
Autenticar e importar a chave pública	1018
Verificar a assinatura do pacote	1018
Como trabalhar com EC2Rescue para Linux	1019
Executar o EC2Rescue para Linux	1019
Como fazer upload dos resultados	1020
Criação de backups	1020
Receber ajuda	1021
Desenvolvimento de módulos do EC2Rescue	1021
Como adicionar atributos de módulo	1021
Como adicionar variáveis de ambiente	1024
Uso da sintaxe de YAML	1024
Exemplos de módulo	1025
Solução de problemas	1026
Solução de problemas de execução	1026
Limite de instâncias excedido	1026
Capacidade insuficiente da instância	1027
A instância é encerrada imediatamente	1027
Conectar à sua instância	1028
Erro ao se conectar à sua instância: limite de tempo da conexão atingido	1029
Erro: Chave do usuário não reconhecida pelo servidor	1031

Erro: Chave do host não encontrada, permissão negada (publickey) ou Falha na autenticação, permissão negada	1032
Erro: Arquivo de chave privada desprotegido	1033
Erro: a chave privada deve começar com "----BEGIN RSA PRIVATE KEY----" e terminar com "----END RSA PRIVATE KEY----"	1034
Erro: O servidor recursou nossa chave ou Não há métodos de autenticação compatíveis	1034
Erro ao usar o MindTerm no navegador Safari	1035
Não é possível fazer o ping da instância	1035
Interrupção da instância	1035
Criar uma instância de substituição	1036
Encerrar sua instância	1037
Encerramento atrasado da instância	1037
Instância encerrada ainda sendo exibida	1037
Execute ou encerre automaticamente as instâncias	1037
Falha nas verificações de status	1038
Analizar informações de verificação de status	1039
Recuperar os logs do sistema	1039
Resolução de problemas dos erros no log do sistema para instâncias baseadas em Linux	1040
Sem memória: encerrar processo	1041
ERRO: falha em mmu_update (falha na atualização do gerenciamento de memória)	1041
Erro de E/S (Falha de dispositivo de blocos)	1042
ERRO DE E/S: nem disco local nem disco remoto (o dispositivo de blocos distribuído está quebrado)	1043
request_module: modprobe de loop descontrolado (modprobe do kernel legado do looping, em versões mais antigas do Linux)	1044
"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)	1045
"FATAL: Não foi possível carregar os módulos /lib/" ou "BusyBox" (módulos do kernel ausentes)	1045
ERRO Kernel inválido (kernel incompatível com EC2)	1047
request_module: modprobe de loop descontrolado (modprobe do kernel legado do looping, em versões mais antigas do Linux)	1048
fsck: Nenhum arquivo ou diretório ao tentar abrir... (Sistema de arquivos não encontrado)	1049
Erro geral ao montar os sistemas de arquivos (falha na montagem)	1050
VFS: Não foi possível montar o fs raiz em um bloco desconhecido (falta de correspondência no sistema de arquivos-raiz)	1052
Erro: não foi possível determinar o número principal/secundário do dispositivo raiz... (Incompatibilidade entre sistema de arquivos/dispositivo raiz)	1053
XENBUS: Dispositivo sem driver...	1054
...dias sem ser verificada, verificação forçada (verificação necessária para o sistema de arquivos)	1055
O fsck morreu com status de saída... (Dispositivo ausente)	1055
Prompt do GRUB (grubdom>)	1056
Acessando a interface eth0: O dispositivo eth0 tem um endereço MAC diferente do esperado, ignorando. (Endereço MAC hard-coded)	1058
Não foi possível carregar a Política do SELinux. A máquina está no modo de força. Parando agora. (Erro de configuração do SELinux)	1059
XENBUS: Excedido o limite de tempo para se conectar a dispositivos (tempo limite do Xenbus) ..	1060
Falhas de recuperação da instância	1061
Obtenção de instâncias de saída e reinicialização do console	1061
Reinicialização da instância	1062
Saída do console da instância	1062
Faça uma captura de tela da instância inatingível	1063
Recuperação da instância quando um computador host falhar	1063
Inicialização a partir do volume errado	1064
Histórico do documento	1066
AWS Glossary	1091

O que é o Amazon EC2?

O Amazon Elastic Compute Cloud (Amazon EC2) oferece uma capacidade de computação dimensionável 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. Você pode usar o Amazon EC2 para executar o número de servidores virtuais que precisar, configurar a segurança e a rede, e gerenciar o armazenamento. O Amazon EC2 também permite a expansão ou a redução para gerenciar as alterações de requisitos ou picos de popularidade, reduzindo, assim, a sua necessidade de prever o tráfego do servidor.

Para obter mais informações sobre computação em nuvem, consulte [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 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 conectar à sua própria rede, conhecidas como nuvens privadas virtuais (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 [Hospedagem na web](#).

Conceitos básicos do Amazon EC2

Primeiro, você precisa fazer é configurar o Amazon EC2 para ser usado. Após a configuração, você estará pronto para concluir o tutorial 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

- [Como configurar com o Amazon EC2 \(p. 21\)](#)
- [Conceitos básicos das instâncias do Amazon EC2 do Linux \(p. 30\)](#)

Conceitos básicos

- [Instâncias e AMIs \(p. 4\)](#)
- [Regiões e zonas de disponibilidade \(p. 7\)](#)
- [Tipos de instância \(p. 176\)](#)
- [Tags \(p. 1003\)](#)

Redes e segurança

- [Pares de chaves do Amazon EC2 \(p. 616\)](#)
- [Grupos de segurança \(p. 626\)](#)
- [Endereços Elastic IP \(p. 742\)](#)
- [Amazon EC2 e Amazon VPC \(p. 804\)](#)

Armazenamento

- [Amazon EBS \(p. 839\)](#)
- [Armazenamento de instâncias \(p. 958\)](#)

Como trabalhar com instâncias do Linux

- [Gerenciamento remoto \(Run Command\)](#)
- [Tutorial: Instalar um servidor web LAMP no Amazon Linux 2 \(p. 36\)](#)
- [Tutorial: Configurar o servidor web Apache no Amazon Linux 2 para usar SSL/TLS \(p. 65\)](#)
- [Conceitos básicos da AWS: Hospedar uma aplicação web para Linux](#)

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 [Amazon EC2 forum](#).

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 da AWS. Para obter mais informações, consulte a documentação a seguir:

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

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

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 automatizar as ações, como a ativação de uma função do Lambda sempre que uma nova instância do Amazon EC2 é iniciada ou a invocação do comando de execução do SSM sempre que ocorre um evento em outro serviço da AWS, use o Eventos do Amazon CloudWatch. Para obter mais informações, consulte [Guia do usuário do Eventos do Amazon CloudWatch](#).

Para monitorar as chamadas feitas para a API do Amazon EC2 para sua conta, incluindo as chamadas feitas pelo Console de gerenciamento da AWS, ferramentas de linha de comando e outros serviços, use o AWS CloudTrail. Para obter mais informações, consulte o [AWS CloudTrail User Guide](#).

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 [Guia do desenvolvedor do Amazon Relational Database Service](#).

Para importar imagens de máquina virtual (VM) de seu ambiente local para a AWS e convertê-las em AMIs ou instâncias prontas para uso, use o VM Import/Export. Para mais informações, consulte o [Guia do usuário de VM Import/Export](#).

Acessando 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 Console de gerenciamento da AWS e selecionando EC2 na página inicial do console.

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

Interface da linha de comando (CLI) da AWS

Fornece comandos para um conjunto amplo de produtos da AWS e é compatível com Windows, Mac e Linux. Para começar, consulte o [Guia do usuário do AWS Command Line Interface](#). Para obter mais informações sobre comandos para o Amazon EC2, consulte `ec2` no AWS CLI Command Reference.

AWS Tools para Windows PowerShell

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

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 [SDKs e ferramentas da 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:

Instâncias on-demand

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

Instâncias reservadas

Faça um pagamento inicial baixo e único por uma instância, reserve-a pelo prazo de um ou de três anos e pague uma taxa significativamente menor por hora por essas instâncias.

Instâncias spot

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

Para obter uma lista completa de cobranças e preços específicos para o 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 a [página Atividade da conta da AWS](#). Sua fatura contém links para relatórios de uso que fornecem detalhes sobre sua conta. Para saber mais sobre o faturamento de contas da AWS, consulte [Faturamento de contas da AWS](#).

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

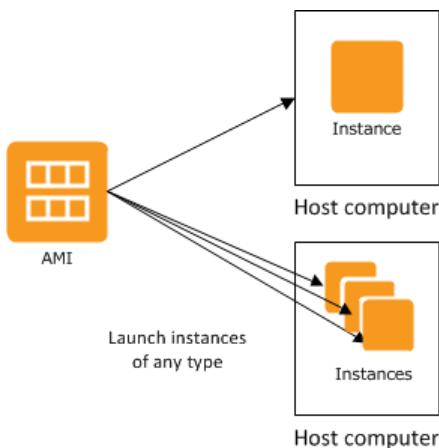
Para obter uma visão geral do Trusted Advisor, um serviço que ajuda você a aperfeiçoar os custos, a segurança e o desempenho do ambiente da AWS, consulte [AWS Trusted Advisor](#).

Conformidade do PCI DSS

Amazon EC2 oferece suporte a processamento, armazenamento e transmissão de dados de cartão de crédito por um comerciante ou provedor de serviços, e foi validado como em conformidade com o Data Security Standard (DSS – Padrão de segurança de dados) da Payment Card Industry (PCI – Setor de cartão de crédito). Para obter mais informações sobre PCI DSS, incluindo como solicitar uma cópia do pacote de conformidade com PCI da AWS, consulte [Nível 1 do PCI DSS](#).

Instâncias e AMIs

Uma Imagem de máquina da Amazon (AMI) é um modelo que contém uma configuração de software (por exemplo, sistema operacional, servidor de aplicativo e aplicativos). 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 ou encerre, ou até que elas falhem. Se uma instância falhar, você pode executar uma nova instância a partir da AMI.

Instâncias

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 o aplicativo ou software que você pretende executar na instância. Para obter mais informações sobre as especificações de hardware para cada tipo de instância do Amazon EC2, veja [Tipos de instâncias 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 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. Para obter mais informações, consulte [Volume do dispositivo raiz do Amazon EC2 \(p. 15\)](#).

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 [Mapeamento de dispositivos de blocos \(p. 979\)](#). 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 [Armazenamento \(p. 838\)](#).

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 da IAM sob sua conta da AWS,

atribuir credenciais de segurança a cada um e controlar o acesso que cada tem dos recursos e serviços da AWS. Para obter mais informações, consulte [Como controlar o acesso aos recursos do Amazon EC2 \(p. 641\)](#).

- 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 \(p. 626\)](#).
- 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 [Desabilite logins remotos com senha para raiz \(p. 104\)](#). Para obter mais informações sobre compartilhamento seguro das AMIs, consulte [AMIs compartilhadas \(p. 97\)](#).

Interrupção, início e encerramento das instâncias

Como parar 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 \(p. 385\)](#).

AMIs

A Amazon Web Services (AWS) publica muitas imagens de máquina da Amazon (AMI) 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 seu aplicativo 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 seu aplicativo fica pronto 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 \(p. 91\)](#).

Regiões e Zonas de disponibilidade

O Amazon EC2 está hospedado em vários locais no mundo todo. Esses locais são compostos por regiões e zonas de disponibilidade. Cada região é uma área geográfica separada. Cada região possui vários locais isolados conhecidos como Zonas de disponibilidade. O Amazon EC2 lhe oferece a possibilidade de colocar recursos, como instâncias e dados em vários locais. Os recursos não são replicados entre as diversas regiões, a menos que você especifique isso.

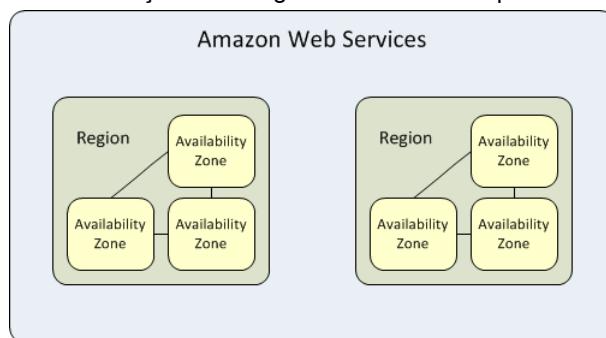
A Amazon opera datacenters de última geração e altamente disponíveis. Embora sejam raras, podem ocorrer falhas que afetam a disponibilidade das instâncias que estão no mesmo local. Se você hospedar todas as suas instâncias em um único local afetado por tal falha, nenhuma delas ficará disponível.

Tópicos

- [Conceitos sobre região e zona de disponibilidade \(p. 7\)](#)
- [Regiões disponíveis \(p. 8\)](#)
- [Regiões e endpoints \(p. 10\)](#)
- [Descrição de regiões e zonas de disponibilidade \(p. 10\)](#)
- [Especificação da região para um recurso \(p. 12\)](#)
- [Execução de instâncias em uma zona de disponibilidade \(p. 14\)](#)
- [Migração de uma instância para outra zona de disponibilidade \(p. 14\)](#)

Conceitos sobre região e zona de disponibilidade

Cada região é totalmente independente. Cada zona de disponibilidade é isolada, mas as zonas de disponibilidade de uma região são conectadas por meio de links de baixa latência. O diagrama a seguir ilustra a relação entre regiões e zonas de disponibilidade.



Os recursos do Amazon EC2 podem ser globais, vinculados a uma região ou a uma zona de disponibilidade. Para obter mais informações, consulte [Locais de recursos \(p. 992\)](#).

Regiões

Cada região da Amazon EC2 é completamente independente e isolada das outras regiões da Amazon EC2. Isso proporciona a maior tolerância a falhas e estabilidade possível.

Quando você visualizar seus recursos, somente verá os que estiverem vinculados à região especificada. Isso ocorre porque as regiões são isoladas entre si e nós não replicamos os recursos entre regiões automaticamente.

Quando você executa uma instância, 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 [Cópia de uma AMI \(p. 150\)](#).

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](#).

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 seu aplicativo para que uma instância em outra zona de disponibilidade possa processar solicitações.

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 Elastic IP \(p. 742\)](#).

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 nomes de cada conta da AWS. Por exemplo, a zona de disponibilidade us-east-1a de sua conta da AWS pode não estar no mesmo local que a us-east-1a para 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.

A visualização de IDs de AZs permite 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 [Como trabalhar com o compartilhamento de VPC](#) 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 com outra conta.

Você pode listar as zonas de disponibilidade que estão disponíveis para sua conta. Para obter mais informações, consulte [Descrição de regiões e zonas de disponibilidade \(p. 10\)](#).

Regiões disponíveis

Sua conta determina as regiões que estão disponíveis para você. Por exemplo:

- Uma conta da AWS fornece várias regiões de modo que você possa executar instâncias do Amazon EC2 em locais que atendam a seus requisitos. 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 à região AWS GovCloud (Oeste dos EUA) somente. Para obter mais informações, consulte [Região AWS GovCloud \(Oeste dos EUA\)](#).
- 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. Você não pode descrever ou acessar regiões adicionais de uma conta da AWS, como AWS GovCloud (Oeste dos EUA) ou as regiões da China.

Código	Nome
us-east-1	Leste dos EUA (Norte da Virgínia)
us-east-2	Leste dos EUA (Ohio)
us-west-1	Oeste dos EUA (Norte da Califórnia)
us-west-2	Oeste dos EUA (Oregon)
ca-central-1	Canadá (Central)
eu-central-1	UE (Frankfurt)
eu-west-1	UE (Irlanda)
eu-west-2	UE (Londres)
eu-west-3	UE (Paris)
eu-north-1	UE (Estocolmo)
ap-northeast-1	Ásia-Pacífico (Tóquio)
ap-northeast-2	Ásia-Pacífico (Seul)
ap-northeast-3	Ásia-Pacífico (Osaka – Local)
ap-southeast-1	Ásia-Pacífico (Cingapura)
ap-southeast-2	Ásia-Pacífico (Sydney)
ap-south-1	Ásia Pacífico (Mumbai)
sa-east-1	América do Sul (São Paulo)

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 [Descrição de regiões e zonas de disponibilidade \(p. 10\)](#).

Regiões e endpoints

Ao trabalhar com uma instância usando a interface de linha de comando ou ações de API, você deve especificar seu endpoint regional. Para obter mais informações sobre as regiões e os endpoints do Amazon EC2, consulte [Regiões e endpoints](#) no Referência geral do Amazon Web Services.

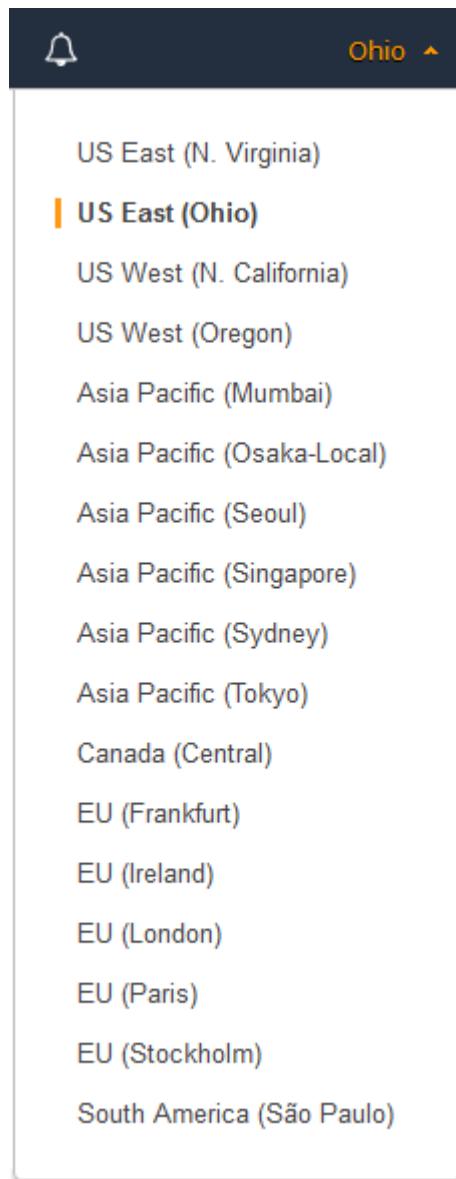
Para obter mais informações sobre os endpoints e os protocolos em AWS GovCloud (Oeste dos EUA), consulte [Endpoints AWS GovCloud \(Oeste dos EUA\)](#) no AWS GovCloud (US) User Guide.

Descrição de regiões e zonas de disponibilidade

Você pode usar o console do Amazon EC2 ou a interface de linha de comando para determinar quais regiões e zonas de disponibilidade estão disponíveis para sua conta. Para obter mais informações sobre essas interfaces de linha de comando, consulte [Acessando o Amazon EC2 \(p. 3\)](#).

Para encontrar suas regiões e 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, Availability Zone Status.

Para encontrar suas regiões e zonas de disponibilidade usando a linha de comando

1. [AWS CLI] Use o comando `describe-regions` como se segue para descrever as regiões para sua conta.

```
aws ec2 describe-regions
```

2. [AWS CLI] Use o comando `describe-availability-zones` como se segue para descrever as zonas de disponibilidade na região especificada.

```
aws ec2 describe-availability-zones --region region-name
```

3. [AWS Tools para Windows PowerShell] Use o comando [Get-EC2Region](#) como se segue para descrever as regiões para sua conta.

```
PS C:\> Get-EC2Region
```

4. [AWS Tools para Windows PowerShell] Use o comando [Get-EC2AvailabilityZone](#) como se segue para descrever as zonas de disponibilidade na região especificada.

```
PS C:\> Get-EC2AvailabilityZone -Region region-name
```

Especificação da região para um recurso

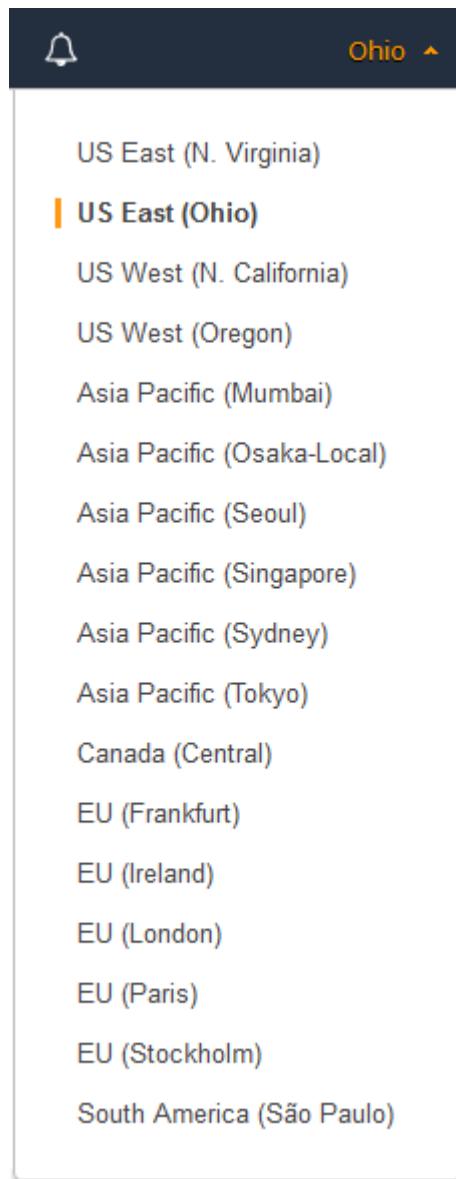
Sempre que você cria um recurso do Amazon EC2, pode especificar a região para o recurso. Você pode especificar a região para um recurso usando o Console de gerenciamento da AWS ou a linha de comando.

Note

Alguns recursos da AWS podem não estar disponíveis em todas as regiões e zonas de disponibilidade. Verifique se você pode criar os recursos necessários nas regiões ou na zona de disponibilidade desejadas antes de executar uma instância em uma zona de disponibilidade específica.

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 região 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 para Windows PowerShell)

Como alternativa, você pode usar o código `--region` (AWS CLI) ou a opção da linha de comando `-Region` (AWS Tools para 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](#).

Execução de 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 seus aplicativos 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, nós selecionaremos uma para você. Ao executar suas instâncias iniciais, recomendamos que você aceite a zona de disponibilidade padrão. Assim, nós 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, somente especifique uma zona de disponibilidade se as novas instâncias tiverem de estar próximas ou separadas de suas instâncias em execução.

Migração de uma instância para outra zona de disponibilidade

Se você precisar, poderá migrar uma instância de uma zona de disponibilidade para outra. Por exemplo, se você estiver tentando modificar o tipo de instância de sua instância e não pudermos executar uma instância do novo tipo de instância na zona de disponibilidade atual, você poderá migrar a instância para uma zona de disponibilidade onde possamos executar uma instância desse tipo de instância.

O processo de migração envolve criar uma AMI da instância original, executar uma instância na nova zona de disponibilidade e atualizar a configuração da nova instância, conforme exibido no seguinte procedimento.

Para migrar uma instância para outra zona de disponibilidade

1. Crie uma AMI 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:
 - [Criação de uma AMI do Linux com Amazon EBS \(p. 111\)](#)
 - [Criação de uma AMI em Linux com armazenamento de instâncias \(p. 115\)](#)
 - [Criação de uma AMI do Windows baseada em Amazon EBS](#)
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, deve criar AMIs de todas as instâncias em sua sub-rede de modo que você 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 [Execução de instâncias em uma zona de disponibilidade \(p. 14\)](#).
4. Se a instância original tiver um endereço IP elástico associado, associe-o à nova instância. Para obter mais informações, consulte [Desassociar um endereço IP elástico e reassociá-lo a outra instância \(p. 745\)](#).
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 [Envio de solicitações da modificação \(p. 283\)](#).

6. (Opcional) Encerre a instância original. Para obter mais informações, consulte [Como encerrar uma instância \(p. 472\)](#).

Volume do dispositivo raiz 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.

Para obter mais informações sobre os nomes de dispositivos usados pelo Amazon EC2 para seus volumes raiz, consulte [Nomenclatura de dispositivos nas instâncias do Linux \(p. 978\)](#).

Tópicos

- [Conceitos de armazenamento do dispositivo raiz \(p. 15\)](#)
- [Escolha de uma AMI por tipo de dispositivo raiz \(p. 17\)](#)
- [Determinação do tipo de dispositivo raiz da sua instância \(p. 18\)](#)
- [Alteração do volume do dispositivo raiz para persistência \(p. 18\)](#)

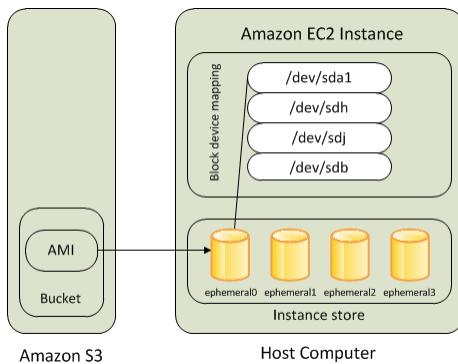
Conceitos de armazenamento do dispositivo raiz

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 \(p. 91\)](#).

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).

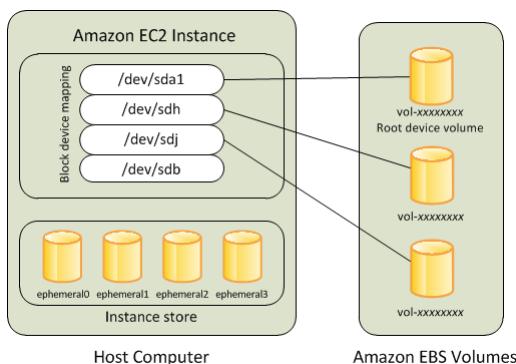


Após uma instância com armazenamento de instâncias falhar ou ser encerrada, ela não poderá ser restaurada. Se você planeja usar as instâncias baseadas em armazenamento de instâncias no Amazon EC2, recomendamos enfaticamente que distribua os dados nos seus armazenamentos de instâncias através de várias 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 \(p. 958\)](#).

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 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 [Criação de uma AMI do Linux com Amazon EBS \(p. 111\)](#).
- 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 \(p. 841\)](#).

Escolha de 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.

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.

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 [Acessando o Amazon EC2 \(p. 3\)](#).

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

Determinação do tipo de dispositivo raiz da sua instância

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

1. Abra o console do Amazon EC2.
2. No painel de navegação, selecione Instâncias e selecione a instância.
3. Verifique o valor de Root device type (Tipo de dispositivo raiz) na guia Description (Descrição), 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.

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 [Acessando o Amazon EC2 \(p. 3\)](#).

- `describe-instances` (AWS CLI)
- `Get-EC2InstanceState`

Alteração do volume do dispositivo raiz para persistência

Por padrão, o volume do dispositivo raiz de uma AMI com Amazon EBS é excluído quando a instância é encerrada. Para alterar o comportamento padrão, defina o atributo `DeleteOnTermination` como `false` usando um mapeamento de dispositivos de blocos.

Alteração do volume do dispositivo raiz para persistir 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 do dispositivo raiz de uma instância para persistir na execução usando o console

1. Abra o console do Amazon EC2.
2. No painel do console do Amazon EC2, selecione Launch Instance (Iniciar 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), desmarque Delete On Termination (Excluir ao encerrar) no volume raiz.
6. Preencha as páginas restantes do assistente e escolha Launch (Executar).

Você pode verificar a configuração exibindo detalhes do volume do dispositivo raiz 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.

Alteração do volume do dispositivo raiz de uma instância para persistir com a utilização da AWS CLI

Usando a AWS CLI, você pode alterar o atributo DeleteOnTermination quando executar uma instância ou enquanto a instância estiver sendo executada.

Example na execução

Use o comando [run-instances](#) para preservar o volume raiz incluindo um mapeamento de dispositivos de blocos 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  
    }  
  }  
]
```

Você pode confirmar se DeleteOnTermination é false usando o comando [describe-instances](#) e procurando a entrada BlockDeviceMappings para o dispositivo na saída de comando, como mostrado aqui.

```
...  
"BlockDeviceMappings": [  
  {  
    "DeviceName": "/dev/sda1",  
    "Ebs": {  
      "Status": "attached",  
      "DeleteOnTermination": false,  
      "VolumeId": "vol-1234567890abcdef0",  
      "AttachTime": "2013-07-19T02:42:39.000Z"  
    }  
  }  
...  
]
```

Example Enquanto a instância estiver sendo executada

Use o comando [modify-instance-attribute](#) para preservar o volume do dispositivo raiz incluindo um mapeamento de dispositivos 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/sda1",  
  }  
]
```

```
        "Ebs" : {  
            "DeleteOnTermination": false  
        }  
    ]
```

Como configurar com o Amazon EC2

Se já tiver se cadastrado na Amazon Web Services (AWS), você poderá começar a usar o Amazon EC2 imediatamente. Abra o console do Amazon EC2, escolha Launch Instance e siga as etapas no assistente de execução para executar a primeira instância.

Se não estiver cadastrado na AWS ou se precisar de assistência para executar a primeira instância, conclua as tarefas a seguir para se preparar para usar o Amazon EC2:

1. Cadastre-se na AWS (p. 21)
2. Criar um usuário da IAM (p. 21)
3. Criar um par de chaves (p. 23)
4. Criar uma Virtual Private Cloud (VPC) (p. 26)
5. Criar um security group (p. 26)

Cadastre-se na AWS

Quando você se cadastra na Amazon Web Services (AWS), a conta da AWS é cadastrada automaticamente em todos os serviços 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 é um novo cliente da AWS, pode começar a usar o Amazon EC2 gratuitamente. Para obter mais informações, consulte Nível gratuito da AWS.

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

Para criar uma conta da AWS

1. Abra <https://aws.amazon.com/> e escolha Create an AWS Account (Criar uma conta da AWS).

Note

Se você fez login no Console de gerenciamento da AWS usando credenciais do Usuário raiz da conta da AWS, escolha Sign in to a different account (Fazer login em uma conta diferente). Se você fez login no console usando as credenciais do IAM, escolha Sign-in using root account credentials (Fazer login usando credenciais da conta raiz). Em seguida, escolha Create a new AWS account (Criar uma conta da AWS).

2. Siga as instruções online.

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

Observe o número da conta da AWS, porque você precisará dele na próxima tarefa.

Criar um usuário da IAM

Serviços na AWS, como o Amazon EC2, exigem que você forneça credenciais ao acessá-los, para que assim possam determinar se você tem permissão para acessar seus recursos. O console requer sua

senha. Você pode criar chaves de acesso para sua conta da AWS para acessar a interface de linha de comando ou a API. Mas não recomendamos que você acesse a AWS usando as credenciais de sua conta da AWS; recomendamos que você use o AWS Identity and Access Management (IAM). Crie um usuário do IAM e, em seguida, adicione o usuário a um grupo do IAM com permissões administrativas ou conceda permissões administrativas a esse usuário. Depois você pode acessar o AWS usando um URL especial e credenciais para o usuário do IAM.

Se você tiver se cadastrado na AWS, mas não tiver criado um usuário do IAM para você mesmo, poderá criar um usando o console do IAM. Se você não estiver familiarizado com o uso do console, consulte [Como trabalhar com o Console de gerenciamento da AWS](#) para obter uma visão geral.

Para criar um usuário IAM para você mesmo e adicionar o usuário a um grupo de Administradores

1. Use seu endereço de e-mail e senha da conta da AWS para fazer login como [Usuário raiz da conta da AWS](#) no console do IAM em <https://console.aws.amazon.com/iam/>.

Note

Recomendamos que você siga as melhores práticas para utilizar o usuário do **Administrator** IAM abaixo e armazene as credenciais do usuário raiz com segurança. Faça login como usuário raiz para executar somente algumas [tarefas de gerenciamento de serviços e contas](#).

2. No painel de navegação do console, selecione Users (Usuários) e Add user (Adicionar usuário).
3. Para User name (Nome do usuário), digite **Administrator**.
4. Marque a caixa de seleção ao lado de Console de gerenciamento da AWS access (Acesso do Console de gerenciamento da AWS), selecione Custom password (Senha personalizada) e digite a senha do novo usuário na caixa de texto. Também é possível selecionar Require password reset (Exigir redefinição de senha) para forçar o usuário a criar uma nova senha na próxima vez em que fizer login.
5. Escolha Próximo: Permissões.
6. Na página Definir permissões, escolha Adicionar usuário a grupo.
7. Escolha Criar grupo.
8. Na caixa de diálogo Criar grupo, em Nome do grupo, digite **Administrators**.
9. Em Filtrar políticas, marque a caixa de seleção em Função de trabalho gerenciada pela AWS.
10. Na lista de políticas, marque a caixa de seleção AdministratorAccess. A seguir escolha Criar grupo.
11. Superte a lista de grupos, selecione a caixa de seleção para seu novo grupo. Escolha Atualizar caso necessário, para ver o grupo na lista.
12. Selecione Next: Tags (Próximo: tags) para adicionar metadados ao usuário anexando tags como pares chave-valor.
13. Escolha Próximo: Análise para ver uma lista de associações de grupos a serem adicionadas ao novo usuário. Quando você estiver pronto para continuar, selecione Criar usuário.

Você pode usar esse mesmo processo para criar mais grupos e usuários, e conceder aos seus usuários acesso aos seus recursos de conta AWS. Para saber como usar políticas para restringir as permissões de usuários a recursos específicos da AWS, acesse [Gerenciamento de acesso e Políticas de exemplo](#).

Para fazer login como esse novo usuário da IAM, faça logout do console da AWS e use a seguinte URL, em que your_aws_account_id é o número da sua conta da AWS sem os hifens (por exemplo, se o número da conta da AWS for 1234-5678-9012, o ID da conta da AWS será 123456789012):

`https://your_aws_account_id.signin.aws.amazon.com/console/`

Digite o nome do usuário do IAM (não o seu endereço de e-mail) e a senha que você acabou de criar. Quando você está conectado, a barra de navegação exibe "your_user_name @ your_aws_account_id".

Se não quiser que o URL da página de cadastro contenha o ID da sua conta da AWS, crie um alias da conta. No console do IAM, escolha Dashboard no painel de navegação. No painel, escolha Customize e insira um alias, por exemplo, o nome da sua empresa. Para fazer o login depois de criar o alias de uma conta, use o seguinte URL:

```
https://your_account_alias.signin.aws.amazon.com/console/
```

Para verificar o link de login de usuários do IAM para sua conta, abra o console do IAM e verifique o link de login de usuários do IAM no painel.

Para obter mais informações sobre IAM, consulte [IAM e Amazon EC2 \(p. 642\)](#).

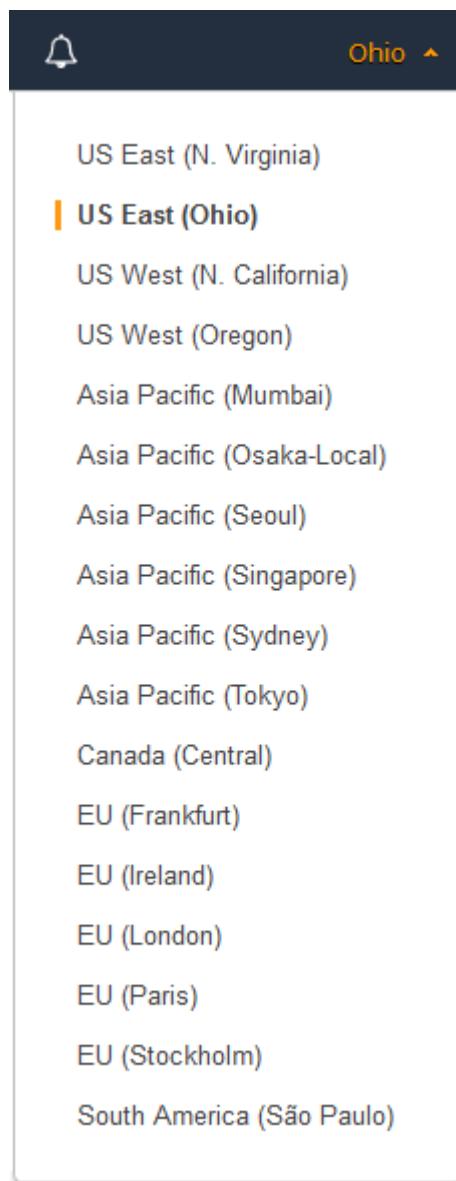
Criar um par de chaves

A 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 você planeja 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 de disponibilidade \(p. 7\)](#).

Para criar um par de chaves

1. Faça login na AWS usando a URL criada na seção anterior.
2. No painel da AWS, escolha EC2 para abrir o console do Amazon EC2.
3. Na barra de navegação, selecione uma região para o par de chaves. Selecione qualquer região que estiver disponível para você, independentemente do seu local. No entanto, os pares de chaves são específicos para uma região; por exemplo, se você planejar executar uma instância no Região do Leste dos EUA (Ohio), deverá criar um par de chaves para a instância no Região do Leste dos EUA (Ohio).



4. No painel de navegação, em REDE E SEGURANÇA, escolha Pares de chaves.

Tip

O painel de navegação está no lado esquerdo do console. Se você não vir o painel, ele pode estar minimizado; selecione a seta para expandir o painel. Pode ser necessário rolar para baixo para ver o link Key Pairs.

NETWORK & SECURITY

Security Groups

Elastic IPs

Placement Groups

Key Pairs

Network Interfaces

5. Escolha Criar par de chaves.
6. Digite um nome para o novo par de chaves no campo Nome do par de chaves da caixa de diálogo Criar par de chaves e selecione Criar. Use um nome que seja fácil de lembrar, como o nome de usuário do IAM, seguido de `-key-pair` mais o nome da região. Por exemplo, me-key-pair-useast2.
7. O arquivo de chave privada é baixado automaticamente pelo navegador. O nome do arquivo base é o nome especificado como sendo o nome do par de chaves e a extensão do nome do arquivo é `.pem`. Salve o arquivo de chave privada em um lugar seguro.

Important

Esta é a única chance de você salvar o arquivo de chave privada. Você precisará fornecer o nome do par de chaves ao iniciar uma instância e a chave privada correspondente sempre que se conectar à instância.

8. Se você usar um cliente de SSH em um computador Mac ou Linux para se conectar 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 your_user_name-key-pair-region_name.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 \(p. 1033\)](#).

Para obter mais informações, consulte [Pares de chaves do Amazon EC2 \(p. 616\)](#).

Para se conectar à instância usando o par de chaves

Para conectar-se à instância do Linux em um computador que executa o Mac ou o Linux, especifique o arquivo `.pem` para o cliente SSH com a opção `-i` e o caminho para a chave privada. Para se conectar à instância do Linux em um computador no qual o Windows esteja em execução, você pode usar MindTerm ou PuTTY. Se quiser usar PuTTY, você precisará instalá-lo e usar o seguinte procedimento para converter o arquivo `.pem` em um arquivo `.ppk`.

(Opcional) Para se preparar para se conectar a uma instância do Linux a partir do Windows usando PuTTY

1. Faça download e instale o PuTTY em <http://www.chiark.greenend.org.uk/~sgtatham/putty/>. Instale o pacote inteiro.
2. Inicie o PuTTYgen (por exemplo, no menu Start (Iniciar), selecione All Programs (Todos os programas) > PuTTY > PuTTYgen).
3. Em Tipo de chave a ser gerada, escolha RSA.



4. Escolha Load (Carregar). Por padrão, o PuTTYgen exibe somente arquivos com a extensão .ppk. Para localizar o arquivo .pem, selecione a opção para exibir arquivos de todos os tipos.

The screenshot shows a file selection dialog with a dropdown menu. The option 'All Files (*.*)' is highlighted, indicating that all file types will be shown.
5. Selecione o arquivo de chave privada que você criou no procedimento anterior e escolha Abrir. Escolha OK para descartar a caixa de diálogo de confirmação.
6. Escolha Save private key (Salvar chave privada). PuTTYgen exibe um aviso sobre salvar a chave sem uma senha. Escolha Sim.
7. Especifique o mesmo nome da chave usado para o par de chaves. O PuTTY adiciona automaticamente a extensão de arquivo .ppk.

Criar uma Virtual Private Cloud (VPC)

O Amazon VPC permite executar recurso da AWS em uma rede virtual que você define, conhecida como virtual private cloud (VPC). Os tipos de instância do EC2 mais recentes exigem que você execute as instâncias em uma VPC. Se você tiver uma VPC padrão, poderá ignorar esta seção e avançar para a próxima tarefa, [Criar um security group \(p. 26\)](#). Para determinar se você tem uma VPC padrão, abra o console do Amazon EC2 e procure Default VPC em Account Attributes no painel. Se você não tiver uma VPC padrão listada no painel, poderá criar uma VPC não padrão usando as etapas abaixo.

Para criar um VPC não padrão

1. Abra o console de Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. Na barra de navegação, selecione uma região para a VPC. Os VPCs são específicos para uma região, portanto, você deve selecionar a mesma região em que criou o par de chaves.
3. No painel da VPC, selecione Launch VPC Wizard (Iniciar assistente da VPC).
4. Na página Etapa 1: selecione uma configuração de VPC, verifique se VPC com uma única sub-rede pública está selecionado e escolha Selecionar.
5. Na página Step 2: VPC with a Single Public Subnet, insira um nome amigável para a VPC no campo VPC name. Deixe as outras definições de configuração padrão e escolha Create VPC. Na página de confirmação, escolha OK.

Para obter mais informações sobre VPCs, consulte [Guia do usuário da Amazon VPC](#).

Criar um security group

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 security group que permitam que você se conecte à instância em seu endereço IP usando o SSH. Você também pode adicionar regras que permitam o acesso HTTP e HTTPS de entrada e saída de qualquer lugar.

Observe que para executar instâncias em várias regiões, você precisa criar um security group em cada região. Para obter mais informações sobre as regiões, consulte [Regiões e Zonas de disponibilidade \(p. 7\)](#).

Pré-requisitos

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.

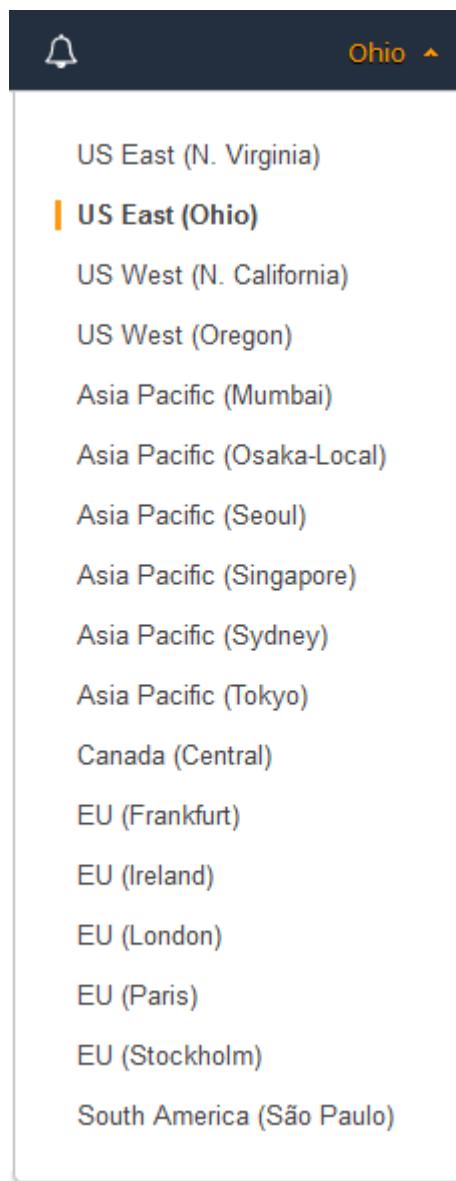
Para criar um security group com o menor privilégio

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.

Tip

Como alternativa, você pode usar o console da Amazon VPC para criar um security group. No entanto, as instruções deste procedimento não correspondem ao console da Amazon VPC. Portanto, se você tiver alternado para o console da Amazon VPC na seção anterior, alterne para o console do Amazon EC2 e use estas instruções ou use as instruções em [Configurar um grupo de segurança para a VPC](#) no Guia de conceitos básicos do Amazon VPC.

2. Na barra de navegação, selecione uma região para o security group. Os security groups são específicos para uma região, portanto, você deve selecionar a mesma região em que criou o par de chaves.



3. No painel de navegação, escolha Security Groups.
4. Escolha Create Security Group.
5. Insira um nome para o novo security group e uma descrição. Use um nome que seja fácil de lembrar, como o nome de usuário do IAM, seguido de _SG_ mais o nome da região. Por exemplo, me_SG_uswest2.
6. Na lista VPC, selecione sua VPC. Se você tiver uma VPC padrão, ela será a que estiver marcada com um asterisco (*).
7. Na guia Entrada, crie as seguintes regras (escolha Adicionar regra para cada nova regra) e selecione Criar:
 - 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 recomendamos permitir acesso SSH de todos os endereços IPv4 (0.0.0.0/0) à instância, exceto para fins de teste e somente por um curto período.

Para obter mais informações, consulte [Grupos de segurança do Amazon EC2 para instâncias do Linux \(p. 626\)](#).

Conceitos básicos das instâncias do Amazon EC2 do Linux

Vamos começar a usar o Amazon Elastic Compute Cloud (Amazon EC2) executando, conectando e usando uma instância do Linux. Uma instância é um servidor virtual na nuvem AWS. Com o Amazon EC2 você pode definir e configurar o sistema operacional e os aplicativos que são executados em sua instância.

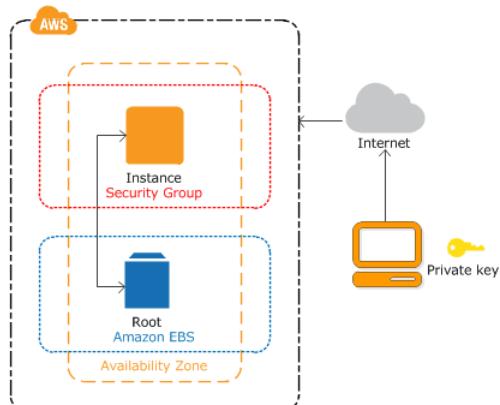
Ao se cadastrar na AWS, você poderá começar a usar o Amazon EC2 usando o [Nível gratuito da AWS](#). Se você tiver criado sua conta da AWS há menos de 12 meses e ainda não tiver excedido os benefícios de nível gratuito para Amazon EC2, não será cobrado para concluir este tutorial, pois nós o ajudamos 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

- [Visão geral \(p. 30\)](#)
- [Pré-requisitos \(p. 31\)](#)
- [Etapa 1: Executar uma instância \(p. 31\)](#)
- [Etapa 2: Conecte-se à sua instância \(p. 32\)](#)
- [Etapa 3: Limpar a instância \(p. 32\)](#)
- [Próximas etapas \(p. 33\)](#)

Visão geral

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.



Tarefas

Para concluir este tutorial, realize as seguintes tarefas:

1. Inicie uma instância (p. 31)
2. Conecte-se à sua instância (p. 32)
3. Limpe sua instância (p. 32)

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 Guia do usuário do AWS Command Line Interface: [Uso do Amazon EC2 pela CLI da AWS](#).

Pré-requisitos

Antes de começar, você deve concluir as etapas em [Como configurar com o Amazon EC2 \(p. 21\)](#).

Etapa 1: Executar uma instância

Você pode executar uma instância do Linux utilizando o Console de gerenciamento da AWS como descrito no seguinte procedimento. 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 as opções avançadas, consulte [Execução de uma instância](#).

Inicie 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 `t2.micro`, que é selecionado por padrão. Observe que este tipo de instância está qualificado para o nível gratuito.
5. Escolha 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.

Como alternativa, você pode criar um novo par de chaves. Selecione Create a new key pair, insira um nome para o par de chaves e, em seguida, escolha Download Key Pair. Esta é a única chance de você salvar o arquivo de chave privada, logo, não deixe de fazer download dele. Salve o arquivo de

chave privada em um lugar seguro. Você precisará fornecer o nome do par de chaves ao iniciar uma instância e a chave privada correspondente sempre que se conectar à instância.

Warning

Não selecione a opção Proceed without a key pair. 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 DNS (IPv4) estiver oculta, escolha Mostrar/ocultar colunas (o ícone de engrenagem) no canto superior direito da página e selecione Public DNS (IPv4).)
11. Pode levar alguns minutos até que a instância esteja pronta para que você possa se conectar a ela. Certifique-se de que sua instância tenha sido aprovada nas verificações de status. É possível visualizar essas informações na coluna Status Checks.

Etapa 2: Conecte-se à sua instância

Há várias formas de conectar-se a sua instância do Linux. Para obter mais informações, consulte [Conecte-se à sua instância do Linux \(p. 439\)](#).

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 [Resolução de problemas para se conectar à sua instância \(p. 1028\)](#) 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 \(p. 33\)](#).

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. Se você quiser manter sua instância para depois, sem a cobrança de taxas, poderá interromper a instância agora e iniciá-la novamente mais tarde. Para obter mais informações, consulte [Interrupção de instâncias](#).

Para encerrar sua instância

1. No painel de navegação, escolha Instances (Instâncias). Na lista de instâncias, selecione a instância.
2. Escolha Actions (Ações), Instance State (Estado da instância), Terminate (Encerrar).

3. Quando a confirmação for solicitada, escolha Sim, 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, em seguida, a entrada será excluída.

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 [Tutorial: Gerenciar remotamente instâncias do Amazon EC2 \(p. 84\)](#) e [Gerenciamento remoto do Systems Manager \(Run Command\)](#).
- Configure um alarme do CloudWatch para notificá-lo caso seu uso ultrapasse o Nível gratuito. Para obter mais informações, consulte [Criar um alarme de faturamento no Guia do usuário do AWS Billing and Cost Management](#).
- Adicione um volume do EBS. Para obter mais informações, consulte [Criação de um volume do Amazon EBS \(p. 860\)](#) e [Associação de um volume do Amazon EBS a uma instância \(p. 863\)](#).
- Instale a pilha LAMP. Para obter mais informações, consulte [Tutorial: Instalar um servidor web LAMP no Amazon Linux 2 \(p. 36\)](#).

Práticas recomendadas para o Amazon EC2

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

Segurança e rede

- 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 security groups \(p. 627\)](#).
- 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](#). Para obter mais informações sobre como atualizar a instância Windows, consulte [Como atualizar a instância Windows](#) no Guia do usuário do Amazon EC2 para instâncias do Windows.

Armazenamento

- 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 \(p. 91\)](#).
- 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 [Preservação de volumes do Amazon EBS no encerramento da instância \(p. 474\)](#).
- 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 para 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.

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 \(p. 516\)](#) e [Marcação dos seus recursos do Amazon EC2 \(p. 1003\)](#).
- 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 [Limites de serviço do Amazon EC2 \(p. 1013\)](#).

Backup e recuperação

- Faça backup de seus volumes do EBS regularmente usando [Screenshots do Amazon EBS \(p. 896\)](#) e crie uma [Imagen de máquina da Amazon \(AMI\) \(p. 89\)](#) 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 \(p. 723\)](#).
- Monitorar e responder a eventos. Para obter mais informações, consulte [Monitoramento do Amazon EC2 \(p. 562\)](#).
- 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 \(p. 747\)](#). Para uma solução automatizada, você pode usar o Amazon EC2 Auto Scaling. Para mais informações, consulte o .
- Teste regularmente o processo de recuperação de suas instâncias e de volumes do Amazon EBS em caso de falha.

Tutoriais para instâncias do Amazon EC2 que executam no Linux

Os seguintes tutoriais mostram como executar tarefas comuns usando instâncias do EC2 que executam no Linux. Para acessar vídeos, consulte [Vídeos e laboratórios instrucionais da AWS](#).

Tutoriais

- [Tutorial: Instalar um servidor web LAMP no Amazon Linux 2 \(p. 36\)](#)
- [Tutorial: Instalar um servidor web do LAMP com Amazon Linux AMI \(p. 46\)](#)
- [Tutorial: Hospedagem de um blog do WordPress com Amazon Linux \(p. 56\)](#)
- [Tutorial: Configurar o servidor web Apache no Amazon Linux 2 para usar SSL/TLS \(p. 65\)](#)
- [Tutorial: Aumente a disponibilidade do seu aplicativo no Amazon EC2 \(p. 80\)](#)
- [Tutorial: Gerenciar remotamente instâncias do Amazon EC2 \(p. 84\)](#)

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.

Para configurar um servidor web LAMP na Amazon Linux AMI, consulte [Tutorial: Instalar um servidor web do LAMP com Amazon Linux AMI \(p. 46\)](#).

Important

Se você estiver tentando configurar um servidor web LAMP em uma instância do Ubuntu ou do Red Hat Enterprise Linux, este tutorial não funcionará para você. Para obter mais informações sobre outras distribuições, consulte a documentação específica. Para obter informações sobre servidores web do LAMP no Ubuntu, consulte o tópico [ApacheMySQLPHP](#) na documentação da comunidade do Ubuntu.

Etapa 1: Preparar o servidor LAMP

Pré-requisitos

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 \(p. 31\)](#). 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 [Como configurar com o Amazon EC2 \(p. 21\)](#).

Note

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 \(p. 32\).](#)
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
```

Note

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 com o comando a seguir.

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

Para configurar um servidor web LAMP na Amazon Linux AMI, consulte [Tutorial: Instalar um servidor web do LAMP com Amazon Linux AMI \(p. 46\)](#).

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
```

Note

Você pode visualizar as versões atuais desses pacotes com 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. Em Security groups (Grupos de segurança), escolha view inbound rules (visualizar regras de entrada).
 - d. Você verá a lista de regras a seguir no security group padrão:

```
Security Groups associated with i-1234567890abcdef0
Ports      Protocol      Source      launch-wizard-N
22         tcp           0.0.0.0/0   #
```

Usando os procedimentos contidos em [Como adicionar regras a um security group \(p. 632\)](#), 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)).

Caso não seja possível visualizar a página de teste Apache, verifique se o grupo de segurança que você está usando contém uma regra para permitir tráfego HTTP (porta 80). Para obter informações sobre como adicionar uma regra de HTTP ao grupo de segurança, consulte [Como adicionar regras a um security group \(p. 632\)](#).

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, 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 served, follow the instructions in the file `/etc/httpd/conf/wELCOME.conf`.

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



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 servidor web Apache no Amazon Linux 2 para usar SSL/TLS](#).

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 \(p. 39\)](#).

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
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-dba.ini, /etc/php.d/20-dom.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-mysqlind.ini, /etc/php.d/20-pdo.ini, /etc/php.d/20-phar.ini, /etc/php.d/20-pspell.ini, /etc/php.d/20-session.ini, /etc/php.d/20-tokenizer.ini, /etc/php.d/30-mysqli.ini, /etc/php.d/30-pspell.ini, /etc/php.d/30-session.ini, /etc/php.d/pdo_sqlite.ini
PHP API	20170718
PHP Extension	20170718
Zend Extension	320170718
Zend Extension Build	API320170718,NTS
PHP Extension Build	API20170718,NTS

Note

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`. Também 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.

Note

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 servidor web Apache no Amazon Linux para usar SSL/TLS.

Para instalar o phpMyAdmin

1. Instale as dependências necessárias.

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

2. Reinicie o Apache.

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

3. Reinicie php-fpm.

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

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

```
[ec2-user ~]$ cd /var/www/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 systemctl start mariadb
```

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](#).

Solução de problemas

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 ~]$ sudo systemctl is-enabled httpd
```

Se o processo httpd não estiver em execução, repita as etapas descritas em [Para preparar o servidor LAMP \(p. 37\)](#).

- O firewall está configurado corretamente?

Caso não seja possível visualizar a página de teste Apache, verifique se o grupo de segurança que você está usando contém uma regra para permitir tráfego HTTP (porta 80). Para obter informações sobre como adicionar uma regra de HTTP ao grupo de segurança, consulte [Como adicionar regras a um security group \(p. 632\)](#).

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:

- Transferência de arquivos para sua instância do Linux usando WinSCP (p. 449)
- Transferência de arquivos para instâncias do Linux usando SCP (p. 442)
- Tutorial: Hospedagem de um blog do WordPress com Amazon Linux (p. 56)

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: Instalar um servidor web do LAMP com 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.

Para configurar um servidor web LAMP na Amazon Linux 2, consulte [Tutorial: Instalar um servidor web LAMP no Amazon Linux 2 \(p. 36\)](#).

Para configurar um servidor web LAMP seguro usando criptografia SSL/TLS padrão do setor, use [Tutorial: Instalar um servidor web LAMP no Amazon Linux 2 \(p. 36\)](#) juntamente com [Tutorial: Configurar o servidor web Apache no Amazon Linux 2 para usar SSL/TLS \(p. 65\)](#).

Important

Se você estiver tentando configurar um servidor web LAMP em uma instância do Ubuntu ou do Red Hat Enterprise Linux, este tutorial não funcionará para você. Para obter mais informações sobre outras distribuições, consulte a documentação específica. Para obter informações sobre servidores web do LAMP no Ubuntu, consulte o tópico [ApacheMySQLPHP](#) na documentação da comunidade do Ubuntu.

Pré-requisitos

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 \(p. 31\)](#). 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 [Como configurar com o Amazon EC2 \(p. 21\)](#).

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

1. [Conecte-se à sua instância \(p. 32\)](#).
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.

Note

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, consulte [O software aplicativo compatível que desejo executar no meu servidor é incompatível com a versão PHP instalada ou outro software \(p. 55\)](#).

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 php56 mysql55-server php56-mysqlnd
```

Note

Se receber o erro No package *package-name* available, isso significa que sua instância não foi executada com 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
```

Para configurar um servidor web LAMP na Amazon Linux 2, consulte [Tutorial: Instalar um servidor web LAMP no Amazon Linux 2 \(p. 36\)](#).

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 em 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. Em Security groups (Grupos de segurança), escolha view inbound rules (visualizar regras de entrada).
 - d. Você verá a lista de regras a seguir no security group padrão:

```
Security Groups associated with i-1234567890abcdef0
Ports      Protocol      Source      launch-wizard-N
22         tcp          0.0.0.0/0    #
```

Usando os procedimentos contidos em [Como adicionar regras a um security group \(p. 632\)](#), 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. 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)).

Caso não seja possível visualizar a página de teste Apache, verifique se o grupo de segurança que você está usando contém uma regra para permitir tráfego HTTP (porta 80). Para obter informações sobre como adicionar uma regra de HTTP ao grupo de segurança, consulte [Como adicionar regras a um security group \(p. 632\)](#).

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.

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"](mailto: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!



Note

Esta página de teste é exibida somente quando não há conteúdo no `/var/www/html`. Quando você adiciona conteúdo ao diretório base, o conteúdo aparece no endereço DNS público da instância em vez desta página de teste.

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 servidor web Apache no Amazon Linux para usar SSL/TLS](#).

Para testar o servidor web do 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.

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 \(p. 49\)](#).

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 5.6.6

System	Linux ip-172-31-7-35 3.14.35-28.38.amzn1.x86_64 #1 SMP Wed Mar 11 22:50:37 UTC 2015 x86_64
Build Date	Mar 5 2015 23:26:53
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-5.6.d
Additional .ini files parsed	/etc/php-5.6.d/20-bz2.ini, /etc/php-5.6.d/20-calendar.ini, /etc/php-5.6.d/20-ctype.ini, /etc/php-5.6.d/20-crypt.ini, /etc/php-5.6.d/20-dom.ini, /etc/php-5.6.d/20-exif.ini, /etc/php-5.6.d/20-fileinfo.ini, /etc/php-5.6.d/20-ftp.ini, /etc/php-5.6.d/20-gettext.ini, /etc/php-5.6.d/20-iconv.ini, /etc/php-5.6.d/20-mysqlind.ini, /etc/php-5.6.d/20-pdo.ini, /etc/php-5.6.d/20-phar.ini, /etc/php-5.6.d/20-posix.ini, /etc/php-5.6.d/20-shmop.ini, /etc/php-5.6.d/20-simplexml.ini, /etc/php-5.6.d/20-sockets.ini, /etc/php-5.6.d/20-sqlite3.ini, /etc/php-5.6.d/20-sysvmsg.ini, /etc/php-5.6.d/20-sysvshm.ini, /etc/php-5.6.d/20-tokenizer.ini, /etc/php-5.6.d/20-xml.ini, /etc/php-5.6.d/20-xmlwriter.ini, /etc/php-5.6.d/20-xsl.ini, /etc/php-5.6.d/20-zip.ini, /etc/php-5.6.d/30-mysqli.ini, /etc/php-5.6.d/30-mysqlind.ini, /etc/php-5.6.d/30-pdo_mysql.ini, /etc/php-5.6.d/30-pdo_sqlite.ini, /etc/php-5.6.d/30-wddx.ini, /etc/php-5.6.d/30-xmlreader.ini, /etc/php-5.6.d/40-json.ini, /etc/php-5.6.d/php.ini
PHP API	20131106
PHP Extension	20131226
Zend Extension	220131226
Zend Extension Build	API220131226,NTS
PHP Extension Build	API20131226,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 php56 mysql55-server php56-mysqlind
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-mysqlind.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
```

Para 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.

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.

Note

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.

- Digite **Y** para remover as contas de usuários anônimos.
 - Digite **Y** para desabilitar o recurso de login remoto da raiz.
 - Digite **Y** para remover o banco de dados de teste.
 - Digite **Y** para recarregar as tabelas de privilégios e salvar suas alterações.
- (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 ]
```

- (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.

(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 servidor web Apache no Amazon Linux para usar SSL/TLS](#).

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 php70-mbstring.x86_64 php70-zip.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](#).

Solução de problemas

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 em 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 [Para instalar e iniciar o servidor web do LAMP com a Amazon Linux AMI \(p. 46\)](#).

- O firewall está configurado corretamente?

Caso não seja possível visualizar a página de teste Apache, verifique se o grupo de segurança que você está usando contém uma regra para permitir tráfego HTTP (porta 80). Para obter informações sobre como adicionar uma regra de HTTP ao grupo de segurança, consulte [Como adicionar regras a um security group \(p. 632\)](#).

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 php56 mysql55-server php56-mysqlnd perl-DBD-MySQL56
```

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-MySQL55
```

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:

- [Transferência de arquivos para sua instância do Linux usando WinSCP \(p. 449\)](#)
- [Transferência de arquivos para instâncias do Linux usando SCP \(p. 442\)](#)
- [Tutorial: Hospedagem de um blog do WordPress com Amazon Linux \(p. 56\)](#)

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: Hospedagem de um blog do WordPress com Amazon Linux

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 para 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 [Conceitos básicos](#) no Guia do usuário do AWS CloudFormation. Se você preferir hospedar seu blog do WordPress em uma instância Windows, consulte [Implantação de um blog do WordPress na sua instância Windows do Amazon EC2](#) no Guia do usuário do Amazon EC2 para instâncias do Windows. Se você precisar de uma solução de alta disponibilidade com um banco de dados desacoplado, consulte [Implantação de um website do WordPress de alta disponibilidade](#).

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.

Pré-requisitos

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 do LAMP com Amazon Linux AMI \(p. 46\)](#) para a AMI do Amazon Linux ou [Tutorial: Instalar um servidor web LAMP no Amazon Linux 2 \(p. 36\)](#) 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 [Como adicionar regras a um security group \(p. 632\)](#).

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 Elastic IP \(p. 742\)](#).

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 [Registro de 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 sempre 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 pode ser diferente da sua senha do sistema de `root` ou pode 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 do banco de dados \(p. 51\)](#).

```
[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 original 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 \(p. 58\)](#) de [Para criar um usuário de banco de dados e um banco de dados para a instalação do WordPress \(p. 58\)](#).

```
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 \(p. 58\)](#) de [Para criar um usuário de banco de dados e um banco de dados para a instalação do WordPress \(p. 58\)](#).

```
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 \(p. 58\)](#) de [Para criar um usuário de banco de dados e um banco de dados para a instalação do WordPress \(p. 58\)](#).

```
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 http://codex.wordpress.org/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^-L_0(WU_+ c+WFkI~c]o]-bHw+/'
Ajl[wTwSiz<qb[mghEXcRh-');
```

```
define('SECURE_AUTH_KEY', 'Zsz._P=l/|y.Lq)Xjlkws1y5Nj76E6EJ.AV0pCKZZB,*~r?6OP
$eJ@;+(ndLg');
define('LOGGED_IN_KEY', 'ju}qwre3V*+8f_zOWf?{LlGsQ]Ye@2Jh^,8x>)Y|;([Iw]Pi
+LG#A4R?7N`YB3');
define('NONCE_KEY', 'P(g62HeZxEes/LnI^i=H,[XwK9I&[2s|:?ON}VJM%?;v2v]v+;
+^9eXUahg@:Cj');
define('AUTH_SALT', 'C$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-
ES7Q10-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?Zy4zUU4r99QQ_rGs2LTd%P;|
_eits)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

1. 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) ou em um subdiretório ou em uma pasta sob a raiz (por exemplo, my.public.dns.amazonaws.com/blog).
2. 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/
```

3. 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 quanto ao 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 é 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.

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 \(p. 46\)](#)).

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 chkconfig para garantir que httpd e os serviços do banco de dados iniciem 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 [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 iniciem 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 [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 http://codex.wordpress.org/Changing_The_Site_URL.

[Configure 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 [Como criar sua própria AMI \(p. 89\)](#).

[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 [Como modificar o tamanho, o desempenho ou o tipo de um volume do EBS \(p. 882\)](#).
- Mova o banco de dados MySQL para o [Amazon RDS](#) para aproveitar a capacidade de dimensionamento que o serviço oferece.
- Migre para um tipo de instância maior. Para obter mais informações, consulte [Alterar o tipo de instância \(p. 247\)](#).

-
- Adicione instâncias adicionais. Para obter mais informações, consulte [Tutorial: Aumente a disponibilidade do seu aplicativo no Amazon EC2 \(p. 80\)](#).

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 a solução de problemas da sua instalação, acesse http://codex.wordpress.org/Installing_WordPress#Common_Installation_Problems. Para obter informações sobre como deixar o blog do WordPress mais seguro, acesse http://codex.wordpress.org/Hardening_WordPress. Para obter informações sobre como manter o blog do WordPress atualizado, acesse http://codex.wordpress.org/Updating_WordPress.

Ajuda! Meu nome DNS público mudou e agora meu blog quebrou

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 são esboçadas em http://codex.wordpress.org/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 http://codex.wordpress.org/Changing_The_Site_URL.

Tutorial: Configurar o servidor web Apache no Amazon Linux 2 para usar SSL/TLS

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 habilitar manualmente compatibilidade para SSL/TLS em uma única instância do Amazon Linux 2 que executa o servidor web do Apache. Se você planeja oferecer serviços em nível comercial, o [AWS Certificate Manager](#), que não é abordado aqui, é uma boa opção.

Por motivos históricos, a criptografia na web é conhecida simplesmente como SSL. Embora navegadores da web ainda ofereçam suporte a SSL, o protocolo sucessor TLS é menos vulnerável a ataques. O Amazon Linux 2 desabilita todas as versões do SSL por padrão e recomenda a desativação do TLS versão 1.0, conforme descrito abaixo. Somente o TLS 1.1 e 1.2 pode ser habilitado com segurança. Para obter mais informações sobre o padrão de criptografia atualizado, consulte [RFC 7568](#).

Important

Esses procedimentos são destinados ao Amazon Linux 2. Também supomos que você esteja começando com uma nova instância do EC2. Se você estiver tentando configurar um servidor web LAMP em uma outra distribuição ou se estiver reformulando uma instância mais antiga, alguns procedimentos neste tutorial poderão não funcionar para você. Para obter informações sobre servidores web do LAMP no Ubuntu, consulte o tópico [ApacheMySQLPHP](#) na documentação da comunidade do Ubuntu. Para obter informações sobre o Red Hat Enterprise Linux, consulte o tópico [Servidores web](#) no Portal do cliente.

A versão deste tutorial para uso com a Amazon Linux AMI não é mais mantida, mas você ainda pode localizá-la no [Internet Archive](#).

Tópicos

- [Pré-requisitos \(p. 65\)](#)
- [Etapa 1: Habilitar SSL/TLS no servidor \(p. 66\)](#)
- [Etapa 2: Obter um certificado assinado por uma CA \(p. 68\)](#)
- [Etapa 3: Testar e intensificar a configuração de segurança \(p. 73\)](#)
- [Solução de problemas \(p. 75\)](#)
- [Apêndice: Let's Encrypt com o Certbot no Amazon Linux 2 \(p. 76\)](#)

Pré-requisitos

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 \(p. 31\)](#).
- 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 [Como autorizar tráfego de entrada em suas instâncias Linux \(p. 720\)](#).

- Instale o servidor da web Apache. Para obter instruções passo a passo, consulte [Tutorial: Instalar um servidor web LAMP no Amazon Linux 2 \(p. 36\)](#). 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 SSL/TLS depende do Domain Name System (DNS). Se você planeja usar sua instância do EC2 para hospedar um site público, 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 SSL/TLS no servidor

Este procedimento o auxilia no processo de configuração do SSL/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 permitir o SSL/TLS em um servidor

1. [Conecte-se à sua instância \(p. 32\)](#) 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 SSL/TLS instalando o módulo `mod_ssl` do Apache:

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

Posteriormente neste tutorial, você trabalhará com três arquivos importantes que foram instalados:

- `/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 SSL/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).

Note

Se você não pode visualizar este arquivo em uma lista de diretório, pode ser devido às permissões de acesso restritivas. Tente executar `sudo ls -al` dentro do diretório.

- `/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 SSL/TLS.

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

```
-----BEGIN CERTIFICATE-----
MIIEazCCA1OgAwIBAgICWxQwDQYJKoZIhvcNAQELBQAwgbExCzAJBgNVBAYTAi0t
MRIwEAYDVQQIDA1Tb21lU3RhGUxETAPBgNVBAcMCFNvbWVDaXR5MRkwFwYDVQQK
DBBTb21lT3JnYW5pemF0aW9uMR8wHQYDVQQLDBZTb21lT3JnYW5pemF0aW9uYWhv
bmlOMRkwFwYDVQODDBpcC0xNzItMzEtMjAtMjM2MSQwIgYJKoZIhvcNAQkBFhVy
...
z5rRUE/XzxRLBZOoWZpNWTXJkQ3uFYH6s/
sBwtHpKKZMzOvDedREjNKAvk4ws6F0
WanXWehT6FiSzvB4sTEXXJN2jdw8g
+sHGnZ8zCOsclknYhHrCVD2vnB1ZJKSzvak
3ZazhBxtQSukFMOnWPP2a0DMMFGYUHod0BQE8sBJxg==
-----END CERTIFICATE-----
```

Os nomes de arquivos e as extensões são uma conveniência e não têm efeito na função. 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 SSL/TLS padrão por seus próprios arquivos personalizados, verifique se eles estão no formato PEM.

4. Reinicie a instância e reconecte-se a ela.
5. 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 acima.

6. 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 SSL/TLS no servidor estará correta. Todos os dados que passam entre o navegador e o servidor agora estão criptografados.

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

Etapa 2: Obter um certificado assinado por uma CA

Esta seção descreve o processo de geração de uma solicitação de assinatura de certificado (CSR) a partir de uma chave privada, enviando a CSR a uma autoridade de certificação (CA), obtendo um certificado de host assinado e configurando o Apache para usá-lo.

Um certificado de host SSL/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. Uma lista de CAs conhecidas pode ser encontrada em [dmoztols.net](#). Algumas CAs oferecem certificados de nível básico gratuitamente. Entre essas, 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 [Apêndice: Let's Encrypt com o Certbot no Amazon Linux 2 \(p. 76\)](#).

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 2 é de 2048 bits, o que significa que a chave existente gerada automaticamente é adequada para ser usada 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.

Para obter um certificado assinado por uma CA

1. [Conecte-se à sua instância \(p. 32\)](#) e navegue até `/etc/pki/tls/private/`. Esse é o diretório onde a chave privada do servidor para SSL/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. Aqui estão 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.
 1. Como um ponto de partida, aqui está o comando para criar uma chave de RSA que é semelhante à chave de host padrão em sua instância:

```
[ec2-user ~]$ sudo openssl genrsa -out custom.key 2048
```

O arquivo resultante, `custom.key`, é uma chave privada de RSA de 2048 bits.

2. Para criar uma chave de RSA mais forte com um módulo maior, use o seguinte comando:

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

O arquivo resultante, **custom.key**, é uma chave privada de RSA de 4096 bits.

3. Para criar uma chave de RSA de 4096 bits criptografada com proteção de senha, use o seguinte comando:

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

Esse comando resulta em uma chave privada de RSA de 4096 bits que foi 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 “abcde12345” por meio de uma conexão SSH.

4. A criptografia de RSA pode ser relativamente lenta porque sua segurança depende da dificuldade de fatorar o produto de dois números primos grandes. No entanto, é possível criar chaves para SSL/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. Aqui está um exemplo:

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

A saída nesse caso é uma chave privada de curva elíptica de 256 bits que usa prime256v1, uma “curva nomeada” que tem suporte da 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 preferida. 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 as informações mostradas 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 www.example.com . 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 *.example.com .	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 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 for aprovada, você receberá 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
```

Examine a saída das linhas indicadoras descritas acima. Não use os arquivos que terminam com `.p7b`, `.p7c` ou extensões semelhantes.

5. Remova ou renomeie o certificado de host autoassinado antigo `localhost.crt` no diretório `/etc/pki/tls/certs` e coloque o novo certificado assinado pela CA no lugar (juntamente com qualquer certificado intermediário).

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 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.

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). Os comandos seriam os seguintes:

```
[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.

No 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 2 (owner=root, group=root, leitura/gravação para o proprietário somente). 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. Como o nome do arquivo do certificado do host assinado pela CA (**custom.crt** neste exemplo) provavelmente difere do certificado antigo, edite o /etc/httpd/conf.d/ssl.conf e forneça o caminho e o nome do arquivo corretos usando a diretiva SSLCertificateFile do Apache:

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

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.

Se você tiver instalado uma chave privada personalizada (**custom.key** neste exemplo), forneça o caminho e o nome do arquivo usando a 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
```

Etapa 3: Testar e intensificar a configuração de segurança

Depois que o SSL/TLS estiver operacional e exposto ao público, você deve testar sua segurança real. 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 da Certbot:

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

O relatório mostra que a configuração é em sua maior parte sólida, com avaliações aceitáveis para o certificado, o suporte ao protocolo, a troca de chaves e os problemas de intensidade do código. A configuração também oferece suporte a [Forward secrecy](#), um recurso de protocolos 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. No entanto, o relatório também sinaliza uma vulnerabilidade séria que é responsável pela redução da classificação geral e aponta para um potencial problema adicional:

1. Suporte à cifra RC4: uma cifra é o núcleo matemático de um algoritmo de criptografia. A RC4, uma cifra rápida usada para criptografar fluxos de dados SSL/TLS, é conhecida por ter várias [fraquezas sérias](#). A correção é desabilitar completamente o suporte à RC4. Também especificamos uma ordem explícita de cifras e uma lista de cifras proibidas.

No 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 com apenas uma vírgula (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:

- a. Suporte para forward secrecy
- b. Força
- c. Velocidade
- d. Cifras específicas antes das famílias de cifras
- e. Cifras permitidas antes das cifras negadas

As cifras de alta classificação 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. 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.

Important

A lista de cifras mostrada aqui é apenas uma das muitas possíveis listas. Por exemplo, você pode otimizar uma lista para obter mais 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.

Finalmente, 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. Para obter mais informações, consulte [Políticas de segurança SSL predefinidas para Elastic Load Balancing](#) no Guia do usuário para Classic Load Balancers.

Finalmente, 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.

2. Suporte a protocolo no futuro: a configuração oferece suporte às versões 1.0 e 1.1 do TLS, que estão em vias de reprovação, com a versão 1.2 do TLS recomendada depois de junho de 2018. Para comprovação futura do suporte ao protocolo, 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
```

Em seguida, adicione as seguintes diretrizes:

```
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 as versões compatíveis do TLS. 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.

Reinic peace o Apache depois de salvar essas alterações no arquivo de configuração editado.

Se você testar o domínio novamente no [Qualys SSL Labs](#), verá que a vulnerabilidade do RC4 desapareceu e que o resumo é semelhante ao seguinte:

Classificação geral	A
Certificado	100%
Suporte ao protocolo	100%
Troca de chaves	90%
Intensidade da cifra	90%

Solução de problemas

- Meu servidor da web Apache não inicia a menos que eu forneça 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 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 em 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.

- Eu recebo erros ao executar `sudo yum install -y mod_ssl`.

Quando estiver instalando os pacotes necessários para SSL, você verá erros como estes:

```
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.

Apêndice: 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 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 \(p. 79\)](#). Para obter mais informações, consulte o [Guia do usuário](#) e as [páginas do manual](#) do Certbot.



Certbot é um utilitário cliente para o serviço de certificado Let's Encrypt do EFF.

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, obtenha um snapshot de seu volume raiz do EBS. Isso permite que você restaure o estado original de sua instância do EC2. Para obter informações sobre como criar snapshots do EBS, consulte [Criação de um snapshot do Amazon EBS \(p. 898\)](#).
- 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 seguinte comando:

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

- b. Instale os pacotes do repositório da seguinte maneira:

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

- c. Habilite o EPEL:

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

Você pode confirmar se EPEL está habilitado com o seguinte comando, deve retornar os informações como snippet mostrado:

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

...
!epel/x86_64                               Extra Packages for Enterprise Linux 7 -
  x86_64                                     enabled: 12,184+105
!epel-debuginfo/x86_64                         Extra Packages for Enterprise Linux 7 -
  x86_64 - Debug                             enabled:      2,717
!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:    959+10
!epel-testing-debuginfo/x86_64                Extra Packages for Enterprise Linux 7 -
  Testing - x86_64 - Debug                     enabled:      142
!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) a ser configurado:

```
<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. Para fazer uma experiência com chaves personalizadas, você pode começar com [Como usar certificados ECDSA com Let's Encrypt](#).

1. Instale pacotes e dependências do Certbot usando o seguinte comando:

```
[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:

```
Starting new HTTPS connection (1): acme-v01.api.letsencrypt.org
```

```
-----  
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-v01.api.letsencrypt.org/directory
```

```
-----  
(A)gree/(C)ancel: A
```

5. Na autorização para o EFF colocar você na lista de correspondência deles, 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  
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/example.com/fullchain.pem`
Your key file has been saved at:
`/etc/letsencrypt/live/example.com/privkey.pem`
Your cert will expire on **2018-05-28**. 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 \(p. 73\)](#).

Configurar a renovação automatizada de certificado

Para automatizar o Certbot

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.

1. Abra `/etc/crontab` em um editor de texto e adicione uma linha semelhante ao seguinte:

```
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 executa com privilégios de 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.

Salve o arquivo ao concluir.

2. Reinicie o daemon cron:

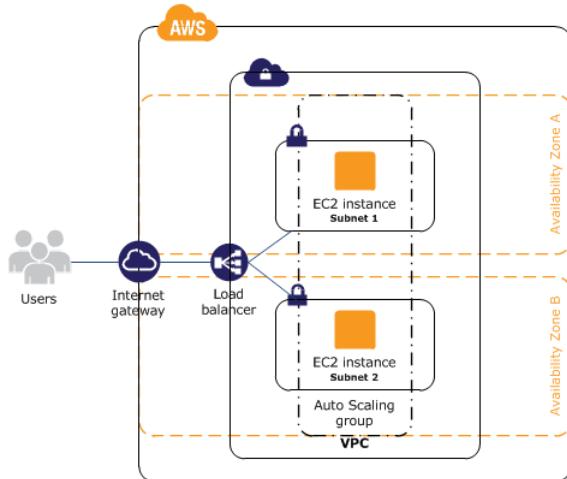
```
[ec2-user ~]$ sudo systemctl restart crond
```

Tutorial: Aumente a disponibilidade do seu aplicativo no Amazon EC2

Vamos supor que você comece executando seu aplicativo ou seu site em uma única instância do EC2 e, com o tempo, o tráfego aumenta a ponto de você precisar mais de uma instância para atender à demanda. Você pode executar várias instâncias do EC2 a partir da sua AMI e então usar o Elastic Load Balancing para distribuir o tráfego de entrada para seu aplicativo nessas instâncias do EC2. Isso aumenta a disponibilidade do seu aplicativo. Colocar suas instâncias em várias zonas de disponibilidade também melhora a tolerância a falhas no seu aplicativo. Se uma zona de disponibilidade tiver uma interrupção, o tráfego será roteado para a outra zona de disponibilidade.

Você pode usar o Amazon EC2 Auto Scaling para manter um número mínimo de instâncias em execução para seu aplicativo durante todo o tempo. O Amazon EC2 Auto Scaling pode detectar quando sua instância ou aplicativo não está íntegro e substituí-lo automaticamente para manter a disponibilidade do aplicativo. Você também pode usar o Amazon EC2 Auto Scaling para expandir ou reduzir a capacidade do Amazon EC2 automaticamente com base na demanda, usando critérios que você especifica.

Neste tutorial, nós usamos o Amazon EC2 Auto Scaling com o Elastic Load Balancing para garantir a manutenção de um número específico de instâncias do EC2 íntegras por trás do load balancer. Observe que essas instâncias não precisam de endereços IP públicos, pois o tráfego vai para o load balancer e é roteado para as instâncias. Para obter mais informações, consulte [Amazon EC2 Auto Scaling](#) e [Elastic Load Balancing](#).



Tópicos

- [Pré-requisitos \(p. 81\)](#)
- [Dimensione e faça o load balancing do seu aplicativo \(p. 81\)](#)
- [Teste seu load balancer \(p. 83\)](#)

Pré-requisitos

Este tutorial pressupõe que você já tenha feito o seguinte:

1. Criado uma nuvem privada virtual (VPC) com uma sub-rede pública em duas ou mais zonas de disponibilidade. Se você ainda não fez isso, consulte [Criar uma Virtual Private Cloud \(VPC\) \(p. 26\)](#).
2. Executado uma instância na VPC.
3. Conectado-se à instância e a personalizado. Por exemplo, instalando software e aplicativos, copiando dados e anexando volumes adicionais do EBS. Para obter informações sobre como configurar um servidor web na sua instância, consulte [Tutorial: Instalar um servidor web do LAMP com Amazon Linux AMI \(p. 46\)](#).
4. Testado o aplicativo na sua instância para garantir que ela está configurada corretamente.
5. Criado uma imagem de máquina da Amazon (AMI) a partir da sua instância. Para obter mais informações, consulte [Criação de uma AMI do Linux com Amazon EBS \(p. 111\)](#) ou [Criação de uma AMI em Linux com armazenamento de instâncias \(p. 115\)](#).
6. (Opcional) Encerrado a instância se não precisar mais dela.
7. Criado uma função do IAM que conceda a seu aplicativo o acesso de que ele precisa à AWS. Para obter mais informações, consulte [Para criar uma função do IAM usando o console do IAM \(p. 715\)](#).

Dimensione e faça o load balancing do seu aplicativo

Use os procedimentos a seguir para criar um load balancer, criar uma configuração de execução para suas instâncias, criar um grupo do Auto Scaling com duas ou mais instâncias e associar o load balancer com o grupo do Auto Scaling.

Para dimensionar e fazer load balancing do seu aplicativo

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, em LOAD BALANCING, escolha Load balancers.
3. Selecione Criar load balancer.

4. Para Application Load Balancer, escolha Create (Criar).
5. Na página Configure Load Balancer (Configurar load balancer), faça o seguinte:
 - a. Em Name (Nome), insira um nome para o load balancer. Por exemplo, **my-lb**.
 - b. Para Scheme (Esquema), mantenha o valor padrão, internet-facing (voltado para a Internet).
 - c. Para Listeners, mantenha o padrão, que é um listener que aceita tráfego HTTP na porta 80.
 - d. Em Availability Zones (Zonas de disponibilidade), selecione a VPC usada nas suas instâncias. Selecione uma zona de disponibilidade e, em seguida, selecione a sub-rede pública para essa zona de disponibilidade. Repita para uma segunda zona de disponibilidade.
 - e. Selecione Next: Configure Security Settings (Próximo: Definir configurações de segurança).
6. Para este tutorial, você não está usando um listener seguro. Selecione Next: Configure Security Groups (Próximo: Configurar grupos de segurança).
7. Na página Configure Security Groups (Configurar grupos de segurança), faça o seguinte:
 - a. Escolha Create a new security group (Criar um novo grupo de segurança).
 - b. Digite um nome e uma descrição para o security group ou mantenha o nome e a descrição padrão. Esse novo security group contém uma regra que permite tráfego para a porta configurada para o listener.
 - c. Selecione Next: Configure Routing (Próximo: Configurar roteamento).
8. Na página Configure Routing (Configurar roteamento), faça o seguinte:
 - a. No Target group (Grupo de destino), mantenha o padrão, o New target group (Novo grupo de destino).
 - b. Em Name (Nome), digite um nome para o grupo de destino.
 - c. Mantenha Protocol (Protocolo) como HTTP, Port (Porta) como 80 e Target type (Tipo de destino) como instância.
 - d. Em Health checks (Verificações de integridade), mantenha o protocolo e o caminho padrão.
 - e. Selecione Next: Register Targets (Próximo: Registrar destinos).
9. Na página Register Targets (Registrar destinos), escolha Next: Review (Próximo: Revisar) para continuar para a página seguinte, pois usaremos o Amazon EC2 Auto Scaling para adicionar instâncias do EC2 ao grupo de destino.
10. Na página Review (Revisar), selecione Create (Criar). Após a criação do load balancer, selecione Close (Fechar).
11. No painel de navegação, em AUTO SCALING, escolha Launch Configurations (Configurações de execução).
 - Se você estiver começando a usar o Amazon EC2 Auto Scaling, verá uma página de boas-vindas. Escolha Create Auto Scaling group (Criar grupo de Auto Scaling) para iniciar o assistente de criação de grupo de Auto Scaling e selecione Create launch configuration (Criar configuração de execução).
 - Caso contrário, escolha Create launch configuration (Criar configuração de execução).
12. Na página Choose AMI (Selecionar AMI), selecione a guia My AMIs (Minhas AMIs) e escolha a AMI que você criou em [Pré-requisitos \(p. 81\)](#).
13. Na página Choose Instance Type (Selecionar tipo de instância), selecione um tipo de instância e escolha Next: Configure details (Próximo: Configurar detalhes).
14. Na página Configure details (Configurar detalhes), faça o seguinte:
 - a. Em Name (Nome), digite um nome para sua configuração de execução (por exemplo, **my-launch-config**).
 - b. Em IAM role (Função do IAM), selecione a função do IAM criada em [Pré-requisitos \(p. 81\)](#).
 - c. (Opcional) Se você precisar executar um script de inicialização, expanda Advanced Details (Detalhes avançados) e digite o script em User data (Dados de usuário).

- d. Escolha Skip to review (Pular para revisão).
15. Na página Review (Revisão), escolha Edit security groups (Editar grupos de segurança). Você pode selecionar um security group existente ou criar um novo. Esse security group deve permitir tráfego HTTP e verificações de integridade pelo load balancer. Se suas instâncias tiverem endereços IP públicos, você pode permitir tráfego de SSH se você precisar se conectar a instâncias. Quando terminar, escolha Review (Revisão).
16. Na página Review (Revisão), selecione Create launch configuration (Criar configuração de execução).
17. Quando solicitado, selecione um par de chaves existente, crie um novo par de chaves ou continue sem um par de chaves. Selecione a caixa de confirmação e escolha Create launch configuration (Criar configuração de execução).
18. Depois de a configuração de execução ser criada, crie um grupo do Auto Scaling.
 - Se você for novo ao Amazon EC2 Auto Scaling e estiver usando o assistente Criar grupo do Auto Scaling, será direcionado para a próxima etapa automaticamente.
 - Caso contrário, escolha Create an Auto Scaling group using this launch configuration (Criar um grupo de Auto Scaling que usa essa configuração de execução).
19. Na página Configure Auto Scaling group details (Configurar detalhes do grupo de Auto Scaling), faça o seguinte:
 - a. Em Group name (Nome do grupo), digite um nome para o grupo de Auto Scaling. Por exemplo, **my-asg**.
 - b. Em Group size (Tamanho do grupo), digite o número de instâncias (por exemplo, **2**). Observe que recomendamos que você mantenha mais ou menos o mesmo número de instâncias em cada zona de disponibilidade.
 - c. Selecione sua VPC em Network (Rede) e suas duas sub-redes públicas em Subnet (Sub-rede).
 - d. Em Advanced Details (Detalhes avançados), selecione Receive traffic from one or more load balancers (Receber tráfego de um ou mais load balancers). Selecione seu grupo de destino em Target Groups (Grupos de destino).
 - e. Escolha Next: Configure scaling policies (Próximo: Configurar políticas de escalabilidade).
20. Na página Configure scaling policies (Configurar políticas de escalabilidade), selecione Review (Revisão), pois deixaremos o Amazon EC2 Auto Scaling manter o grupo no tamanho especificado. Observe que, posteriormente, você pode escalar manualmente esse grupo do Auto Scaling, configurar o grupo para escalar em uma programação ou configurar o grupo para escalar com base na demanda.
21. Na página Review (Revisar), escolha Create Auto Scaling group (Criar grupo de Auto Scaling).
22. Após o grupo ser criado, escolha Close (Fechar).

Teste seu load balancer

Quando um cliente enviar uma solicitação para seu load balancer, este roteará a solicitação para uma de suas instâncias registradas.

Para testar seu load balancer

1. Verifique se suas instâncias estão prontas. Na página Auto Scaling Groups (Grupos de Auto Scaling), selecione seu grupo do Auto Scaling e escolha a guia Instances (Instâncias). Inicialmente, suas instâncias estão no estado **Pending**. Quando os estados forem **InService**, eles estarão prontos para uso.
2. Verifique se suas instâncias estão registradas do load balancer. Na página Target Groups (Grupos de destino), selecione seu grupo de destino e escolha a guia Targets (Destinos). Se o estado de suas instâncias for **initial**, é possível que ainda estejam sendo registradas. Quando o estado das suas instâncias for **healthy**, elas estarão prontas para uso. Quando suas instâncias estiverem prontas, você poderá testar o load balancer da forma a seguir.

3. Na página Load balancers, selecione seu load balancer.
4. Na guia Description (Descrição), localize o nome DNS. Esse nome tem o seguinte formato:

`my-lb-xxxxxxxxxx.us-west-2.elb.amazonaws.com`

5. Em um navegador, cole o nome DNS para o load balancer na barra de endereço e pressione Enter. Seu site será exibido.

Tutorial: Gerenciar remotamente instâncias do Amazon EC2

Este tutorial mostra a você como gerenciar remotamente a instância do Amazon EC2 usando Run Command do Systems Manager de sua máquina local. Este tutorial inclui procedimentos para executar comandos usando o console do Amazon EC2 ou AWS Tools para Windows PowerShell, e a AWS Command Line Interface.

Note

Com Executar comando, você também pode gerenciar seus servidores e máquinas virtuais (VMs) em seu ambiente local ou em um ambiente fornecido por outros provedores de nuvem. Para obter mais informações, consulte [Configuração do Systems Manager em ambientes híbridos](#).

Antes de começar

Você deve configurar uma função de perfil de instância do AWS Identity and Access Management (IAM) para o Systems Manager. Anexe uma função do IAM com a política gerenciada AmazonEC2RoleforSSM a uma instância do Amazon EC2. Essa função permite que a instância se comunique com a API do Systems Manager. Para obter mais informações sobre como anexar a função a uma instância existente, consulte [Como anexar uma função do IAM a uma instância \(p. 718\)](#).

Você também deve configurar a conta de usuário do IAM para o Systems Manager, como descrito na próxima seção.

Conceder o acesso à conta de usuário ao Systems Manager

Sua conta de usuário deve ser configurada para se comunicar com a API do SSM. Use o seguinte procedimento para anexar uma política gerenciada do AWS Identity and Access Management (IAM) à sua conta de usuário que lhe garanta acesso total a ações de API do SSM.

Para criar a política de IAM para sua conta de usuário

1. Abra o console do IAM em <https://console.aws.amazon.com/iam/>.
2. No painel de navegação, selecione Policies (Políticas). (Se esta for a primeira vez que você usa o IAM, escolha Get Started (Começar a usar) e Create Policy (Criar política).)
3. No campo Filter (Filtro), digite **AmazonSSMFullAccess** e pressione Enter.
4. Marque a caixa de seleção ao lado de AmazonSSMFullAccess e escolha Policy Actions (Ações da política), Attach (Anexar).
5. Na página Attach Policy (Anexar política), escolha sua conta de usuário e, em seguida, escolha Attach Policy (Anexar política).

Instalar o agente de SSM

O agente de SSM processa as solicitações do Run Command e configura as instâncias especificadas na solicitação. O agente é instalado por padrão nas AMIs do Windows de novembro de 2016 em diante, nas AMIs do Amazon Linux de setembro de 2017 em diante e em todas as AMIs do Amazon Linux 2.

Para instalar o agente no Linux, consulte [Instalação e configuração do SSM Agent em instâncias Linux](#) no Guia do usuário do AWS Systems Manager.

Para instalar o agente no Windows, consulte [Instalação e configuração do SSM Agent em instâncias Windows](#) no Guia do usuário do AWS Systems Manager.

Enviar um comando usando o console do EC2

Use o seguinte procedimento para listar todos os serviços em execução na instância usando Executar comando no console do Amazon EC2.

Para executar um comando usando Executar comando do console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Run Command (Executar comando).
3. Escolha Run a command.
4. Em Command document (Documento do comando), escolha AWS-RunPowerShellScript para instâncias Windows e AWS-RunShellScript para instâncias Linux.
5. Em Target instances (Instâncias de destino), escolha a instância que você criou. Se você não vir a instância, verifique se está atualmente na mesma região que a instância criada. Também verifique se configurou a função e as políticas de confiança do IAM como descrito anteriormente.
6. Em Commands (Comandos), digite **Get-Service** para Windows ou **ps aux** para Linux.
7. (Opcional) Em Working Directory (Diretório de trabalho), especifique um caminho para a pasta em suas instâncias do EC2 onde você deseja executar o comando.
8. (Opcional) Em Execution Timeout (Tempo limite da execução), especifique o número de segundos que o serviço EC2Config ou o agente de SSM tentará executar o comando antes de atingir o tempo limite e falhar.
9. Em Comment (Comentários), recomendamos fornecer informações que o ajudarão a identificar o comando em sua lista de comandos.
10. Em Timeout (seconds) (Tempo limite (segundos)), digite o número de segundos durante os quais o Run Command deve tentar acessar uma instância antes que ela seja considerada inacessível e a execução do comando falhe.
11. Escolha Run (Executar) para executar o comando. Executar comando exibe uma tela de status. Escolha View result (Visualizar resultado).
12. Para visualizar a saída, escolha a chamada do comando, escolha a guia Output (Saída) e, depois, escolha View Output (Visualizar saída).

The screenshot shows the AWS Systems Manager Run Command interface. At the top, there are two tabs: "Run a command" and "Actions". Below the tabs is a search bar labeled "Filter by attributes". A table lists several commands with columns: "Command ID", "Instance ID", "Document name", "Status", "Requested date", and "Comments". One command is highlighted with a red border: "65555b90-ee60-45...". The status for this command is "Success". Below the table, the "Command ID" and "Instance ID" are displayed as "65555b90-ee60-4520-9dc3-e42e94445469" and "i-8fd6aa30". Under the "Output" tab, detailed information about the selected command is shown, including its "Command ID", "Document name", "Date requested", and "Output S3 bucket".

Para obter mais exemplos sobre como executar os comandos usando Run Command, consulte [Execução de comandos usando Run Command do Systems Manager](#).

Enviar um comando usando AWS Tools para Windows PowerShell

Use o seguinte procedimento para listar todos os serviços em execução na instância usando Executar comando no AWS Tools para Windows PowerShell.

Para executar um comando

1. Em seu computador local, faça download da versão mais recente do [AWS Tools para Windows PowerShell](#).
2. Abra o AWS Tools para Windows PowerShell no computador local e execute o seguinte comando para especificar suas credenciais.

```
Set-AWSCredentials -AccessKey key -SecretKey key
```

3. Execute o seguinte comando para definir a região para sua sessão de PowerShell. Especifique a região onde você criou a instância no procedimento anterior. Este exemplo usa a região us-west-2.

```
Set-DefaultAWSRegion -Region us-west-2
```

4. Execute o seguinte comando para recuperar os serviços em execução na instância.

```
Send-SSMCommand -InstanceId 'Instance-ID' -DocumentName AWS-RunPowerShellScript -Comment 'listing services on the instance' -Parameter @{'commands'=@('Get-Service')}
```

O comando retorna um ID de comando, que você usará para visualizar os resultados.

5. O seguinte comando retorna a saída do Send-SSMCommand original. A saída ficará truncada se tiver mais de 2.500 caracteres. Para visualizar uma lista completa dos serviços, especifique o bucket do Amazon S3 no comando usando o parâmetro -OutputS3BucketName *bucket_name*.

```
Get-SSMCommandInvocation -CommandId Command-ID -Details $true | select -ExpandProperty CommandPlugins
```

Para obter mais exemplos sobre como executar comandos usando Run Command com o Tools para Windows PowerShell, consulte [Demonstração do Run Command do Systems Manager usando o AWS Tools para Windows PowerShell](#).

Enviar um comando usando a AWS CLI

Use o seguinte procedimento para listar todos os serviços em execução na instância usando Executar comando na AWS CLI.

Para executar um comando

1. No computador local, faça download da versão mais recente da [AWS Command Line Interface \(AWS CLI\)](#).
2. Abra a CLI da AWS no computador local e execute o seguinte comando para especificar suas credenciais e a região.

```
aws configure
```

3. O sistema solicita que você especifique o seguinte.

```
AWS Access Key ID [None]: key
AWS Secret Access Key [None]: key
Default region name [None]: region, for example us-east-1
Default output format [None]: ENTER
```

4. Execute o seguinte comando para recuperar os serviços em execução na instância.

```
aws ssm send-command --document-name "AWS-RunShellScript" --comment "listing services"
--instance-ids "Instance-ID" --parameters commands="service --status-all" --region us-west-2 --output text
```

O comando retorna um ID de comando, que você usará para visualizar os resultados.

5. O seguinte comando retorna a saída do Send-SSMCommand original. A saída ficará truncada se tiver mais de 2.500 caracteres. Para visualizar uma lista completa de serviços, é necessário especificar um bucket do Amazon S3 no comando usando o parâmetro --output-s3-bucket-name *bucket_name*.

```
aws ssm list-command-invocations --command-id "command ID" --details
```

Para obter mais exemplos sobre como executar comandos usando Run Command com a AWS CLI, consulte [Demonstração do Run Command do Systems Manager usando a AWS CLI](#).

Conteúdo relacionado

Para obter mais informações sobre Executar comando e Systems Manager, consulte as seguintes referências.

- [Guia do usuário do AWS Systems Manager](#)
- [Amazon EC2 Systems Manager API Reference](#)
- [Systems Manager AWS Tools para PowerShell Cmdlet Reference](#)
- [Systems Manager AWS CLI Command Reference](#)
- [SDKs da AWS](#)

Imagens de máquina da Amazon (AMIs)

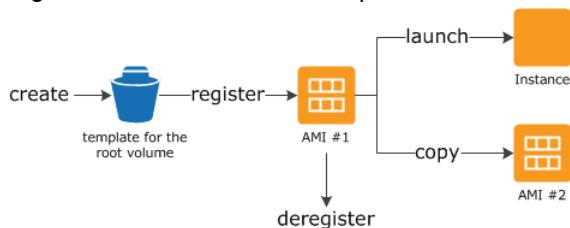
Uma Imagem de máquina da Amazon (AMI) fornece as informações necessárias para iniciar uma instância. Você deve especificar uma AMI ao iniciar uma instância. Você pode executar várias instâncias em uma única AMI quando precisa de várias instâncias com a mesma configuração. Você pode usar AMIs diferentes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

Uma AMI inclui o seguinte:

- Um modelo para o volume raiz de uma instância (por exemplo, um sistema operacional, um servidor de aplicativo e aplicativos)
- 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

Como 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 região ou para regiões 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 \(p. 91\)](#) e [Localizar uma AMI do Linux \(p. 95\)](#).

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 [Instâncias do Amazon EC2 \(p. 176\)](#).

Como criar sua própria AMI

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

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 EBS ou um volume de armazenamento de instâncias. Para obter mais informações, consulte [Volume do dispositivo raiz do Amazon EC2 \(p. 15\)](#).

Para criar uma AMI com Amazon EBS, consulte [Criação de uma AMI do Linux com Amazon EBS \(p. 111\)](#). Para criar uma AMI com armazenamento de instâncias, consulte [Criação de uma AMI em Linux com armazenamento de instâncias \(p. 115\)](#).

Para ajudar a categorizar e gerenciar suas AMIs, você pode atribuir tags personalizadas a elas. Para obter mais informações, consulte [Marcação dos seus recursos do Amazon EC2 \(p. 1003\)](#).

Como 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 \(p. 97\)](#).

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 \(p. 107\)](#).

Cancelamento do registro da sua 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 o registro da AMI do Linux \(p. 156\)](#).

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 alto desempenho para aplicativos 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 serviços 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 \(p. 158\)](#).

Tipos de AMI

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

- Região (consulte [Regiões e Zonas de disponibilidade \(p. 7\)](#))
- Sistema operacional
- Arquitetura (32 bits ou 64 bits)
- [Permissões de execução \(p. 91\)](#)
- [Armazenamento para o dispositivo raiz \(p. 91\)](#)

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 \(p. 97\)](#). Os desenvolvedores podem cobrar por suas AMIs. Para obter mais informações, consulte [AMIs pagas \(p. 107\)](#).

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 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 do Amazon EC2 \(p. 15\)](#).

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

Característica	AMI baseado em 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	16 TiB	10 GiB
Volume do dispositivo raiz	Volume do Amazon EBS	Volumes de armazenamento de instâncias
Persistência de dados	Por padrão, o volume raiz é excluído quando a instância é encerrada.* Os	Os dados em qualquer volume do armazenamento de instâncias

Característica	AMI baseado em Amazon EBS	AMI com armazenamento de instâncias da Amazon
	dados em todos os outros volumes do Amazon EBS persistem após o encerramento da instância, por padrão.	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 Amazon EBS e pelo armazenamento da AMI como um snapshot do Amazon 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
Estado parado	Pode ser colocada em estado parado quando a instância não está em execução, mas o volume raiz é persistido no Amazon EBS	Não pode estar no estado parado. As instâncias estão em execução ou encerradas

* Por padrão, os volumes raiz de instâncias com Amazon 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 [Alteração do volume do dispositivo raiz para persistência \(p. 18\)](#).

Como 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 [Acessando o Amazon EC2 \(p. 3\)](#).

- [describe-images](#) (AWS CLI)
- [Get-EC2Image](#) (AWS Tools para 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 [Interrompa e inicie sua instância \(p. 458\)](#).

Persistência e armazenamento físico 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 Amazon 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 \(p. 958\)](#).

As instâncias que usam o Amazon EBS para dispositivo raiz automaticamente têm um volume do Amazon 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 Amazon EBS adicionais um mapeamento de dispositivos de blocos. Para obter mais informações, consulte [Mapeamento de dispositivos de blocos \(p. 979\)](#).

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, o desempenho de uma instância que usa um volume do Amazon 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 Amazon 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 Console de gerenciamento da AWS que permite criar uma AMI em uma instância em execução. Para obter mais informações, consulte [Criação de uma AMI do Linux com Amazon EBS \(p. 111\)](#).

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. Nas AMIs com Amazon EBS, você é cobrado pelo uso da instância, pelo uso e volume de armazenamento do Amazon EBS e por armazenar a AMI como um snapshot do Amazon 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 desempenho.

Para melhor desempenho, 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](#).

AMIs HVM

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

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 [Intel Virtualization Technology](#), 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 informações, consulte [Rede avançada no Linux \(p. 768\)](#) e [Linux Instâncias de computação acelerada \(p. 237\)](#).

Todos os tipos de instância são compatíveis com AMIs HVM.

Para encontrar a AMI HVM, verifique se o tipo de virtualização da AMI está definido como `hvm` usando o console ou o comando [describe-images](#).

AMIs PV

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.1st` da sua imagem. Os guests paravirtuais podem ser executados no hardware host que não tenha suporte explícito para virtualização, mas não podem aproveitar as extensões especiais de hardware, como rede aumentada ou processamento de GPU. Historicamente, os guests PV têm melhor desempenho 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 [Como habilitar seus próprios kernels do Linux \(p. 169\)](#).

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.

As seguintes regiões da AWS oferecem suporte a instâncias PV: Ásia-Pacífico (Tóquio), Ásia-Pacífico (Cingapura), Ásia-Pacífico (Sydney), UE (Frankfurt), UE (Irlanda), América do Sul (São Paulo), Leste dos EUA (Norte da Virgínia), Oeste dos EUA (Norte da Califórnia) e Oeste dos EUA (Oregon).

Para encontrar uma AMI PV, verifique se o tipo de virtualização da AMI está definido como `paravirtual` usando o console ou o comando [describe-images](#).

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 desempenho no armazenamento e na E/S de rede usando-os. Com esses drivers de PV em HVM, os convidados recebem desempenho igual, ou melhor, que os guests paravirtuais.

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`) ou 64-bits (`x86_64`)
- 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 AMIs do Windows, consulte [Localizar AMI do Windows](#) no Guia do usuário do Amazon EC2 para instâncias do Windows.

Tópicos

- [Localizar AMI do Linux usando o console do Amazon EC2 \(p. 95\)](#)
- [Localizar uma AMI usando o AWS CLI \(p. 96\)](#)
- [Encontrar uma AMI de início rápido \(p. 96\)](#)

Localizar AMI do Linux usando o console do Amazon EC2

É possível localizar AMIs do Linux usando o console do Amazon EC2. Você pode pesquisar todas as AMIs disponíveis usando a página **Images (Imagens)** ou selecionar AMIs comumente usadas na guia **Quick Start (Início rápido)** ao usar o console para executar uma instância. Os IDs da AMI são exclusivos de cada região.

Para encontrar uma AMI do Linux usando a página **Choose AMI (Escolher AMI)**

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**.

4. Na guia Quick Start (Início rápido), selecione uma das AMIs mais usadas na lista. Se não vir a AMI de que você precisa, selecione AWS Marketplace ou a guia Community AMIs (AMIs da comunidade) para localizar AMIs adicionais.

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 \(p. 91\)](#).
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 \(p. 393\)](#). 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 [Execução de uma instância usando a AWS CLI](#) no Guia do usuário do 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.

Encontrar uma AMI de início rápido

Ao executar uma instância usando o console do Amazon EC2, a página Choose an Amazon Machine Image (AMI) (Escolher uma Imagem de máquina da Amazon (AMI)) inclui uma lista de AMIs populares

na guia Quick Start (Início rápido). Se você deseja automatizar a execução de uma instância usando uma dessas AMIs de início rápido, é necessário localizar de maneira programática o ID da versão atual da AMI.

Para localizar a versão atual de uma AMI de início rápido, você pode enumerar todas as AMIs com o seu nome e localizar a AMI com a data de criação mais recente.

Example Exemplo: encontrar a AMI do Amazon Linux 2 atual

```
aws ec2 describe-images --owners amazon --filters 'Name=name,Values=amzn2-ami-hvm-2.0.??????-x86_64-gp2' 'Name=state,Values=available' --output json | jq -r '.Images | sort_by(.CreationDate) | last().[].ImageId'
```

Example Exemplo: encontrar a AMI do Amazon Linux atual

```
aws ec2 describe-images --owners amazon --filters 'Name=name,Values=amzn-ami-hvm-????.???.??.??????-x86_64-gp2' 'Name=state,Values=available' --output json | jq -r '.Images | sort_by(.CreationDate) | last().[].ImageId'
```

Example Exemplo: encontrar a AMI do Ubuntu Server 16.04 LTS atual

```
aws ec2 describe-images --owners 099720109477 --filters 'Name=name,Values=ubuntu/images/hvm-ssd/ubuntu-xenial-16.04-amd64-server-???????' 'Name=state,Values=available' --output json | jq -r '.Images | sort_by(.CreationDate) | last().[].ImageId'
```

Example Exemplo: encontrar a AMI do Red Hat Enterprise Linux 7.5 atual

```
aws ec2 describe-images --owners 309956199498 --filters 'Name=name,Values=RHEL-7.5_HVM_GA*' 'Name=state,Values=available' --output json | jq -r '.Images | sort_by(.CreationDate) | last().[].ImageId'
```

Example Exemplo: encontrar a AMI do SUSE Linux Enterprise Server 15 atual

```
aws ec2 describe-images --owners amazon --filters 'Name=name,Values=suse-sles-15-v??????-hvm-ssd-x86_64' 'Name=state,Values=available' --output json | jq -r '.Images | sort_by(.CreationDate) | last().[].ImageId'
```

AMIs compartilhadas

A AMI compartilhada é aquela 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. Se tiver dúvidas ou observações sobre uma AMI compartilhada, use os [Fóruns da AWS](#).

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 com armazenamento de instâncias](#) ou [Criação de uma AMI do Linux com Amazon EBS](#). Para obter mais informações sobre como criar, entregar e manter seus aplicativos no AWS Marketplace, consulte [Guia do usuário do AWS Marketplace](#) e [Guia do vendedor do AWS Marketplace](#).

Tópicos

- [Localização de AMIs compartilhadas \(p. 98\)](#)
- [Transformação em AMI pública \(p. 100\)](#)
- [Compartilhamento de uma AMI com contas específicas da AWS \(p. 101\)](#)
- [Uso de favoritos \(p. 103\)](#)
- [Diretrizes para AMIs em Linux compartilhadas \(p. 103\)](#)

Localização de AMIs compartilhadas

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

Note

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 uma AMI](#).

Localização de 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.

Localização de 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"
```

Uso de 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
```

Reinic peace 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.config
[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](#).

Transformação em AMI pública

O Amazon EC2 permite que você compartilhe suas AMIs com outras contas da AWS. Você pode permitir que todas as contas da AWS executem a AMI (tornem a AMI pública) ou permitir que só algumas contas específicas executem a AMI (consulte [Compartilhamento de uma AMI com contas específicas da AWS \(p. 101\)](#)). Você não será cobrado quando sua AMI for executada por outras contas da AWS; serão cobradas apenas as contas que executarem a AMI.

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 [Cópia de uma AMI \(p. 150\)](#).

Para evitar expor dados confidenciais ao compartilhar uma AMI, leia as considerações de segurança em [Diretrizes para AMIs em Linux compartilhadas \(p. 103\)](#) e siga as ações recomendadas.

Note

Se uma AMI tem um código de produto ou contém um snapshot de um volume criptografado, você não pode torná-la pública. Você deve compartilhar a AMI apenas com contas específicas da AWS.

Compartilhamento de 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.

Compartilhamento de uma AMI com todas as contas da AWS (AWS CLI)

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

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

Para tornar um AMI pública

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

```
aws ec2 modify-image-attribute --image-id ami-12345678 --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-12345678 --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-12345678 --launch-permission "Remove=[{Group=all}]"
```

Compartilhamento de 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.

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 [Cópia de uma AMI \(p. 150\)](#).

Não há limite para o número de contas da AWS com as quais uma AMI pode ser compartilhada.

Note

Não é possível compartilhar diretamente uma AMI que contenha um snapshot de um volume criptografado. Você pode compartilhar os snapshots criptografados com outras contas da AWS. Isso permite que a outra conta copie snapshots em outras regiões, criptografe novamente

os snapshots e crie AMIs usando os snapshots criptografados. Para obter mais informações, consulte [Compartilhamento de um snapshot do Amazon EBS \(p. 905\)](#).

Compartilhamento de 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.

5. Para permitir a criação de permissões de volume para snapshots, selecione Adicionar permissões de "criar volume" aos snapshots associados a seguir ao criar permissões.

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.

6. Escolha Save (Salvar) quando terminar.
7. (Opcional) Para visualizar os IDs de conta da AWS com que você compartilhou a AMI, selecione a AMI na lista e selecione a guia Permissions. Para localizar as AMIs que são compartilhadas com você, consulte [Localização de AMIs compartilhadas \(p. 98\)](#).

Compartilhamento de 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-12345678 --launch-permission  
"Add=[{UserId=123456789012}]"
```

O comando a seguir concede permissão de criação de volume a um snapshot.

```
aws ec2 modify-snapshot-attribute --snapshot-id snap-1234567890abcdef0 --attribute  
createVolumePermission --operation-type add --user-ids 123456789012
```

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-12345678 --launch-permission  
"Remove=[{UserId=123456789012}]"
```

O comando a seguir remove a permissão de criação de volume de um snapshot.

```
aws ec2 modify-snapshot-attribute --snapshot-id snap-1234567890abcdef0 --attribute createVolumePermission --operation-type remove --user-ids 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-12345678 --attribute launchPermission
```

Uso de favoritos

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, este URL executa uma instância a partir da AMI ami-12345678 na região us-east-1:

```
https://console.aws.amazon.com/ec2/v2/home?region=us-  
east-1#LaunchInstanceWizard:ami=ami-12345678
```

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.

Note

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 de usá-las \(p. 104\)](#)
- [Desabilite logins remotos com senha para raiz \(p. 104\)](#)
- [Desabilite o acesso à raiz local \(p. 105\)](#)

- [Remova os pares de chave do host SSH \(p. 105\)](#)
- [Instalação de credenciais de chave pública \(p. 106\)](#)
- [Desabilitação de verificações DNS sshd \(opcional\) \(p. 106\)](#)
- [Identifique-se \(p. 107\)](#)
- [Proteja-se \(p. 107\)](#)

Se você estiver criando AMIs para o AWS Marketplace, consulte [Criação de AMIs para o 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 de usá-las

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.

Desabilite 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.

Desabilite 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.

Remova os 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.

```
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.

Desabilitação de 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 [Amazon EC2 forum](#). Esse é um local central conveniente para usuários que estão interessados em experimentar novas AMIs compartilhadas.

Proteja-se

As seções anteriores descreveram como deixar suas AMIs compartilhadas protegidas, seguras e utilizáveis pelos usuários que as executarem. Esta seção descreve as diretrizes para proteger-se dos usuários da sua AMI.

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 \(p. 133\)](#).
- 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 se integra ao AWS Marketplace, permitindo aos desenvolvedores cobrar 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 de desenvolvedor, para permitir que você encontre produtos para atender às suas necessidades. Para obter mais informações sobre o AWS Marketplace, consulte o site do [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

Amazon DevPay não está mais aceitando novos vendedores ou produtos. O AWS Marketplace agora é a única plataforma unificada de comércio eletrônico para vender softwares 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 Amazon EBS.

Tópicos

- [Como vender sua AMI \(p. 108\)](#)
- [Como encontrar uma AMI paga \(p. 108\)](#)
- [Comprar uma AMI paga \(p. 109\)](#)
- [Como obter o código de produto para sua instância \(p. 110\)](#)
- [Como usar suporte pago \(p. 110\)](#)
- [Faturas para AMI pagas e compatíveis \(p. 111\)](#)
- [Gerenciamento de suas assinaturas do AWS Marketplace \(p. 111\)](#)

Como vender sua AMI

Você pode vender sua AMI usando AWS Marketplace. 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 sua AMI no AWS Marketplace, consulte [Como vender no AWS Marketplace](#).

Como encontrar 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.

Como 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 de pesquisa, escolha Proprietário e, em seguida, AWS Marketplace.
5. Se você souber o código do produto, escolha Product Code e digite o código do produto.

Como encontrar 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**.

Como encontrar uma AMI paga usando a 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.

Como 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 do AWS Marketplace \(p. 410\)](#).

Como 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 do 1-Click.
- 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 do AWS Marketplace \(p. 410\)](#).

Como obter o código de produto para sua instância

Você pode recuperar 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 \(p. 516\)](#).

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

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/product-codes
```

Se sua instância oferecer suporte a isso, você poderá usar o comando GET:

```
[ec2-user ~]$ GET http://169.254.169.254/latest/meta-data/product-codes
```

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

Como 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 para 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 do AWS Marketplace](#).

Gerenciamento de 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 assistente de execução no console do Amazon EC2.

Criação de uma AMI do Linux com 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 com volumes do 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 \(p. 91\)](#). Para obter mais informações sobre como criar uma AMI do Linux com armazenamento de instâncias, consulte [Criação de uma AMI em Linux com armazenamento de instâncias \(p. 115\)](#).

Para obter mais informações sobre como criar uma AMI do Windows com Amazon EBS, consulte [Criação de uma AMI do Windows com 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 o registro da AMI do Linux \(p. 156\)](#). Se qualquer volume anexado à instância estiver criptografado, a nova AMI só será executada com êxito em instâncias compatíveis com a Criptografia de Amazon EBS. Para obter mais informações, consulte [Amazon EBS Encryption \(p. 926\)](#).

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 [Criação de um snapshot do Amazon EBS \(p. 898\)](#).

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 [Mapeamento de dispositivos de blocos \(p. 979\)](#).

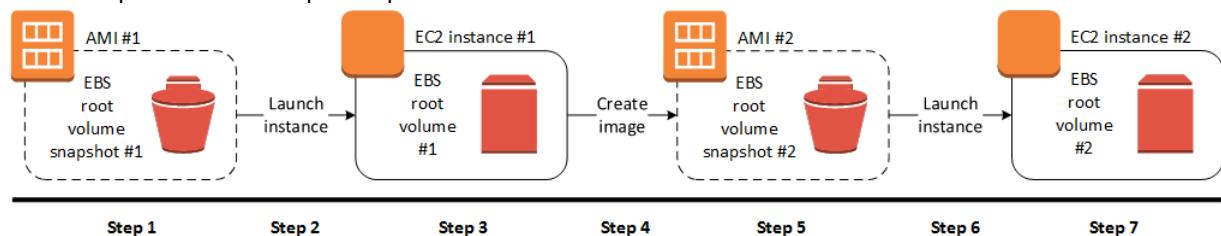
Note

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 [Como inicializar volumes do Amazon EBS](#).

Criação de uma AMI do Linux de uma instância

Você pode criar uma AMI usando o Console de gerenciamento da AWS 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.



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 [Execução de uma instância usando o assistente de execução de instância \(p. 391\)](#).
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 [Execução de uma instância usando o assistente de execução de instância \(p. 391\)](#).
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 aplicativos
 - Copiar dados
 - Reduzir o tempo de inicialização excluindo arquivos temporários, desfragmentando o disco rígido e liberando o espaço livre
 - Anexar volumes adicionais do Amazon EBS
4. (Opcional) Criar snapshots de todos os volumes anexados à sua instância. Para obter mais informações sobre como criar snapshots, consulte [Criação de um snapshot do Amazon EBS \(p. 898\)](#).
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) – esta opção não é selecionada por padrão. O Amazon EC2 encerra a instância, faz snapshots dos volumes anexados, cria e registra a AMI e, em seguida, reinicializa 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 instâncias 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.

Note

Delete on Termination (Excluir ao encerrar) determina se o volume do EBS é excluído ou não. Isso não afeta a instância ou a AMI.

- Para adicionar um volume do Amazon EBS, escolha Add New Volume (Adicionar volume novo) (que acrescenta uma linha nova). Em Volume Type (Tipo de volume), escolha EBS, e preencha os campos na 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 [Como adicionar volumes de armazenamento de instâncias a uma AMI \(p. 963\)](#). 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 [Execução de uma instância usando o assistente de execução de instância \(p. 391\)](#).
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 [Acessando o Amazon EC2 \(p. 3\)](#).

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

Criação de uma AMI do Linux de um snapshot

Se você tiver um snapshot do volume do dispositivo raiz de uma instância, poderá criar uma AMI desse snapshot usando o Console de gerenciamento da AWS ou a linha de comando.

Important

Algumas distribuições do Linux, como o Red Hat Enterprise Linux (RHEL) e o SUSE Linux Enterprise Server (SLES), usam o código `billingProduct` do Amazon EC2; associado a uma AMI para verificar o status da assinatura para atualizações de pacote. A criação de uma AMI de um snapshot do EBS não mantém esse código de faturamento, e as instâncias executadas dessa AMI não podem se conectar à infraestrutura de atualização de pacote. Se você adquiriu uma oferta de Instância reservada para uma dessas distribuições Linux e executou as instâncias

usando uma AMI que não contém o código de fatura necessário, sua Instância reservada não é aplicada a essas instâncias.

Da mesma forma, embora você possa criar uma AMI do Windows de um snapshot, você não pode executar uma instância da AMI com êxito.

Geralmente, a AWS não recomenda criar AMIs manualmente a partir de snapshots.

Para obter mais informações sobre como criar AMIs do Windows ou AMIs para os sistemas operacionais Linux que devem manter os códigos de faturamento da AMI para funcionar corretamente, consulte [Criação de uma AMI do Linux de uma instância \(p. 112\)](#).

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 [Nomenclatura de dispositivos nas instâncias do Linux \(p. 978\)](#).
 - 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 \(p. 94\)](#).
 - (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 [Como estender um sistema de arquivos Linux após um redimensionamento de volume \(p. 890\)](#).

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 [Acessando o Amazon EC2 \(p. 3\)](#).

- [register-image](#) (CLI da AWS)
- [Register-EC2Image](#) (AWS Tools para Windows PowerShell)

Criação de uma AMI em Linux com armazenamento de instâncias

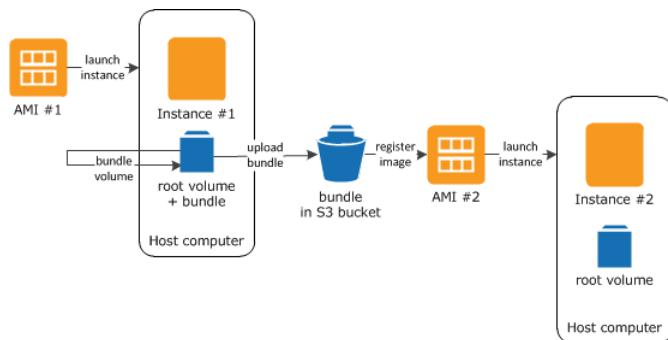
Para criar uma AMI em Linux com armazenamento de instâncias, inicie a instância que você executou a partir de uma AMI em Linux com o armazenamento de instâncias existente. Depois de personalizar a instância para atender às suas necessidades, empacote o volume e registre uma nova AMI, que você pode usar para executar novas instâncias com essas personalizações.

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 \(p. 91\)](#). Se você precisar criar uma AMI do Linux com Amazon EBS, consulte [Criação de uma AMI do Linux com Amazon EBS \(p. 111\)](#).

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 o registro da AMI do Linux \(p. 156\)](#).

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 [Mapeamento de dispositivos de blocos \(p. 979\)](#).

Pré-requisitos

Antes que você crie uma AMI, é preciso concluir as tarefas seguir:

- Instale as ferramentas da AMI. Para obter mais informações, consulte [Configuração das ferramentas de AMI \(p. 117\)](#).
- Instale a 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 AWS General Reference.
- 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 AWS General Reference.

- Verifique se você tem um certificado x.509 e a chave privada correspondente.
 - Se você precisar criar um certificado X.509, consulte [Gerenciamento da assinatura dos certificados \(p. 119\)](#). 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 aplicativos, copiar dados, excluir arquivos temporários e modificar a configuração do Linux.

Tarefas

- [Configuração das ferramentas de AMI \(p. 117\)](#)
- [Criação de uma AMI a partir de uma instância do Amazon Linux com armazenamento de instâncias \(p. 120\)](#)
- [Criação de uma AMI a partir de uma instância em Ubuntu com armazenamento de instâncias \(p. 123\)](#)
- [Conversão de uma AMI com armazenamento de instâncias em uma AMI com Amazon EBS \(p. 127\)](#)

Configuração das ferramentas de 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 \(p. 131\)](#).

```
[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 \(p. 131\)](#).

```
[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).

- 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
```

- Adicione as ferramentas à sua variável de ambiente PATH. Por exemplo:

```
[ec2-user ~]$ export PATH=$EC2_AMITOOL_HOME/bin:$PATH
```

- Você pode verificar a instalação das suas ferramentas da AMI usando o comando [ec2-ami-tools-version](#) (p. 131).

```
[ec2-user ~]$ ec2-ami-tools-version
```

Gerenciamento da assinatura dos certificados

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

- Instale e configure o OpenSSL.
- 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
```

- Gere um certificado usando o comando openssl req.

```
openssl req -new -x509 -nodes -sha256 -days 365 -key private-key.pem -outform 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
```

Criação de uma AMI com base em 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 \(p. 116\)](#).

Tópicos

- [Criação de uma AMI a partir de uma instância do Amazon Linux com armazenamento de instâncias \(p. 120\)](#)
- [Criação de uma AMI a partir de uma instância em Ubuntu com armazenamento de instâncias \(p. 123\)](#)

Criação de 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 [Criação de uma AMI a partir de uma instância em Ubuntu com armazenamento de instâncias \(p. 123\)](#).

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 [Pré-requisitos \(p. 116\)](#).

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 \(p. 442\)](#). 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 \(p. 133\)](#) 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 \(p. 860\)](#), [associar \(p. 863\)](#) e [montar \(p. 864\)](#) um novo volume do 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 \(p. 133\)](#) 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 \(p. 116\)](#).

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 [Mapeamento de dispositivos de blocos \(p. 979\)](#).

- 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 > sudo /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 \(p. 133\)](#).

```
<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/sdai</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 \(p. 144\)](#) 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 sua AMI em uma região diferente de Leste dos EUA (Norte da Virgínia), 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 \(p. 121\)](#), 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 \(p. 144\)](#), especifique essa região novamente para esse comando.

Criação de uma AMI a partir de uma instância em Ubuntu com armazenamento de instâncias

Esta seção descreve a criação da AMI a partir de uma instância em Ubuntu Linux. Os procedimentos a seguir podem não funcionar para instâncias que executam outras distribuições do Linux. Para procedimentos específicos do Amazon Linux, consulte [Criação de uma AMI a partir de uma instância do Amazon Linux com armazenamento de instâncias \(p. 120\)](#).

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, por isso o GRUB Legacy deve ser instalado. Vá para [Step 1.b \(p. 123\)](#). Se o GRUB Legacy já estiver presente, vá direto para [Step 2 \(p. 124\)](#).

- b. Instale o pacote grub usando o comando a seguir.

```
ubuntu:~$ sudo apt-get install -y grub
```

Verifique se sua instância está usando o GRUB Legacy.

```
ubuntu:~$ grub --version
```

```
grub (GNU GRUB 0.97)
```

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
```

Amazon Elastic Compute Cloud
User Guide for Linux Instances
Criação de uma AMI com base em uma
instância com armazenamento de instâncias

-
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 [Pré-requisitos \(p. 116\)](#).

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 \(p. 442\)](#). 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 \(p. 133\)](#) 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 \(p. 860\)](#), [associar \(p. 863\)](#) e [montar \(p. 864\)](#) um novo volume do 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 \(p. 133\)](#) 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 [Mapeamento de dispositivos de blocos \(p. 979\)](#).

- 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 \(p. 144\)](#) 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 sua AMI em uma região diferente de Leste dos EUA (Norte da Virgínia), 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 \(p. 125\)](#), 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 \(p. 144\)](#), 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.

Conversão 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 [Execução de uma instância usando o assistente de execução de instância \(p. 391\)](#). As instâncias do Amazon Linux já têm a AWS CLI e as ferramentas de 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 \(p. 442\)](#). 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 EBS para sua nova AMI.

- a. Crie um o volume do Amazon 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 Amazon 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 \(p. 139\)](#).

```
[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 \(p. 143\)](#).

- a. Altere os diretórios para a pasta de pacotes.

```
[ec2-user ~]$ cd /tmp/bundle/
```

- b. Execute o comando [ec2-unbundle](#) (p. 143).

```
[ec2-user bundle]$ ec2-unbundle -m image.manifest.xml --privatekey /path/to/pk-HKZYKTAIG2ECMXYTBH3HXV4ZBEXAMPLE.pem
```

8. Copie os arquivos da imagem não empacotada para o novo volume do Amazon 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/sdb
```

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 Amazon 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 Amazon EBS é montado em `/mnt/ebs`, o arquivo `fstab` está 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 do novo volume do Amazon EBS, da forma a seguir.

- a. Crie um snapshot de novo volume do Amazon EBS.

```
[ec2-user bundle]$ aws ec2 create-snapshot --region us-west-2 --description "your_snapshot_description" --volume-id volume_id
```

- b. 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 Amazon 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 testar que você pode executar uma instância a partir da nova AMI, você pode excluir o volume do Amazon EBS criado para esse procedimento.

```
aws ec2 delete-volume --volume-id volume_id
```

Referência ferramentas de 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 [Configuração das ferramentas de AMI \(p. 117\)](#).

Para obter informações sobre suas chaves de acesso, consulte [Práticas recomendadas para gerenciar chaves de acesso da AWS](#).

Comandos

- [ec2-ami-tools-version \(p. 131\)](#)
- [ec2-bundle-image \(p. 131\)](#)
- [ec2-bundle-vol \(p. 133\)](#)
- [ec2-delete-bundle \(p. 137\)](#)
- [ec2-download-bundle \(p. 139\)](#)
- [ec2-migrate-manifest \(p. 141\)](#)
- [ec2-unbundle \(p. 143\)](#)

- [ec2-upload-bundle \(p. 144\)](#)
- [Opções comuns para ferramentas AMI \(p. 147\)](#)

ec2-ami-tools-version

Descrição

Descreve a versão das ferramentas da AMI.

Sintaxe

ec2-ami-tools-version

Resultado

As informações da versão.

Exemplo

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

Descrição

Crie uma AMI em Linux com armazenamento de instâncias a partir de uma imagem de sistema operacional criada em um arquivo de loopback.

Sintaxe

```
ec2-bundle-image -c path -k path -u account -i path [-d path] [--ec2cert path]
[-r architecture] [--productcodes code1,code2,...] [-B mapping] [-p prefix]
```

Opções

-c, --cert path

O arquivo de certificado de chave pública RSA codificado por PEM do usuário.

Exigido: 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.

Exigido: sim

-u, --user account

O ID da conta da AWS do usuário, sem traços.

Exigido: sim

-i, --image path

O caminho até imagem para fazer o pacote.

Exigido: 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 [Configuração das ferramentas de AMI \(p. 117\)](#), 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

Suspensão. Use [register-image](#) para configurar o kernel.

Exigido: Não
--ramdisk ramdisk_id

Suspensão. Use [register-image](#) para configurar o disco RAM, se necessário.

Exigido: Não

Resultado

Mensagens de status que descrevem os estágios e o status do processo de empacotamento.

Exemplo

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

Descrição

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 [Criação de uma AMI em Linux com armazenamento de instâncias \(p. 115\)](#).

Sintaxe

```
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]
```

Opções

-c, --cert *path*

O arquivo de certificado de chave pública RSA codificado por PEM do usuário.

Exigido: sim

-k, --privatekey *path*

O caminho até o arquivo de chaves RSA codificado por PEM do usuário.

Exigido: sim

-u, --user *account*

O ID da conta da AWS do usuário, sem traços.

Exigido: 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 [Configuração das ferramentas de AMI \(p. 117\)](#), 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

Resultado

Mensagens de status que descrevem os estágios e o status do empacotamento.

Exemplo

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

Descrição

Exclui o pacote especificado do armazenamento Amazon S3. Após excluir um pacote, você não pode executar instâncias a partir da AMI correspondente.

Sintaxe

```
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]
```

Opções

-b, --bucket bucket

O nome do bucket do Amazon S3 que contém a AMI empacotada, seguido por um prefixo de caminho opcional delimitado por '/'

Exigido: sim

-a, --access-key access_key_id

O ID da chave de acesso da AWS.

Exigido: sim

-s, --secret-key secret_access_key

A chave de acesso secreta da AWS.

Exigido: sim

-t, --delegation-token token

O token de delegação para repassar à solicitação da AWS. Para mais informações, consulte o [Uso de 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).

--regionregion

A região a ser usada na assinatura da solicitação.

Padrão: `us-east-1`

Obrigatório: Sim se estiver usando a assinatura versão 4

--sigvversion

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 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

Resultado

O Amazon EC2 exibe mensagens de status indicando os estágios e o status do processo de exclusão.

Exemplo

Este exemplo exclui um pacote do Amazon S3.

```
[ec2-user ~]$ ec2-delete-bundle -b myawsbucket -a your_access_key_id -s your_secret_access_key
Deleting files:
myawsbucket/image.manifest.xml
myawsbucket/image.part.00
myawsbucket/image.part.01
myawsbucket/image.part.02
myawsbucket/image.part.03
myawsbucket/image.part.04
myawsbucket/image.part.05
myawsbucket/image.part.06
Continue? [y/n]
y
Deleted myawsbucket/image.manifest.xml
Deleted myawsbucket/image.part.00
Deleted myawsbucket/image.part.01
Deleted myawsbucket/image.part.02
Deleted myawsbucket/image.part.03
Deleted myawsbucket/image.part.04
Deleted myawsbucket/image.part.05
Deleted myawsbucket/image.part.06
ec2-delete-bundle complete.
```

ec2-download-bundle

Descrição

Faz download das AMIs do Linux com armazenamento de instâncias especificadas a partir do armazenamento do Amazon S3.

Sintaxe

```
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]
```

Opções

-b, --bucket bucket

O nome do bucket Amazon S3 no qual o pacote está localizado, seguido por um prefixo de caminho opcional delimitado por '/'.

Exigido: sim

-a, --access-key access_key_id

O ID da chave de acesso da AWS.

Exigido: sim

-s, --secret-key secret_access_key

A chave de acesso secreta da AWS.

Exigido: sim

-k, --privatekey path

A chave privada usada para descriptografar o manifesto.

Exigido: 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

Resultado

São exibidas as mensagens de status que indicam os vários estágios do processo de download.

Exemplo

Este exemplo cria o diretório `bundled` (usando o comando Linux `mkdir`) e faz download do pacote do bucket `myawsbucket` do Amazon S3.

```
[ec2-user ~]$ mkdir bundled
[ec2-user ~]$ ec2-download-bundle -b myawsbucket/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 myawsbucket to mybundle/image.manifest.xml ...
Downloading part image.part.00 from myawsbucket/bundles/bundle_name to mybundle/
image.part.00 ...
Downloaded image.part.00 from myawsbucket
Downloading part image.part.01 from myawsbucket/bundles/bundle_name to mybundle/
image.part.01 ...
Downloaded image.part.01 from myawsbucket
Downloading part image.part.02 from myawsbucket/bundles/bundle_name to mybundle/
image.part.02 ...
Downloaded image.part.02 from myawsbucket
Downloading part image.part.03 from myawsbucket/bundles/bundle_name to mybundle/
image.part.03 ...
Downloaded image.part.03 from myawsbucket
Downloading part image.part.04 from myawsbucket/bundles/bundle_name to mybundle/
image.part.04 ...
Downloaded image.part.04 from myawsbucket
Downloading part image.part.05 from myawsbucket/bundles/bundle_name to mybundle/
image.part.05 ...
Downloaded image.part.05 from myawsbucket
Downloading part image.part.06 from myawsbucket/bundles/bundle_name to mybundle/
image.part.06 ...
Downloaded image.part.06 from myawsbucket
```

ec2-migrate-manifest

Descrição

Modifica uma AMI em Linux com armazenamento de instâncias (por exemplo, seu certificado, kernel e disco RAM), de forma que suporte uma região diferente.

Sintaxe

```
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]
```

Opções

`-c, --cert path`

O arquivo de certificado de chave pública RSA codificado por PEM do usuário.

Exigido: sim

`-k, --privatekey path`

O caminho até o arquivo de chaves RSA codificado por PEM do usuário.

Exigido: sim

--manifest path

O caminho até o arquivo manifesto.

Exigido: 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 [Configuração das ferramentas de AMI \(p. 117\)](#), 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 [Como habilitar seus próprios kernels do Linux \(p. 169\)](#).

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 [Como habilitar seus próprios kernels do Linux \(p. 169\)](#).

Exigido: Não

Resultado

Mensagens de status que descrevem os estágios e o status do processo de empacotamento.

Exemplo

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-HKZYKTAIG2ECMXYIBH3HXV4ZBZQ55CLO.pem --privatekey pk-HKZYKTAIG2ECMXYIBH3HXV4ZBZQ55CLO.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

Descrição

Recria o pacote a partir de uma AMI em Linux com armazenamento de instâncias.

Sintaxe

```
ec2-unbundle -k path -m path [-s source_directory] [-d destination_directory]
```

Opções

-k, --privatekey *path*

O caminho para seu arquivo de chave RSA codificado por PEM.

Exigido: sim

-m, --manifest *path*

O caminho até o arquivo manifesto.

Exigido: 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

Exemplo

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
```

Resultado

São exibidas mensagens de status indicando os vários estágios do processo de desempacotamento.

ec2-upload-bundle

Descrição

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 [Criação de uma AMI em Linux com armazenamento de instâncias \(p. 115\)](#).

Sintaxe

```
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]
```

Opções

-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.

Exigido: sim

-a, --access-key *access_key_id*

Seu ID de chave de acesso da AWS.

Exigido: sim

-s, --secret-key *secret_access_key*

Sua chave de acesso secreta da AWS.

Exigido: sim

-t, --delegation-token *token*

O token de delegação para repassar à solicitação da AWS. Para mais informações, consulte o [Uso de 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.

Exigido: 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 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 sobreescritos.
- 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

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.

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

Resultado

O Amazon EC2 exibe mensagens de status que indicam os estágios e o status do processo de upload.

Exemplo

Esse exemplo faz uploads do pacote especificado pelo manifesto `image.manifest.xml`.

```
[ec2-user ~]$ ec2-upload-bundle -b myawsbucket/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 myawsbucket ...
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 para ferramentas 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.

AMIs com snapshots criptografados

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.

As instâncias do EC2 com volumes criptografados são executadas em AMIs da mesma forma como outras instâncias.

A ação `CopyImage` pode ser usada para criar uma AMI com snapshots criptografados a partir de uma AMI com snapshots descriptografados. Por padrão, `CopyImage` preserva o status de criptografia dos snapshots de origem ao criar cópias de destino. No entanto, você pode configurar os parâmetros do processo de cópia também para criptografar os snapshots de destino.

Os snapshots podem ser criptografados com a chave mestra do cliente (CMK) do AWS Key Management Service padrão ou com uma chave personalizada que você especifica. Em todos os casos, você deve ter permissão para usar a chave selecionada. Se você tiver uma AMI com snapshots criptografados, poderá optar por criptografá-los novamente com outra chave de criptografia como parte da ação `CopyImage`. A `CopyImage` aceita apenas uma chave de cada vez e criptografa todos os snapshots de uma imagem (raiz ou dados) para essa chave. Contudo, é possível criar manualmente uma AMI com snapshots criptografados com várias chaves.

O suporte para criar AMIs com os snapshots criptografados pode ser acessado por meio do console do Amazon EC2, da API do Amazon EC2 ou da AWS CLI.

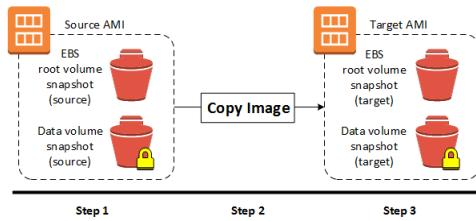
Os parâmetros de criptografia de `CopyImage` estão disponíveis em todas as regiões onde o AWS KMS está disponível.

Cenários de AMIs que envolvem snapshots criptografados do EBS

Você pode copiar uma AMI e criptografar simultaneamente seus snapshots do EBS associados usando o Console de gerenciamento da AWS ou a linha de comando.

Como copiar uma AMI com um snapshot de dados criptografado

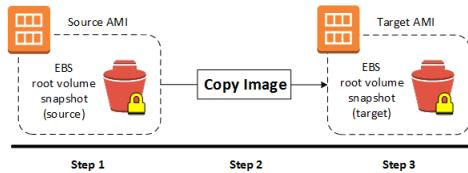
Neste cenário, uma AMI com suporte do EBS tem um snapshot raiz não criptografado e um snapshot de dados criptografado, mostrados na etapa 1. A ação `CopyImage` é invocada na etapa 2 sem parâmetros de criptografia. Como resultado, o status da criptografia de cada snapshot é preservado, de modo que a AMI de destino, na etapa 3, também tem suporte do snapshot raiz não criptografado e de um snapshot de dados criptografado. Embora os snapshots contenham os mesmos dados, eles são distintos um do outro, e você será cobrado pelo armazenamento dos snapshots nas duas AMIs, bem como por qualquer instância que você execute em qualquer uma das AMI.



Você pode executar uma cópia simples como esta usando o console do Amazon EC2 ou a linha de comando. Para obter mais informações, consulte [Cópia de uma AMI \(p. 150\)](#).

Como copiar uma AMI com suporte de um snapshot raiz criptografado

Neste cenário, uma AMI com Amazon EBS tem um snapshot raiz criptografado, como mostrado na etapa 1. A ação `CopyImage` é invocada na etapa 2 sem parâmetros de criptografia. Como resultado, o status da criptografia do snapshot é preservado, de modo que a AMI de destino, na etapa 3, também tem suporte de um snapshot raiz criptografado. Embora os snapshots raiz contenham dados de sistema idênticos, eles são distintos um do outro, e você será cobrado pelo armazenamento dos snapshots nas duas AMIs, bem como por qualquer instância que você execute em qualquer uma das AMI.

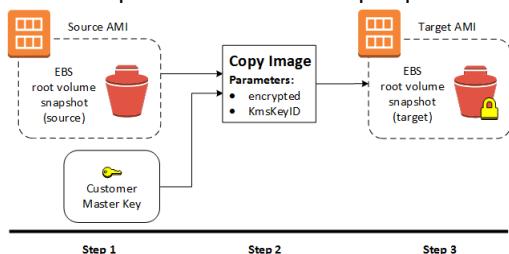


Você pode executar uma cópia simples como esta usando o console do Amazon EC2 ou a linha de comando. Para obter mais informações, consulte [Cópia de uma AMI \(p. 150\)](#).

Como criar uma AMI com snapshot raiz criptografado de uma AMI não criptografada

Neste cenário, uma AMI com Amazon EBS tem um snapshot raiz descriptografado, como mostrado na etapa 1, e uma AMI é criada com um snapshot raiz criptografado, como mostrado na etapa 3. A ação

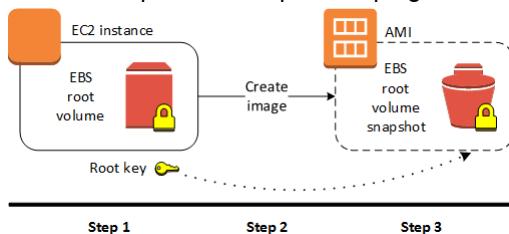
CopyImage na etapa 2 é invocada com dois parâmetros de criptografia incluindo a opção de uma CMK. Como resultado, o status da criptografia do snapshot raiz é alterado, de modo que a AMI de destino tem o suporte de um snapshot raiz que contém os mesmos dados que o snapshot de origem, mas criptografados usando a chave especificada. Você será cobrado pelos snapshots nas duas AMIs, bem como por qualquer instância que você execute em qualquer uma das AMI.



Você pode executar uma operação de cópia e de criptografia como esta usando o console do Amazon EC2 ou a linha de comando. Para obter mais informações, consulte [Cópia de uma AMI](#) (p. 150).

Como criar uma AMI com um snapshot raiz criptografado a partir de uma instância em execução

Neste cenário, uma AMI é criada a partir de uma instância do EC2 em execução. A instância em execução na etapa 1 tem um volume raiz criptografado, e a AMI criada na etapa 3 tem um snapshot raiz criptografado com a mesma chave que o volume de origem. A ação CreateImage tem exatamente o mesmo comportamento quer a criptografia esteja ou não presente.



Você pode criar uma AMI a partir de uma instância do Amazon EC2 em execução (com ou sem volumes criptografados) usando o console do Amazon EC2 ou a linha de comando. Para obter mais informações, consulte [Criação de uma AMI do Linux com Amazon EBS](#) (p. 111).

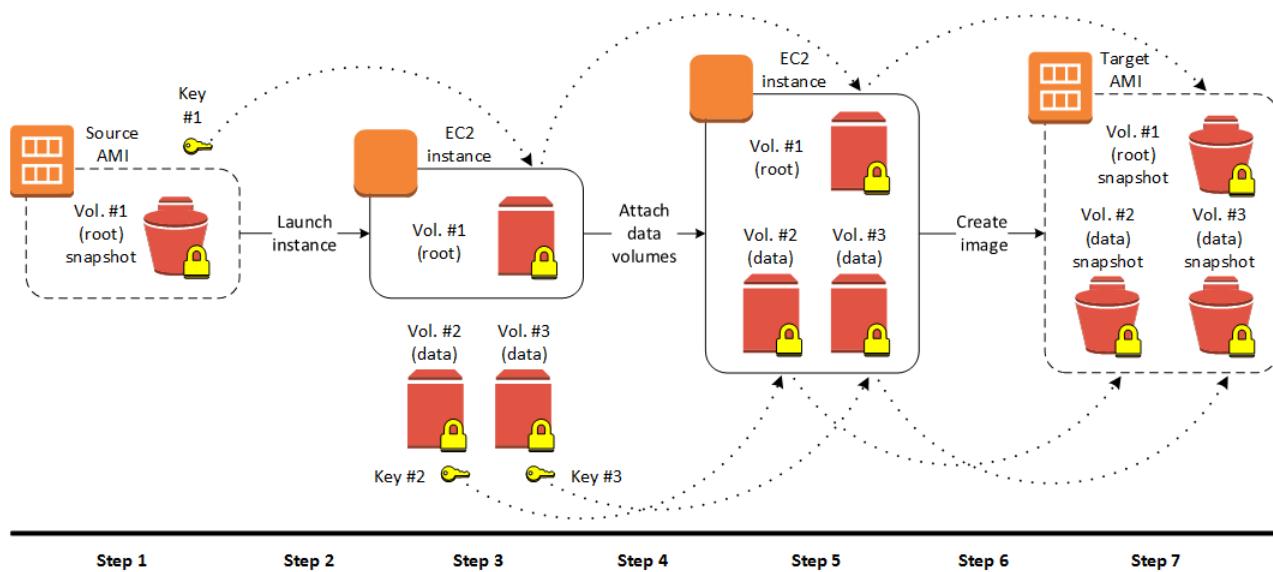
Como criar uma AMI com CMKs exclusivas para cada snapshot criptografado

Este cenário começa com uma AMI com snapshot de volume raiz (criptografado com a chave nº 1) e termina com uma AMI que tem dois snapshots de volumes de dados adicionais anexados (criptografados com as chaves nº 2 e nº 3). A ação CopyImage não pode aplicar mais de uma chave de criptografia em uma única operação. No entanto, você pode criar uma AMI a partir de uma instância que tem vários volumes anexados criptografados com chaves diferentes. A AMI resultante tem snapshots criptografados com essas chaves e qualquer instância executada nessa nova AMI também terá volumes criptografados com essas chaves.

As etapas deste procedimento de exemplo correspondem ao diagrama a seguir.

1. Comece com a AMI de origem com vol. nº 1 (raiz), que é criptografado com a chave nº 1.
2. Execute uma instância do EC2 na AMI de origem.
3. Crie volumes do EBS vol. nº 2 (dados) e vol. nº 3 (dados), criptografados com as chaves nº 2 e nº 3, respectivamente.

4. Anexe os volumes de dados criptografados à instância do EC2.
5. A instância do EC2 agora tem um volume raiz criptografado e dois volumes de dados criptografados, todos usando chaves diferentes.
6. Use a ação `CreateImage` na instância do EC2.
7. A AMI de destino resultante contém snapshots criptografados de três volumes do EBS, todos usando chaves diferentes.



Você pode executar este procedimento usando o console do Amazon EC2 ou a linha de comando. Para obter mais informações, consulte os tópicos a seguir:

- [Executar sua instância \(p. 390\)](#)
- [Criação de uma AMI do Linux com Amazon EBS \(p. 111\).](#)
- [Volumes do Amazon EBS \(p. 841\)](#)
- [AWS Key Management](#) no AWS Key Management Service Developer Guide

Cópia de uma AMI

Você pode copiar uma Imagem de Máquina da Amazon (AMI) para dentro ou para outra região da AWS usando o Console de gerenciamento da AWS, a AWS Command Line Interface ou os SDKs da AWS ou a API do Amazon EC2, sendo que todos oferecem suporte à ação `CopyImage`. Você pode copiar as AMIs com Amazon EBS e as AMIs com armazenamento de instâncias. Você pode copiar AMIs criptografadas e AMIs com snapshots criptografados.

Copiar uma AMI de origem resulta em uma AMI de destino idêntica, mas com seu próprio identificador exclusivo. No caso de uma AMI com Amazon EBS, cada um de seus snapshots de suporte é, por padrão, copiado para um snapshot de destino idêntico, mas distinto. (A única exceção é quando você optar por criptografar o snapshot.) Você pode alterar ou cancelar o registro da AMI de origem sem afetar a AMI de destino. O inverso também é verdadeiro.

Não há cobrança para copiar uma AMI. Mas aplicam-se as taxas padrão de transferência de dados e armazenamento.

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 operação de cópia ser concluída, você poderá aplicar permissões de execução, tags definidas pelo usuário e permissões do bucket do Amazon S3 para a nova AMI.

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 no <https://console.aws.amazon.com/ec2/>. Em seguida, no painel de navegação, escolha AMIs e localize o nome do bucket na coluna Source (Origem).

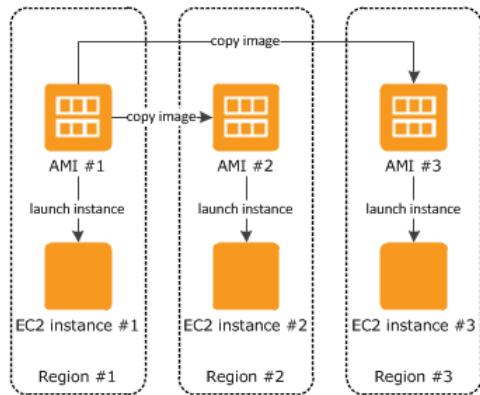
Cópia da AMI de outra região

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 aplicativos globais que atendam às necessidades dos seus usuários, onde quer que estejam.

- Desempenho: Você pode aumentar o desempenho ao distribuir seu aplicativo, além de localizar os componentes essenciais do seu aplicativo 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 aplicativos 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`.

Pré-requisito

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 aplicativo 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 o desempenho e o custo.

Limites

- As regiões de destino estão limitadas a 50 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 \(p. 94\)](#).

Cópia da AMI entre contas

É possível compartilhar uma AMI com outra conta da AWS. O compartilhamento da AMI não afeta a propriedade da AMI. A conta proprietária é cobrada pelo armazenamento na região. Para obter mais informações, consulte [Compartilhamento de uma AMI com contas específicas da AWS \(p. 101\)](#).

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 suporte a AMI, seu snapshots EBS associados (para uma AMI com Amazon EBS) ou um bucket S3 associado (para uma AMI com armazenamento de instâncias).

Limites

- Não é possível copiar uma AMI criptografada compartilhada com você por outra conta. Em vez disso, se o snapshot e a chave de criptografia subjacentes tiverem sido compartilhados com você, será possível copiar o snapshot ao recriptografá-lo com uma chave própria. Você é proprietário do snapshot copiado e pode registrá-lo como AMI nova.
- Você não pode copiar uma AMI com um código associado `billingProduct` que é compartilhado com você de outra conta. Isso inclui AMIs do Windows e AMIs do AWS Marketplace. Para copiar uma AMI compartilhada com um código `billingProduct`, execute uma instância do EC2 na sua conta usando a AMI compartilhada e crie uma AMI a partir da instância. Para obter mais informações, consulte [Criação de uma AMI do Linux com Amazon EBS \(p. 111\)](#).

Criptografia e cópia de AMI

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

Você pode usar uma cópia da AMI para criar uma nova AMI com snapshots do Amazon EBS criptografados. Se você invocar a criptografia enquanto copia uma AMI, cada snapshot tirado dos volumes do Amazon EBS associados – inclusive o volume do dispositivo raiz – será criptografado usando uma chave que você especificar. Para obter mais informações sobre o uso das AMIs com snapshots criptografados, consulte [AMIs com snapshots criptografados \(p. 147\)](#).

Por padrão, 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 criptografado para a chave especificada. Copiar uma AMI baseada em múltiplos snapshots preserva o status de criptografia de origem em cada snapshot de destino. Para obter mais informações sobre como copiar AMIs com vários snapshots, consulte [AMIs com snapshots criptografados \(p. 147\)](#).

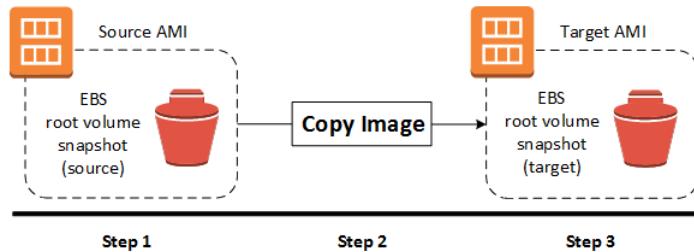
A tabela a seguir mostra o suporte a criptografia para vários cenários. Observe que, apesar de ser possível copiar um snapshot não criptografado para render um snapshot criptografado, você não pode copiar um snapshot criptografado para render um não criptografado.

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

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

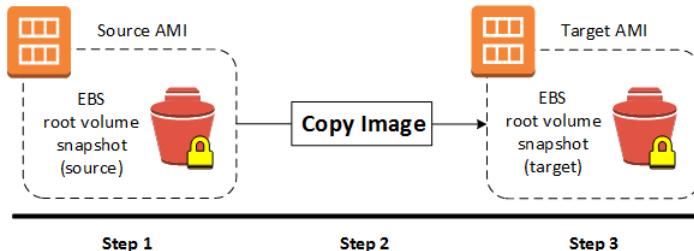
Neste cenário, uma cópia de uma AMI com um único snapshot de suporte não criptografado é criada na região geográfica especificada (não mostrada). Embora este diagrama mostre uma AMI com um único snapshot de suporte, você também copiar uma AMI com múltiplos snapshots. O status da criptografia de

cada snapshot é preservado. Portanto, um snapshot não criptografado na AMI de origem resulta em um snapshot não criptografado na AMI de destino, e um snapshot criptografado na AMI de origem resulta em um snapshot criptografado na AMI de destino.



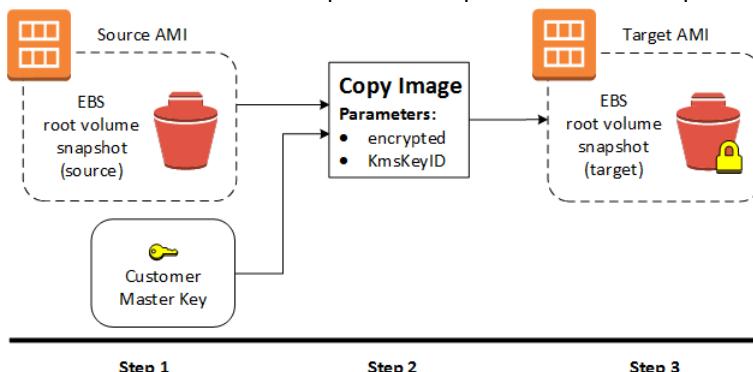
Copiar uma AMI de origem criptografada para uma AMI de destino criptografada

Embora esse cenário envolva snapshots criptografados, ele é funcionalmente equivalente ao cenário anterior. Se você aplicar a criptografia ao copiar uma AMI multi-snapshot, todos os snapshots de destino serão criptografados usando a chave especificada ou a chave padrão, se nenhuma tiver sido especificada.



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

Nesse cenário, copiar uma AMI muda o status de criptografia da imagem de destino; por exemplo, ao criptografar um snapshot não criptografado ou ao recriptografar um snapshot criptografado com uma chave diferente. Para aplicar a criptografia durante a cópia, é preciso fornecer um indicador de criptografia e uma chave. Os volumes criados a partir do snapshot de destino só podem ser acessados usando essa chave.



Cópia de uma AMI

Você pode copiar uma AMI da forma a seguir.

Pré-requisito

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 [Criação de uma AMI do Linux com Amazon EBS \(p. 111\)](#) e [Localizar uma AMI do Linux \(p. 95\)](#).

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.
 - 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.
 - Master Key (Chave mestre): 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 para 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.

Parada de 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 [Acessando o Amazon EC2 \(p. 3\)](#).

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

Cancelar o registro da 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 [Como determinar o tipo de dispositivo raiz da AMI \(p. 92\)](#).

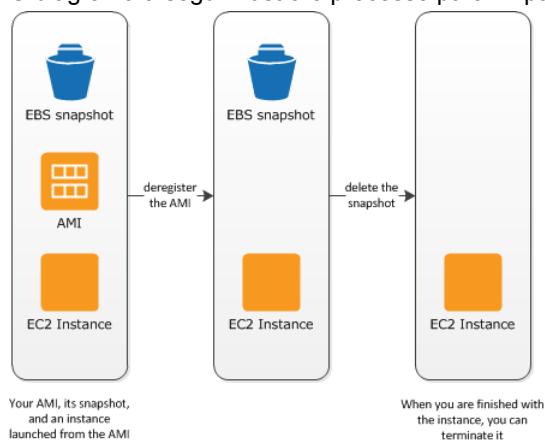
Tópicos

- [Limpeza da sua AMI com Amazon EBS \(p. 156\)](#)
- [Limpeza da sua AMI com armazenamento de instâncias \(p. 157\)](#)

Limpeza da sua AMI com Amazon EBS

Quando você cancelar o registro de uma AMI com Amazon EBS, isso não afetará o snapshot criado para o volume do dispositivo raiz da instância durante o processo de criação da AMI. Você continuará a acumular custos de armazenamento para esse snapshot. Portanto, se você tiver terminado de usar o snapshot, deverá excluí-lo.

O diagrama a seguir ilustra o processo para limpar a AMI com Amazon EBS.



Para limpar sua AMI com Amazon EBS

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

Note

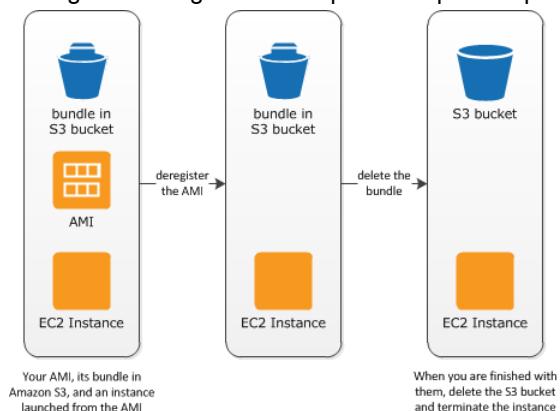
A remoção do AMI da lista pelo console pode demorar alguns minutos. Escolha Refresh (Atualizar) para atualizar o status.

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

Limpeza da 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. 137) (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).

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 alto desempenho para aplicativos 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. Muitos aplicativos desenvolvidos no CentOS (e distribuições similares) são executados no Amazon Linux.

A AWS fornece duas versões do Amazon Linux: Amazon Linux 2 e Amazon Linux AMI. Para obter mais informações, incluindo a lista completa de AMIs, consulte [Amazon Linux 2](#) e [Amazon Linux AMI](#). Para obter imagens de contêiner do Docker do Amazon Linux, consulte [amazonlinux](#) no Docker Hub.

Se você estiver migrando de outra distribuição do Linux para o Amazon Linux, recomendamos migrar para o Amazon Linux 2. 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. Instale o aplicativo no Amazon Linux 2, além de todos os pacotes exigidos pelo aplicativo. Teste o aplicativo e faça todas as alterações necessárias para que ele seja executado no Amazon Linux 2. Para obter mais informações sobre como executar o Amazon Linux fora da AWS, consulte [Execução do Amazon Linux 2 como uma máquina virtual local \(p. 166\)](#).

Tópicos

- [Conexão com uma instância do Amazon Linux \(p. 158\)](#)
- [Identificação de imagens do Amazon Linux \(p. 159\)](#)
- [Ferramentas de linha de comando da AWS \(p. 160\)](#)
- [Repositório de pacotes \(p. 161\)](#)
- [Biblioteca de extras \(Amazon Linux 2\) \(p. 163\)](#)
- [Como acessar pacotes de origem para referência \(p. 163\)](#)
- [cloud-init \(p. 163\)](#)
- [Como assinar notificações do Amazon Linux \(p. 165\)](#)
- [Execução do Amazon Linux 2 como uma máquina virtual local \(p. 166\)](#)

Conexão com 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.

Identificação de 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/"
```

Amazon Linux AMI

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="2015.09"
image_arch="x86_64"
image_file="amzn-ami-hvm-2015.09.0.x86_64.ext4.gpt"
image_stamp="f819-da48"
image_date="20150916025513"
recipe_name="amzn ami"
recipe_id="b4b7f85d-c9b8-99ae-c1bb-634d-20d8-50a5-3aa92282"
```

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 2015.09
```

Ferramentas de linha de comando da AWS

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-ec2
- 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 do Amazon EC2. Esses repositórios fornecem atualizações contínuas para pacotes no Amazon Linux 2 e no Amazon Linux AMI, assim como acesso a centenas de aplicativos 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
```

No 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 AWS não oferece suporte a pacotes de terceiros. 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 Amazon Linux não contém um aplicativo de que precisa, pode simplesmente instalar o aplicativo diretamente em sua instância Amazon Linux. O Amazon Linux usa RPMs e yum para gerenciamento de pacotes, e essa provavelmente é a maneira mais simples de instalar novos aplicativos. Você sempre deve verificar se um aplicativo está disponível em nosso repositório central do Amazon Linux primeiro, porque muitos aplicativos estão disponíveis nele. Esses aplicativos podem ser facilmente adicionados à sua instância Amazon Linux.

Para fazer upload de seus aplicativos em uma instância do Amazon Linux em execução, use scp ou sftp e configure o aplicativo fazendo login em sua instância. Os aplicativos também podem ser carregados durante a execução da instância usando a ação PACKAGE_SETUP no pacote cloud-init incorporado. Para obter mais informações, consulte [cloud-init \(p. 163\)](#).

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 no momento da execução. 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:

security

Aplicar atualizações pendentes 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 na inicialização.

A configuração padrão para `repo_upgrade` é segurança. Ou seja, se você não especificar um valor diferente em seus dados do usuário, por padrão, Amazon Linux executará as atualizações de segurança no lançamento para todos os pacotes instalados nesse momento. O Amazon Linux também notifica você sobre quaisquer atualizações aos pacotes instalados listando o número de atualizações disponíveis no 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 do Amazon Linux AMI (como as 2015.03 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 2015.03 definir que ela receba somente as atualizações que forem liberadas antes da AMI 2015.09, até que você esteja pronto para migrar para a AMI 2015.09.

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: 2015.03
```

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 aplicativo 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
```

Como 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 um aplicativo 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 de 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-los dinamicamente na inicialização. 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 executada, portanto, você deve particioná-los e formata-los para poder montá-los. Para obter mais informações, consulte [Suporte a TRIM do volume de armazenamento de instâncias \(p. 966\)](#). 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
 - 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.

Como 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/v2/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. Para Protocolo, selecione Email.
 - d. Para Endpoint, digite um endereço de e-mail que você pode usar para receber as 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/v2/home>.
2. Na barra de navegação, altere a região para Leste dos EUA (Norte da Virgínia), se necessário. Você deve usar esta região, já que a notificação do SNS foi criada nesta região.
3. No painel de navegação, selecione Inscrições, selecione o volume e escolha Ações, Excluir assinaturas.
4. Quando a confirmação for solicitada, escolha Excluir.

Execução do Amazon Linux 2 como uma máquina virtual 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 suportadas, é necessário fazer o seguinte:

- [Etapa 1: Preparar a imagem de inicialização seed.iso \(p. 166\)](#)
- [Etapa 2: fazer download da imagem da VM do Amazon Linux 2 \(p. 169\)](#)
- [Etapa 3: Inicializar e se conectar com sua nova VM \(p. 169\)](#)

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. Não inclui os arquivos do sistema operacional 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` para armazenar seus arquivos de configuração `meta-data` e `user-data`.
2. Crie o arquivo de configuração `meta-data`.
 - a. Adicione o nome do host da VM.

```
local-hostname: vm_hostname
```

- b. Especifique quaisquer configurações de rede personalizadas, como o nome da interface de rede.

```
#network-interfaces: |
#  iface interface_name inet static
```

Por exemplo, o bloco de código a seguir mostra o conteúdo de um 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.

```
local-hostname: amazonlinux.onprem
# 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
```

3. Crie o arquivo de configuração `user-data`.

- a. Especifique uma senha personalizada, em formato de texto simples, para a conta de usuário padrão `ec2-user`:

```
#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:'.
```

Note

Substitua o espaço reservado `plain_text_password` por uma senha de texto simples da sua escolha.

-
- b. (Opcional) Crie contas de usuário adicionais e especifique seus mecanismos de acesso, senhas e pares de chaves. Para obter mais informações sobre as diretivas suportadas, consulte [Módulos](#).
 - c. (Opcional) Por padrão, o cloud-init aplica as configurações de rede sempre que a VM é inicializada. Adicione o seguinte código ao arquivo de configuração user-data 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
```

Por exemplo, o bloco de código a seguir mostra o conteúdo de um arquivo de configuração user-data que cria três usuários adicionais, especifica uma senha personalizada para a conta de usuário padrão ec2-user e impede que o cloud-init aplique as configurações de rede em cada inicialização.

```
#cloud-config
# vim:syntax=yaml
users:
# A user by the name ec2-user is created in the image by default.
- default
# The following entry creates user1 and assigns a plain text password.
# Please note that the use of a plain text password is not recommended from security
best practices standpoint.
- name: user1
  groups: sudo
  sudo: ['ALL=(ALL) NOPASSWD:ALL']
  plain_text_passwd: myp@ssw0rd
  lock_passwd: false
# The following entry creates user2 and attaches a hashed password to the user.
# Hashed passwords can be generated with the following command on Amazon Linux 2:
# python -c 'import crypt,getpass; print(crypt.crypt(getpass().))'
- name: user2
  passwd: hashed-password
  lock_passwd: false
# The following entry creates user3, disables password-based login and enables an SSH
public key.
- name: user3
  ssh-authorized-keys:
    - ssh-public-key-information
  lock_passwd: true
chpasswd:
  list: |
    ec2-user:myp@ssw0rd
# In the above line, do not add any spaces after 'ec2-user:'.

# NOTE: Cloud-init applies network settings on every boot by default. To retain network
settings from first
boot, uncomment the 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
```

4. Coloque seus arquivos de configuração meta-data e user-data na pasta seedconfig criada na Etapa 1.
5. 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 seguinte comando:

```
$ genisoimage -output seed.iso -volid cidata -joliet -rock user-data meta-data
```

Para macOS, usar uma ferramenta como hdiutil. Navegue mais um nível, até a pasta seedconfig e execute o seguinte comando:

```
$ 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 se conectar com sua nova VM

Para inicializar e se conectar 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).

Note

Você precisa conectar a imagem de inicialização seed.iso à VM na primeira inicialização. seed.iso é avaliado somente durante a primeira inicialização.

Após a inicialização da VM, faça login usando uma das contas de usuário definidas no arquivo de configuração user-data. Você pode desanexar a imagem de inicialização da VM depois de ter feito login pela primeira vez.

Kernels fornecidos pelo usuário

Se você tiver necessidade de um kernel personalizado nas suas instâncias do Amazon EC2, pode iniciar com uma AMI próxima da que você deseja, compilar o kernel personalizado na sua instância e modificar o arquivo menu.lst 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 \(p. 94\)](#).

Tópicos

- [AMIs HVM \(GRUB\) \(p. 170\)](#)

- AMIs paravirtuais (PV-GRUB) (p. 171)

AMIs HVM (GRUB)

Volumes de instância HVM são tratados como discos físicos reais. O processo de inicialização é semelhante ao de um sistema operacional do zero, com um disco particionado e um bootloader, que permite funcionar com todas as distribuições Linux atualmente suportadas. O bootloader mais comum é GRUB, e a seção a seguir descreve a configuração do GRUB para usar um kernel personalizado.

Configuração do GRUB para AMIs HVM

A seguir está o exemplo de um arquivo de configuração `menu.lst` para a AMI com HVM. Neste exemplo, há duas entradas de kernel para escolher: 2015.09 do Amazon Linux (o kernel original desta AMI) e 4.3 do Vanilla Linux (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 para o bootloader para a primeira entrada que vê (nesse caso, a entrada do Vanilla), e o parâmetro `fallback 1` aponta para o bootloader para a entrada seguinte se houver um problema em inicializar o primeiro.

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 \(p. 1062\)](#). Se você estiver instalando um kernel personalizado, deve considerar habilitar a saída do GRUB ao excluir a linha `hiddenmenu` e adicionar as linhas `serial` e `terminal` a `/boot/grub/menu.lst`, conforme exibido no exemplo abaixo.

Important

Evite imprimir grandes quantidades de informações de depuração durante o processo de inicialização; o console de série não suporta transferência de dados em alta velocidade.

```
default=0
fallback=1
timeout=5
serial --unit=0 --speed=9600
terminal --dumb --timeout=5 serial console

title Vanilla Linux 4.3
root (hd0)
kernel /boot/vmlinuz-4.3 root=LABEL=/ console=tty1 console=ttyS0
initrd /boot/initrd.img-4.3

title Amazon Linux 2015.09 (4.1.10-17.31.amzn1.x86_64)
root (hd0,0)
kernel /boot/vmlinuz-4.1.10-17.31.amzn1.x86_64 root=LABEL=/ console=tty1 console=ttyS0
initrd /boot/initramfs-4.1.10-17.31.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 GRUB podem recuar para outro kernel no caso de o novo kernel falhar. Ter um kernel de fallback reserva permite que a instância inicialize mesmo se o novo kernel não for encontrado.

Se o novo kernel Vanilla Linux falhar, o resultado será semelhante ao exemplo abaixo.

```
^M Entry 0 will be booted automatically in 3 seconds. ^M Entry 0 will be booted
automatically in 2 seconds. ^M Entry 0 will be booted automatically in 1 seconds.

Error 13: Invalid or unsupported executable format
[ 0.000000] Initializing cgroup subsys cpuset
```

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 assistente de inicialização 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 em sua instância é começar com a AMI mais próxima à que você deseja, compilar o kernel personalizado na sua instância e modificar o arquivo `menu.lst` conforme exibido em [Configurar GRUB \(p. 172\)](#) para inicializar com esse kernel.

Você pode verificar se a imagem de kernel de uma AMI é a AKI PV-GRUB executando o seguinte comando `describe-images` com as ferramentas de linha de comando do Amazon EC2 (substituindo o ID da imagem do kernel que você deseja verificar):

```
aws ec2 describe-images --filters Name=image-id,Values=aki-880531cd
```

Verifique se o campo `Name` começa com `pv-grub`.

Tópicos

- [Limitações do PV-GRUB \(p. 171\)](#)
- [Configuração do GRUB para AMIs paravirtuais \(p. 172\)](#)
- [IDs da imagem do kernel do PV-GRUB da Amazon \(p. 172\)](#)
- [Atualização do PV-GRUB \(p. 174\)](#)

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.
- A AWS 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, lzo 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 do zero 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 EBS, precisa de uma partição de inicialização separada do LVM. Então, você pode criar volumes lógicos com o LVM.

Configuração do 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: 2015.09 do Amazon Linux (o kernel original desta AMI) e 4.3 do Vanilla Linux (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 4.3
root (hd0)
kernel /boot/vmlinuz-4.3 root=LABEL=/ console=hvc0
initrd /boot/initrd.img-4.3

title Amazon Linux 2015.09 (4.1.10-17.31.amzn1.x86_64)
root (hd0)
kernel /boot/vmlinuz-4.1.10-17.31.amzn1.x86_64 root=LABEL=/ console=hvc0
initrd /boot/initramfs-4.1.10-17.31.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 inicialize 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. 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
```

Observe que 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.

A seguir estão 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 estavam anteriormente disponíveis.

ap-northeast-1, Ásia-Pacífico (Tóquio)

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, Região Ásia-Pacífico (Cingapura)

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, Ásia-Pacífico (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, UE (Frankfurt)

ID da imagem	Nome da imagem
aki-1419e57b	pv-grub-hd0_1.05-i386.gz
aki-931fe3fc	pv-grub-hd0_1.05-x86_64.gz

eu-west-1, UE (Irlanda)

ID da imagem	Nome da imagem
aki-1c9fd86f	pv-grub-hd0_1.05-i386.gz

ID da imagem	Nome da imagem
aki-dc9ed9af	pv-grub-hd0_1.05-x86_64.gz

sa-east-1, América do Sul (São Paulo)

ID da imagem	Nome da imagem
aki-7cd34110	pv-grub-hd0_1.05-i386.gz
aki-912fbccfd	pv-grub-hd0_1.05-x86_64.gz

us-east-1, Leste dos EUA (Norte da Virgínia)

ID da imagem	Nome da imagem
aki-04206613	pv-grub-hd0_1.05-i386.gz
aki-5c21674b	pv-grub-hd0_1.05-x86_64.gz

us-gov-west-1, AWS GovCloud (US-West)

ID da imagem	Nome da imagem
aki-5ee9573f	pv-grub-hd0_1.05-i386.gz
aki-9ee55bff	pv-grub-hd0_1.05-x86_64.gz

us-west-1, Oeste dos EUA (Norte da Califórnia)

ID da imagem	Nome da imagem
aki-43cf8123	pv-grub-hd0_1.05-i386.gz
aki-59cc8239	pv-grub-hd0_1.05-x86_64.gz

us-west-2, Oeste dos EUA (Oregon)

ID da imagem	Nome da imagem
aki-7a69931a	pv-grub-hd0_1.05-i386.gz
aki-70cb0e10	pv-grub-hd0_1.05-x86_64.gz

Atualização do 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 \(p. 172\)](#)), 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 \(p. 172\)](#).
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
```

Instâncias do Amazon EC2

Se você for novo no Amazon EC2, consulte os seguintes tópicos para começar:

- [O que é o Amazon EC2? \(p. 1\)](#)
- [Como configurar com o Amazon EC2 \(p. 21\)](#)
- [Conceitos básicos das instâncias do Amazon EC2 do Linux \(p. 30\)](#)
- [Ciclo de vida da instância \(p. 385\)](#)

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 seus aplicativos. Para obter mais informações, consulte [Tipos de instância \(p. 176\)](#).

P: Qual opção de compra melhor atende às minhas necessidades?

O Amazon EC2 oferece suporte a instâncias sob demanda (o padrão), instâncias spot e reservadas. Para obter mais informações, consulte [Opções de compra de instância \(p. 251\)](#).

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 \(p. 91\)](#).

P: Posso gerenciar remotamente uma frota de instâncias do EC2 e máquinas no meu ambiente híbrido?

O comando de execução do Amazon Elastic Compute Cloud (Amazon EC2) permite gerenciar, de forma remota e segura, a configuração de suas instâncias do Amazon EC2, máquinas virtuais (VMs) e servidores em ambientes híbridos, ou VMs de outros provedores de nuvem. Para obter mais informações, consulte [Gerenciamento remoto do Systems Manager \(Run Command\)](#).

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 uma memória de computação diferente e os recursos de armazenamento são agrupados em famílias de instâncias de acordo com esses recursos. Selecione um tipo de instância com base nos requisitos do aplicativo 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, para 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 um desempenho mínimo superior ou inferior com base em um recurso compartilhado. Por exemplo, tipos de instância com desempenho alto de E/S têm uma alocação maior

dos recursos compartilhados. A alocação de uma parte maior dos recursos compartilhados também reduz a variação do desempenho de E/S. Para a maioria dos aplicativos, o desempenho moderado de E/S é mais do que suficiente. No entanto, para aplicativos que exigem um desempenho de E/S maior ou mais consistente, considere um tipo de instância com desempenho mais alto de E/S.

Tópicos

- [Tipos de instância disponíveis \(p. 177\)](#)
- [Especificações de hardware \(p. 178\)](#)
- [Tipos de virtualização de AMI \(p. 179\)](#)
- [Instâncias baseadas em Nitro \(p. 179\)](#)
- [Recursos de redes e armazenamento \(p. 180\)](#)
- [Limites das instâncias \(p. 182\)](#)
- [Instâncias de uso geral \(p. 182\)](#)
- [Instâncias otimizadas para computação \(p. 219\)](#)
- [Instâncias otimizadas para memória \(p. 223\)](#)
- [Instâncias otimizadas para armazenamento \(p. 231\)](#)
- [Linux Instâncias de computação acelerada \(p. 237\)](#)
- [Alterar o tipo de instância \(p. 247\)](#)

Tipos de instância disponíveis

O Amazon EC2 fornece os tipos de instância listados nas tabelas a seguir.

Atuais instâncias de geração

Para melhor desempenho, recomendamos que você use os tipos de instância da geração atual quando executar novas instâncias.

Para obter mais informações sobre os tipos de instância da geração atual, consulte [Tipos de instância do Amazon EC2](#).

Família de instâncias	Tipos de instância da geração atual
Propósito geral	a1.medium a1.large a1.xlarge a1.2xlarge a1.4xlarge m4.large m4.xlarge m4.2xlarge m4.4xlarge m4.10xlarge m4.16xlarge m5.large m5.xlarge m5.2xlarge m5.4xlarge m5.12xlarge m5.24xlarge m5a.large m5a.xlarge m5a.2xlarge m5a.4xlarge m5a.12xlarge m5a.24xlarge m5d.large m5d.xlarge m5d.2xlarge m5d.4xlarge m5d.12xlarge m5d.24xlarge t2.nano t2.micro t2.small t2.medium t2.large t2.xlarge t2.2xlarge t3.nano t3.micro t3.small t3.medium t3.large t3.xlarge t3.2xlarge
Otimizadas para computação	c4.large c4.xlarge c4.2xlarge c4.4xlarge c4.8xlarge c5.large c5.xlarge c5.2xlarge c5.4xlarge c5.9xlarge c5.18xlarge c5d.xlarge c5d.2xlarge c5d.4xlarge c5d.9xlarge c5d.18xlarge c5n.large c5n.xlarge c5n.2xlarge c5n.4xlarge c5n.9xlarge c5n.18xlarge
Otimizado para memória	r4.large r4.xlarge r4.2xlarge r4.4xlarge r4.8xlarge r4.16xlarge r5.large r5.xlarge

Família de instâncias	Tipos de instância da geração atual
	r5.2xlarge r5.4xlarge r5.12xlarge r5.24xlarge r5a.large r5a.xlarge r5a.2xlarge r5a.4xlarge r5a.12xlarge r5a.24xlarge r5d.large r5d.xlarge r5d.2xlarge r5d.4xlarge r5d.12xlarge r5d.24xlarge x1.16xlarge x1.32xlarge x1e.xlarge x1e.2xlarge x1e.4xlarge x1e.8xlarge x1e.16xlarge x1e.32xlarge z1d.large z1d.xlarge z1d.2xlarge z1d.3xlarge z1d.6xlarge z1d.12xlarge
Otimizada para armazenamento	d2.xlarge d2.2xlarge d2.4xlarge d2.8xlarge h1.2xlarge h1.4xlarge h1.8xlarge h1.16xlarge i3.large i3.xlarge i3.2xlarge i3.4xlarge i3.8xlarge i3.16xlarge
Computação acelerada	f1.2xlarge f1.4xlarge f1.16xlarge g3s.xlarge g3.4xlarge g3.8xlarge g3.16xlarge p2.xlarge p2.8xlarge p2.16xlarge p3.2xlarge p3.8xlarge p3.16xlarge p3dn.24xlarge

Instâncias de gerações anteriores

O Amazon Web Services oferece instâncias da geração anterior para usuários que otimizaram seus aplicativos acerca dessas instâncias e ainda têm de atualizar. Incentivamos você a usar geração mais recente de instâncias para obter o melhor desempenho, mas continuaremos dando suporte a essas instâncias de geração anterior. Se você estiver usando atualmente uma instância de geração anterior, pode ver que a instância da geração atual seria uma atualização apropriada. Para obter mais informações, consulte [Instâncias da geração anterior](#).

Família de instâncias	Tipos de instância de gerações anteriores
Propósito geral	m1.small m1.medium m1.large m1.xlarge m3.medium m3.large m3.xlarge m3.2xlarge t1.micro
Otimizadas para computação	c1.medium c1.xlarge cc2.8xlarge c3.large c3.xlarge c3.2xlarge c3.4xlarge c3.8xlarge
Otimizado para memória	m2.xlarge m2.2xlarge m2.4xlarge cr1.8xlarge r3.large r3.xlarge r3.2xlarge r3.4xlarge r3.8xlarge
Otimizada para armazenamento	hs1.8xlarge i2.xlarge i2.2xlarge i2.4xlarge i2.8xlarge
Computação acelerada	g2.2xlarge g2.8xlarge

Especificações de hardware

Para obter mais informações sobre as especificações de hardware para cada tipo de instância do Amazon EC2, veja [Tipos de instâncias do Amazon EC2](#).

Para determinar que tipo de instância atende melhor às suas necessidades, recomendamos executar uma instância e usar seu próprio aplicativo de referência. Como você paga pela 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 \(p. 247\)](#).

Note

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 para cada tipo de instância do Amazon EC2, veja [Tipos de instâncias do Amazon EC2](#). Contudo, pode haver confusão com as convenções de nomeação 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.

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 suportam paravirtual (PV) e algumas regiões AWS suportam instâncias PV. Para obter mais informações, consulte [Tipos de virtualização da AMI em Linux \(p. 94\)](#).

Para o melhor desempenho, 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 o desempenho.

Instâncias baseadas em Nitro

O sistema Nitro é uma coleção de hardware e componentes de software criados pela AWS que permitem alto desempenho, alta disponibilidade e alta segurança. Além disso, o sistema Nitro fornece recursos de bare metal que eliminam a sobrecarga da virtualização e oferecem suporte a cargas de trabalho que exigem acesso total ao hardware do host.

Componentes do Nitro

Os componentes a seguir fazem parte do sistema Nitro:

- Hipervisor do Nitro - um hipervisor leve que gerencia a alocação de memória e de CPU e fornece desempenho que não é diferenciado de bare metal para a maioria das cargas de trabalho.
- Cartão Nitro
 - Volumes de armazenamento NVMe locais
 - Suporte a hardware de rede
 - Gerenciamento
 - Monitoramento
 - Segurança
- Chip de segurança do Nitro, integrado na placa-mãe

Tipos de instância

As seguintes instâncias são baseadas no sistema Nitro:

- A1, C5, C5d, C5n, M5, M5a, M5d, p3dn.24xlarge, R5, R5a, R5d, T3 e z1d
- Bare metal: i3.metal, u-6tb1.metal, u-9tb1.metal, and u-12tb1.metal

Recursos

Para obter mais informações, assista aos seguintes vídeos:

- [AWS re:Invent 2017: The Amazon EC2 Nitro System Architecture](#)
- [AWS re:Invent 2017: Amazon EC2 Bare Metal Instances](#)
- [O projeto Nitro: infraestrutura do EC2 de próxima geração](#)

Recursos de redes e armazenamento

Ao selecionar um tipo de instância, isso determinará os recursos de rede e armazenamento disponíveis.

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 o desempenho 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 aplicativos 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 [Placement groups \(p. 793\)](#).
 - Habilite rede avançada para tipos de instâncias da geração atual compatíveis para obter desempenho 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 \(p. 768\)](#).
- Os tipos de instância da geração atual habilitados para redes aprimoradas têm os seguintes atributos de desempenho 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 multifluxo (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.
 - O MTU máximo suportado varia entre 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 sua instância do EC2 \(p. 801\)](#).

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 [Armazenamento \(p. 838\)](#).
- 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 [Amazon EBS – instâncias otimizadas \(p. 916\)](#).

A tabela a seguir resume os recursos de rede e armazenamento com suporte dos tipos de instância da geração atual.

	Somente EBS	EBS de NVMe	Armazenamento de instâncias	Placement group	Redes avançadas
A1	Sim	Sim	Não	Sim	ENA
C4	Sim	Não	Não	Sim	Intel 82599 VF
C5	Sim	Sim	Não	Sim	ENA
C5d	Não	Sim	NVMe *	Sim	ENA
C5n	Sim	Sim	Não	Sim	ENA
D2	Não	Não	HDD	Sim	Intel 82599 VF
F1	Não	Não	NVMe *	Sim	ENA
G3	Sim	Não	Não	Sim	ENA
H1	Não	Não	HDD	Sim	ENA
I3	Não	Não	NVMe *	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
M5d	Não	Sim	NVMe *	Sim	ENA
P2	Sim	Não	Não	Sim	ENA
P3	p3dn.24xlarge não	p3dn.24xlarge sim	p3dn.24xlarge Sim NVMe *		ENA
	Todos os outros tamanhos: sim	Todos os outros tamanhos: não			
R4	Sim	Não	Não	Sim	ENA
R5	Sim	Sim	Não	Sim	ENA
R5a	Sim	Sim	Não	Sim	ENA
R5d	Não	Sim	NVMe *	Sim	ENA
T2	Sim	Não	Não	Não	Não

	Somente EBS	EBS de NVMe	Armazenamento de instâncias	Placement group	Redes avançadas
T3	Sim	Sim	Não	Não	ENA
u-xtb1.metal	Sim	Sim	Não	Não	ENA
X 1	Não	Não	SSD	Sim	ENA
X1e	Não	Não	SSD	Sim	ENA
z1d	Não	Sim	NVMe *	Sim	ENA

* O volume do dispositivo raiz deve ser um volume do Amazon EBS.

A tabela a seguir resume os recursos de rede e armazenamento comportados por 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 das 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 [Limites de serviço do Amazon EC2 \(p. 1013\)](#).

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 cargas de trabalho.

Instâncias A1

As instâncias A1 são ideais para cargas de trabalho expandidas que são compatíveis com o ecossistema Arm. Essas instâncias são ideais para os seguintes aplicativos:

- Servidores da web
- Microsserviços em contêineres

- Frotas de cache
- Armazenamentos de dados distribuídos
- Aplicativos que exigem o conjunto de instruções do Arm

Para obter mais informações, consulte [Instâncias A1 do Amazon EC2](#).

Instâncias M5, M5a e M5d

Essas instâncias fornecem uma infraestrutura em nuvem ideal, oferecendo um equilíbrio entre recursos de computação, memória e redes para uma ampla variedade de aplicativos implantados na nuvem. As instâncias M5 são indicadas para os seguintes aplicativos:

- Servidores web e de aplicativos
- Bancos de dados pequenos e médios
- Servidores de jogos
- Frotas de cache
- Executando servidores back-end para SAP, Microsoft SharePoint, computação em cluster e outros aplicativos empresariais

As instâncias `m5.metal` e `m5d.metal` fornecem aos aplicativos acesso direto aos recursos físicos do servidor host, como processadores e memória. Essas instâncias são ideais para o seguinte:

- Cargas de trabalho 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
- Aplicativos que exigem um ambiente não virtualizado para licenciamento ou suporte

Para obter mais informações, consulte [Instâncias M5 do Amazon EC2](#).

Instâncias T2 e T3

Essas instâncias fornecem um nível de linha de base de desempenho de CPU com a capacidade de intermitência até um nível superior quando exigido por sua carga de trabalho. Uma instância ilimitada pode sustentar alto desempenho de CPU por qualquer período, sempre que necessário. Para obter mais informações, consulte [Instâncias de desempenho com capacidade de intermitência \(p. 189\)](#). Essas instâncias são ideais para os seguintes aplicativos:

- Sites e aplicativos web
- Repositórios de códigos
- Ambientes de desenvolvimento, criação, teste e preparação
- Microsserviços

Para obter mais informações, consulte [Instâncias T2 do Amazon EC2](#) e [Instâncias T3 do Amazon EC2](#).

Tópicos

- [Especificações de hardware \(p. 184\)](#)
- [Performance da instância \(p. 185\)](#)
- [Desempenho de rede \(p. 186\)](#)
- [Desempenho de E/S SSD \(p. 187\)](#)
- [Recursos das instâncias \(p. 187\)](#)
- [Notas de release \(p. 188\)](#)

- [Instâncias de desempenho com capacidade de intermitência \(p. 189\)](#)

Especificações de hardware

Este é um resumo das especificações de hardware para instâncias de uso geral.

Tipo de instância	vCPUs padrão	Memória (GiB)
a1.medium	1	2
a1.large	2	4
a1.xlarge	4	8
a1.2xlarge	8	16
a1.4xlarge	16	32
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
m5.12xlarge	48	192
m5.24xlarge	96	384
m5.metal	96	384
m5a.large	2	8
m5a.xlarge	4	16
m5a.2xlarge	8	32
m5a.4xlarge	16	64
m5a.12xlarge	48	192
m5a.24xlarge	96	384
m5d.large	2	8
m5d.xlarge	4	16
m5d.2xlarge	8	32

Tipo de instância	vCPUs padrão	Memória (GiB)
m5d.4xlarge	16	64
m5d.12xlarge	48	192
m5d.24xlarge	96	384
m5d.metal	96	384
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

Para obter mais informações sobre as especificações de hardware para cada tipo de instância do Amazon EC2, veja [Tipos de instâncias do Amazon EC2](#).

Para obter mais informações sobre como especificar opções de CPU, consulte [Otimizar opções de CPU \(p. 495\)](#).

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 [Amazon EBS – instâncias otimizadas \(p. 916\)](#).

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 o desempenho desejado (em frequência da CPU) de um núcleo. Para obter mais informações, consulte [Controle do estado do processo para sua instância do EC2 \(p. 485\)](#).

Desempenho de rede

Você pode habilitar recursos de rede aprimoradas em tipos de instância compatíveis. O uso avançado de rede fornece um desempenho significativamente maior de pacotes por segundo (PPS), menor jitter de rede e latências mais baixas. Para obter mais informações, consulte [Rede avançada no Linux \(p. 768\)](#).

Os tipos de instâncias que usam Elastic Network Adapter (ENA) para networking avançado fornecem alto desempenho de pacotes por segundo com latências consistentemente baixas. A maioria dos aplicativos não precisa de um alto nível de desempenho de rede constantemente, mas podem se beneficiar com uma largura de banda maior quando enviam ou recebem dados. Os tamanhos de instância que usam ENA e estão documentados com desempenho de rede de "Até 10 Gbps" ou "Até 25 Gbps" usam um mecanismo de crédito de E/S de rede para alocar largura de banda a instâncias baseadas na utilização média da largura de banda. Essas instâncias acumulam créditos quando a largura de banda da rede está abaixo dos limites de linha de base e podem usar esses créditos ao executar transferências de dados pela rede.

Este é um resumo da performance de rede para instâncias de uso geral que oferecem suporte às redes aprimoradas.

Tipo de instância	Desempenho das redes	Redes avançadas
t2.nano, t2.micro, t2.small, t2.medium, t2.large, t2.xlarge, t2.2xlarge	Até 1 Gbps	
t3.nano, t3.micro, t3.small, t3.medium, t3.large, t3.xlarge, t3.2xlarge	Até 5 Gbps	ENA (p. 769)
m4.large	Moderada	Intel 82599 VF (p. 780)
m4.xlarge, m4.2xlarge, m4.4xlarge	Alto	Intel 82599 VF (p. 780)
a1.medium, a1.large, a1.xlarge, a1.2xlarge, a1.4xlarge, m5.large, m5.xlarge, m5.2xlarge, m5.4xlarge, m5a.large, m5a.xlarge, m5a.2xlarge, m5a.4xlarge, m5d.large, m5d.xlarge, m5d.2xlarge, m5d.4xlarge	Até 10 Gbps	ENA (p. 769)
m4.10xlarge	10 Gbps	Intel 82599 VF (p. 780)
m5.12xlarge, m5a.12xlarge, m5d.12xlarge	10 Gbps	ENA (p. 769)
m5a.24xlarge	20 Gbps	ENA (p. 769)
m4.16xlarge, m5.24xlarge, m5.metal, m5d.24xlarge, m5d.metal	25 Gbps	ENA (p. 769)

Desempenho de E/S 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 o desempenho 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
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.12xlarge	700.000	340.000
m5d.24xlarge	1.400.000	680.000
m5d.metal	1.400.000	680.000

* Para essas instâncias, você pode obter o desempenho especificado.

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 no desempenho 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 um desempenho de E/S drasticamente reduzido.

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 o desempenho 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 o desempenho. Para obter mais informações, consulte [Suporte a TRIM do volume de armazenamento de instâncias \(p. 966\)](#).

Recursos das instâncias

Este é um resumo dos recursos de instâncias de uso geral:

	Somente EBS	EBS de NVMe	Armazenamento de instâncias	Placement group
A1	Sim	Sim	Não	Sim
M4	Sim	Não	Não	Sim
M5	Sim	Sim	Não	Sim
M5a	Sim	Sim	Não	Sim
M5d	Não	Sim	NVMe *	Sim
T2	Sim	Não	Não	Não
T3	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 \(p. 929\)](#)
- [Armazenamento de instâncias do Amazon EC2 \(p. 958\)](#)
- [Placement groups \(p. 793\)](#)

Notas de release

- As instâncias M5, M5d e T3 têm um processador da série Intel Xeon Platinum 8000 de 3.1 GHz.
- As instâncias M5a têm um processador da série AMD EPYC 7000 de 2.5 GHz.
- As instância A1 têm um processador AWS Graviton de 2.3 GHz baseado na arquitetura Arm de 64 bits.
- Os tipos de instância M4, M5, M5a, M5d, t2.large e maior e t3.large e maior 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 desempenho 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 A1 têm os seguintes requisitos:
 - Deve ter os drivers de NVMe instalados. Os volumes do EBS são expostos como [dispositivos de bloco NVMe \(p. 929\)](#).
 - Deve ter os drivers do Elastic Network Adapter ([ENA \(p. 769\)](#)) instalados.
 - Deve usar uma AMI para a arquitetura Arm de 64 bits.
 - Deve oferecer 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 7.6 ou posterior (Arm de 64 bits)
- As instâncias M5, M5a, M5d, e T3 têm os seguintes requisitos:

As AMIs a seguir atendem a esses requisitos:

- As instâncias A1, M5, M5a, M5d, e T3 oferecem suporte a um máximo de 28 anexos, incluindo interfaces de rede, volumes do EBS e volumes de armazenamento de instâncias NVMe. Cada instância tem pelo

menos um anexo de interface de rede. Por exemplo, se você não tiver anexos de interface de rede adicionais em uma instância somente EBS, poderá anexar 27 volumes do EBS a essa instância.

- 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. Amazon Linux 2 e as versões mais recentes do Amazon Linux AMI 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 A1, M5, M5a, M5d., T3 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?](#). Para solicitar um aumento do limite, use o [Formulário de solicitação de instâncias do Amazon EC2](#).

Instâncias de desempenho com capacidade de intermitência

As instâncias de desempenho com capacidade de intermitência, que incluem as instâncias T3 e T2, foram criadas para fornecer um nível de linha de base de desempenho de CPU com capacidade de intermitência para um nível superior quando exigido pela carga de trabalho. As instâncias de desempenho com capacidade de intermitência são ideais para uma ampla variedade de aplicativos de uso geral. Os exemplos incluem microsserviços, aplicativos interativos de baixa latência, bancos de dados pequenos e médios, desktops virtuais, ambientes de desenvolvimento, criação e estágios, repositórios de código e protótipos de produtos.

As instâncias de desempenho com capacidade de intermitência são os únicos tipos de instância que usam créditos para uso de CPU. Para obter mais informações sobre definição de preço de instâncias e detalhes adicionais de hardware, consulte [Definição de preço 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 em determinados limites de uso. Para obter mais informações, consulte [Nível gratuito da AWS](#).

Tópicos

- [Requisitos de instâncias de desempenho com capacidade de intermitência \(p. 190\)](#)
- [Melhores práticas \(p. 190\)](#)
- [Créditos de CPU e linha de base para instância de desempenho com capacidade de intermitência \(p. 190\)](#)
- [Modo ilimitado de instâncias de desempenho com capacidade de intermitência \(p. 193\)](#)
- [Modo padrão de instâncias de desempenho com capacidade de intermitência \(p. 201\)](#)
- [Trabalhando com instâncias com ampliação de desempenho \(p. 211\)](#)
- [Como monitorar seus créditos de CPU \(p. 216\)](#)

Requisitos de instâncias de desempenho com capacidade de intermitência

Veja a seguir os requisitos para essas instâncias:

- Essas instâncias estão disponíveis como Instâncias on-demand, Instâncias reservadas e Instâncias spot, mas não estão disponíveis como instâncias programadas ou Instâncias dedicadas. Também não são compatíveis em um Host dedicado. Para obter mais informações, consulte [Opções de compra de instância \(p. 251\)](#).
- Verifique se o tamanho da instância escolhido ultrapassa os requisitos mínimos de memória do sistema operacional e dos aplicativos. 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 t2.micro, ou maior, para muitos casos de uso. À medida que os requisitos de memória e de CPU de sua carga de trabalho aumentam, você pode dimensionar para tamanhos de instâncias maiores do mesmo tipo ou para outro tipo de instância.
- Para obter requisitos adicionais, consulte [Notas de release de instâncias de uso geral \(p. 188\)](#).

Melhores práticas

Siga estas melhores práticas para obter o benefício máximo com as instâncias de desempenho com capacidade de intermitência.

- Use uma AMI recomendada – Use uma AMI que forneça os drivers necessários. Para obter mais informações, consulte [Notas de release \(p. 188\)](#).
- Ative a recuperação da instância – Crie um alarme do CloudWatch que monitore uma instância do EC2 e recupere a instância automaticamente se ela for danificada por qualquer motivo. Para obter mais informações, consulte [Inclusão de ações de recuperar em alarmes do Amazon CloudWatch \(p. 599\)](#).

Créditos de CPU e linha de base para instância de desempenho com capacidade de intermitência

Os tipos de instância do Amazon EC2 tradicionais fornecem desempenho fixo, enquanto as instâncias de desempenho com capacidade de intermitência fornecem a um nível de linha de base de desempenho de CPU a capacidade de intermitência acima desse nível da linha de base. O desempenho de linha de base e a capacidade de intermitência são governados por créditos de CPU. Um crédito de CPU oferece o desempenho de um núcleo de CPU completo por um minuto.

Tópicos

- [Créditos da CPU \(p. 190\)](#)
- [Desempenho de linha de base \(p. 192\)](#)

Créditos da CPU

Um crédito de CPU é igual a uma vCPU em execução em 100% de utilização por um minuto. Outras combinações de número de vCPUs, utilização e hora também podem ser equivalentes a um único crédito de CPU. Por exemplo, um crédito de CPU equivale a uma vCPU em execução com 50% de utilização por dois minutos ou duas vCPUs em execução com 25% de utilização por dois minutos.

Obtenção de créditos de CPU

Cada instância de desempenho com capacidade de intermitência 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 de desempenho com capacidade de intermitência usar menos recursos de CPU do que o necessário para o desempenho 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 de desempenho com capacidade de intermitência precisar de intermitência acima do nível do desempenho da linha de base, ela gastará os créditos acumulados. Quanto mais créditos a instância de desempenho com capacidade de intermitência acumular, mais tempo de intermitência ela poderá ter acima da linha de base quando mais desempenho for necessário.

A tabela a seguir lista os tipos de instância de desempenho com capacidade de intermitência, 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 nível de desempenho da linha de base como uma porcentagem do desempenho 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	Desempenho de linha de base por vCPU
t1.micro	6	144	1	10%
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.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%**

* O número de créditos que podem ser acumulados é equivalente ao número de créditos que podem ser obtidos em um período de 24 horas.

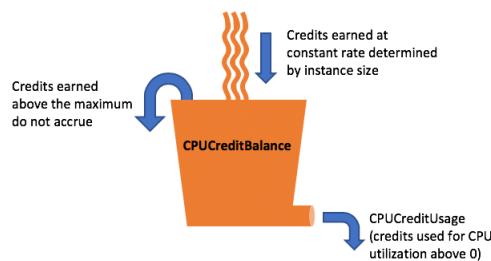
** O desempenho de linha de base na tabela é por vCPU. Para tamanhos de instância que têm mais de uma vCPU, para calcular a utilização de linha de base da CPU da instância, multiplique a porcentagem de vCPU pelo número de vCPUs. Por exemplo, uma instância t3.large tem duas vCPUs, que oferecem uma utilização de CPU da linha de base para a instância de 60% (2 vCPUs x 30% desempenho da linha de base de uma vCPU). Em CloudWatch, a utilização da CPU é exibida por vCPU. Portanto, a utilização de CPU para uma instância t3.large que opera no desempenho de linha de base é mostrada como 30% nas métricas de CPU do CloudWatch.

Taxa de ganhos de crédito de CPU

O número de créditos de CPU ganhos por hora é determinado pelo tamanho da instância. Por exemplo, `t3.nano` ganha seis créditos por hora, enquanto `t3.small` ganha 24 créditos por hora. A tabela anterior lista a taxa de ganhos de crédito de todas as instâncias.

Límite de acúmulo de créditos de CPU

Embora os créditos obtidos nunca expirem em uma instância em execução, há um limite para o número de créditos obtidos que uma instância pode acumular. O limite é determinado pelo limite de saldo de créditos de CPU. Após o limite ser atingido, todos os créditos novos que foram ganhos serão rejeitados, como indicado na imagem a seguir. O bucket completo indica o limite de saldo de créditos de CPU, e o spillover indica os créditos ganhos recentemente que excedem o limite.



O limite de saldo de créditos de CPU difere para cada tamanho de instância. Por exemplo, uma instância `t3.micro` pode acumular no máximo 288 créditos no saldo de créditos de CPU. A tabela anterior lista o número máximo de créditos ganhos que cada instância pode acumular.

Note

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 \(p. 201\)](#).

As instâncias T3 não ganham créditos de execução. Essas instâncias são executadas como `unlimited` por padrão e, portanto, podem apresentar intermitência imediatamente desde o início, sem nenhum crédito de execução.

Duração dos créditos de CPU acumulados

Os créditos de CPU de uma instância em execução não expiram.

Para 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 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 obter mais informações, consulte `CPUCreditBalance` na [Tabela de métricas do CloudWatch \(p. 216\)](#).

Desempenho de linha de base

O número de créditos obtidos por uma instância por hora pode ser expresso como uma porcentagem da utilização da CPU. É conhecido como desempenho de linha de base e às vezes como a linha de base. Por exemplo, uma instância `t3.nano`, com duas vCPUs, ganha seis créditos por hora, resultando em um

desempenho de linha de base de 5% (3/60 minutos) por vCPU. Uma instância `t3.xlarge`, com quatro vCPUs, ganha 96 créditos por hora, resultando em um desempenho de linha de base de 40% (24/60 minutos) por vCPU.

Modo ilimitado de instâncias de desempenho com capacidade de intermitência

Uma instância de desempenho com capacidade de intermitência configurada como `unlimited` pode sustentar alto desempenho 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 cargas de trabalho de uso geral, as instâncias configuradas como `unlimited` fornecem um desempenho amplo 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 a definição de preço de instâncias, consulte [Definição de preço do Amazon EC2](#) e a seção de definição de preço ilimitada em [Definição de preço sob demanda do Amazon EC2](#).

Important

Se você usar uma instância `t2.micro` na oferta do [Nível gratuito da AWS](#) e configurá-la como `unlimited`, cobranças poderão ser aplicadas se a sua utilização média durante um período contínuo de 24 horas exceder a linha de base da instância.

Tópicos

- [Conceitos do modo ilimitado \(p. 193\)](#)
- [Exemplos: modo ilimitado \(p. 197\)](#)

Conceitos do modo ilimitado

O modo `unlimited` é uma opção de configuração de crédito para instâncias de desempenho com capacidade de intermitência. Ele pode ser habilitado ou desabilitado a qualquer momento para uma instância interrompida ou em execução.

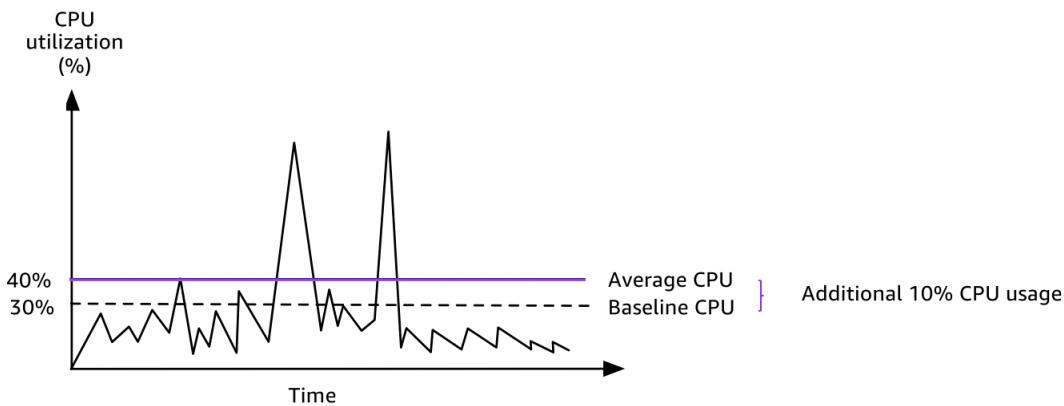
Note

As instâncias T3 são executadas como `unlimited` por padrão. As instâncias T2 são executadas como `standard` por padrão.

Como funcionam as instâncias ilimitadas de desempenho com capacidade de intermitência

Se uma instância de desempenho com capacidade de intermitência configurada como `unlimited` esgota seu crédito de CPU, ela pode gastar créditos excedentes para ter intermitência acima da linha de base. 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.

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 um [taxa adicional fixa](#) por hora de vCPU.



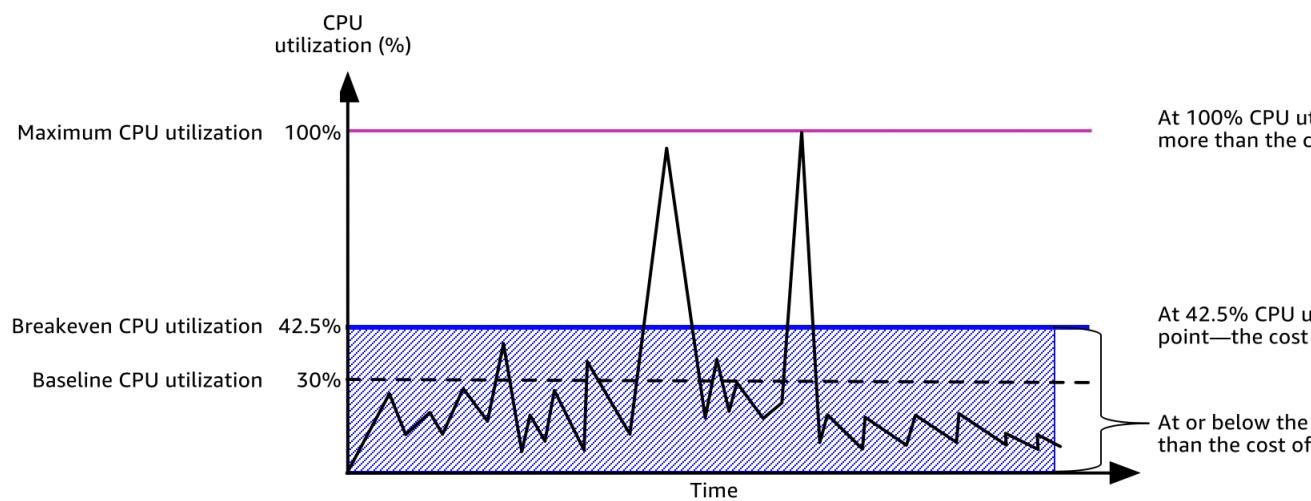
Para obter mais informações sobre o desempenho da linha de base por vCPU para cada tipo de instância e quantos créditos cada tipo de instância recebe, consulte a [tabela de créditos \(p. 191\)](#).

Quando usar o modo ilimitado vs. CPU fixa

Ao determinar se você deve usar uma instância de desempenho expansível no modo `unlimited`, como um T3, ou uma instância de desempenho fixo, como um M5, você precisa determinar o uso da CPU de equilíbrio. O uso da CPU de equilíbrio para uma instância de desempenho expansível é o ponto em que uma instância de desempenho expansível custa o mesmo que uma instância de desempenho fixo. 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 de desempenho expansível no modo `unlimited` para que você possa se beneficiar do preço mais baixo de uma instância de desempenho expansível enquanto obtém o mesmo desempenho de uma instância de desempenho fixo.
- Se o uso médio da CPU durante um período de 24 horas estiver acima do uso de CPU de equilíbrio, a instância de desempenho expansível custará mais do que a instância de desempenho fixo 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 carga de trabalho precisar de menos de 42,5% do uso médio da CPU, você poderá se beneficiar do preço mais baixo do `t3.large` ao obter o mesmo desempenho 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 para usar uma instância de desempenho expansível no modo `unlimited` ou uma instância de desempenho fixo. 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	Desempenho de linha de base de T3	Cobrança por hora de vCPU base de T3	Cobrança por minuto de vCPU excedente	Mais minutos de intermitência disponíveis	% de CPU adicional	% de CPU de equilíbrio
A	B	C	D	E = D - C	F	G	H = G / 60	I = E / H	J = (I / 60) / B	K = F + J
t3.large	2	US\$ 0,096 0,0835	US\$ 0,125 0,1175	USD 30%	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 o desempenho 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 a que uma instância é cobrada se apresentar uma intermitência para 100% da CPU depois de ter esgotado seus créditos ganhos.

- A coluna H mostra a taxa adicional fixa por minuto de vCPU a que uma instância é cobrada se apresentar uma intermitência para 100% da CPU depois de ter esgotado seus créditos ganhos.
- A coluna I mostra o número de minutos adicionais que o `t3.large` pode apresentar uma intermitência por hora para 100% da CPU pagando o mesmo preço por hora que um `m5.large`.
- A coluna J mostra o uso adicional da CPU (em %) ao longo da linha de base em que a instância pode apresentar uma intermitência enquanto paga o mesmo preço por hora que um `m5.large`.
- A coluna K mostra o uso da CPU de equilíbrio (em%) em que o `t3.large` pode apresentar uma intermitência sem pagar mais do que o `m5.large`. Qualquer coisa acima disso, e o `t3.large` custará mais do que o `m5.large`.

A tabela a seguir mostra o uso da CPU de equilíbrio (em%) para os tipos de instância T3 em comparação com os tipos de instância M5 de tamanho semelhante.

Tipo de instância do T3	Uso da CPU de equilíbrio (em %) para T3 comparado a M5
<code>t3.large</code>	42,5%
<code>t3.xlarge</code>	52,5 %
<code>t3.2xlarge</code>	52,5 %

Os créditos excedentes podem gerar cobranças

Se a utilização média de CPU de um instância for igual ou inferior à linha de base, a instância não incorrerá encargos adicionais. Como uma instância ganha um [número máximo de créditos \(p. 191\)](#) em um período de 24 horas (por exemplo, uma instância `t3.micro` pode ganhar no máximo 288 créditos em um período de 24 horas), ela pode gastar créditos excedentes até esse limite máximo sem gerar uma cobranças imediatamente.

Contudo, se a utilização de CPU permanecer acima da linha de base, a instância não poderá obter créditos suficientes para pagar os créditos excedentes que ela gastou. Os créditos excedentes que não são pagos são cobrados a uma taxa adicional fixa por hora de vCPU.

Os créditos excedentes que foram gastos anteriormente são cobrados quando uma das seguintes situações ocorre:

- Os créditos excedentes ultrapassaram o [número máximo de créditos \(p. 191\)](#) que a instância pode obter em um período de 24 horas. Os créditos excedentes gastos acima do limite máximo são cobrados no final da hora.
- A instância é interrompida ou encerrada.
- A instância é alterada de `unlimited` para `standard`.

Os créditos excedentes gastos são monitorados pela métrica CloudWatch do `CPUSurplusCreditBalance`. Os créditos excedentes cobrados são monitorados pela métrica CloudWatch do `CPUSurplusCreditsCharged`. Para obter mais informações, consulte [Métricas adicionais do CloudWatch para instâncias de desempenho com capacidade de intermitência \(p. 216\)](#).

Nenhum crédito de execução para T2 ilimitada

As instâncias T2 padrão recebem [créditos de execução \(p. 201\)](#), mas as instâncias T2 ilimitadas não as recebem. Uma instância T2 ilimitada pode apresentar intermitência acima da linha de base a qualquer momento, sem encargos adicionais, desde que sua utilização média de CPU seja igual ou inferior à linha de base em um período contínuo de 24 horas ou durante sua vida útil, o que for menor. Como tal, as

instâncias T2 ilimitadas não requerem créditos de execução para atingir alto desempenho imediatamente após a execução.

Se uma instância T2 for alterada de `standard` para `unlimited`, todos os créditos de execução acumulados serão removidos do `CPUCreditBalance` antes do `CPUCreditBalance` restante ser transferido.

Note

As instâncias T3 nunca recebem créditos de execução.

Habilitar o modo ilimitado

As instâncias T3 são executadas como `unlimited` por padrão. As instâncias T2 são executadas como `standard` por padrão, mas é possível habilitar `unlimited` na execução.

Você pode alterar de `unlimited` para `standard` e de `standard` para `unlimited` a qualquer momento em uma instância interrompida ou em execução. Para obter mais informações, consulte [Iniciando uma instância de desempenho com capacidade de intermitência como ilimitada ou padrão \(p. 212\)](#) e [Modificando a opção de crédito para instâncias de desempenho com capacidade de intermitência \(p. 215\)](#).

É possível verificar se uma instância de desempenho com capacidade de intermitência está configurada como `unlimited` ou `standard` usando o console do Amazon EC2 ou a AWS CLI. Para obter mais informações, consulte [Visualizando a opção de crédito para instâncias de desempenho com capacidade de intermitência \(p. 214\)](#).

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.

Monitoramento do uso de créditos

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 [Como monitorar seus créditos de CPU \(p. 216\)](#).

Exemplos: modo ilimitado

Os seguintes exemplos explicam o uso de créditos para instâncias configuradas como `unlimited`.

Exemplos

- [Exemplo 1: Explicação do uso de crédito com T3 ilimitada \(p. 198\)](#)
- [Exemplo 2: explicar o uso de créditos com T2 ilimitada \(p. 199\)](#)

[Exemplo 1: Explicação do uso de crédito com T3 ilimitada](#)

Neste exemplo, você verá a utilização de CPU de uma instância `t3.nano` configurada como `unlimited` e como ela gasta créditos ganhos e excedentes para sustentar o desempenho 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.

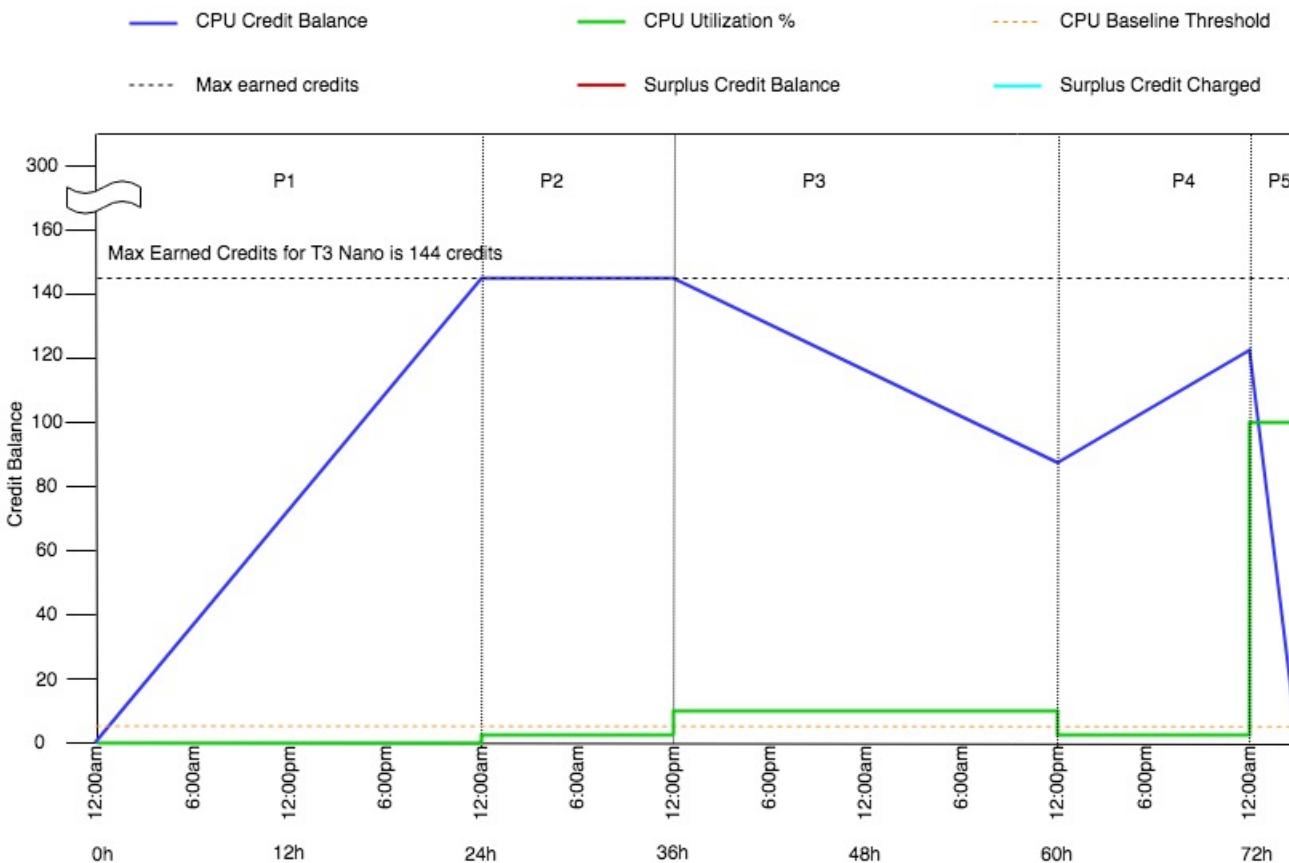
P3 – nas próximas 24 horas, a utilização de CPU é de 7% (acima da linha de base), o que exige um gasto de 57,6 créditos. A instância gasta mais do que ganha, e o valor `CPUCreditBalance` diminui para 86,4 créditos.

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 desempenho 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 configurada como `unlimited` e como ela gasta créditos ganhos e excedentes para sustentar o desempenho de CPU.

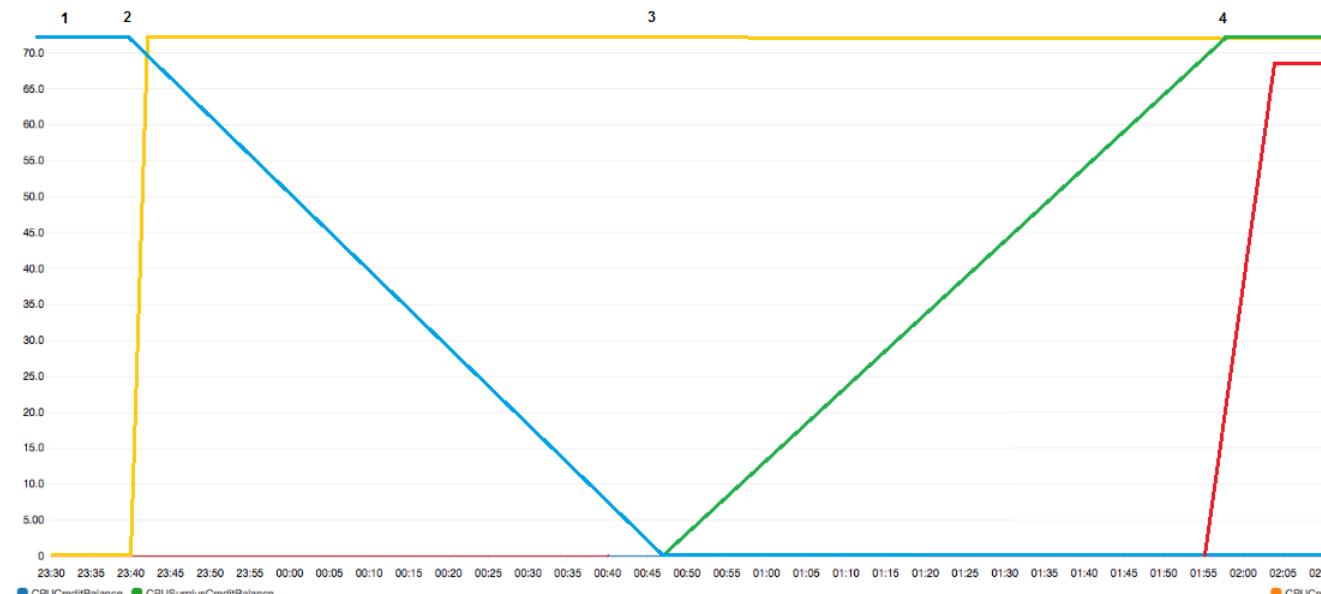
A instância t2.nano ganha 72 créditos de CPU em um período contínuo de 24 horas, que ela pode resgatar para 72 minutos de uso de vCPU. Quando ela esgotar o saldo de créditos de CPU (representado pela métrica CloudWatch do `CPUCreditBalance`), poderá gastar os créditos de CPU—excedentes, que ela ainda 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 desempenho da CPU.

4 – Os créditos excedentes são gastos até 01h55, quando o valor `CPUSurplusCreditBalance` atinge 72 créditos de CPU. Isso é igual ao limite máximo que uma instância t2.nano pode ganhar em um período de 24 horas. Qualquer crédito excedente gasto a partir daí não poderá ser compensado pelos créditos ganhos no período de 24 horas, o que resultará em uma pequena taxa adicional no final da hora.

5 – A instância continua a gastar os créditos excedentes até às 02h20. Nesse momento, a utilização da CPU cai abaixo da linha de base, e a instância começa a ganhar 3 créditos por hora (ou 0,25 crédito a cada 5 minutos), que ela usa para pagar o `CPUSurplusCreditBalance`. Quando o valor `CPUSurplusCreditBalance` reduz para 0, a instância começa a acumular créditos ganhos em seu `CPUCreditBalance` a 0,25 crédito a cada 5 minutos.



Label		Details	Statistic	Period
■	CPUCreditBalance	EC2 * InstanceId:i-0aa4b948d7eb37d6b * CPUCreditBalance	Maximum	5 Minutes
■	CPUCreditUsage	EC2 * InstanceId:i-0aa4b948d7eb37d6b * CPUCreditUsage	Maximum	5 Minutes
■	CPUSurplusCreditBalance	EC2 * InstanceId:i-0aa4b948d7eb37d6b * CPUSurplusCreditBalance	Maximum	5 Minutes
■	CPUSurplusCreditsCharged	EC2 * InstanceId:i-0aa4b948d7eb37d6b * CPUSurplusCreditsCharged	Maximum	5 Minutes

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 hora de vCPU x 0,05 USD/hora de vCPU = 0,021 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 de desempenho com capacidade de intermitência

Uma instância de desempenho com capacidade de intermitência configurada como **standard** é adequada para cargas de trabalho com uma utilização média de CPU consistentemente abaixo do desempenho 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 desempenho será gradualmente reduzido para o nível de desempenho da linha de base, para que a instância não experimente uma queda de desempenho acentuada quando o saldo de créditos de CPU acumulado se esgotar. Para obter mais informações, consulte [Créditos de CPU e linha de base para instância de desempenho com capacidade de intermitência \(p. 190\)](#).

Tópicos

- [Conceitos do modo padrão \(p. 201\)](#)
- [Exemplos: modo padrão \(p. 203\)](#)

Conceitos do modo padrão

O modo **standard** é uma opção de configuração para instâncias de desempenho com capacidade de intermitência. Ele pode ser habilitado ou desabilitado a qualquer momento para uma instância interrompida ou em execução.

Note

As instâncias T3 são executadas como **unlimited** por padrão. As instâncias T2 são executadas como **standard** por padrão.

Como funcionam as instâncias padrão de desempenho com capacidade de intermitência

Quando uma instância de desempenho com capacidade de intermitência 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 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.

Uma instância padrão T2 recebe dois tipos de créditos de CPU: créditos ganhos e créditos de execução. Quando uma instância T2 padrão estiver em um estado de execução, ela recebe continuamente (a uma resolução no nível de milissegundo) uma taxa definida de créditos ganhos por hora. No começo, ela ainda não ganhou créditos para uma boa experiência de inicialização. Portanto, para oferecer uma boa experiência de inicialização, ela recebe créditos de execução para começar, que ela gasta primeiro ao acumular créditos ganhos.

As instâncias T3 padrão não recebem créditos de execução.

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 inicialização, 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 gastos 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 \(p. 191\)](#).

A tabela a seguir lista a alocação de crédito de CPU inicial recebida na execução ou na inicialização, e o número de vCPUs.

Tipo de instância	Créditos de execução	vCPUs
t1.micro	15	1
t2.nano	30	1
t2.micro	30	1
t2.small	30	1
t2.medium	60	2
t2.large	60	2
t2.xlarge	120	4
t2.2xlarge	240	8

Limites de créditos 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 cargas de trabalho sempre obtenham o desempenho de que precisam, alterne para [Modo ilimitado de instâncias de desempenho com capacidade de intermitência \(p. 193\)](#) ou considere o uso de uma instância maior.

Diferenças entre créditos de execução e créditos ganhos

A tabela a seguir lista as diferenças entre créditos de execução e créditos ganhos.

	Créditos de execução	Créditos ganhos
Taxa de ganhos de crédito	As instâncias T2 padrão recebem 30 créditos de execução por vCPU na execução ou inicialização. Se uma instância T2 for alterada de <code>unlimited</code> para <code>standard</code> , ela não obtém créditos de execução no momento em que é alterada.	Cada instância T2 obtém continuamente (a uma resolução no nível de milissegundo) uma taxa definida de créditos de CPU por hora, dependendo do tamanho da instância. Para obter mais informações sobre o número de créditos de CPU ganhos por tamanho de instância, consulte a Tabela de créditos (p. 191) .

	Créditos de execução	Créditos ganhos
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 Tabela de créditos (p. 191) .
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 do `CloudWatchCPUCreditBalance`. Para obter mais informações, consulte `CPUCreditBalance` na [Tabela de métricas do CloudWatch \(p. 216\)](#).

Exemplos: modo padrão

Os seguintes exemplos explicam o uso de créditos quando as instâncias estão configuradas como `standard`.

Exemplos

- [Exemplo 1: como explicar o uso de créditos com T3 padrão \(p. 203\)](#)
- [Exemplo 2: como explicar o uso de créditos com T2 padrão \(p. 204\)](#)

[Exemplo 1: como 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.

Note

As instâncias T3 configuradas como `standard` não recebem créditos de execução.

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 \(p. 191\)](#).

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 aplicativos. 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.

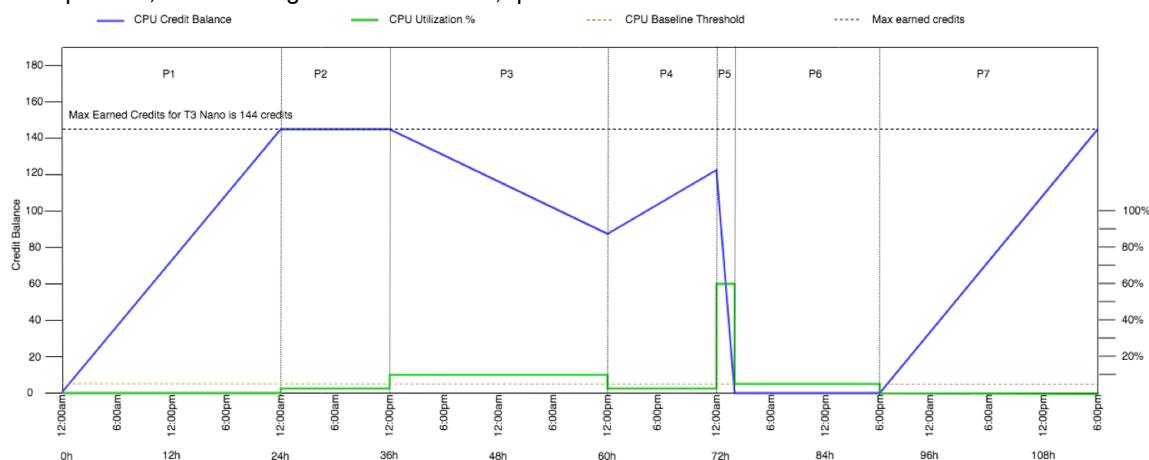
P3 – nas próximas 24 horas, a utilização de CPU é de 7% (acima da linha de base), o que exige um gasto de 57,6 créditos. A instância gasta mais do que ganha, e o valor CPUCreditBalance diminui para 86,4 créditos.

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, como o CPUCreditBalance em zero, a utilização de CPU é forçada a diminuir o nível de desempenho 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: como explicar o uso de créditos com T2 padrão

Neste exemplo, você verá como uma instância t2.nano executada como **standard** ganha, acumula e gasta créditos ganhos e de execução. Você verá como o saldo de crédito reflete não somente os créditos ganhos acumulados, como também os créditos de execução acumulados.

A instância t2.nano obtém 30 créditos de execução quando é executada e ganha 72 créditos a cada 24 horas. Seu limite de saldo é de 72 créditos ganhados. Os créditos de execução não são considerados no limite. Assim que o limite é atingido, os novos créditos ganhos são descartados. Para obter mais informações sobre o número de créditos que podem ser ganhos e acumulados, consulte a [Tabela](#)

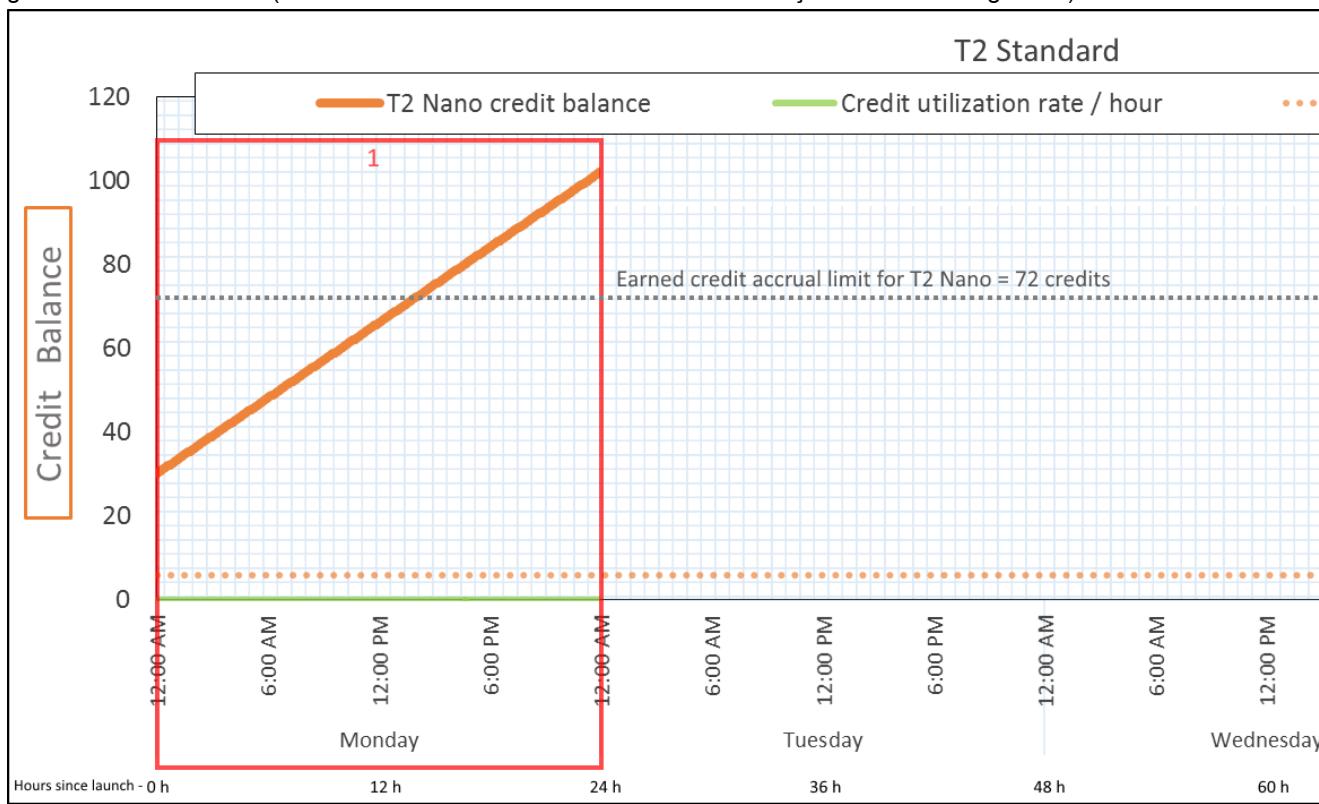
de créditos (p. 191). Para obter mais informações sobre limites, consulte [Limites de créditos de execução \(p. 202\)](#).

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 aplicativos. 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)

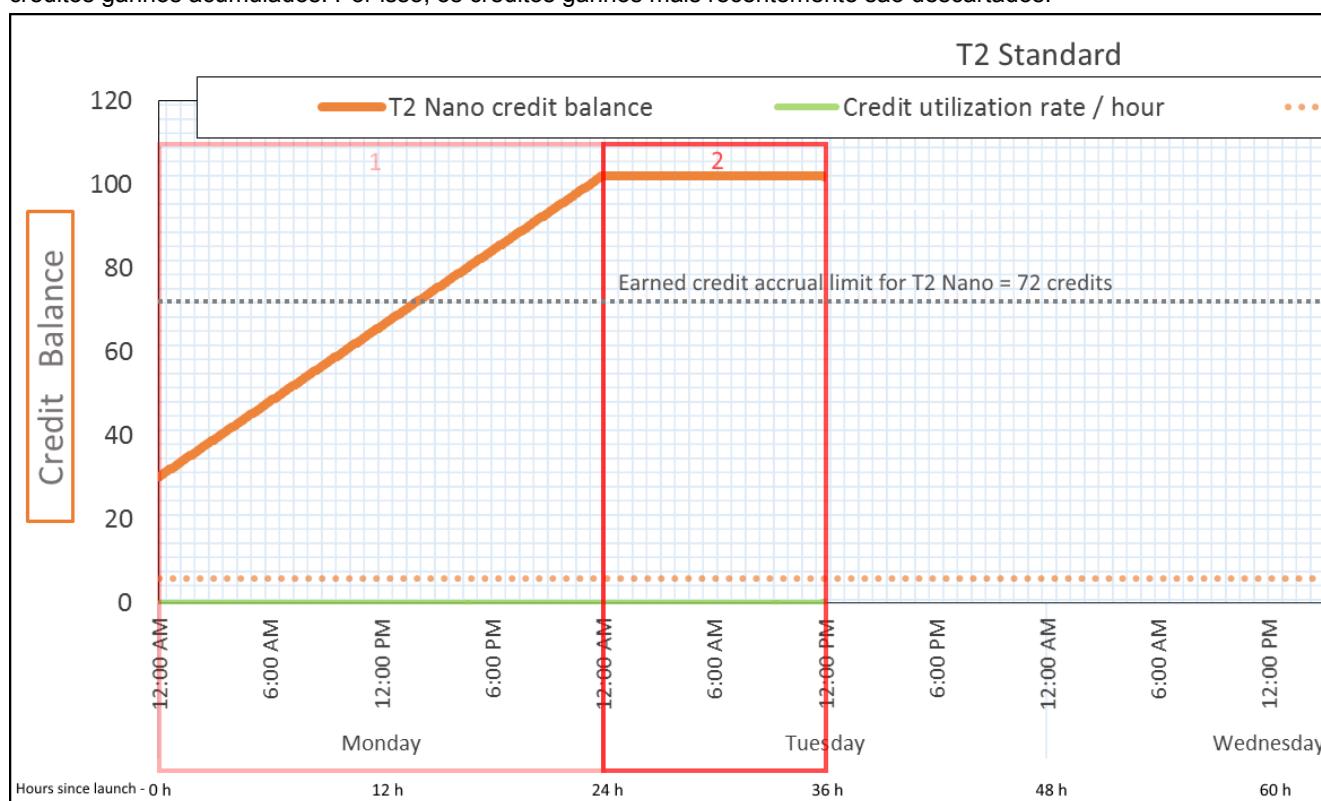
Conclusão

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.



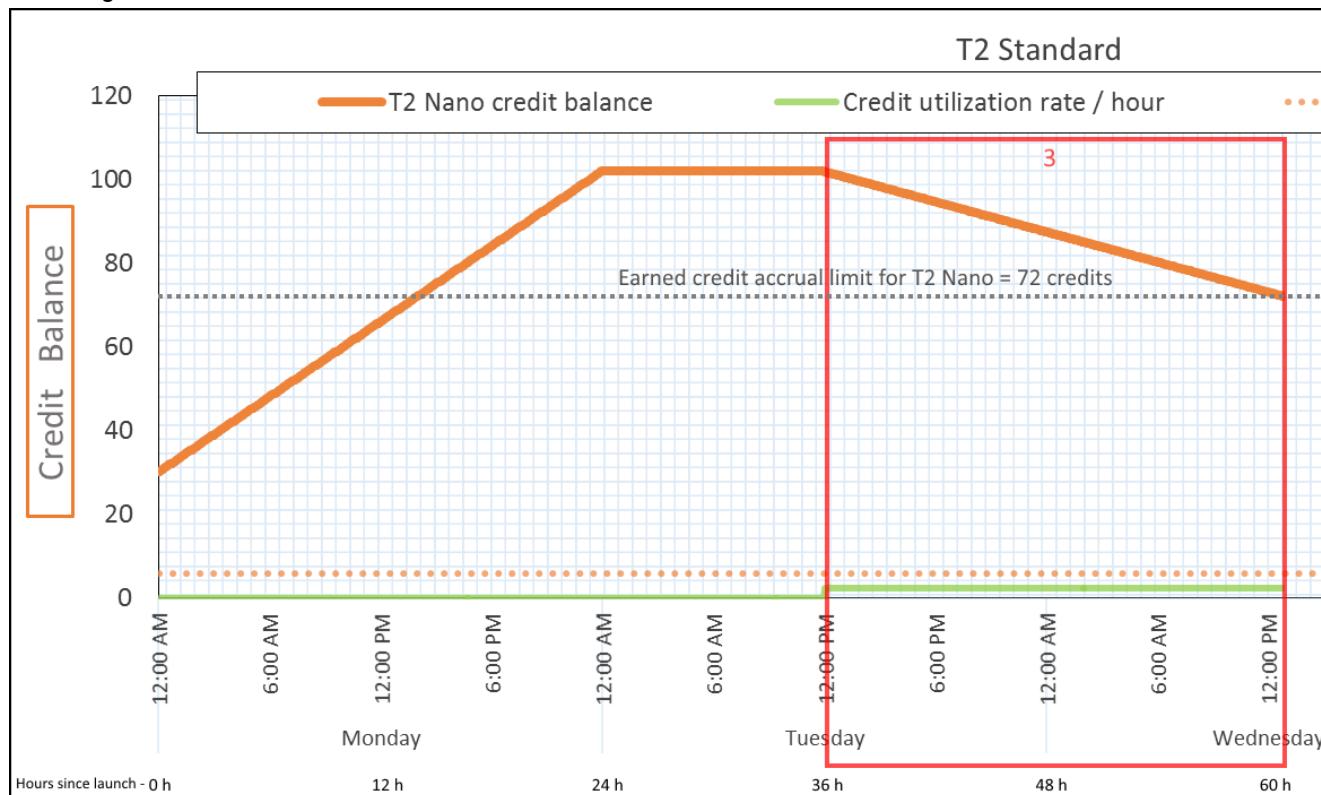
Taxa de gasto de crédito	0 crédito por 24 horas (0% de uso da CPU)
Taxa de ganhos de crédito	72 créditos por 24 horas (3 créditos por hora)
Taxa de descarte de crédito	72 créditos por 24 horas (100% de taxa de ganhos de crédito)
Saldo de crédito	102 créditos (30 créditos de execução + 72 créditos ganhos) – o saldo não é alterado

Conclusão

Uma instância ganha constantemente créditos, mas, se atingir o limite, não poderá acumular mais créditos. Assim que o limite é atingido, os créditos ganhos mais recentemente são descartados. Os créditos de execução não são contabilizados para o limite de saldo de créditos de execução. Se incluir créditos de execução acumulados, o saldo parecerá estar acima do limite.

Período 3: 37 a 61 horas

Nas próximas 25 horas, a instância usa 2% da CPU. Isso requer 30 créditos. No mesmo período, ela ganha 75 créditos, mas o saldo 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 ganho 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)

Conclusão

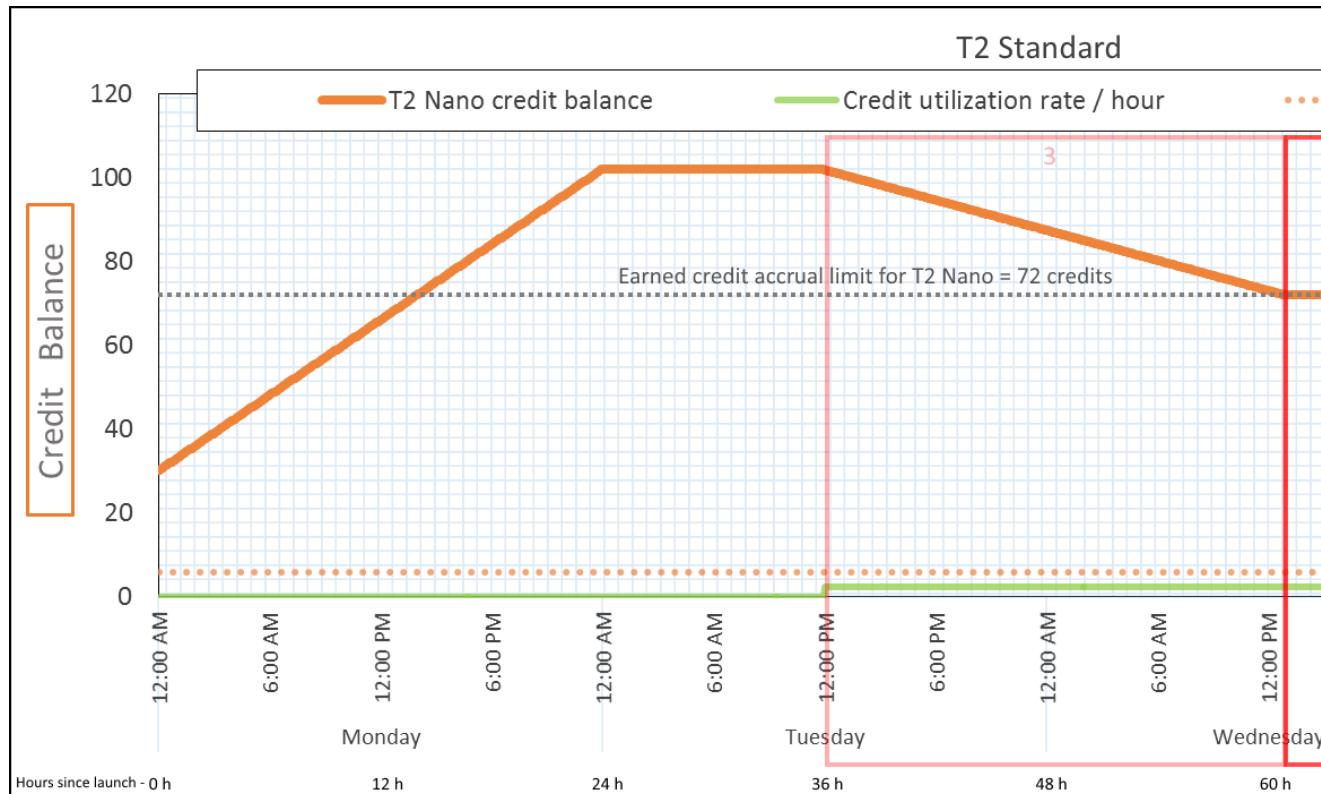
A instância gasta créditos de execução primeiro, antes dos crédito ganhos. Os créditos de execução não são contabilizados para o limite de créditos. Após o gasto dos créditos de execução, o saldo nunca pode

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.



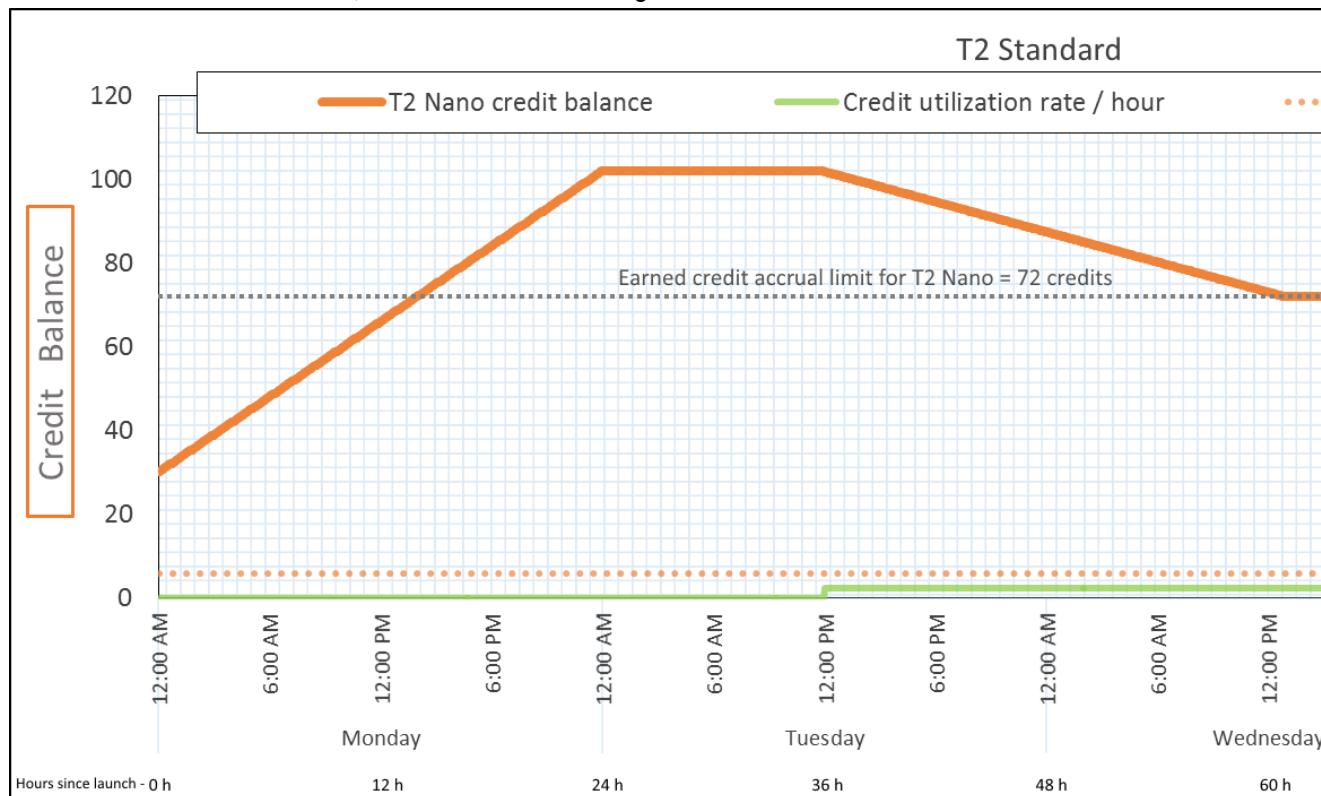
Taxa de gasto de crédito	28,8 créditos por 24 horas (1,2 créditos por hora, 2% de utilização da CPU, 40% de taxa de ganhos de crédito) – 13,2 —créditos em 11 horas
Taxa de ganhos de crédito	72 créditos por 24 horas
Taxa de descarte de crédito	43,2 créditos por 24 horas (60% de taxa de ganhos de crédito)
Saldo de crédito	72 créditos (0 créditos de execução, 72 créditos ganhos) – 0 —saldo está no limite

Conclusão

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)) – 0 — saldo diminui a uma taxa de 216 créditos por 24 horas (taxa de gastos de 288/24 + taxa de ganhos de 72/24 = taxa de diminuição do saldo de 216/24)

Conclusão

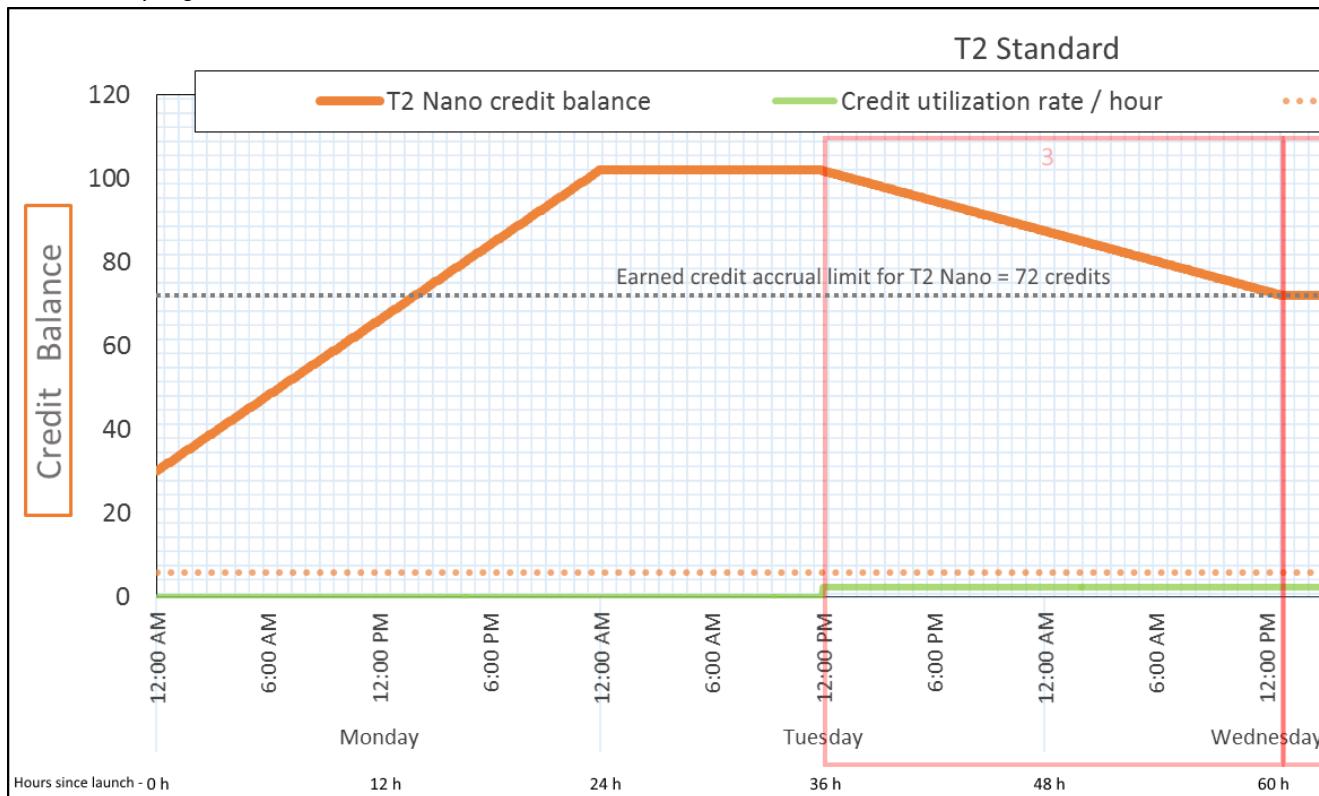
Se uma instância gastar mais créditos do que ganhar, seu balanço diminuirá.

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)

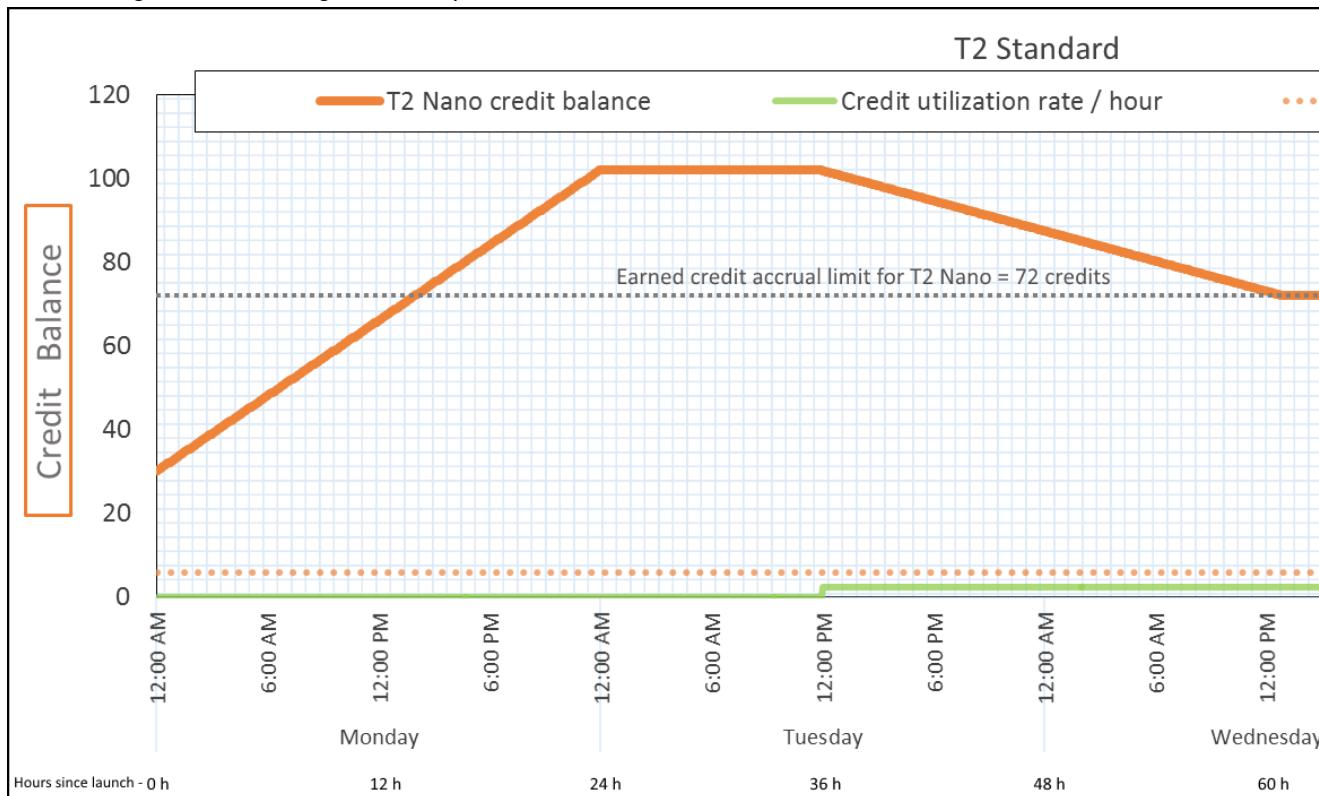
Conclusão

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)

Conclusão

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 \(p. 191\)](#).

Trabalhando com instâncias com ampliação de desempenho

As etapas de execução, monitoramento e modificação dessas instâncias são semelhantes. A principal diferença é a especificação de crédito padrão na execução:

- As instâncias T3 são executadas como `unlimited` por padrão.
- As instâncias T2 são executadas como `standard` por padrão.

Tópicos

- [Iniciando uma instância de desempenho com capacidade de intermitência como ilimitada ou padrão \(p. 212\)](#)
- [Uso de um grupo do Auto Scaling para executar uma instância de desempenho com capacidade de intermitência como ilimitada \(p. 213\)](#)
- [Visualizando a opção de crédito para instâncias de desempenho com capacidade de intermitência \(p. 214\)](#)
- [Modificando a opção de crédito para instâncias de desempenho com capacidade de intermitência \(p. 215\)](#)

Iniciando uma instância de desempenho com capacidade de intermitência como ilimitada ou padrão

As instâncias T3 são executadas como `unlimited` por padrão. As instâncias T2 são executadas como `standard` por padrão.

Para obter mais informações sobre os requisitos de driver de AMI para essas instâncias, consulte [Notas de release \(p. 188\)](#).

Você deve executar as instâncias usando um volume do Amazon EBS como o dispositivo raiz. Para obter mais informações, consulte [Volume do dispositivo raiz do Amazon EC2 \(p. 15\)](#).

Você pode executar suas instâncias como `unlimited` ou `standard` usando o console do Amazon EC2, um SDK da AWS, uma ferramenta de linha de comando ou um grupo do Auto Scaling. Para obter mais informações, consulte [Uso de um grupo do Auto Scaling para executar uma instância de desempenho com capacidade de intermitência como ilimitada \(p. 213\)](#).

Para executar uma instância de desempenho com capacidade de intermitência como ilimitada ou padrão (console)

1. Siga o procedimento do [Execução de uma instância usando o assistente de execução de instância \(p. 391\)](#).
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. O padrão para T3 é `unlimited`, e para T2 é `standard`.
 - a. Para executar uma instância T3 como `standard`, na página Configure Instance Details (Configurar detalhes da instância), para T2/T3 Unlimited (T2/T3 ilimitada), desmarque Enable (Habilitar).
 - b. Para executar uma instância T2 como `unlimited`, na página Configure Instance Details (Configurar detalhes da instância), em T2/T3 Unlimited (T2/T3 ilimitada), selecione Enable (Habilitar).
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 [Execução de uma instância usando o assistente de execução de instância \(p. 391\)](#).

Para iniciar uma instância de desempenho com capacidade de intermitência 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 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"
```

Uso de um grupo do Auto Scaling para executar uma instância de desempenho com capacidade de intermitência como ilimitada

Quando as instâncias de desempenho com capacidade de intermitência 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 desempenho.

Criação de 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`.

Para criar um modelo de execução que execute instâncias como ilimitadas (console)

- Siga o procedimento [Criando um modelo de execução para um grupo do Auto Scaling](#).
- Em Launch template contents (Conteúdo do modelo de execução), para Instance type (Tipo de instância), escolha um tipo de instância T3 ou T2.
- Para executar instâncias como `unlimited` em um grupo do Auto Scaling, em Advanced details (Detalhes avançados), para T2/T3 Unlimited (T2/T3 ilimitada), escolha Enable (Habilitar).
- Ao terminar de definir os parâmetros do modelo de execução, escolha Create launch template (Criar modelo de execução). Para obter mais informações, consulte [Criando um modelo de execução para um grupo do 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 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 do 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)

- Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
- 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`.

[Visualizando a opção de crédito para instâncias de desempenho com capacidade de intermitência](#)

Você pode exibir a especificação de crédito (`unlimited` ou `standard`) de uma instância em execução ou interrompida.

Para visualizar a especificação de crédito para uma instância com capacidade de intermitência (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. 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 de desempenho com capacidade de intermitência (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"  
        }  
    ]  
}
```

Modificando a opção de crédito para instâncias de desempenho com capacidade de intermitência

Você pode alterar a especificação de crédito de uma instância interrompida ou em execução a qualquer momento entre **unlimited** e **standard**.

Para modificar a especificação de crédito de uma instância de desempenho com capacidade de intermitência (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. Para modificar a especificação de crédito para várias instâncias de uma vez, selecione todas as instâncias aplicáveis.
3. Selecione Actions (Ações), Instance Settings (Configurações da instância), Change T2/T3 Unlimited (Alterar T2/T3 ilimitada).

Note

A opção Change T2/T3 Unlimited (Alterar T2/T3 ilimitada) estará habilitada somente se você selecionar uma instância T3 ou T2.

4. Para alterar a opção de crédito para **unlimited**, escolha Enable (Ativar). Para alterar a opção de crédito para **standard**, escolha Disable (Desativar). A especificação de crédito atual para a instância aparece entre parênteses após o ID da instância.

Para modificar a opção de crédito para instâncias de desempenho com capacidade de intermitência (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": []  
}
```

Como monitorar seus créditos de 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 de desempenho com capacidade de intermitência \(p. 216\)](#)
- [Cálculo de uso de créditos de CPU \(p. 217\)](#)

Métricas adicionais do CloudWatch para instâncias de desempenho com capacidade de intermitência

As instâncias T3 e T2 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 o desempenho de CPU quando o `CPUCreditBalance` é zero.
- `CPUSurplusCreditsCharged` – o número de créditos de CPU excedentes que ultrapassam o [número máximo de créditos de CPU \(p. 191\)](#) 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 de desempenho com capacidade de intermitência. Para obter mais informações, consulte [Lista as métricas disponíveis do CloudWatch para suas instâncias \(p. 577\)](#).

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 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>.</p> <p>Unidades: créditos (minutos de vCPU)</p>
<code>CPUCreditBalance</code>	<p>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.</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</p>

Métrica	Descrição
	<p>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 <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 T3 é interrompida, o valor <code>CPUCreditBalance</code> persiste por sete dias. Consequentemente, todos os créditos acumulados são perdidos. Quando uma instância T2 é interrompida, o valor <code>CPUCreditBalance</code> não persiste, e todos os créditos acumulados são perdidos.</p> <p>As métricas de crédito de CPU estão disponíveis a uma frequência de apenas 5 minutos.</p> <p>Unidades: créditos (minutos de vCPU)</p>
<code>CPUSurplusCreditBalance</code>	<p>O número de créditos excedentes gastos por uma instância <code>unlimited</code> quando seu valor <code>CPUCreditBalance</code> é zero.</p> <p>O valor <code>CPUSurplusCreditBalance</code> é pago pelos créditos de CPU ganhos. Se o número de créditos excedentes ultrapassar o número máximo de créditos que a instância pode ganhar em um período de 24 horas, os créditos excedentes gastos acima do limite máximo incorrerão em uma taxa adicional.</p> <p>Unidades: créditos (minutos de vCPU)</p>
<code>CPUSurplusCreditsCharged</code>	<p>O número de créditos excedentes gastos que não são pagos pelos créditos de CPU ganhos e que, portanto, incorrem em uma cobrança adicional.</p> <p>Os créditos excedentes gastos são cobrados quando uma das seguintes situações ocorre:</p> <ul style="list-style-type: none"> • Os créditos excedentes ultrapassaram o número máximo de créditos que a instância pode obter em um período de 24 horas. Os créditos excedentes gastos acima do limite máximo são cobrados no final da hora. • A instância é interrompida ou encerrada. • A instância é alterada de <code>unlimited</code> para <code>standard</code>. <p>Unidades: créditos (minutos de vCPU)</p>

Cálculo de uso de créditos de 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.

Cálculo de 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 \(p. 191\)](#).

Exemplo

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 T3 ou T2 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 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 \(p. 191\)](#) 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 \(p. 191\)](#) que ela pode acumular.

Example

```
CPUSurplusCreditBalance = min [max earned credit balance, -Adjusted balance]  
CPUCreditBalance = 0
```

Se os créditos excedentes gastos ultrapassarem o máximo de créditos que a instância pode acumular, o saldo de créditos excedentes será definido como o número máximo, conforme exibido na equação anterior. Os créditos excedentes restantes serão cobrados conforme representados pela métrica `CPUSurplusCreditsCharged`.

Example

```
CPUSurplusCreditsCharged = max [-Adjusted balance - max earned credit balance, 0]
```

Por fim, quando a instância for encerrada, todos os créditos excedentes monitorados pelo `CPUSurplusCreditBalance` serão cobrados. Se a instância for alterada de `unlimited` para `standard`, todo o `CPUSurplusCreditBalance` restante também será cobrado.

Instâncias otimizadas para computação

Instâncias otimizadas para computação são ideais para aplicativos com uso intensivo de computação que se beneficiam de processadores de alta performance. Elas são ideais para os seguintes aplicativos:

- 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 outros aplicativos com uso intensivo de computação

Para obter mais informações, consulte [Instâncias C5 do Amazon EC2](#).

Tópicos

- [Especificações de hardware \(p. 220\)](#)
- [Performance da instância \(p. 221\)](#)
- [Desempenho de rede \(p. 221\)](#)
- [Desempenho de E/S SSD \(p. 222\)](#)
- [Recursos das instâncias \(p. 223\)](#)
- [Notas de release \(p. 223\)](#)

Especificações de hardware

Este é um resumo das especificações de hardware para instâncias otimizadas para computação.

Tipo de instância	vCPUs padrão	Memória (GiB)
c4.large	2	3,75
c4.xlarge	4	7,5
c4.2xlarge	8	15
c4.4xlarge	16	30
c4.8xlarge	36	60
c5.large	2	4
c5.xlarge	4	8
c5.2xlarge	8	16
c5.4xlarge	16	32
c5.9xlarge	36	72
c5.18xlarge	72	144
c5d.large	2	4
c5d.xlarge	4	8
c5d.2xlarge	8	16
c5d.4xlarge	16	32
c5d.9xlarge	36	72
c5d.18xlarge	72	144
c5n.large	2	5.25
c5n.xlarge	4	10.5
c5n.2xlarge	8	21
c5n.4xlarge	16	42
c5n.9xlarge	36	96

Tipo de instância	vCPUs padrão	Memória (GiB)
c5n.18xlarge	72	192

Para obter mais informações sobre as especificações de hardware para cada tipo de instância do Amazon EC2, veja [Tipos de instâncias do Amazon EC2](#).

Para obter mais informações sobre como especificar opções de CPU, consulte [Optimizar opções de CPU \(p. 495\)](#).

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 [Amazon EBS – instâncias otimizadas \(p. 916\)](#).

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 o desempenho desejado (em frequência da CPU) de um núcleo. Para obter mais informações, consulte [Controle do estado do processo para sua instância do EC2 \(p. 485\)](#).

Desempenho de rede

Você pode habilitar recursos de rede aprimoradas em tipos de instância compatíveis. O uso avançado de rede fornece um desempenho significativamente maior de pacotes por segundo (PPS), menor jitter de rede e latências mais baixas. Para obter mais informações, consulte [Rede avançada no Linux \(p. 768\)](#).

Os tipos de instâncias que usam Elastic Network Adapter (ENA) para networking avançado fornecem alto desempenho de pacotes por segundo com latências consistentemente baixas. A maioria dos aplicativos não precisa de um alto nível de desempenho de rede constantemente, mas podem se beneficiar com uma largura de banda maior quando enviam ou recebem dados. Os tamanhos de instância que usam ENA e estão documentados com desempenho de rede de "Até 10 Gbps" ou "Até 25 Gbps" usam um mecanismo de crédito de E/S de rede para alocar largura de banda a instâncias baseadas na utilização média da largura de banda. Essas instâncias acumulam créditos quando a largura de banda da rede está abaixo dos limites de linha de base e podem usar esses créditos ao executar transferências de dados pela rede.

Este é um resumo do desempenho de rede para instâncias otimizadas para computação que oferecem suporte às redes aprimoradas.

Tipo de instância	Desempenho das redes	Redes avançadas
c5.4xlarge e menor c5d.4xlarge e menor	Até 10 Gbps	ENA (p. 769)
c5.9xlarge c5d.9xlarge	10 Gbps	ENA (p. 769)
c5n.4xlarge e menor	Até 25 Gbps	ENA (p. 769)
c5.18xlarge c5d.18xlarge	25 Gbps	ENA (p. 769)
c5n.9xlarge	50 Gbps	ENA (p. 769)
c5n.18xlarge	100 Gbps	ENA (p. 769)
c4.large	Moderada	Intel 82599 VF (p. 780)

Tipo de instância	Desempenho das redes	Redes avançadas
c4.xlarge c4.2xlarge c4.4xlarge	Alto	Intel 82599 VF (p. 780)
c4.8xlarge	10 Gbps	Intel 82599 VF (p. 780)

Desempenho de E/S 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 o desempenho 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
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.18xlarge	700.000	340.000

* Para essas instâncias, você pode obter o desempenho especificado.

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 no desempenho 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 um desempenho de E/S drasticamente reduzido.

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 o desempenho 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 o desempenho. Para obter mais informações, consulte [Suporte a TRIM do volume de armazenamento de instâncias \(p. 966\)](#).

Recursos das instâncias

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
C5d	Não	Sim	NVMe *	Sim
C5n	Sim	Sim	Não	Sim

* O volume do dispositivo raiz deve ser um volume do Amazon EBS.

Para obter mais informações, consulte:

- [Amazon EBS e NVMe \(p. 929\)](#)
- [Armazenamento de instâncias do Amazon EC2 \(p. 958\)](#)
- [Placement groups \(p. 793\)](#)

Notas de release

- Instâncias C4, C5, e C5d e C5n exigem AMIs de HVM baseadas em 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 desempenho 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 C5, C5d e C5n têm os seguintes requisitos:

As AMIs a seguir atendem a esses requisitos:

- As instâncias C5, C5d e C5n oferecem suporte a um máximo de 28 anexos, incluindo interfaces de rede, volumes do EBS e volumes de armazenamento de instâncias do NVMe. Cada instância tem pelo menos um anexo de interface de rede.
- As instâncias C5, C5d e C5n devem ter o 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?](#). Para solicitar um aumento do limite, use o [Formulário de solicitação de instâncias do Amazon EC2](#).

Instâncias otimizadas para memória

As instâncias otimizadas na memória são projetadas para fornecer desempenho rápido para cargas de trabalho que processam grandes bancos de dados na memória.

Instâncias R4, R5, R5a e R5d

Essas instâncias são ideais para os seguintes aplicativos:

- Bancos de dados relacionais de alto desempenho (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).
- Aplicativos que executam processamento em tempo real de dados não estruturados grandes (serviços financeiros, clusters Hadoop/Spark).
- computação de alta performance (HPC) e aplicativos de Electronic Design Automation (EDA).

As instâncias `r5.metal` e `r5d.metal` fornecem aos aplicativos acesso direto aos recursos físicos do servidor host, como processadores e memória. Essas instâncias são ideais para o seguinte:

- Cargas de trabalho 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
- Aplicativos que exigem um ambiente não virtualizado para licenciamento ou suporte

Para obter mais informações, consulte [Instâncias R5 do Amazon EC2](#).

Instâncias com mais memória

Instâncias com mais memória (`u-6tb1.metal`, `u-9tb1.metal`, and `u-12tb1.metal`) oferecem 6 TiB, 9 TiB e 12 TiB de memória por instância. Essas instâncias foram desenvolvidas para executar grandes bancos de dados na memória, incluindo instalações de produção do SAP HANA. Eles oferecem desempenho bare metal com acesso direto ao hardware do host.

Instâncias X1

Essas instâncias são ideais para os seguintes aplicativos:

- 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.
- Aplicativos de computação de alta performance (HPC).

Para obter mais informações, consulte [Instâncias X1 do Amazon EC2](#).

Instâncias X1e

Essas instâncias são ideais para os seguintes aplicativos:

- Banco de dados de alto desempenho.
- Bancos de dados mantidos na memória como o SAP HANA. Para obter mais informações, consulte [SAP HANA na Nuvem AWS](#).
- Aplicativos empresariais com uso intensivo de memória.

Para obter mais informações, consulte [Instâncias X1e do Amazon EC2](#).

Instâncias z1d

Essas instâncias oferecem computação e memória elevadas e são adequadas para os seguintes aplicativos:

- Electronic Design Automation (EDA)
- Cargas de trabalho de bancos de dados relacionais

As instâncias `z1d.metal` fornecem aos aplicativos acesso direto aos recursos físicos do servidor host, como processadores e memória. Essas instâncias são ideais para o seguinte:

- Cargas de trabalho 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
- Aplicativos que exigem um ambiente não virtualizado para licenciamento ou suporte

Para obter mais informações, consulte [Instâncias z1d do Amazon EC2](#).

Tópicos

- [Especificações de hardware \(p. 225\)](#)
- [Desempenho da memória \(p. 227\)](#)
- [Performance da instância \(p. 227\)](#)
- [Desempenho de rede \(p. 227\)](#)
- [Desempenho de E/S SSD \(p. 228\)](#)
- [Recursos das instâncias \(p. 229\)](#)
- [Suporte para vCPUs \(p. 230\)](#)
- [Notas de release \(p. 230\)](#)

Especificações de hardware

Este é um resumo das especificações de hardware para instâncias otimizadas para memória.

Tipo de instância	vCPUs padrão	Memória (GiB)
<code>r4.large</code>	2	15.25
<code>r4.xlarge</code>	4	30.5
<code>r4.2xlarge</code>	8	61
<code>r4.4xlarge</code>	16	122
<code>r4.8xlarge</code>	32	244
<code>r4.16xlarge</code>	64	488
<code>r5.large</code>	2	16
<code>r5.xlarge</code>	4	32
<code>r5.2xlarge</code>	8	64
<code>r5.4xlarge</code>	16	128
<code>r5.12xlarge</code>	48	384
<code>r5.24xlarge</code>	96	768
<code>r5.metal</code>	96	768
<code>r5a.large</code>	2	16
<code>r5a.xlarge</code>	4	32
<code>r5a.2xlarge</code>	8	64

Tipo de instância	vCPUs padrão	Memória (GiB)
r5a.4xlarge	16	128
r5a.12xlarge	48	384
r5a.24xlarge	96	768
r5d.large	2	16
r5d.xlarge	4	32
r5d.2xlarge	8	64
r5d.4xlarge	16	128
r5d.12xlarge	48	384
r5d.24xlarge	96	768
r5d.metal	96	768
u-6tb1.metal	448 *	6,144
u-9tb1.metal	448 *	9,216
u-12tb1.metal	448 *	12,288
x1.16xlarge	64	976
x1.32xlarge	128	1,952
x1e.xlarge	4	122
x1e.2xlarge	8	244
x1e.4xlarge	16	488
x1e.8xlarge	32	976
x1e.16xlarge	64	1,952
x1e.32xlarge	128	3,904
z1d.large	2	16
z1d.xlarge	4	32
z1d.2xlarge	8	64
z1d.3xlarge	12	96
z1d.6xlarge	24	192
z1d.12xlarge	48	384
z1d.metal	48	384

* Cada processador lógico é uma hyperthread em 224 cores.

Para obter mais informações sobre as especificações de hardware para cada tipo de instância do Amazon EC2, veja [Tipos de instâncias do Amazon EC2](#).

Para obter mais informações sobre como especificar opções de CPU, consulte [Otimizar opções de CPU \(p. 495\)](#).

Desempenho da memória

As instâncias X1 incluem Intel Scalable Memory Buffers, 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 \(p. 225\)](#).

As instâncias otimizadas na memória possuem mais memória e exigem AMIs HVM de 64 bits para tirar proveito dessa capacidade. As AMIs HVM fornecem desempenho 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 \(p. 94\)](#).

Performance da instância

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 o desempenho de aplicativos na memória.

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 o desempenho de aplicativos na memória.

As instâncias com mais memória (`u-6tb1.metal`, `u-9tb1.metal`, and `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 cargas de trabalho corporativas de missão crítica.

As instâncias otimizadas na memória permitem maior desempenho criptográfico por meio do recurso Intel AES-NI mais recente, suporte ao Intel Transactional Synchronization Extensions (TSX) para impulsionar o desempenho 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 o desempenho desejado (medido pela frequência da CPU) de um núcleo. Para obter mais informações, consulte [Controle do estado do processo para sua instância do EC2 \(p. 485\)](#).

Desempenho de rede

Você pode habilitar recursos de rede aprimoradas em tipos de instância compatíveis. O uso avançado de rede fornece um desempenho significativamente maior de pacotes por segundo (PPS), menor jitter de rede e latências mais baixas. Para obter mais informações, consulte [Rede avançada no Linux \(p. 768\)](#).

Os tipos de instâncias que usam Elastic Network Adapter (ENA) para networking avançado fornecem alto desempenho de pacotes por segundo com latências consistentemente baixas. A maioria dos aplicativos não precisa de um alto nível de desempenho de rede constantemente, mas podem se beneficiar com uma largura de banda maior quando enviam ou recebem dados. Os tamanhos de instância que usam ENA e estão documentados com desempenho de rede de "Até 10 Gbps" ou "Até 25 Gbps" usam um mecanismo de crédito de E/S de rede para alocar largura de banda a instâncias baseadas na utilização média da largura de banda. Essas instâncias acumulam créditos quando a largura de banda da rede está abaixo dos limites de linha de base e podem usar esses créditos ao executar transferências de dados pela rede.

Este é um resumo da performance de rede para instâncias otimizadas para memória que oferecem suporte às redes aprimoradas.

Tipo de instância	Desempenho das redes	Redes avançadas
r4.4xlarge e menor r5.4xlarge e menor r5a.4xlarge e menor r5d.4xlarge e menor x1e.8large e menor z1d.3xlarge e menor	Até 10 Gbps	ENA (p. 769)
r4.8xlarge r5.12xlarge r5a.12xlarge r5d.12xlarge x1.16xlarge x1e.16xlarge z1d.6xlarge	10 Gbps	ENA (p. 769)
r5a.24xlarge	20 Gbps	ENA (p. 769)
r4.16xlarge r5.24xlarge r5.metal r5d.24xlarge r5d.metal u-6tb1.metal u-9tb1.metal u-12tb1.metal x1.32xlarge x1e.32xlarge z1d.12xlarge z1d.metal	25 Gbps	ENA (p. 769)

Desempenho de E/S 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 o desempenho 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
r5d.large *	30.000	15.000
r5d.xlarge *	59.000	29.000
r5d.2xlarge *	117.000	57.000
r5d.4xlarge *	234.000	114.000
r5d.12xlarge	700.000	340.000
r5d.24xlarge	1.400.000	680.000
r5d.metal	1.400.000	680.000
z1d.large *	30.000	15.000
z1d.xlarge *	59.000	29.000
z1d.2xlarge *	117.000	57.000
z1d.3xlarge *	175.000	75.000
z1d.6xlarge	350.000	170.000
z1d.12xlarge	700.000	340.000
z1d.metal	700.000	340.000

* Para essas instâncias, você pode obter o desempenho especificado.

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 no desempenho 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 um desempenho de E/S drasticamente reduzido.

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 o desempenho 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 o desempenho. Para obter mais informações, consulte [Suporte a TRIM do volume de armazenamento de instâncias \(p. 966\)](#).

Recursos das instâncias

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
R5d	Não	Sim	NVME *	Sim
u-6tb1.me	Sim	Sim	Não	Não
u-9tb1.me	Sim	Sim	Não	Não
u-12tb1.me	Sim	Sim	Não	Não
X 1	Não	Não	SSD	Sim
X1e	Não	Não	SSD	Sim
z1d	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 \(p. 929\)](#)
- [Armazenamento de instâncias do Amazon EC2 \(p. 958\)](#)
- [Placement groups \(p. 793\)](#)

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 R5 e R5d têm um processador da série Intel Xeon Platinum 8000 de 3,1 GHz.
- As instâncias R5a têm um processador da série AMD EPYC 7000 de 2,5 GHz.
- Os seguintes são os requisitos para instâncias de alta memória R5, R5a, R5d e z1d:

As AMIs a seguir atendem a esses requisitos:

- As instâncias R5, R5a e R5d oferecem suporte a um máximo de 28 anexos, incluindo interfaces de rede, volumes do EBS e volumes de armazenamento de instâncias do NVMe. Cada instância tem pelo menos um anexo de interface de rede. Por exemplo, se você não tiver anexos de interface de rede adicionais em uma instância somente EBS, poderá anexar 27 volumes do EBS a essa instância.
- 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. Amazon Linux 2 e as versões mais recentes do Amazon Linux AMI 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.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?](#). Para solicitar um aumento do limite, use o [Formulário de solicitação de instâncias do Amazon EC2](#).

Instâncias otimizadas para armazenamento

As instâncias otimizadas para armazenamento foram projetadas para cargas de trabalho 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 aplicativos.

Instâncias D2

As instâncias D2 são ideais para os seguintes aplicativos:

- Data warehouse de processamento paralelo maciço (MPP)
- Computação distribuída de MapReduce e Hadoop
- Aplicativos de processamento de dados ou log

Instâncias H1

As instâncias H1 são ideais para os seguintes aplicativos:

- Cargas de trabalho com muitos dados, como MapReduce e sistemas de arquivos distribuídos
- Aplicativos que exigem acesso sequencial a grandes quantidades de dados em armazenamento de instâncias com vínculo direto
- Aplicativos que exigem acesso com alta taxa de transferência a grandes quantidades de dados

Instâncias I3

As instâncias I3 são ideais para os seguintes aplicativos:

- 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)
- Aplicativos de data warehousing
- Aplicativos de fornecimento de AD-Tech de baixa latência

As instâncias `i3.meta1` fornecem aos aplicativos acesso direto aos recursos físicos do servidor host, como processadores e memória. Essas instâncias são ideais para o seguinte:

- Cargas de trabalho 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
- Aplicativos que exigem um ambiente não virtualizado para licenciamento ou suporte

Para obter mais informações, consulte [Instâncias I3 do Amazon EC2](#).

Tópicos

- [Especificações de hardware \(p. 232\)](#)
- [Performance da instância \(p. 233\)](#)
- [Desempenho de rede \(p. 233\)](#)
- [Desempenho de E/S SSD \(p. 234\)](#)
- [Recursos das instâncias \(p. 235\)](#)
- [Suporte para vCPUs \(p. 235\)](#)
- [Notas de release \(p. 236\)](#)

Especificações de hardware

O armazenamento físico de dados primário para instâncias D2 são volumes de armazenamento de instâncias HDD. O armazenamento físico de dados primário para instâncias I3 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 ou encerra uma instância, os aplicativos 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 \(p. 958\)](#) e [Volumes de armazenamento de instâncias SSD \(p. 965\)](#).

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
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

Para obter mais informações sobre as especificações de hardware para cada tipo de instância do Amazon EC2, veja [Tipos de instâncias do Amazon EC2](#).

Para obter mais informações sobre como especificar opções de CPU, consulte [Otimizar opções de CPU \(p. 495\)](#).

Performance da instância

Para garantir o melhor desempenho 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 o desempenho máximo de IOPS disponível.

As instâncias D2 oferecem o melhor desempenho 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 [Amazon EBS – instâncias otimizadas \(p. 916\)](#).

Alguns tipos de instância otimizadas 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 o desempenho desejado (em frequência da CPU) de um núcleo. Para obter mais informações, consulte [Controle do estado do processo para sua instância do EC2 \(p. 485\)](#).

Desempenho de rede

Você pode habilitar recursos de rede aprimoradas em tipos de instância compatíveis. O uso avançado de rede fornece um desempenho significativamente maior de pacotes por segundo (PPS), menor jitter de rede e latências mais baixas. Para obter mais informações, consulte [Rede avançada no Linux \(p. 768\)](#).

Os tipos de instâncias que usam Elastic Network Adapter (ENA) para networking avançado fornecem alto desempenho de pacotes por segundo com latências consistentemente baixas. A maioria dos aplicativos não precisa de um alto nível de desempenho de rede constantemente, mas podem se beneficiar com uma largura de banda maior quando enviam ou recebem dados. Os tamanhos de instância que usam ENA e estão documentados com desempenho de rede de "Até 10 Gbps" ou "Até 25 Gbps" usam um mecanismo de crédito de E/S de rede para alocar largura de banda a instâncias baseadas na utilização média da largura de banda. Essas instâncias acumulam créditos quando a largura de banda da rede está abaixo dos limites de linha de base e podem usar esses créditos ao executar transferências de dados pela rede.

Este é um resumo da performance de rede para instâncias otimizadas para armazenamento que oferecem suporte às redes aprimoradas.

Tipo de instância	Desempenho das redes	Redes avançadas
i3.4xlarge e menor	Até 10 Gbps, usar mecanismo de crédito de E/S da rede	ENA (p. 769)
i3.8xlarge h1.8xlarge	10 Gbps	ENA (p. 769)

Tipo de instância	Desempenho das redes	Redes avançadas
i3.16xlarge i3.metal h1.16xlarge	25 Gbps	ENA (p. 769)
d2.xlarge	Moderada	Intel 82599 VF (p. 780)
d2.2xlarge d2.4xlarge	Alto	Intel 82599 VF (p. 780)
d2.8xlarge	10 Gbps	Intel 82599 VF (p. 780)

Desempenho de E/S 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 o desempenho de IOPS (tamanho de bloco de 4.096 bytes) na tabela a seguir (na saturação de profundidade de fila). Do contrário, você terá uma performance de IOPS inferior.

Tamanho de instância	100% de IOPS de leitura aleatória	IOPS de gravação
i3.large *	100,125	35,000
i3.xlarge *	206,250	70.000
i3.2xlarge	412,500	180.000
i3.4xlarge	825,000	360.000
i3.8xlarge	1,65 milhão	720.000
i3.16xlarge	3.3 milhões	1,4 milhão

* Para as instâncias i3.large e i3.xlarge, você pode obter o desempenho especificado.

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 no desempenho 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 um desempenho de E/S drasticamente reduzido.

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 o desempenho 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 o desempenho. Para obter mais informações, consulte [Suporte a TRIM do volume de armazenamento de instâncias \(p. 966\)](#).

Recursos das instâncias

Veja a seguir um resumo dos recursos para instâncias otimizadas de armazenamento:

	Somente EBS	Armazenamento de instâncias	Placement group
D2	Não	HDD	Sim
H1	Não	HDD	Sim
I3	Não	NVMe *	Sim

* O volume do dispositivo raiz deve ser um volume do Amazon EBS.

Para obter mais informações, consulte:

- [Amazon EBS e NVMe \(p. 929\)](#)
- [Armazenamento de instâncias do Amazon EC2 \(p. 958\)](#)
- [Placement groups \(p. 793\)](#)

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 \(HVM\)](#)
- [Amazon Linux AMI 2015.09 \(HVM\)](#)
- [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 seu aplicativo 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 Ações, Configurações da instância, 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 Ações, Configurações da instância, 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 Ações, Configurações da instância, 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 \(p. 94\)](#).
- Você deve executar instâncias I3 usando uma AMI baseada no Amazon EBS.
- Os seguintes são os requisitos das instâncias i3.metal:

As AMIs a seguir atendem a esses requisitos:

- Executar uma instância i3.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 EVS ou interfaces de rede secundárias de uma instância do i3.metal, é necessário ter suporte PCIe hotplug nativo. Amazon Linux 2 e as versões mais recentes do Amazon Linux AMI 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=`

- As instâncias `i3.metal` usam um dispositivo serial baseado em PCI em vez de um dispositivo serial baseado em porta de E/S. O kernel Linux principal e as AMIs Linux mais recentes da Amazon são compatíveis com este dispositivo. As instâncias `i3.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, `i3.metal` as instâncias 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 \(p. 235\)](#).
- 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?](#). Para solicitar um aumento do limite, use o [Formulário de solicitação de instâncias do Amazon EC2](#).

Linux Instâncias de computação acelerada

Se você precisar de alta capacidade de processamento, se beneficiará do uso das instâncias de computação acelerada que concedem acesso a aceleradores de computação com base em hardware como GPUs ou FPGAs. As instâncias de computação aceleradas permitem mais paralelismo para obter uma taxa de transferência maior em cargas de trabalho com alta quantidade de computação.

As instâncias baseadas em GPU concedem acesso a GPUs NVIDIA com milhares de núcleos de computação. Você pode usar instâncias de computação acelerada baseadas em GPU para acelerar aplicativos científicos, de engenharia e renderização utilizando as estruturas de computação paralela CUDA ou Open Computing Language (OpenCL). Você também pode usá-las para aplicativos gráficos, incluindo streaming de jogos, streaming de aplicativos 3-D e outras cargas de trabalho gráficas.

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 cargas de trabalho, como análise financeira, genômica, processamento de vídeo em tempo real, análise de big data e cargas de trabalho 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](#).

Important

As instâncias baseadas em FPGA não oferecem suporte ao Microsoft Windows.

Você pode agrupar as instâncias de computação acelerada em um placement group de cluster. Os placement groups de cluster fornecem baixa latência e alta conectividade de largura de banda entre as instâncias em uma única zona de disponibilidade. Para obter mais informações, consulte [Placement groups \(p. 793\)](#).

Tópicos

- [Famílias de instâncias de computação acelerada \(p. 238\)](#)
- [Especificações de hardware \(p. 239\)](#)
- [Performance da instância \(p. 240\)](#)

- Desempenho de rede (p. 240)
- Recursos das instâncias (p. 241)
- Notas de release (p. 241)
- AMIs para instâncias de computação acelerada baseadas em GPU (p. 242)
- Instalação do driver NVIDIA em instâncias Linux (p. 242)
- Ative os NVIDIA GRID Virtual Applications (somente instâncias G3) (p. 245)
- Otimização de configurações de GPU (instâncias P2, P3 e G3) (p. 246)
- Conceitos básicos do desenvolvimento da FPGA (p. 247)

Para obter informações sobre instâncias de computação acelerada Windows, consulte [Instâncias de computação acelerada Windows](#) no Guia do usuário do Amazon EC2 para instâncias do Windows.

Famílias de instâncias de computação acelerada

As famílias de 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. As seguintes famílias de instâncias de computação acelerada estão disponíveis para execução no Amazon EC2.

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, 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 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](#).

Instâncias P3

As instâncias P3 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 uma estrutura 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 cargas de trabalho 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 visualizar as informações de topologia do sistema, execute o comando a seguir:

```
nvidia-smi topo -m
```

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 cargas de trabalho de computação de GPU no lado do servidor.

As instâncias P2 oferecem suporte a transferências par a par NVIDIA GPUDirect.

Para visualizar as informações de topologia do sistema, execute o comando a seguir:

```
nvidia-smi topo -m
```

Para obter mais informações, consulte [NVIDIA GPUDirect](#).

Instâncias G3

As instâncias G3 usam GPUs NVIDIA Tesla M60 e fornecem uma plataforma de alto desempenho, econômica, para aplicativos gráficos 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 cargas de trabalho gráfico no lado do servidor, que exigem potência de processamento altamente paralela.

As instâncias G3 oferecem suporte a NVIDIA GRID Virtual Workstation e NVIDIA GRID Virtual Applications. Para ativar qualquer um desses recursos, consulte [Ative os NVIDIA GRID Virtual Applications \(somente instâncias G3\) \(p. 245\)](#).

Instâncias G2

As instâncias G2 usam GPUs NVIDIA GRID K520 e fornecem uma plataforma de alto desempenho, econômica, para aplicativos gráficos que utilizam DirectX ou OpenGL. Os GPUs NVIDIA GRID também oferecem suporte às operações de API de codificação e captura rápida NVIDIA. Os aplicativos de exemplo incluem serviços de criação de vídeo, visualizações 3D, aplicativos de uso intenso de gráfico de streaming e outras cargas de trabalho no lado do servidor.

Especificações de hardware

Este é um resumo das especificações de hardware para instâncias de computação acelerada.

Tipo de instância	vCPUs padrão	Memória (GiB)
p2.xlarge	4	61
p2.8xlarge	32	488
p2.16xlarge	64	732
p3.2xlarge	8	61
p3.8xlarge	32	244
p3.16xlarge	64	488

Tipo de instância	vCPUs padrão	Memória (GiB)
p3dn.24xlarge	96	768
g2.2xlarge	8	15
g2.8xlarge	32	60
g3s.xlarge	4	30.5
g3.4xlarge	16	122
g3.8xlarge	32	244
g3.16xlarge	64	488
f1.2xlarge	8	122
f1.4xlarge	16	244
f1.16xlarge	64	976

Para obter mais informações sobre as especificações de hardware para cada tipo de instância do Amazon EC2, veja [Tipos de instâncias do Amazon EC2](#).

Para obter mais informações sobre como especificar opções de CPU, consulte [Otimizar opções de CPU \(p. 495\)](#).

Performance da instância

Há várias otimizações de configuração de GPU que você pode executar para obter melhor desempenho em suas instâncias. Para obter mais informações, consulte [Otimização de configurações de GPU \(Instâncias P2, P3 e G3\) \(p. 246\)](#).

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 [Amazon EBS – instâncias otimizadas \(p. 916\)](#).

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 o desempenho desejado (em frequência da CPU) de um núcleo. Para obter mais informações, consulte [Controle do estado do processo para sua instância do EC2 \(p. 485\)](#).

Desempenho de rede

Você pode habilitar recursos de rede aprimoradas em tipos de instância compatíveis. O uso avançado de rede fornece um desempenho significativamente maior de pacotes por segundo (PPS), menor jitter de rede e latências mais baixas. Para obter mais informações, consulte [Rede avançada no Linux \(p. 768\)](#).

Os tipos de instâncias que usam Elastic Network Adapter (ENA) para networking avançado fornecem alto desempenho de pacotes por segundo com latências consistentemente baixas. A maioria dos aplicativos não precisa de um alto nível de desempenho de rede constantemente, mas podem se beneficiar com uma largura de banda maior quando enviam ou recebem dados. Os tamanhos de instância que usam ENA e estão documentados com desempenho de rede de "Até 10 Gbps" ou "Até 25 Gbps" usam um mecanismo de crédito de E/S de rede para alocar largura de banda a instâncias baseadas na utilização média da largura de banda. Essas instâncias acumulam créditos quando a largura de banda da rede está abaixo dos limites de linha de base e podem usar esses créditos ao executar transferências de dados pela rede.

Este é um resumo da performance de rede para instâncias de computação acelerada que oferecem suporte às redes aprimoradas.

Tipo de instância	Desempenho das redes	Redes avançadas
f1.2xlarge f1.4xlarge g3.4xlarge p3.2xlarge	Até 10 Gbps	ENA (p. 769)
g3s.xlarge g3.8xlarge p2.8xlarge p3.8xlarge	10 Gbps	ENA (p. 769)
f1.16xlarge g3.16.xlarge g3.16.xlarge p2.16xlarge p3.16xlarge	25 Gbps	ENA (p. 769)
p3dn.24xlarge	100 Gbps	ENA (p. 769)

Recursos das instâncias

Este é um resumo de recursos para instâncias de computação acelerada.

	Somente EBS	EBS de NVMe	Armazenamento de instâncias	Placement group
G2	Não	Não	SSD	Sim
G3	Sim	Não	Não	Sim
P2	Sim	Não	Não	Sim
P3	p3dn.24xlarge: não Todos os outros tamanhos: sim	p3dn.24xlarge: sim Todos os outros tamanhos: não	p3dn.24xlarge: NVMe *	Sim
F1	Não	Não	NVMe *	Sim

* O volume do dispositivo raiz deve ser um volume do Amazon EBS.

Para obter mais informações, consulte:

- [Amazon EBS e NVMe \(p. 929\)](#)
- [Armazenamento de instâncias do Amazon EC2 \(p. 958\)](#)
- [Placement groups \(p. 793\)](#)

Notas de release

- Você deve executar a instância usando uma AMI de HVM.
- As instâncias baseadas em GPU não podem acessar a GPU, a menos que os drivers NVIDIA sejam instalados.
- Há um limite de 100 AFIs por região.
- Há um limite em relação à quantidade de instâncias que você pode executar. Para obter mais informações, consulte [Quantas instâncias posso executar no Amazon EC2?](#) nas perguntas frequentes

do Amazon EC2. Para solicitar um aumento desses limites, use o seguinte formulário: [Solicitação para aumentar o limite de instâncias do Amazon EC2](#).

AMIs para instâncias de computação acelerada baseadas em GPU

Para ajudá-lo a começar, a NVIDIA e outros fornecem AMIs para instâncias de computação acelerada baseadas em GPU. Essas AMIs de referência incluem o driver NVIDIA, que permite a funcionalidade e o desempenho completos de GPUs NVIDIA.

Para obter uma lista de AMIs com o driver NVIDIA, pesquise o AWS Marketplace da seguinte maneira:

- [NVIDIA P3 AMIs](#)
- [NVIDIA P2 AMIs](#)
- [NVIDIA GRID G3 AMIs](#)
- [NVIDIA GRID G2 AMIs](#)

Você pode executar instâncias de computação acelerada usando qualquer AMI de HVM.

Important

Essas AMIs incluem drivers, softwares ou toolkits desenvolvidos, propriedades da NVIDIA Corporation ou fornecidos por ela. Ao usar essas AMIs, você concorda em usar esses drivers, softwares ou toolkits NVIDIA apenas em instâncias do Amazon EC2 que incluam hardware NVIDIA.

Você também pode instalar o driver NVIDIA manualmente. Para obter mais informações, consulte [Instalação do driver NVIDIA em instâncias Linux \(p. 242\)](#).

Instalação do driver NVIDIA em instâncias Linux

Uma instância de computação acelerada baseada em GPU deve ter o driver NVIDIA apropriado. O driver NVIDIA que você instalar deve ser compilado com o kernel que você planeja executar em sua instância.

A Amazon fornece AMIs com builds atualizadas e compatíveis dos drivers de kernel NVIDIA para cada atualização oficial de kernel no AWS Marketplace. Se você decidir usar uma versão do driver NVIDIA diferente da oferecida pela Amazon ou decidir usar um kernel que não seja uma build oficial da Amazon, deverá desinstalar os pacotes NVIDIA fornecidos pela Amazon de seu sistema para evitar conflitos com as versões dos drivers que você está tentando instalar.

Use este comando para desinstalar os pacotes NVIDIA fornecidos pela Amazon:

```
[ec2-user ~]$ sudo yum erase nvidia cuda
```

O pacote de toolkit CUDA fornecido pela Amazon 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.

Fazer download do driver NVIDIA GRID (G3)

Para instâncias G3, você pode fazer download do driver NVIDIA GRID a partir do Amazon S3 usando a AWS CLI ou SDKs. Para instalar a AWS CLI, consulte [Instalação do AWS Command Line Interface](#) no Guia do usuário do AWS Command Line Interface.

Important

Esse download só está disponível para os clientes da AWS. Ao fazer download, você concorda que usará o software baixado somente para desenvolver AMIs para uso com o hardware NVIDIA Tesla M60. Após a instalação do software, você estará vinculado aos termos do [Contrato de licença de usuário final do NVIDIA GRID Cloud](#).

Use o comando da AWS CLI a seguir para fazer download do driver mais recente:

```
[ec2-user ~]$ aws s3 cp --recursive s3://ec2-linux-nvidia-drivers/latest/ .
```

Várias versões de driver NVIDIA GRID são armazenadas nesse bucket. Você pode visualizar todas as versões disponíveis com o seguinte comando:

```
[ec2-user ~]$ aws s3 ls --recursive s3://ec2-linux-nvidia-drivers/
```

Se você receber um erro `Unable to locate credentials`, a AWS CLI na instância não estará configurada para usar suas credenciais da AWS. Para configurar a AWS CLI para usar suas credenciais da AWS, consulte [Configuração rápida](#) no Guia do usuário do AWS Command Line Interface.

Fazer download de um driver NVIDIA público (G2, P2, P3)

Para tipos de instância diferentes de G3 ou se você não estiver usando a funcionalidade do NVIDIA GRID em uma instância G3, poderá fazer download de drivers NVIDIA públicos.

Faça o download do driver NVIDIA de 64 bits apropriado para seu tipo de instância a partir de <http://www.nvidia.com/Download/Find.aspx>.

Instâncias	Tipo de produto	Séries de produtos	Produto
G2	GRID	Série GRID	GRID K520
P2	Tesla	K-Series	K-80
P3	Tesla	V-Series	V100

Para obter mais informações sobre a instalação e a configuração do driver, selecione a guia INFORMAÇÕES ADICIONAIS na página de download no driver no site da NVIDIA e escolha o link LEIAIME.

Instalação manual do driver NVIDIA

Se estiver usando uma AMI que não tenha o driver NVIDIA necessário, você poderá instalar o driver em sua instância.

Para instalar o driver NVIDIA

1. Atualize o cache de pacotes e obtenha as atualizações necessárias de pacotes para sua instância.

- Para 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
```

2. (Ubuntu 16.04 e posterior, com o pacote `linux-aws`) Atualize o pacote `linux-aws` para receber a versão mais recente.

```
[ec2-user ~]$ sudo apt-get upgrade -y linux-aws
```

3. Reinicialize sua instância para carregar a versão mais recente do kernel.

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

4. Reconecte-se à sua instância depois de reinicializá-la.
5. 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:

```
[ec2-user ~]$ sudo apt-get install -y gcc make linux-headers-$(uname -r)
```

6. Desabilite o driver de código aberto `nouveau` para placas gráficas NVIDIA.

- a. Adicione o `nouveau` ao arquivo de lista negra `/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:

```
[ec2-user ~]$ sudo update-grub
```

7. Faça download do pacote de drivers que você identificou anteriormente, da seguinte maneira.

- Para instâncias P2 e P3, o seguinte comando faz download da versão 367.106 do driver NVIDIA, em que `xxx.xxx` representa a versão do driver NVIDIA.

```
[ec2-user ~]$ wget http://us.download.nvidia.com/tesla/xxx.xxx/NVIDIA-Linux-
x86_64-xxx.xxx.run
```

- Para instâncias G2, o seguinte comando faz download da versão 367.106 do driver NVIDIA, em que `xxx.xxx` representa a versão do driver NVIDIA.

```
[ec2-user ~]$ wget http://us.download.nvidia.com/XFree86/Linux-x86_64/xxx.xxx/NVIDIA-Linux-x86_64-xxx.xxx.run
```

- Para instâncias G3, você pode fazer download do driver do Amazon S3 usando a AWS CLI ou SDKs. Para instalar a AWS CLI, consulte [Instalação do AWS Command Line Interface](#) no Guia do usuário do AWS Command Line Interface. Use o comando da AWS CLI a seguir para fazer download do driver mais recente:

```
[ec2-user ~]$ aws s3 cp --recursive s3://ec2-linux-nvidia-drivers/latest/ .
```

Important

Esse download só está disponível para os clientes da AWS. Ao fazer download, você concorda que usará o software baixado somente para desenvolver AMIs para uso com o hardware NVIDIA Tesla M60. Após a instalação do software, você estará vinculado aos termos do [Contrato de licença de usuário final do NVIDIA GRID Cloud](#).

Várias versões de driver NVIDIA GRID são armazenadas nesse bucket. Você pode visualizar todas as versões disponíveis com o seguinte comando:

```
[ec2-user ~]$ aws s3 ls --recursive s3://ec2-linux-nvidia-drivers/
```

8. Execute o script de autoinstalação para instalar o driver NVIDIA do qual você fez download na etapa anterior. 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).

9. Reinicialize a instância.

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

10. Verifique se o driver está funcionando. A resposta para o comando a seguir lista a versão do driver NVIDIA instalado e os detalhes sobre as GPUs.

Note

Esse comando pode levar alguns minutos para ser executado.

```
[ec2-user ~]$ nvidia-smi -q | head
```

11. [Apenas instâncias G3] Para habilitar os NVIDIA GRID Virtual Applications em uma instância G3, siga as etapas de ativação do GRID em [Ative os NVIDIA GRID Virtual Applications \(somente instâncias G3\) \(p. 245\)](#) (a NVIDIA GRID Virtual Workstation é habilitada por padrão).
12. (Instâncias P2, P3 e G3) Conclua as etapas de otimização em [Otimização de configurações de GPU \(instâncias P2, P3 e G3\) \(p. 246\)](#) para obter o melhor desempenho de sua GPU.

Ative os NVIDIA GRID Virtual Applications (somente instâncias G3)

Para ativar GRID Virtual Applications em instâncias G3 (a NVIDIA GRID Virtual Workstation é habilitada por padrão), você deve definir o tipo de produto para o driver no arquivo `/etc/nvidia/gridd.conf`.

Para ativar os GRID Virtual Applications em instâncias G3 Linux

1. Crie o arquivo /etc/nvidia/gridd.conf 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
```

Otimização de configurações de GPU (instâncias P2, P3 e G3)

Há várias otimizações de configuração de GPU que você pode executar para obter melhor desempenho em instâncias P2, P3 e G3. Por padrão, o driver NVIDIA usa um recurso de autobost, que varia as velocidades do relógio de GPU. Ao desativar o recurso de autobost e definir as velocidades de relógio de GPU como a frequência máxima, você pode atingir o desempenho máximo 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 autobost e definir as velocidades do relógio 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. Desabilite o recurso de autobost para todas as GPUs na instância.

```
[ec2-user ~]$ sudo nvidia-smi --auto-boost-default=0
```

Note

As GPUs em instâncias P3 não são compatíveis com autobost.

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.

Note

Algumas versões do driver NVIDIA não permitem definir a velocidade do relógio do aplicativo e lançam um erro "Setting applications clocks is not supported for GPU ...", que você pode ignorar.

- Instâncias P2:

```
[ec2-user ~]$ sudo nvidia-smi -ac 2505,875
```

- Instâncias P3:

```
[ec2-user ~]$ sudo nvidia-smi -ac 877,1530
```

- Instâncias G3:

```
[ec2-user ~]$ sudo nvidia-smi -ac 2505,1177
```

Conceitos básicos do desenvolvimento da FPGA

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 da AWS FPGA](#).

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). Nesse caso, você pode alterar o tamanho da instância. Por exemplo, se a instância `t2.micro` for muito pequena para sua carga de trabalho, você poderá alterá-la para outra tipo de instância apropriado para a carga de trabalho.

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 o dispositivo raiz da instância estiver em um volume do EBS, você poderá alterar o tamanho da instância simplesmente alterando o tipo de instância, o que é conhecido como redimensionamento. Se o dispositivo raiz da instância estiver em um volume de armazenamento de instâncias, você deverá migrar o aplicativo para uma nova instância com o tipo de instância necessário. Para obter mais informações sobre volumes de dispositivos raiz, consulte [Armazenamento para o dispositivo raiz \(p. 91\)](#).

Quando redimensiona uma instância, 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 o aplicativo para uma nova instância com o tipo de instância de que você precisa.

Important

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 seu aplicativo 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.

Tópicos

- [Compatibilidade para redimensionamento de instâncias \(p. 248\)](#)
- [Como redimensionar uma instância com suporte do Amazon EBS \(p. 248\)](#)
- [Como migrar uma instância com suporte de armazenamento de instâncias \(p. 250\)](#)
- [Como migrar para uma nova configuração de instância \(p. 250\)](#)

Compatibilidade para redimensionamento de instâncias

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 \(p. 94\)](#). 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:
 - As instâncias A1 são as únicas instâncias que oferecem suporte a processadores com base na arquitetura do Arm. 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.
 - 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 [Migração de uma Instância do Linux no EC2-Classic para uma Instância do Linux em uma VPC \(p. 826\)](#).
- Redes aprimoradas: tipos de instância que dão suporte a [redes aprimoradas \(p. 768\)](#) exigem os drivers necessários instalados. Por exemplo, os tipos de instância A1, C5, C5d, C5n, M5, M5a, M5d, p3dn.24xlarge, R5, R5a, R5d, T3 e z1d precisam de AMIs baseadas no EBS com os drivers Elastic Network Adapter (ENA) instalados. Para redimensionar uma instância existente para um tipo de instância que ofereça suporte a redes aprimoradas, você deverá primeiro instalar os [drivers ENA \(p. 769\)](#) ou [drivers ixgbevf \(p. 780\)](#) na instância, conforme apropriado.
- NVMe: os volumes do EBS são expostos como dispositivos de blocos NVMe em [Instâncias baseadas em Nitro \(p. 179\)](#). 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 \(p. 929\)](#) 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 \(p. 182\)](#)
 - [Instâncias otimizadas para computação \(p. 219\)](#)
 - [Instâncias otimizadas para memória \(p. 223\)](#)
 - [Instâncias otimizadas para armazenamento \(p. 231\)](#)

Como redimensionar uma instância com suporte do Amazon EBS

Você deve interromper sua instância com suporte do 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.
- 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. 793) 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 inicialização do aplicativo.

Para obter mais informações, consulte [Interrompa e inicie sua instância](#) (p. 458).

Use o procedimento a seguir para redimensionar uma instância com suporte do Amazon EBS usando o Console de gerenciamento da AWS.

Para redimensionar uma instância com suporte do 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 redimensionamento de instâncias](#) (p. 248).
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 desabilitada 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 redimensionamento de instâncias](#) (p. 248).
 - b. (Opcional) Se o tipo de instância selecionado oferecer suporte a otimização para EBS, selecione EBS-optimized ou cancele a seleção de EBS-optimized para desabilitar 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 de alterar o tipo?](#)

Como migrar uma instância com suporte de armazenamento de instâncias

Quando desejar mover seu aplicativo de uma instância com suporte de armazenamento de instâncias para uma instância com suporte de armazenamento de instâncias com outro tipo de instância, você deve migrá-la criando uma imagem da instância e executando uma nova instância a partir dessa imagem com o tipo de instância necessário. Para garantir que os usuários possam continuar usando os aplicativos 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.

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 [Criação de um snapshot do Amazon EBS \(p. 898\)](#)) ou desanexe o volume da instância para que você possa anexá-lo à nova instância mais tarde (consulte [Separação de um volume do Amazon EBS de uma instância \(p. 893\)](#)).
2. Crie uma AMI de sua instância com suporte do armazenamento de instâncias atendendo aos pré-requisitos e seguindo os procedimentos em [Criação de uma AMI em Linux com armazenamento de instâncias \(p. 115\)](#). 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).

Como 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 seu aplicativo 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:

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 [Criação de um snapshot do Amazon EBS \(p. 898\)](#)) ou desanexe o volume da instância para que você possa anexá-lo à nova instância mais tarde (consulte [Separação de um volume do Amazon EBS de uma instância \(p. 893\)](#)).

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 o aplicativo 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, selecione Elastic IPs (IPs elásticos).
 - 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).

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 on-demand – pague por segundo pelas instâncias executadas.
- Instâncias reservadas – compre com um desconto significativo instâncias que estão sempre disponíveis por um período de vigência de um a três anos.
- Scheduled Instances (Instâncias programadas) – compre instâncias que estão sempre disponíveis na programação recorrente especificada por um período de vigência de um ano.
- Instâncias spot – solicite instâncias do EC2 não utilizadas, o que pode reduzir significativamente seus custos do Amazon EC2.
- 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.
- Instâncias dedicadas – pague por hora pelas instâncias que são executadas no hardware de um único locatário.
- Reserva de capacidades – 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 ou compre instâncias programadas. As Instâncias

spot são uma opção econômica, se você tiver flexibilidade sobre quando executar aplicativos e se eles puderem ser interrompidos. Os Hosts dedicados ou Instâncias dedicadas podem ajudar a resolver os requisitos de conformidade e reduzir custos usando suas licenças de software existentes associadas ao servidor. Para obter mais informações, consulte [Definição de preço do Amazon EC2](#).

Tópicos

- [Determinação do ciclo de vida da instância \(p. 252\)](#)
- [Instâncias reservadas \(p. 253\)](#)
- [Instâncias reservadas programadas \(p. 289\)](#)
- [Instâncias spot \(p. 293\)](#)
- [Hosts dedicados \(p. 356\)](#)
- [Instâncias dedicadas \(p. 371\)](#)
- [Reservas de capacidade sob demanda \(p. 376\)](#)

Determinação do 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. Você pode executar uma instância programada durante o período programado; o Amazon EC2 executa as instâncias e as encerra três minutos antes do término do período de inatividade.

Use o seguinte procedimento para determinar o ciclo de vida de uma instância.

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 scheduled, a instância será programada. 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 \(p. 1015\)](#).

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"
```

Se a instância for programada, o resultado conterá as seguintes informações:

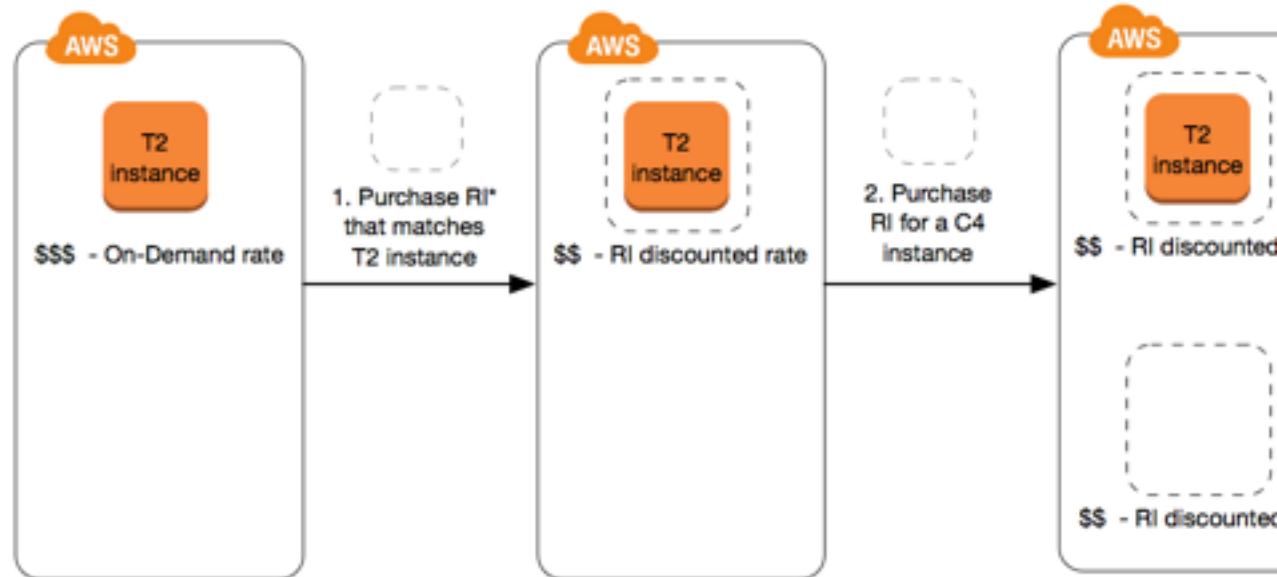
```
"InstanceLifecycle": "scheduled"
```

Caso contrário, o resultado não conterá `InstanceLifecycle`.

Instâncias reservadas

As Instâncias reservadas fornecem um desconto significativo em comparação com a definição de preço de instância sob demanda. As Instâncias reservadas não são instâncias físicas, mas um desconto de faturamento aplicado ao uso de Instâncias on-demand na conta. Essas Instâncias on-demand devem corresponder a determinados atributos para se beneficiar do desconto de faturamento.

O diagrama a seguir mostra uma visão geral básica da compra e do uso das Instâncias reservadas.



*RI = Reserved Instance

Neste cenário, você tem um实例 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.

Ao adquirir a Instância reservada, escolha uma combinação das seguintes alternativas que atendam às suas necessidades:

- Opção de pagamento: sem adiantamento, adiantamento parcial ou adiantamento total.
- Vigência: um ano ou três anos. Um ano é definido como 31536000 segundos (365 dias). Três anos é definido como 94608000 segundos (1095 dias).
- Classe da oferta: conversível ou padrão.

Além disso, uma Instância reservada tem uma série de atributos que determinam como ela é aplicada a uma instância em execução na sua conta:

- Tipo de instância: Por exemplo, `m4.large`. Isso é composto pela família de instâncias (`m4`) e pelo tamanho da instância (grande).
- Escopo: se a Instância reservada se aplica a uma região ou a uma zona de disponibilidade específica.
- Locação: Se sua instância é executada em hardware compartilhado (padrão) ou com grupo de usuários único (dedicado). Para obter mais informações, consulte [Instâncias dedicadas \(p. 371\)](#).
- Plataforma: O sistema operacional; por exemplo, Windows ou Linux/Unix. Para obter mais informações, consulte [Como escolher uma plataforma \(p. 265\)](#).

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.

Após adquirir uma Instância reservada, você não poderá cancelar a compra. Contudo, você poderá [modificar \(p. 278\)](#), [trocar \(p. 285\)](#) ou [vender \(p. 271\)](#) a Instância reservada caso suas necessidades mudem.

Opções de pagamento

As opções de pagamento a seguir estão disponíveis para as Instâncias reservadas.

- Sem pagamento adiantado – é cobrado de você a tarifa por hora com desconto para cada hora do período, independente de a Instância reservada estar sendo usada ou não. 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.

- Adiantamento parcial – parte do custo deve ser paga com adiantamento, 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.
- 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.

Em linhas gerais, você pode economizar mais escolhendo Instâncias reservadas com um pagamento adiantado maior. 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 [Venda no Marketplace de instâncias reservadas \(p. 271\)](#).

Para obter mais informações sobre a definição de preços, consulte [Definição de preço de instâncias reservadas do Amazon EC2](#).

Limites da 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 \(p. 257\)](#) por mês além de um adicional de 20 Instâncias reservadas [zonais \(p. 256\)](#) 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.

Note

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: um 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 [Visualizando seus limites atuais. \(p. 1013\)](#).

Tipos de Instâncias reservadas (classes de oferta)

Ao adquirir uma Instância reservada, você pode escolher entre uma classe de oferta padrão ou conversível. A Instância reservada se aplica a uma única família de instâncias, plataforma, escopo e locação ao longo de um período de vigência. Se sua computação precisar de uma mudança, você talvez consiga modificar ou trocar a Instância reservada, dependendo da classe de oferta. As classes de oferta podem ter também restrições ou limitações adicionais.

A seguir estão as diferenças entre as classes de oferta padrão e conversível.

Instância reservada padrão	Instância reservada convertível
Alguns atributos, como o tamanho da instância, podem ser modificados durante o período de vigência; contudo, o tipo de instância não pode ser modificado. Você não pode trocar uma Instância reservada padrão, mas apenas modificá-la. Para obter mais informações, consulte Modificar Instâncias reservadas (p. 278) .	Pode ser trocada durante o período de vigência por outra Instância reservada convertível com novos atributos, incluindo a família de instâncias, o tipo de instância, a plataforma, o escopo ou a locação. Para obter mais informações, consulte Trocar Instâncias reservadas conversíveis (p. 285) . Você também pode modificar alguns atributos de uma Instância reservada convertível. Para obter mais informações, consulte Modificar Instâncias reservadas (p. 278) .

Instância reservada padrão	Instância reservada convertível
Pode ser vendida no Marketplace de instâncias reservadas.	Não pode ser vendida no Marketplace de instâncias reservadas.

Padrão e Instâncias reservadas conversíveis podem ser adquiridas para serem aplicadas a instâncias em uma zona de disponibilidade específica ou a instâncias em uma região.

Note

- Quando você adquire uma Instância reservada para uma zona de disponibilidade específica, ela é conhecida como uma Instância reservada zonal. Uma Instância reservada zonal fornece uma reserva de capacidade. Para obter mais informações, consulte [Como as Instâncias reservadas zonais são aplicadas \(p. 256\)](#).
- Quando você adquire uma Instância reservada para uma região, ela é conhecida como uma Instância reservada regional. Uma Instância reservada regional não fornece uma reserva de capacidade. Para obter mais informações, consulte [Como as Instâncias reservadas regionais são aplicadas \(p. 257\)](#).

As Instâncias reservadas regionais têm os seguintes atributos:

- Flexibilidade da zona de disponibilidade: o desconto da Instância reservada se aplica ao uso da instância em qualquer zona de disponibilidade em uma região.
- Flexibilidade do tamanho da instância: o desconto da Instância reservada aplica-se ao uso da instância, independentemente do tamanho, dentro dessa família de instâncias. Compatível somente com Instâncias reservadas Linux/Unix com locação padrão.

Para obter mais informações e exemplos, consulte [Como as Instâncias reservadas são aplicadas \(p. 256\)](#).

Se você deseja comprar reservas de capacidade que se repetem diária, semanal ou mensalmente, talvez uma Instância reservada programada atenda às suas necessidades. Para obter mais informações, consulte [Instâncias reservadas programadas \(p. 289\)](#).

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 [Usar as Instâncias reservadas \(p. 270\)](#).

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 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 adquiridas para uma região (Instâncias reservadas regionais) 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 na plataforma Linux/Unix com locação padrão também fornecem flexibilidade de tamanho de instância, em que o desconto da Instância reservada se aplica ao uso da instância nesse tipo de instância, independentemente do tamanho.

Note

A flexibilidade de tamanho de instância não se aplica a Instâncias reservadas adquiridas para uma zona de disponibilidade específica, instâncias bare metal, Instâncias reservadas com locação dedicada e Instâncias reservadas do Windows, do Windows com SQL Standard, do Windows com SQL Server Enterprise, do Windows com SQL Server Web, do RHEL e do SLES.

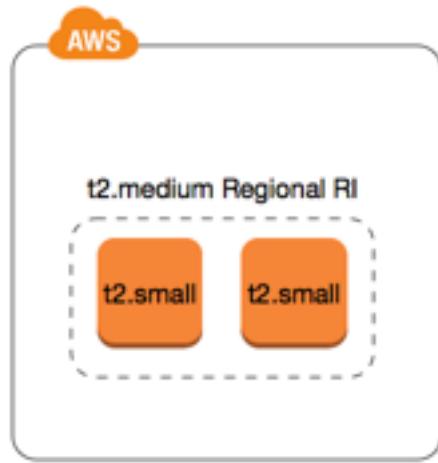
A flexibilidade de tamanho da instância é determinada pelo fator de normalização do tamanho da instância. O desconto se aplica total ou parcialmente às instâncias em execução do mesmo tipo, dependendo do tamanho da instância de reserva, em qualquer zona de disponibilidade na região. Os únicos atributos que devem ser combinados são tipo de instância, locação e plataforma.

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.

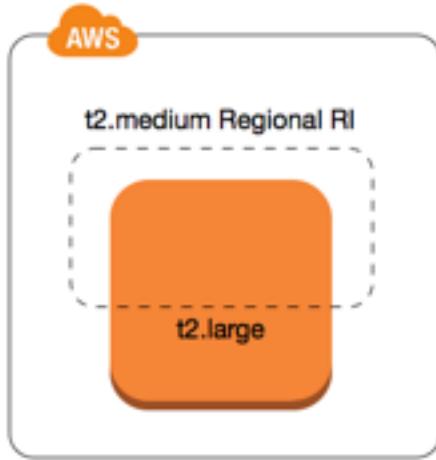
A tabela a seguir descreve os tipos diferentes dentro de um tipo de instância e o fator de normalização correspondente por hora. Essa escala é usada para aplicar a taxa de desconto de Instâncias reservadas ao uso normalizado do tipo de instância.

Tamanho da instância	Fator de normalização
nano	0,25
micro	0,5
pequeno	1
médio	2
grande	4
xlarge	8
2xlarge	16
4xlarge	32
8xlarge	64
9xlarge	72
10xlarge	80
12xlarge	96
16xlarge	128
18xlarge	144
24xlarge	192
32xlarge	256

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 Leste dos EUA (Norte da Virgínia) 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 Leste dos EUA (Norte da Virgínia) o benefício de faturamento será aplicado a 50% do uso da instância.



Note

O fator de normalização é aplicado também ao modificar Instâncias reservadas. Para obter mais informações, consulte [Modificar Instâncias reservadas \(p. 278\)](#).

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 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 \(p. 262\)](#). 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 as seguintes 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** na conta A e a instância **m4.2xlarge** na conta A. As três instâncias correspondem aos atributos (família de instâncias, região, plataforma, locação). Não há reserva de capacidade.
- 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.

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](#).

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 \(p. 254\)](#) especificada para a Instância reservada.

Quando as Instâncias reservadas expirarem, serão cobradas taxas sob demanda pelo uso da instância do EC2. Você pode configurar um alerta de pagamento para adverti-lo quando sua conta ultrapassar um limite definido. Para obter mais informações, consulte [Como monitorar as cobranças com alertas e notificações](#) no Guia do usuário do AWS Billing and Cost Management.

Note

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 mais informações, consulte [Nível gratuito da AWS](#).

Tópicos

- [Faturamento do uso \(p. 261\)](#)
- [Como visualizar sua fatura \(p. 262\)](#)
- [Instâncias reservadas e Faturamento consolidado \(p. 262\)](#)
- [Camadas de preço com desconto da Instância reservada \(p. 262\)](#)

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. Uma hora-relógio é definida como um relógio padrão de 24 horas, que vai da meia-noite até a meia-noite, e é dividida em 24 horas (por exemplo, 1:00:00 a 1:59:59 é uma hora-relógio). Para obter mais informações sobre os estados da instância, consulte [Ciclo de vida da instância \(p. 385\)](#).

Um dos benefícios de faturamento da Instância reservada é aplicado a uma instância em execução com base em uma taxa por segundo. Um dos benefícios de faturamento da Instância reservada pode ser aplicado a um máximo de 3600 segundos (uma hora) de uso de instância por hora fechada. Você pode executar várias instâncias simultaneamente, mas só receber o benefício do desconto da Instância reservada por um total de 3600 segundos por hora fechada; um uso de instância que ultrapasse 3600 segundos em uma hora fechada será cobrado 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` de 15 minutos (900 segundos) cada na 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	Orange			
Instance 2		Orange		
Instance 3			Orange	
Instance 4				Orange

Se várias instâncias qualificadas estiverem sendo executadas simultaneamente, o benefício de faturamento da Instância reservada será aplicado a todas as instâncias ao mesmo tempo até um máximo de 3600 segundos em uma hora fechada; 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.

Como 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 rastrear a utilização da Instância reservada usando o Relatório de uso e de custo da AWS. Para obter mais informações, consulte [Instâncias reservadas](#) em Relatório de uso e de custo no Guia 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 de 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 e AWS Organizations](#) no Guia do usuário do AWS Organizations.

Se você fechar a conta do pagante, todas as contas de membros que se beneficiarem dos descontos no faturamento das Instâncias reservadas continuarão a se beneficiar com o desconto até que as Instâncias reservadas expirem ou até que a conta do membro seja removida.

Camadas 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 da Instância reservada \(p. 263\)](#)
- [Compra com nível de desconto \(p. 264\)](#)
- [Cruzamento de níveis de preços \(p. 264\)](#)
- [Faturamento consolidado para camadas de preços \(p. 264\)](#)

[Calcular descontos de preço da 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) listado na [página de definição de preço das Instâncias reservadas](#) 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)
```

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. Exiba a coluna Upfront Price escolhendo Show/Hide Columns (o ícone com formato de engrenagem) no canto superior direito.

Para ver os valores de preço fixo das Instâncias reservadas usando a linha de comando

- [describe-reserved-instances](#) (AWS CLI)
- [Get-EC2ReservedInstance](#) (AWS Tools para Windows PowerShell)
- [DescribeReservedInstances](#) (API do Amazon EC2)

Compra 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 \(p. 264\)](#).

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 preços \(p. 264\)](#).

Se o valor de tabela ficar abaixo do ponto de preço desse nível de definição de preço com desconto — por exemplo, se algumas das Instâncias reservadas expirarem — as futuras compras de Instâncias reservadas na região não receberão desconto. Contudo, você continua a receber o desconto aplicado em todas as Instâncias reservadas originalmente compradas no nível de preço com desconto.

Estes são os quatro cenários possíveis durante a compra de Instâncias reservadas:

- Sem desconto — sua compra em uma região ainda está abaixo do limite para desconto.
- Desconto parcial — sua compra em uma região ultrapassa o limite do primeiro nível de desconto. Nenhum desconto é aplicado a uma ou mais reservas e a taxa com desconto é aplicada nas reservas restantes.
- Desconto total — sua compra inteira em uma região cai em um nível de desconto e recebe o desconto apropriado.
- Duas taxas com desconto — sua compra em uma região ultrapassa um nível inferior de desconto para um nível superior de desconto. Serão cobradas duas taxas diferentes: uma ou mais reservas na taxa desconto inferior e as reservas restantes com a taxa desconto maior.

Cruzamento de níveis de preços

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 camadas de preços

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 \(p. 262\)](#).

Comprar Instâncias reservadas

Para comprar uma Instância reservada, pesquise por ofertas de Instância reservada na AWS e em vendedores terceirizados, ajustando os parâmetros de pesquisa até encontrar a correspondência exata que está procurando.

Quando você procurar Instâncias reservadas para comprar, receberá um orçamento do custo das ofertas apresentadas. Ao dar continuidade à compra, a AWS colocará automaticamente um preço-limite sobre o preço de compra. O custo total das suas Instâncias reservadas não excederá o valor orçado.

Se o preço aumentar ou mudar por algum motivo, a compra não será concluída. Se, no momento da compra, houver ofertas semelhantes à sua escolha, mas por um preço menor, a AWS venderá as ofertas a preços mais baixos.

Antes de confirmar sua compra, analise os detalhes da Instância reservada que planeja comprar e verifique se todos os parâmetros são precisos. Após adquirir uma Instância reservada (do vendedor terceirizado no Marketplace de instâncias reservadas ou da AWS), você não poderá cancelar sua compra.

Note

Para comprar e modificar instâncias reservadas, assegure-se de que sua conta de usuário na IAM tenha as permissões apropriadas, como capacidade de descrever zonas de disponibilidade.

Para informações, consulte [Políticas de exemplo para trabalhar com a CLI da AWS ou um SDK da AWS](#) e [Políticas de exemplo para trabalhar no console Amazon EC2](#).

Tópicos

- [Como escolher uma plataforma \(p. 265\)](#)
- [Comprar Instâncias reservadas padrão \(p. 265\)](#)
- [Comprar Instâncias reservadas conversíveis \(p. 268\)](#)
- [Visualizar as Instâncias reservadas \(p. 270\)](#)
- [Usar as Instâncias reservadas \(p. 270\)](#)

Como escolher uma plataforma

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, você deve escolher ofertas específicas para essas plataformas. Para todas as demais distribuições do Linux (incluindo Ubuntu), escolha uma oferta para a plataforma Linux/UNIX.

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;

Para comprar Instâncias reservadas padrão 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, Comprar Instâncias reservadas.
3. Para Classe da oferta, escolha 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.

Note

Para comprar uma Instância reservada padrão no Marketplace de instâncias reservadas, procure por 3rd Party na coluna Seller dos resultados de pesquisa. A coluna Termo exibe os termos não padrão.

6. Selecione as Instâncias reservadas a serem compradas, informe a quantidade e escolha Adicionar ao carrinho.
7. Para ver um resumo das Instâncias reservadas selecionadas, escolha View Cart.
8. Para concluir o pedido, escolha Comprar.

Note

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.

9. O status de sua compra está listado na coluna 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-instance-offerings`. Especifique `standard` para o parâmetro `--offering-class` apresentar somente Instâncias reservadas padrão. 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` por um prazo de somente 1 ano:

```
aws ec2 describe-reserved-instances-offerings --instance-type t2.large --offering-class standard --product-description "Linux/UNIX" --instance-tenancy default --filters Name=duration,Values=31536000 Name=scope,Values=Region
```

```
{  
    "ReservedInstancesOfferings": [  
        {  
            "OfferingClass": "standard",  
            "OfferingType": "No Upfront",  
            "ProductDescription": "Linux/UNIX",  
            "InstanceTenancy": "default",  
            "PricingDetails": [],  
            "UsagePrice": 0.0,  
            "RecurringCharges": [  
                {  
                    "Amount": 0.0672,  
                    "Frequency": "Hourly"  
                }  
            ],  
            "Marketplace": false,  
            "CurrencyCode": "USD",  
            "FixedPrice": 0.0,  
            "Duration": 31536000,  
            "Scope": "Region",  
            "ReservedInstancesOfferingId": "bec624df-a8cc-4aad-a72f-4f8abc34caf2",  
            "InstanceType": "t2.large"  
        },  
        {  
            "OfferingClass": "standard",  
            "OfferingType": "Partial Upfront",  
            "ProductDescription": "Linux/UNIX",  
            "InstanceTenancy": "default",  
            "PricingDetails": [],  
            "UsagePrice": 0.0,  
            "RecurringCharges": [  
            ]  
        }  
    ]  
}
```

```
{  
    "Amount": 0.032,  
    "Frequency": "Hourly"  
}  
],  
"Marketplace": false,  
"CurrencyCode": "USD",  
"FixedPrice": 280.0,  
"Duration": 31536000,  
"Scope": "Region",  
"ReservedInstancesOfferingId": "6b15a842-3acb-4320-bd55-fa43a79f3fe3",  
"InstanceType": "t2.large"  
},  
{  
    "OfferingClass": "standard",  
    "OfferingType": "All Upfront",  
    "ProductDescription": "Linux/UNIX",  
    "InstanceTenancy": "default",  
    "PricingDetails": [],  
    "UsagePrice": 0.0,  
    "RecurringCharges": [],  
    "Marketplace": false,  
    "CurrencyCode": "USD",  
    "FixedPrice": 549.0,  
    "Duration": 31536000,  
    "Scope": "Region",  
    "ReservedInstancesOfferingId": "5062dc97-d284-417b-b09e-8abed1e5a183",  
    "InstanceType": "t2.large"  
}  
]  
}
```

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 `ReservedInstancesOfferingId`.

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 ec06327e-dd07-46ee-9398-75b5fexample --instance-count 1
```

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 para 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 [Usar as Instâncias reservadas \(p. 270\)](#).

Para obter exemplos de como as Instâncias reservadas são aplicadas às instâncias em execução, consulte [Como as Instâncias reservadas são aplicadas \(p. 256\)](#).

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.

Para comprar Instâncias reservadas conversíveis 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, Comprar Instâncias reservadas.
3. Em Classe de oferta, escolha 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. Selecione as Instâncias reservadas conversíveis a serem compradas, informe a quantidade e escolha Adicionar ao carrinho.
7. Para ver um resumo da sua seleção, escolha Exibir carrinho.
8. Para concluir o pedido, escolha Comprar.

Note

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.

9. O status de sua compra está listado na coluna 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 convertível 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
```

```
{  
    "ReservedInstancesOfferings": [  
        {
```

```
"OfferingClass": "convertible",
"OfferingType": "No Upfront",
"ProductDescription": "Linux/UNIX",
"InstanceTenancy": "default",
"PricingDetails": [],
"UsagePrice": 0.0,
"RecurringCharges": [
    {
        "Amount": 0.0556,
        "Frequency": "Hourly"
    }
],
"Marketplace": false,
"CurrencyCode": "USD",
"FixedPrice": 0.0,
"Duration": 94608000,
"Scope": "Region",
"ReservedInstancesOfferingId": "e242e87b-b75c-4079-8e87-02d53f145204",
"InstanceType": "t2.large"
},
{
    "OfferingClass": "convertible",
    "OfferingType": "Partial Upfront",
    "ProductDescription": "Linux/UNIX",
    "InstanceTenancy": "default",
    "PricingDetails": [],
    "UsagePrice": 0.0,
    "RecurringCharges": [
        {
            "Amount": 0.0258,
            "Frequency": "Hourly"
        }
    ],
    "Marketplace": false,
    "CurrencyCode": "USD",
    "FixedPrice": 677.0,
    "Duration": 94608000,
    "Scope": "Region",
    "ReservedInstancesOfferingId": "13486b92-bdd6-4b68-894c-509bcf239ccd",
    "InstanceType": "t2.large"
},
{
    "OfferingClass": "convertible",
    "OfferingType": "All Upfront",
    "ProductDescription": "Linux/UNIX",
    "InstanceTenancy": "default",
    "PricingDetails": [],
    "UsagePrice": 0.0,
    "RecurringCharges": [],
    "Marketplace": false,
    "CurrencyCode": "USD",
    "FixedPrice": 1327.0,
    "Duration": 94608000,
    "Scope": "Region",
    "ReservedInstancesOfferingId": "e00ec34b-4674-4fb9-a0a9-213296ab93aa",
    "InstanceType": "t2.large"
}
]
```

Quando encontrar uma Instância reservada que atenda às suas necessidades, anote o ReservedInstancesOfferingId.

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 ec06327e-dd07-46ee-9398-75b5fexample --instance-count 1
```

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 para 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 [Usar as Instâncias reservadas \(p. 270\)](#).

Para obter exemplos de como as Instâncias reservadas são aplicadas às instâncias em execução, consulte [Como as Instâncias reservadas são aplicadas \(p. 256\)](#).

Visualizar as 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. As Instâncias reservadas ativas e desativadas são listadas. A coluna Estado exibe o estado.
4. Se você for um vendedor no Marketplace de instâncias reservadas, a guia Minha lista exibirá o status de uma reserva listada no [Marketplace de instâncias reservadas \(p. 271\)](#). Para obter mais informações, consulte [Estados de listagem da Instância reservada \(p. 276\)](#).

Para visualizar as Instâncias reservadas usando a linha de comando

- [describe-reserved-instances](#) (AWS CLI)
- [Get-EC2ReservedInstance](#) (Tools para Windows PowerShell)

Usar as 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 [Instâncias dedicadas \(p. 371\)](#).

Para obter mais informações, consulte [Execução de uma instância usando o assistente de execução de instância \(p. 391\)](#). Para obter exemplos de como as Instâncias reservadas são aplicadas às instâncias em execução, consulte [Como as Instâncias reservadas são aplicadas \(p. 256\)](#).

Você pode usar o Amazon EC2 Auto Scaling ou outros serviços da AWS para executar as Instâncias on-demand que usam os benefícios da Instância reservada. Para obter mais informações, consulte o [Guia do usuário do Amazon EC2 Auto Scaling](#).

Venda no Marketplace de instâncias reservadas

O Marketplace de instâncias reservadas é uma plataforma compatível com a venda de Instâncias reservadas padrão não utilizadas de clientes da AWS e terceiros, que varia em termos de comprimento 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.

Se você quiser vender suas Instâncias reservadas não utilizadas no Marketplace de instâncias reservadas, deverá atender a determinados critérios de elegibilidade.

Tópicos

- [Venda no Marketplace de instâncias reservadas \(p. 271\)](#)
- [Comprar no Marketplace da Instância reservada \(p. 277\)](#)

Venda no Marketplace de instâncias reservadas

Assim que você listar suas Instâncias reservadas no Marketplace de instâncias reservadas, elas serão disponibilizadas para que compradores potenciais 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, nós vendemos 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.

Tópicos

- [Restrições e limitações \(p. 272\)](#)
- [Registro como vendedor \(p. 272\)](#)

- [Definir o preço das Instâncias reservadas \(p. 274\)](#)
- [Listar as Instâncias reservadas \(p. 275\)](#)
- [Ciclo de vida de uma lista \(p. 276\)](#)
- [Depois que a Instância reservada é vendida \(p. 277\)](#)

Restrições e limitações

Par que você possa vender as reservas não usadas, registre-se como vendedor no Marketplace de instâncias reservadas. Para obter mais informações, consulte [Registro como vendedor \(p. 272\)](#).

As seguintes limitações e restrições são aplicáveis na venda da Instâncias reservadas:

- Somente Instâncias reservadas padrão do Amazon EC2 podem ser vendidas no Marketplace de instâncias reservadas. Instâncias reservadas conversíveis não podem ser vendidas. Deve haver pelo menos um mês restante no período de vigência da Instância reservada 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 Pagamento adiantado 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 a listagem diretamente 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 [Definir o preço das Instâncias reservadas \(p. 274\)](#). Você também pode modificar as Instâncias reservadas antes de listá-las. Para obter mais informações, consulte [Modificar Instâncias reservadas \(p. 278\)](#).
- 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;
- Somente as Amazon EC2 padrão do Instâncias reservadas podem ser vendidas no Marketplace de instâncias reservadas. Outras AWS da Instâncias reservadas, como as Amazon RDS do Amazon ElastiCache e do Instâncias reservadas não podem ser vendidas no Marketplace de instâncias reservadas.

Registro como vendedor

Para vender no Marketplace de instâncias reservadas, você deve primeiro registrar-se 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 [Contas bancárias \(p. 273\)](#).
- **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 \(p. 273\)](#).

Após a AWS receber o registro preenchido do vendedor, você receberá um e-mail confirmando seu registro e informando que você pode começar a vender no Marketplace de instâncias reservadas.

Tópicos

- [Contas bancárias \(p. 273\)](#)
- [Informações fiscais \(p. 273\)](#)
- [Compartilhamento das informações com o comprador \(p. 274\)](#)

- [Recebimentos \(p. 274\)](#)

Contas bancárias

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 registrar uma conta de banco padrão para desembolsos

1. Abra a página [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 [Registro do vendedor do Marketplace de instâncias reservadas](#), faça login na conta usada quando você se registrou.
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 relatório do IRS, 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 após o 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](#).

Compartilhamento das informações 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 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 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](#).

Recebimentos

Assim que a AWS receber fundos do comprador, será enviada uma mensagem ao e-mail da conta do proprietário registrado para a Instância reservada vendida.

A AWS 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. Você pode visualizar o estado desse desembolso ao visualizar o relatório de desembolso da Instância reservada. Os desembolsos ocorrem uma vez por dia. Lembre-se de que você não poderá receber desembolsos até que a AWS tenha recebido verificação do seu banco. Esse período pode demorar até duas semanas.

A Instância reservada que você vendeu continua aparecendo quando você descreve as Instâncias reservadas.

Você recebe um reembolso em dinheiro de 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 previsto total de cada Instância reservada vendido no Marketplace de instâncias reservadas.

Definir o preço das 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. Você não pode especificar a taxa de uso nem a taxa recorrente; o comprador paga as mesmas taxas de uso ou recorrentes definidas quando as reservas foram originalmente compradas.

É importante observar os limites a seguir:

- Você pode vender até 50.000 USD em Instâncias reservadas por ano. Para vender mais, preencha o formulário [Pedir para aumentar o limite de vendas nas Instâncias reservadas do Amazon EC2](#).
- O preço mínimo é 0 USD. 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.

Configuração de uma programação de preços

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.

Listar as 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.

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 lista não estará mais disponível no Marketplace de instâncias reservadas.

Tópicos

- [Listar a Instância reservada usando o Console de gerenciamento da AWS \(p. 275\)](#)
- [Listar a Instâncias reservadas usando a API da AWS CLI ou do Amazon EC2 \(p. 276\)](#)
- [Estados de listagem da Instância reservada \(p. 276\)](#)

Listar a Instância reservada usando o Console de gerenciamento da AWS

Para listar uma Instância reservada no Marketplace de instâncias reservadas usando a Console de gerenciamento da AWS

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 a serem listadas e escolha 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 que você listou e escolha My Listings (Minhas listas).

Listar a Instâncias reservadas usando a API da AWS CLI ou do Amazon EC2

Para listar uma Instância reservada 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](#).

Para cancelar sua lista, use o comando [cancel-reserved-instances-listings](#).

Para listar uma Instância reservada no Marketplace de instâncias reservadas usando a API do Amazon EC2

- [DescribeReservedInstances](#)
- [CreateReservedInstancesListing](#)
- [DescribeReservedInstancesListings](#)
- [CancelReservedInstancesListing](#)

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 Estado da lista são sobre o status da sua lista 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.
- cancelada—A lista 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 listagem for vendida, a AWS eliminará as Instâncias reservadas na lista e criará 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 lista 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 lista não estará mais disponível no Marketplace de instâncias reservadas.

Depois que a Instância reservada é vendida

Quando a Instância reservada for vendida, a AWS lhe 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. Por exemplo, você pode criar ou vender uma lista ou a AWS pode enviar fundos para sua conta.

Para rastrear o status de uma lista de Instância reservada no console, escolha Reserved Instance (Instância reservada), My Listings (Minhas listas). 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.

Comprar no Marketplace da Instância reservada

Você pode adquirir Instâncias reservadas de vendedores terceiros que tenham Instâncias reservadas 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 similar à compra de Instâncias reservadas da AWS. Para obter mais informações, consulte [Comprar Instâncias reservadas \(p. 264\)](#).

Existem poucas diferenças entre as Instâncias reservadas adquiridas no Marketplace de instâncias reservadas e as 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. 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 as Amazon EC2 padrão do Instâncias reservadas podem ser adquiridas no Marketplace de instâncias reservadas. Instâncias reservadas conversíveis, Amazon RDS e Amazon ElastiCache Instâncias reservadas 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 jurídica 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 [Suporte da AWS](#).

Modificar Instâncias reservadas

Quando suas necessidades de computação mudarem, você poderá modificar suas instâncias reservadas padrão ou as Instâncias reservadas conversíveis e continuar usufruindo o benefício de faturamento. Você pode modificar a zona de disponibilidade, o escopo, a plataforma de rede ou o tamanho da instância (no mesmo tipo de instância) da sua Instância reservada. Para modificar uma Instância reservada, você especifica as Instâncias reservadas que deseja modificar e especifica uma ou mais configurações de destino.

Note

Você também pode trocar uma Instância reservada convertível por outra Instância reservada convertível com uma configuração diferente, incluindo a família de instâncias. Para obter mais informações, consulte [Trocar Instâncias reservadas conversíveis \(p. 285\)](#).

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 [Modificação do tamanho da instância das suas reservas \(p. 280\)](#).

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 `effective_date` das Instâncias reservadas modificadas usando a ação de API [DescribeReservedInstances](#) ou o comando `describe-reserved-instances` (AWS CLI).

- 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.

Note

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 \(p. 279\)](#)
- [Modificação do tamanho da instância das suas reservas \(p. 280\)](#)
- [Envio de solicitações da modificação \(p. 283\)](#)
- [Solicitações da modificação de solução de problemas \(p. 284\)](#)

Requisitos e restrições para modificação

Nem todos os atributos de uma Instância reservada podem ser modificados, e as restrições podem ser aplicadas.

Atributo modificável	Plataformas compatíveis	Limitações
Alterar as zonas de disponibilidade na mesma região	Linux e Windows	–
Alterar o escopo de zona de disponibilidade para região e vice-versa	Linux e Windows	<p>Se você alterar o escopo de zona de disponibilidade para região, perderá o benefício da reserva de capacidade.</p> <p>Se você alterar o escopo de região para zona de disponibilidade, perderá a flexibilidade da zona de disponibilidade e a flexibilidade de tamanho de instância (se aplicável). Para obter mais informações, consulte Como as Instâncias reservadas são aplicadas (p. 256).</p>

Atributo modificável	Plataformas compatíveis	Limitações
Altera o tamanho da instância dentro do mesmo tipo de instância	Somente Linux	Para alguns tipos de instância não há suporte, pois não há outros tamanhos disponíveis. Para obter mais informações, consulte Modificação do tamanho da instância das suas reservas (p. 280) .
Alterar a rede do EC2-Classic para a Amazon VPC e vice-versa	Linux e Windows	A plataforma de rede deve estar disponível em sua conta da AWS. Se sua conta da AWS foi criada após 04/12/2013, ela não oferecerá suporte ao EC2-Classic.

O Amazon EC2 processará sua solicitação de modificação se houver capacidade suficiente para sua configuração de destino (se aplicável) e se as condições a seguir forem atendidas.

As Instâncias reservadas que você deseja modificar devem ser:

- Ativo
- Outra solicitação de modificação não deve estar pendente
- Não registrada no Marketplace de instâncias reservadas

Note

Para modificar as Instâncias reservadas listadas no Marketplace de instâncias reservadas, cancele a lista, solicite a modificação e liste-as novamente.

- Encerramento na mesma hora (mas não no mesmo minuto ou segundo)
- Já comprado por você (você não pode modificar uma oferta antes ou ao mesmo tempo que comprá-la)

Sua solicitação de modificação deve atender às seguintes condições:

- Deve haver correspondência entre o tamanho ocupado pela instância da reserva ativa e a configuração de destino. Para obter mais informações, consulte [Modificação do tamanho da instância das suas reservas \(p. 280\)](#).
- As Instâncias reservadas de entrada devem ser Instâncias reservadas ou Instâncias reservadas conversíveis padrão, e não uma combinação de ambas.

Modificação do tamanho da instância das suas reservas

Se você tiver reservas do Amazon Linux em um tipo de instância com vários tamanhos, poderá modificar o tamanho da instância das Instâncias reservadas.

Note

As instâncias são agrupadas por família (com base em capacidade de armazenamento ou CPU); tipo (projeto para casos de uso específicos); e tamanho. Por exemplo, o tipo de instância c4 está na família de instâncias otimizada Computação e disponível em vários tamanhos. Enquanto as instâncias c3 estiverem na mesma família, você não poderá modificar as instâncias c4 para instâncias c3 porque elas têm especificações de hardware diferentes. Para obter mais informações, consulte [Tipos de instância do Amazon EC2](#).

Você não pode modificar o tamanho de instância das Instâncias reservadas para os seguintes tipos de instâncias, pois somente um tamanho está disponível para cada um destes tipos de instância.

- **cc2.8xlarge**
- **cr1.8xlarge**
- **hs1.8xlarge**
- **i3.metal**
- **t1.micro**

Cada Instância reservada tem um espaço para tamanho da instância, que é determinado pelo fator de normalização do tipo de instância e pelo número de instâncias na reserva. Quando você modificar uma Instância reservada, o espaço para configuração de destino deverá corresponder ao da configuração original; caso contrário, a solicitação de modificação não será processada.

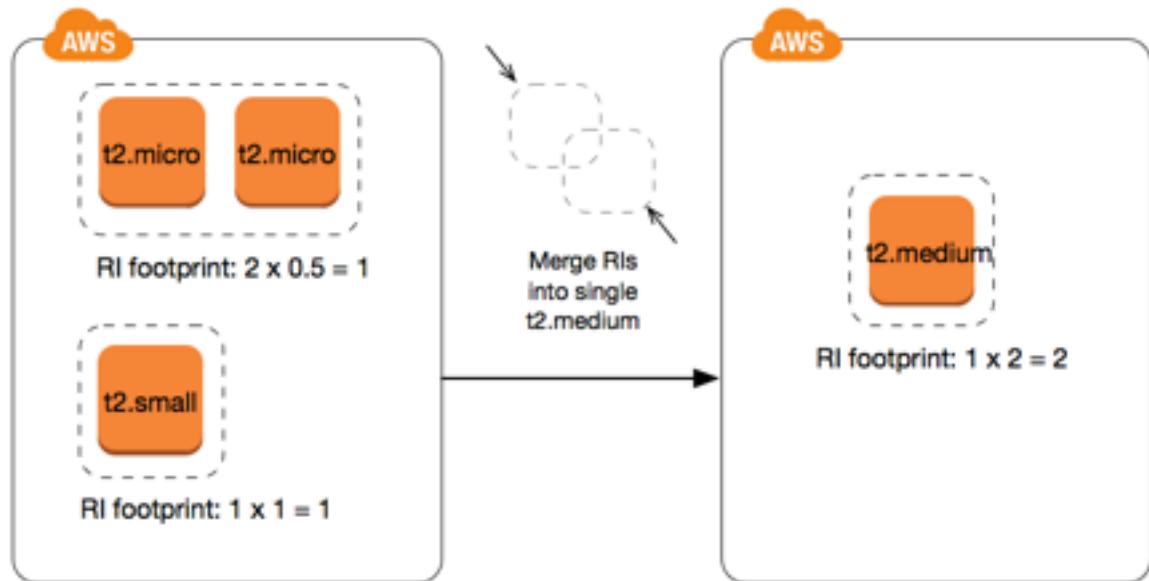
O fator de normalização se baseia no tamanho da instância dentro do tipo da instância (por exemplo, instâncias **m1.xlarge** dentro do tipo de instância **m1**). Isso só é apenas significativo dentro do mesmo tipo de instância. Os tipos de instância não podem ser modificados de um tipo para outro. No console do Amazon EC2, isso é medido em unidades. A tabela a seguir ilustra o fator de normalização que se aplica dentro de um tipo de instância.

Tamanho da instância	Fator de normalização
nano	0.25
micro	0,5
pequeno	1
médio	2
grande	4
xlarge	8
2xlarge	16
4xlarge	32
8xlarge	64
9xlarge	72
10xlarge	80
12xlarge	96
16xlarge	128
18xlarge	144
24xlarge	192
32xlarge	256

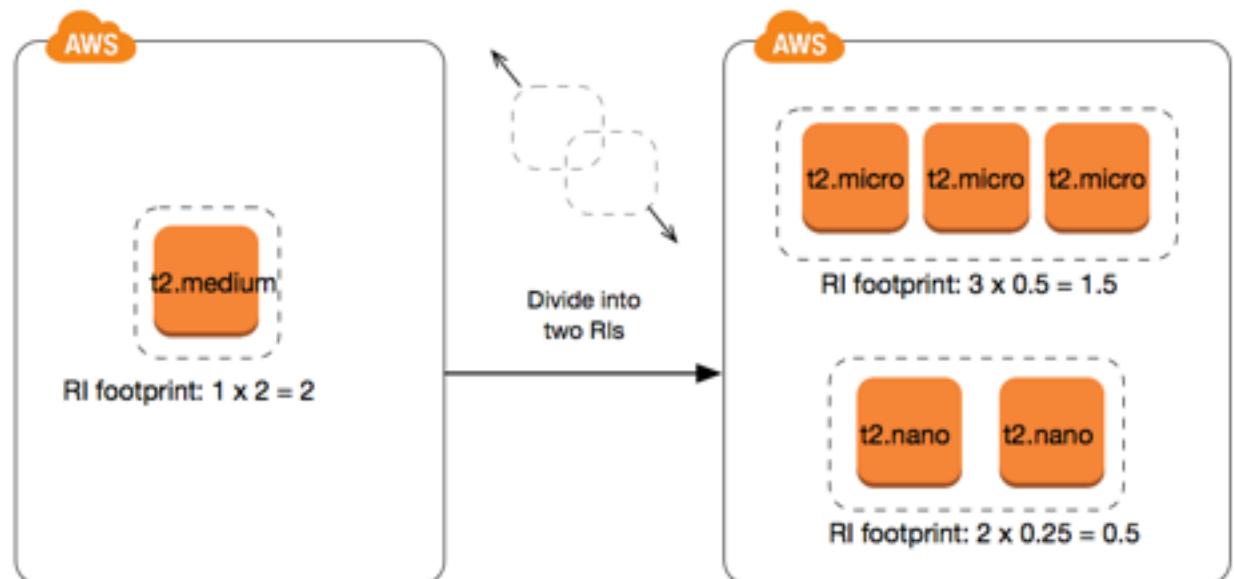
Para calcular o espaço para tamanho de instância de uma Instância reservada, multiplique o número de instâncias pelo fator de normalização. Por exemplo, um **t2.medium** tem um fator de normalização de 2, por isso uma reserva para quatro instâncias **t2.medium** tem uma presença de 8 unidades.

Você pode alocar suas reservas para tamanhos de instância diferentes no mesmo tipo de instância, desde que o espaço para a instância da sua reserva permaneça o mesmo. Por exemplo, você pode dividir uma reserva por uma instância `t2.large` (1×4) em quatro instâncias `t2.small` (4×1) ou 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` (2×1) em uma instância `t2.large` (1×4). Isso ocorre porque o tamanho da instância existente da sua reserva atual é menor que a reserva proposta.

No exemplo a seguir, você tem uma reserva com as duas instâncias `t2.micro` (que dão a você a presença de 1) e uma reserva com uma instância `t2.small` (que oferece a uma presença de 1). Você funde as duas reservas em uma única reserva com uma instância `t2.medium`—o tamanho de instância combinado das duas reservas originais é igual ao tamanho da reserva modificada.



Você também pode modificar uma reserva para dividi-la em duas ou mais reservas. No exemplo a seguir, você tem uma reserva uma instância `t2.medium`. Você divide a reserva em uma reserva com duas instâncias `t2.nano` e uma reserva com três instâncias `t2.micro`.



Envio de solicitações da modificação

Você não pode modificar as Instâncias reservadas usando o console do Amazon EC2, a API do Amazon EC2 ou uma ferramenta de linha de comando.

Console do Amazon EC2

Antes modificar as Instâncias reservadas, leia as [restrições \(p. 279\)](#) aplicáveis. Se você estiver modificando o tamanho da instância, assegure-se de que você calcule o [tamanho total ocupado pela instância \(p. 280\)](#) das reservas que deseja modificar e garantir que corresponde ao tamanho total ocupado pela instância das configurações de destino.

Para modificar as Instâncias reservadas usando o Console de gerenciamento da AWS

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 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 Continuar quando você tiver terminado:
 - Escopo: escolha se a Instância reservada 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.
 - Tipo de instância: Selecione o tipo de instância necessário. Disponível somente para plataformas compatíveis. Para obter mais informações, consulte [Requisitos e restrições para modificação \(p. 279\)](#).
 - Contagem: Especifique o número de instâncias a serem cobertas pela reserva.

Note

Se as configurações de destino combinadas forem maiores ou menores que o espaço para tamanho de instância das Instâncias reservadas originais, o total alocado na coluna Units (Unidades) será exibido em vermelho.

4. Para confirmar suas escolhas quando terminar de especificar as configurações de destino, selecione Enviar modificações. Se você mudar de ideia a qualquer momento, escolha Cancelar para sair do assistente.

Você pode determinar o status de sua solicitação da modificação analisando a coluna State (Estado) na tela de Instâncias reservadas. A tabela a seguir ilustra os valores de Estado possíveis.

Estado	Descrição
ativo (modificação pendente)	Estado de transição das Instâncias reservadas originais.

Estado	Descrição
desativado (modificação pendente)	Estado de transição das Instâncias reservadas originais durante a criação de novas Instâncias reservadas.
desativado	Instâncias reservadas modificadas e substituídas com êxito.
ativo	Novas Instâncias reservadas criadas com base em uma solicitação de modificação bem-sucedida. -Ou- Instâncias reservadas originais após falha na solicitação da modificação.

API ou ferramenta de linha de comando do Amazon EC2

Para modificar as Instâncias reservadas, você pode usar uma das opções a seguir:

- [modify-reserved-instances](#) (AWS CLI)
- [Edit-EC2ReservedInstance](#) (AWS Tools para Windows PowerShell)
- [ModifyReservedInstances](#) (API do Amazon EC2)

Para obter o status da modificação, use uma das opções a seguir:

- [describe-reserved-instances-modifications](#) (AWS CLI)
- [Get-EC2ReservedInstancesModifications](#) (AWS Tools para Windows PowerShell)
- [DescribeReservedInstancesModifications](#) (API do Amazon EC2)

O estado apresentado mostra sua solicitação como `processing`, `fulfilled` ou `failed`.

Solicitações da modificação de solução de problemas

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. 279) 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 Instância reservada convertível de destino tenha valor igual ou superior às Instâncias reservadas conversíveis que você está trocando.

Ao trocar sua Instância reservada convertível, o número de instâncias da sua reserva atual é trocado por um número de instâncias que cobrem o valor igual ou superior da configuração de Instância reservada convertível de destino. O Amazon EC2 calcula o número de Instâncias reservadas que você pode receber como resultado da troca.

Tópicos

- [Requisitos para trocar de Instâncias reservadas conversíveis \(p. 285\)](#)
- [Calcular as trocas de Instâncias reservadas conversíveis \(p. 286\)](#)
- [Mesclar Instâncias reservadas conversíveis \(p. 287\)](#)
- [Trocar uma parte de uma Instância reservada convertível \(p. 287\)](#)
- [Envio de solicitações de troca \(p. 288\)](#)

[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 [Trocar uma parte de uma Instância reservada convertível \(p. 287\)](#). Para obter mais informações sobre como modificar Instâncias reservadas, consulte [Modificar Instâncias reservadas \(p. 278\)](#).
- 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, a AWS fornecerá automaticamente uma quantidade de instâncias na Instância reservada convertível que garantirá o custo alinhado de \$0.00 ou mais.

Note

Se o valor total (preço do adiantamento + preço por hora * número de horas restantes) da nova Instância reservada convertível for menor do que o valor total da Instância reservada convertível que foi trocada, a AWS fornecerá automaticamente uma quantidade de instâncias na Instância reservada convertível que garantirá um valor total igual ou superior ao valor da Instância reservada convertível 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 convertível for menor do que o valor total da Instância reservada convertível que foi trocada, a AWS fornecerá automaticamente uma quantidade de instâncias na Instância reservada convertível que garantirá um valor total igual ou superior ao valor da Instância reservada convertível 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 \(p. 287\)](#).

Calcular as trocas de Instâncias reservadas conversíveis

A troca de Instâncias reservadas conversíveis são gratuitas. No entanto, você pode ser solicitado a pagar um custo alinhado, que é o custo adiantado pro rata da diferença entre as Instâncias reservadas conversíveis que você tinha e as Instâncias reservadas conversíveis que você recebe da troca.

Cada Instância reservada convertível tem um valor de tabela. Esse valor de tabela é comparado ao valor de tabela das Instâncias reservadas conversíveis que você deseja para determinar quantas reservas de instância você pode receber com a troca.

Por exemplo: você tem uma Instância reservada convertível com valor de tabela de 35 USD que deseja trocar por um novo tipo de instância com um valor de tabela de 10 USD.

\$35 / \$10 = 3.5

Você pode trocar sua Instância reservada convertível por três Instâncias reservadas conversíveis de US \$ 10. Não é possível adquirir meias reservas; portanto, é necessário comprar uma Instância reservada convertível adicional que cubra o restante:

3.5 = 3 whole Instâncias reservadas conversíveis + 1 additional Instância reservada convertível.

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 restantes das Instâncias reservadas conversíveis forem 500 USD e a reserva de destino custar normalmente 600 USD pro rata, será cobrado de você 100 USD.

\$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 um ano. 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 um ano. Você não pode trocá-las por uma Instância reservada convertível de um ano. A data de expiração da nova Instância reservada convertível é 31/12/2019.

Trocar uma parte de uma Instância reservada convertível

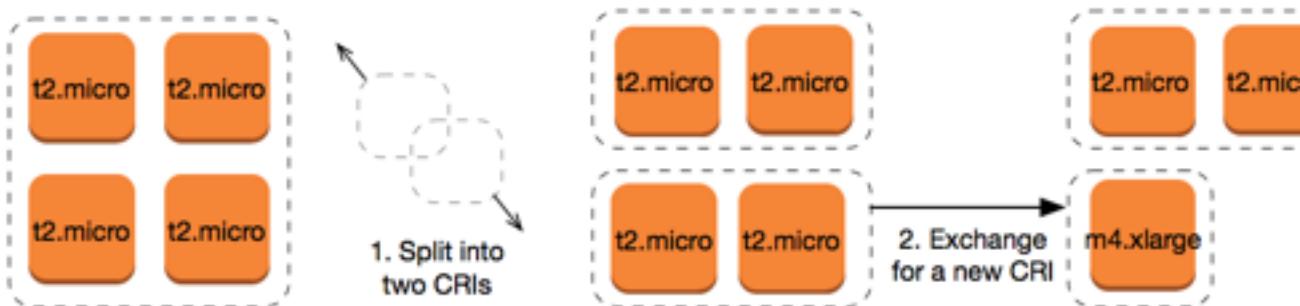
Você pode usar o processo de modificação para dividir a Instância reservada convertível em reservas menores e, em seguida, trocar uma ou mais reservas novas por uma nova Instância reservada convertível. Os exemplos a seguir demonstram como fazer isso.

Example Exemplo: Instância reservada convertível com várias instâncias

Neste exemplo, você tem uma **t2.micro** Instância reservada convertível com quatro instâncias na reserva. Para trocar duas instâncias **t2.micro** por uma instância **m4.xlarge**:

1. Modifique a **t2.micro** Instância reservada convertível dividindo-a em duas **t2.micro** Instâncias reservadas conversíveis com duas instâncias cada uma.

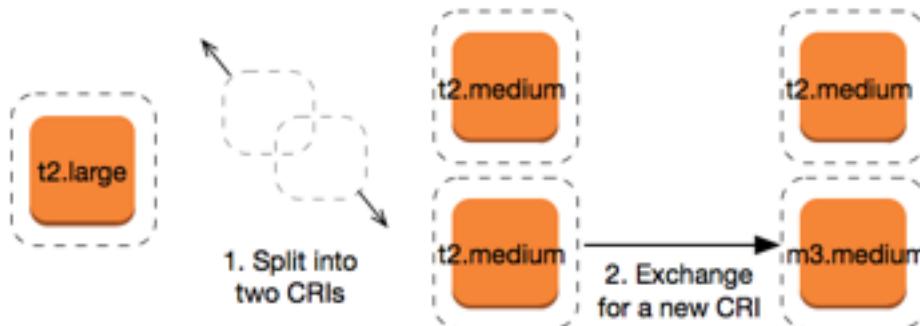
2. Troque uma das novas t2.micro Instâncias reservadas conversíveis por uma m4.xlarge Instância reservada convertível.



Example Exemplo: Instância reservada convertível com uma única instância

Neste exemplo, você tem uma t2.large Instância reservada convertível. Para transformá-la em uma t2.medium menor e em uma m3.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. Para obter mais informações, consulte [Modificação do tamanho da instância das suas reservas \(p. 280\)](#).
2. Troque uma das novas t2.medium Instâncias reservadas conversíveis por uma m3.medium Instância reservada convertível.



Para obter mais informações, consulte [Modificação do tamanho da instância das suas reservas \(p. 280\)](#) e [Envio de solicitações de troca \(p. 288\)](#).

Nem todas as Instâncias reservadas podem ser modificadas. Não deixe de ler as [restrições \(p. 279\)](#) aplicáveis.

[Envio de solicitações de troca](#)

Você pode trocar as Instâncias reservadas conversíveis usando o console do Amazon EC2 ou uma ferramenta de linha de comando.

[Trocá uma Instância reservada convertível usando o console](#)

Você pode procurar ofertas de Instâncias reservadas conversíveis e selecionar sua nova configuração entre as escolhas apresentadas.

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 usando os menus suspensoes e escolha Encontrar 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 de 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 para 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 para Windows PowerShell)

Por fim, execute a troca:

- [accept-reserved-instances-exchange-quote](#) (AWS CLI)
- [Confirm-EC2ReservedInstancesExchangeQuote](#) (Tools para Windows PowerShell)

Instâncias reservadas programadas

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, pelo prazo de um ano. Você reserva a capacidade antecipadamente, para saber que ela está disponível quando precisar. Você paga pelo período de programação das instâncias, mesmo se não usá-las.

As instâncias programadas são uma boa escolha para cargas de trabalho que não são executadas de forma contínua, mas são executadas com base em uma programação regular. Por exemplo, você pode usar instâncias programadas para um aplicativo que seja executado em horário comercial ou para o processamento em lote que ocorre nos finais de semana.

Se você precisar de reserva de capacidade de forma contínua, as Instâncias reservadas podem atender às suas necessidades e diminuir os custos. Para obter mais informações, consulte [Instâncias reservadas \(p. 253\)](#). Se você tiver flexibilidade sobre quando suas instâncias são executadas, Instâncias spot poderão atender às suas necessidades e diminuir os custos. Para obter mais informações, consulte [Instâncias spot \(p. 293\)](#).

Tópicos

- Como as instâncias programadas funcionam (p. 290)
 - Funções vinculadas ao serviço para instâncias programadas (p. 290)
 - Compra de uma instância programada (p. 291)
 - Execução de uma instância programada (p. 292)
 - Limites das instâncias programadas (p. 292)

Como as instâncias programadas funcionam

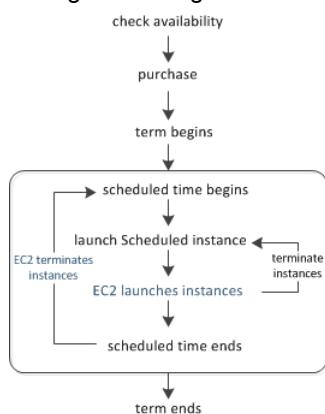
O Amazon EC2 reserva grupos de instâncias do EC2 em cada zona de disponibilidade para uso como instâncias programadas. Cada grupo oferece suporte a uma combinação de tipo de instância, sistema operacional e rede.

Para começar, você precisa pesquisar uma programação disponível. Você pode pesquisar em vários grupos ou em apenas um. Depois de encontrar uma programação apropriada, compre-a.

Você precisa executar suas instâncias programadas durante os períodos programados, usando uma configuração de execução que corresponda aos seguintes atributos da programação adquirida: tipo de instância, zona de disponibilidade, rede e plataforma. Quando você faz isso, o Amazon EC2 executa instâncias do EC2 em seu nome, com base na especificação de execução indicada. O Amazon EC2 precisa garantir que as instâncias do EC2 sejam encerradas no final do período programado atual, de forma que a capacidade esteja disponível para todas as outras instâncias programadas para as quais ela está reservada. Portanto, o Amazon EC2 encerra as instâncias do EC2 três minutos antes do término do período programado atual.

Não é possível interromper nem reinicializar instâncias programadas, mas você pode encerrá-las manualmente, conforme necessário. Se você encerrar uma instância programada antes do término do período programado, poderá executá-la novamente após alguns minutos. Caso contrário, você deverá esperar até o próximo período programado.

O diagrama a seguir ilustra o ciclo de vida de uma instância programada.



Funções vinculadas ao serviço para instâncias programadas

O Amazon EC2 cria uma função vinculada ao serviço quando você compra uma instância programada. Uma função vinculada ao serviço inclui todas as permissões que o Amazon EC2 exige para chamar todos os outros serviços da AWS em seu nome. 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 AWSServiceRoleForEC2ScheduledInstances para concluir as seguintes ações:

- `ec2.TerminateInstances` - Termina instâncias programadas após a conclusão da programação

- `ec2:CreateTags` - Adiciona tags de sistema para instâncias programadas

Se você adquiriu instâncias programadas antes de outubro de 2017, quando o Amazon EC2 começou a suportar esta função vinculada ao serviço, o Amazon EC2 criou a função `AWSServiceRoleForEC2ScheduledInstances` 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 não precisar mais usar instâncias programadas, é recomendável excluir a função `AWSServiceRoleForEC2ScheduledInstances`. Após esta função ser excluída de sua conta, o Amazon EC2 criará a função novamente se você adquirir instâncias programadas.

Compra de uma instância programada

Para comprar uma instância programada, você pode usar o Assistente de reserva de instâncias reservadas programadas.

Warning

Depois de adquirir uma instância programada, você não poderá cancelar, modificar nem revender sua compra.

Para comprar uma instância programada (console)

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, em INSTÂNCIAS, escolha Instâncias programadas. Se a região selecionada atualmente não oferecer suporte a instâncias programadas, a página não estará disponível. [Saiba mais](#)
3. Escolha Comprar instâncias programadas.
4. Na página Encontrar programações disponíveis, faça o seguinte:
 - a. Em Criar uma programação, selecione a data de início em Iniciar em, a recorrência da programação (diariamente, semanalmente ou mensalmente) em Recorrência e a duração mínima em Pela duração. O console garante que você especifique um valor para a duração mínima que atenda à utilização necessária mínima para sua instância programada (1.200 horas por ano).

Create a schedule

Starting on for duration hours

+/- 2 hours

Recurring

- b. Em Detalhes da instância, selecione o sistema operacional e a rede em Plataforma. Para reduzir os resultados, selecione um ou mais tipos em Tipo de instância ou uma ou mais zonas de disponibilidade em Zona de disponibilidade.

Instance details

Platform

Instance type

Availability Zone

- c. Escolha Encontrar programações.
- d. Em Programações disponíveis, selecione uma ou mais programações. Para cada programação selecionada, defina a quantidade de instâncias e escolha Adicionar ao carrinho.
- e. Seu carrinho é exibido na parte inferior da página. Ao terminar de adicionar e remover programações do carrinho, escolha Revisar e comprar.

5. Na página Revisar e comprar, verifique suas seleções e edite-as conforme necessário. Quando terminar, escolha Comprar.

Para comprar uma instância programada (AWS CLI)

Use o comando [describe-scheduled-instance-availability](#) para listar as programações disponíveis que atendam às suas necessidades e, em seguida, use o comando [purchase-scheduled-instances](#) para concluir a compra.

Execução de uma instância programada

Depois de adquirir uma Instância programada, ela estará disponível para execução durante os períodos programados.

Para executar uma instância programada (console)

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, em INSTÂNCIAS, escolha Instâncias programadas. Se a região selecionada atualmente não oferecer suporte a instâncias programadas, a página não estará disponível. [Saiba mais](#)
3. Selecione a instância programada e escolha Executar instâncias programadas.
4. Na página Configurar, complete a especificação de execução para suas instâncias programadas e escolha Revisar.

Important

A especificação de execução deve corresponder ao tipo de instância, zona de disponibilidade, rede e plataforma da programação adquiridos.

5. Na página Revisar, verifique a configuração de execução e modifique-a, conforme necessário. Quando terminar, escolha Executar.

Para executar uma instância programada (AWS CLI)

Use o comando [describe-scheduled-instances](#) para listar suas instâncias programadas e, em seguida, use o comando [run-scheduled-instances](#) para executar cada instância programada nos períodos agendados.

Limites das instâncias programadas

As instâncias programadas estão sujeitas aos limites a seguir:

- Os tipos de instância a seguir são os únicos tipos com suporte: C3, C4, M4 e R3.
- O período de vigência necessário é 365 dias (um ano).
- A utilização necessária mínima é 1.200 horas por ano.
- Você pode comprar uma instância programada com até três meses de antecedência.
- Elas estão disponíveis nas seguintes regiões: Leste dos EUA (Norte da Virgínia), Oeste dos EUA (Oregon) e Europa (Irlanda).

Instâncias spot

A Instância spot é uma instância do EC2 não usada 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 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 os aplicativos serão executados e se os aplicativos poderão ser interrompidos. 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

- [Conceitos \(p. 293\)](#)
- [Como começar \(p. 294\)](#)
- [Serviços relacionados \(p. 295\)](#)
- [Definição de preço e economia \(p. 295\)](#)

Conceitos

Antes de começar a trabalhar com as Instâncias spot, você deve se familiarizar com os seguintes conceitos:

- Grupo de Instância spot – um conjunto de instâncias do EC2 com o mesmo tipo de instância (por exemplo m5.large), sistema operacional, zona de disponibilidade e plataforma de rede.
- Preço spot – O preço atual de uma Instância spot por hora.
- Solicitação de Instância spot – 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 spot persistente depois que a Instância spot associada à solicitação é encerrada. A solicitação de Instância spot pode especificar uma duração para as Instâncias spot.
- Frota spot – conjunto de Instâncias spot que é executado com base nos critérios especificados. A Frota spot seleciona os grupos de Instância spot que atendem às suas necessidades e executa Instâncias spot para atender à capacidade de destino da 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 persists depois que as instâncias são encerradas. Você pode incluir solicitações de instância sob demanda em uma solicitação de Frota spot.
- Interrupção da Instância spot – quando o preço spot excede o preço máximo da sua solicitação ou não há mais capacidade disponível, o Amazon EC2 encerra, interrompe ou deixa em estado de hibernação a sua Instância spot. O Amazon EC2 fornece um aviso de interrupção de Instância spot, que fornece à instância uma advertência de 2 minutos antes de ser interrompida.

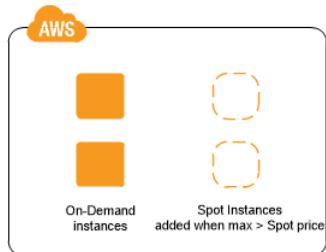
Diferenças principais entre Instâncias spot e Instâncias on-demand

A tabela a seguir lista as principais diferenças entre Instâncias spot e Instâncias on-demand.

	Instâncias spot	Instâncias on-demand
Horário do lançamento	Só poderá ser executado imediatamente se a solicitação spot estiver ativa e se 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 spot continuará a fazer a solicitação de execução 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.
Interrupção de instância	Você não pode interromper e iniciar uma Amazon EBS; baseada no Instância spot. Somente o serviço spot do Amazon EC2 pode fazer isso. O serviço spot do Amazon EC2 poderá interromper (p. 348) 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 um instância sob demanda é interrompido (parado ou encerrado).

Estratégias para usar Instâncias spot

Uma estratégia para manter um nível mínimo de recursos de computação garantidos para seus aplicativos é executar um grupo principal de Instâncias on-demand e complementá-lo com Instâncias spot quando surgir a oportunidade.



Outra estratégia é executar Instâncias spot com uma duração especificada (também conhecidas como blocos spot), que são projetadas para não serem interrompidas e serão executadas continuamente pela duração que você selecionar. Em raras situações, os blocos spot podem ser interrompidos devido a necessidades de capacidade do Amazon EC2. Nesses casos, enviamos um aviso dois minutos antes de encerrarmos uma instância, e você não será cobrado pelas instâncias encerradas mesmo se as usou. Para obter mais informações, consulte [Como especificar a duração para suas Instâncias spot](#) (p. 307).

Como começar

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

- [Como configurar com o Amazon EC2](#) (p. 21)
- [Conceitos básicos das instâncias do Amazon EC2 do Linux](#) (p. 30)

Noções básicas do spot

- [Como as Instâncias spot funcionam \(p. 296\)](#)
- [Como Frota spot funciona \(p. 298\)](#)

Trabalho com Instâncias spot

- [Como preparar-se para interrupções \(p. 351\)](#)
- [Criação da solicitação de Instância spot \(p. 309\)](#)
- [Como obter informações de status da solicitação \(p. 346\)](#)

Trabalho com Frotas spot

- [Pré-requisitos do Fronha spot \(p. 317\)](#)
- [Criação da solicitação de Fronha spot \(p. 320\)](#)

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

Você pode criar configurações de execução com o preço máximo que está disposto a pagar. Assim, o Amazon EC2 Auto Scaling poderá executar as Instâncias spot. Para obter mais informações, consulte [Executar Instâncias spot no seu grupo do Auto Scaling](#) e [Usar vários tipos de instâncias 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.

Modelos AWS CloudFormation

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 [Atualizações de Instância 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 para .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 Auto Scaling do Amazon EC2 as encerre durante o [ajuste de escala](#).

As Instâncias spot com uma duração predefinida usam um preço por hora fixo que permanece em vigor para a Instância spot durante sua execução.

Exibir preços

Para visualizar o menor preço spot atual por região (atualizado a cada cinco minutos) e o tipo de instância, consulte a página [Definição de preços de Instâncias spot](#).

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 de Instância spots \(p. 304\)](#).

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

É possível visualizar a economia feita 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 \(p. 305\)](#).

Exibir faturamento

Para analisar sua fatura, acesse a página [Atividade da conta da AWS](#). Sua fatura contém links para relatórios de uso que fornecem detalhes sobre sua conta. Para obter mais informações, consulte [Faturamento da conta da AWS](#).

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

Como as Instâncias spot funcionam

Para usar Instâncias spot, crie uma solicitação de Instância spot ou uma solicitação de Frota spot. A solicitação pode incluir o preço máximo que você está disposto a pagar por hora por instância (o padrão é o preço sob demanda) e outras limitações como o tipo de instância e a zona de disponibilidade. Se seu preço máximo exceder o preço spot atual da instância especificada, e a capacidade estiver disponível, sua solicitação será atendida imediatamente. Caso contrário, a solicitação será atendida quando o preço máximo exceder o preço spot e houver capacidade disponível. As instâncias spot são executadas até que você as encerre ou o Amazon EC2 as interrompa (isso também é conhecido como interrupção de Instância spot).

Quando usar o Instâncias spot, você deverá estar preparado para interrupções. O Amazon EC2 poderá interromper a Instância spot quando o preço spot exceder o preço máximo, quando a demanda por Instâncias spot aumentar ou quando a oferta de Instâncias spot diminuir. 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 Instância spots \(p. 348\)](#).

Você não pode interromper e iniciar uma instância do Amazon EBS se ela for uma Instância spot (somente o serviço spot pode interromper e iniciar uma Instância spot). No entanto, você pode reiniciar ou encerrar uma Instância spot.

Tópicos

- [Como ativar Instâncias spot em um grupo de execução \(p. 297\)](#)
- [Execução de Instâncias spot em um grupo de zonas de disponibilidade \(p. 297\)](#)
- [Execução de Instâncias spot na VPC \(p. 297\)](#)

Como ativar 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.

Execução de Instâncias spot em um grupo de zonas de disponibilidade

Especifique um grupo de zonas de disponibilidade na solicitação de Instância spot para instruir o serviço spot a 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.

Execução de Instâncias spot na 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.

Como Frota spot funciona

Uma Frota spot é uma coleção, ou frota de Instâncias spot e, opcionalmente, de Instâncias on-demand.

A Frota spot tenta executar o número de Instâncias spot e Instâncias on-demand para atender à capacidade de destino especificada por você na solicitação de Frota spot. A solicitação de Instâncias spot será atendida se o preço máximo especificado na solicitação exceder o preço spot atual e houver capacidade disponível. A Frota spot também tentará manter a capacidade de destino se as Instâncias spot forem interrompidas por causa de uma alteração no preço spot ou na capacidade disponível.

Um Grupo de Instância spot é um conjunto de instâncias do EC2 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 Instância 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

- [Sob demanda na Frota spot \(p. 298\)](#)
- [Estratégia de alocação para Instâncias spot \(p. 299\)](#)
- [Substituições do preço spot \(p. 300\)](#)
- [Peso da instância da Frota spot \(p. 300\)](#)
- [Apresentação: Como usar a Frota spot com o peso da instância \(p. 302\)](#)

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 de destino 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 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`, 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`.

Estratégia de alocação para Instâncias spot

A estratégia de alocação da Instâncias spot no Frota spot determina como ela atenderá à solicitação de Frota spot dos grupos possíveis de Instância 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.

`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`.

Como 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 Instância 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.

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 implemente a combinação mais barata 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 barato com base no preço público sob demanda e continua seguindo a estratégia de alocação (seja `lowestPrice` ou `diversified`) para Instâncias spot.

Configurar a Frota spot para otimização de custos e diversificação

Para criar uma frota de Instâncias spot que seja barata e diversificada, use a estratégia de alocação `lowestPrice` em combinação com `InstancePoolsToUseCount`. O Frota spot 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 spot especificado. Esta combinação pode ser usada para evitar Instâncias spot mais caras.

Escolher uma estratégia de alocação apropriada

Você pode otimizar as Frotas spot com base em seu caso de uso.

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 Instância

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 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 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 executar um serviço da web, recomendamos que especifique um grande número de grupos spot (por exemplo, `InstancePoolsToUseCount=10`) para minimizar o impacto se um grupo de Instância spot ficar temporariamente indisponível.

Substituições do preço spot

Cada solicitação de Frota spot pode incluir um preço máximo global ou usar o padrão (preço sob demanda). O Frota spot usa como o preço máximo padrão para cada especificação 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.

Peso da instância da Frota spot

Ao solicitar uma frota de Instâncias spot, você poderá definir as unidades de capacidade com que cada tipo de instância contribuirá para o desempenho do aplicativo e poderá ajustar corretamente seu preço máximo para cada grupo de Instância 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 seu preço por hora dividindo seu preço para um tipo de instância pelo número de unidades que ele representa. A Frota spot calcula a quantidade de Instâncias spot a ser executada, dividindo a capacidade de destino pelo peso da instância. Se o resultado não for um inteiro, a Frota spot será arredondado para o próximo inteiro, para que o tamanho da frota não fique abaixo da 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
r3.xlarge	2	0,05 USD	0,025	5 (10 dividido por 2)

Tipo de instância	Peso da instância	Preço por hora de instância	Preço por hora	Número de instâncias executadas
			(0,05 dividido por 2)	

Tipo de instância	Peso da instância	Preço por hora de instância	Preço por hora	Número de instâncias executadas
r3.8xlarge	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 da Frota spot 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 spot 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 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.

Apresentação: Como usar a Frota spot com o peso da instância

Esta apresentação usa uma empresa fictícia chamada Exemplo Corp para ilustrar o processo de solicitação de uma Frota spot usando o peso da instância.

Objetivo

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.

Planejamento

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 um aplicativo 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 o aplicativo 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 seu aplicativo (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	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`.

Verificação de 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 [Pré-requisitos do Frota spot \(p. 317\)](#).

Criação da 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 seguinte comando `request-spot-fleet`:

```
aws ec2 request-spot-fleet --spot-fleet-request-config file://config.json
```

Para obter mais informações, consulte [Solicitação de Frota spot \(p. 315\)](#).

Atendimento

A estratégia de alocação determina de quais grupos de Instância spot suas Instâncias spot procedem.

Com a estratégia `lowestPrice` (que é uma estratégia padrão), as instâncias 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).

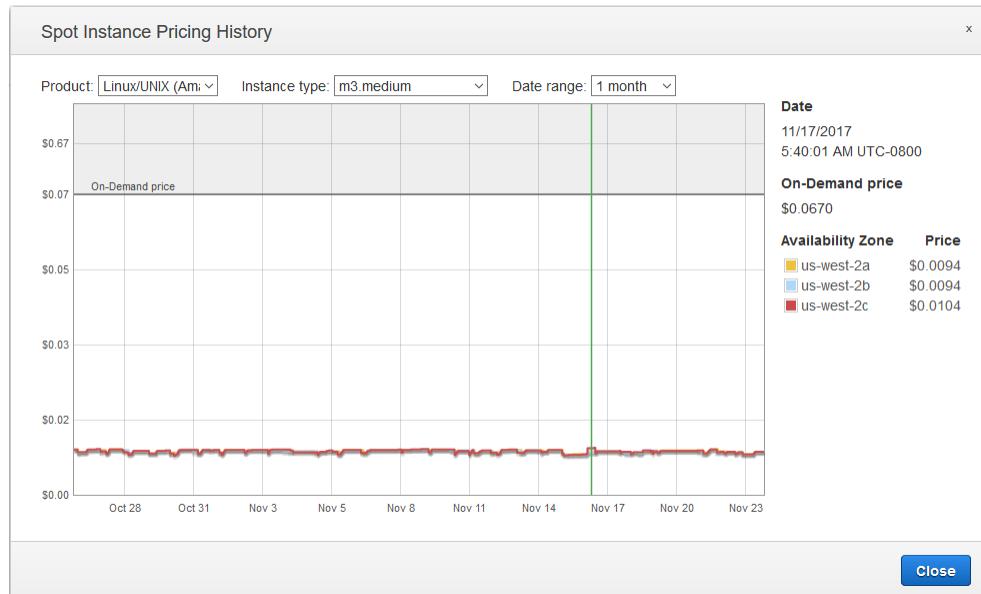
Se a Exemplo Corp usasse a estratégia `diversified`, as Instâncias spot viriam dos três grupos. A Frota spot executaria seis instâncias `r3.2xlarge` (que fornecem 6 unidades), três instâncias `r3.4xlarge` (que fornecem 6 unidades), duas instâncias `r3.8xlarge` (que fornecem 8 unidades), totalizando 20 unidades.

Histórico de definição de preço de Instância spots

Ao solicitar Instâncias spot, recomendamos que você use o preço máximo padrão (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 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. Se você estiver começando a usar o Instâncias spot, verá uma página de boas-vindas. Escolha Conceitos básicos, role até a parte inferior da tela e escolha Cancelar.
4. Escolha Histórico de definição de preço. Por padrão, a página exibe um gráfico de dados para instâncias `t1.micro` Linux em todas as zonas de disponibilidade no dia anterior. Mova o ponteiro do mouse sobre o gráfico para exibir os preços em horas específicas na tabela abaixo do gráfico.



5. (Opcional) Para rever o histórico de preços spot para uma zona de disponibilidade específica, selecione uma zona na lista. Você também pode selecionar outro produto, tipo de instância ou intervalo de datas.

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 [Acessando o Amazon EC2 \(p. 3\)](#).

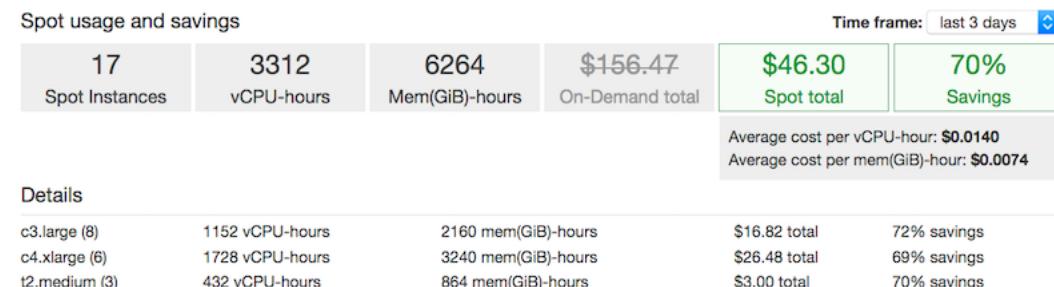
- `describe-spot-price-history` (AWS CLI)

- [Get-EC2SpotPriceHistory](#) (AWS Tools para 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 página Spot Requests (Solicitações spot) mostra as informações de uso e de economia spot para uma Frota spot.



Você pode visualizar as seguintes informações de uso e de economia:

- 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 economias 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 uma solicitação de Frota spot e escolha Savings (Economias).
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.

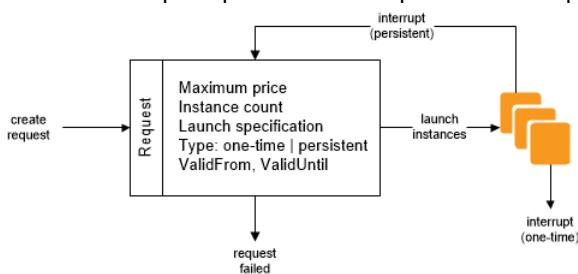
Para visualizar as informações de economias de todas as Instâncias spot em execução (console)

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).

Solicitação de Instância spot

Para usar Instâncias spot, você cria uma solicitação de Instância spot que inclua o número de instâncias, 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 spot funcionam. Observe que a ação tomada para uma interrupção de Instância spot depende do tipo de solicitação (única ou persistente) e do comportamento da interrupção (espera, interrupção ou encerramento). Se a requisição for persistente, ela será aberta novamente depois que a Instância spot for interrompida.



Tópicos

- [Estados das solicitações de Instância spot \(p. 306\)](#)
- [Como especificar a duração para suas Instâncias spot \(p. 307\)](#)
- [Como especificar a locação para suas Instâncias spot \(p. 308\)](#)
- [Função vinculada a serviço para solicitações de Instância spot \(p. 309\)](#)
- [Criação da solicitação de Instância spot \(p. 309\)](#)
- [Como localizar Instâncias spot em execução \(p. 312\)](#)
- [Marcação de solicitações de Instância spot \(p. 313\)](#)
- [Cancelamento de uma solicitação de Instância spot \(p. 313\)](#)
- [Encerramento de uma Instância spot \(p. 313\)](#)
- [Exemplo de especificações de execução de solicitações spot \(p. 314\)](#)

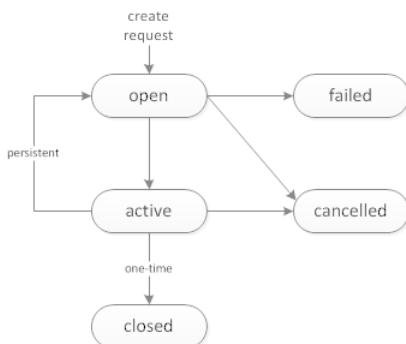
Estados das solicitações de Instância spot

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.
- **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. Se a Instância spot estiver encerrada, a solicitação de Instância spot será aberta novamente e o Amazon EC2 executará uma nova Instância spot.

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 \(p. 342\)](#).

Como especificar a duração para suas Instâncias spot

As Instâncias spot com uma duração especificada (também conhecidas como blocos spot) são projetadas para não serem interrompidas e serão executadas continuamente pela duração que você selecionar. Isso as torna ideais para trabalhos que levam um período finito para serem concluídos, como o processamento em lote, a codificação e a renderização, a modelagem e análise e a integração contínua.

Você pode especificar uma duração de 1, 2, 3, 4, 5 ou 6 horas. O preço que você paga depende da duração especificada. Para visualizar os preços atuais por um período de 1 hora ou de 6 horas, consulte [Preços de Instância spot](#). Você pode usar esses preços para estimar o custo de durações de 2, 3, 4 e 5 horas. Quando uma solicitação com uma duração é atendida, o preço da Instância spot é fixo, e esse preço permanece em vigor até o encerramento da instância. Será cobrado esse preço por cada hora ou hora parcial de execução da instância. Uma hora de instância parcial é faturada para a segunda mais próxima.

Ao especificar uma duração na solicitação spot, a duração de cada Instância spot é iniciada assim que a instância recebe o ID de instância. A Instância spot é executada até que você a encerre ou até o término da duração. No final do período de duração, o Amazon EC2 marca a Instância spot para encerramento e fornece um aviso de encerramento de Instância spot, enviando à instância um aviso de dois minutos antes que ela seja encerrada. Em raras situações, os blocos spot podem ser interrompidos devido a

necessidades de capacidade do Amazon EC2. Nesses casos, enviamos um aviso dois minutos antes de encerrarmos uma instância, e você não será cobrado pelas instâncias encerradas mesmo se as usou.

Para executar Instâncias spot com uma duração especificada (console)

Selecione o tipo apropriado de solicitação. Para obter mais informações, consulte [Criação da solicitação de Instância spot \(p. 309\)](#).

Para executar Instâncias spot com uma duração especificada (AWS CLI)

Para especificar uma duração para as Instâncias spot, inclua a opção `--block-duration-minutes` com o comando `request-spot-instances`. Por exemplo, o comando a seguir criar uma solicitação spot que executa Instâncias spot que foram executadas por duas horas:

```
aws ec2 request-spot-instances --instance-count 5 --block-duration-minutes 120 --type "one-time" --launch-specification file://specification.json
```

Para recuperar o custo de Instâncias spot com uma duração especificada (AWS CLI)

Use o comando `describe-spot-instance-requests` para recuperar o custo fixo das Instâncias spot com uma duração especificada. As informações estão no campo `actualBlockHourlyPrice`.

Como especificar a locação para suas Instâncias spot

Você pode executar uma Instância spot no hardware de locação única. As Instâncias spot dedicadas são fisicamente isoladas de instâncias que pertencem a outras contas da AWS. Para obter mais informações, consulte [Instâncias dedicadas \(p. 371\)](#) 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 [Criação da solicitação de Instância spot \(p. 309\)](#).
- Solicite uma Instância 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 \(p. 373\)](#). Você não pode solicitar uma Instância spot com um locação `default` se solicitá-la em uma VPC com uma locação de instância `dedicated`.

Os tipos de instância a seguir oferecem suporte a instâncias Instâncias spot.

Geração atual

- `c4.8xlarge`
- `d2.8xlarge`
- `i3.16xlarge`
- `m4.10xlarge`
- `m4.16xlarge`
- `p2.16xlarge`
- `r4.16xlarge`
- `x1.32xlarge`

Geração anterior

- `c3.8xlarge`
- `cc2.8xlarge`

- **cri.8xlarge**
- **g2.8xlarge**
- **i2.8xlarge**
- **r3.8xlarge**

Função vinculada a serviço para solicitações de Instância spot

O Amazon EC2 cria uma função vinculada a serviço ao solicitar uma Instâncias spot. Uma função vinculada ao serviço inclui todas as permissões que o Amazon EC2 exige para chamar todos os outros serviços da AWS em seu nome. Para obter mais informações, consulte [Uso de funções vinculadas ao serviço](#) no Guia do usuário do IAM.

O Amazon EC2 usa a função vinculada a serviço chamada AWSServiceRoleForEC2Spot para concluir as seguintes ações:

- **ec2:DescribeInstances** – descrever as Instâncias spot
- **ec2:StopInstances** – interromper as Instâncias spot
- **ec2:StartInstances** – iniciar as Instâncias spot

Se você especificar snapshots do EBS criptografados para as Instâncias spot e usar CMKs gerenciadas pelo cliente para criptografia, deverá conceder acesso à função AWSServiceRoleForEC2Spot às CMKs para que o Amazon EC2 possa executar Instâncias spot em seu nome. O principal é o nome de recurso da Amazon (ARN) da função AWSServiceRoleForEC2Spot. Para obter mais informações, consulte [Como usar políticas de chaves no AWS KMS](#).

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 a 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.

Verifique se esta função está disponível antes de usar a AWS CLI ou uma API para criar uma Frota spot. Para criar a função, use o console do IAM da seguinte forma.

Para criar a função do IAM (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).

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.

Criação da solicitação de Instância spot

O processo de solicitação de uma Instância spot é semelhante ao processo de execução de uma instância sob demanda. Você não pode alterar os parâmetros da solicitação de Instância spot, incluindo seu preço máximo, após enviar a solicitação.

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 Instância spot, consulte [Status da solicitação spot \(p. 342\)](#).

Pré-requisitos

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 de Instância spots \(p. 304\)](#).

Para criar 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, selecione Solicitações spot.
3. Se você estiver começando a usar Instâncias spot, verá uma página de boas-vindas. Escolha Get started (Comece a usar). Caso contrário, selecione Solicitar Instâncias spot.
4. Em Request type (Tipo de solicitação), o padrão será Request (Solicitação), que especifica uma solicitação spot única criada por meio de uma Frota spot. Para usar os blocos spot, escolha Reserve for duration e selecione o número de horas para que o trabalho seja concluído.

Para usar Request and Maintain (Solicitar e manter), consulte [Criação da solicitação de Frota spot \(p. 320\)](#).

5. Em Capacidade de destino, digite o número de unidades a serem solicitadas. Você pode escolher instâncias ou características de desempenho que são importantes para a carga de trabalho de seu aplicativo, como vCPUs, memória e armazenamento.
6. Em Requirements, faça o seguinte:
 - a. [Frota spot] Para Launch template (Modelo de execução), 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.
 - b. Em AMI, escolha uma das AMIs básicas fornecidas pela AWS ou selecione Usar AMI personalizada para especificar sua própria AMI.
 - c. Em Tipo(s) de instância, escolha Selecionar. Selecione os tipos de instâncias que têm as especificações mínimas de hardware necessárias (vCPUs, memória e armazenamento).
 - d. Para Network (Rede), você pode selecionar uma VPC existente ou criar uma nova.

[VPC existente] Selecione a VPC.

[VPC nova] Selecione 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), o padrão é deixar a AWS escolher as zonas de disponibilidade para suas Instâncias spot. Se você preferir, pode selecionar zonas de disponibilidade específicas.

Selecione uma ou mais zonas de disponibilidade. Se houver mais de uma sub-rede em uma zona de disponibilidade, selecione a sub-rede apropriada em Sub-rede. Para adicionar sub-redes, selecione 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) Para adicionar armazenamento, especifique outros volumes de armazenamento de instâncias ou volumes do EBS, dependendo do tipo de instância. Você também pode habilitar a otimização do Amazon EBS.
- g. (Opcional) Por padrão, o monitoramento básico está habilitado para suas instâncias. Para habilitar o monitoramento detalhado, selecione Enable CloudWatch detailed monitoring (Habilitar monitoramento detalhado do CloudWatch).

- h. (Opcional) Para executar uma Instância spot dedicada, em Tenancy (Locação), selecione em Dedicated - run a dedicated instance (Dedicada – executar uma instância dedicada).
 - i. Para Security groups, selecione um ou mais security groups.
 - j. Para se conectar às instâncias, habilite Auto-assign IPv4 Public IP (Atribuir IPv4 público automaticamente).
 - k. (Opcional) Para se conectar às suas instâncias, especifique o par de chaves em Key pair name.
 - l. (Opcional) Para executar as Instâncias spot com uma função do IAM, em IAM instance profile (Perfil de instância do IAM), especifique a função.
 - m. (Opcional) Para executar um script de startup, copie-o para User data.
 - n. [Frota spot] 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.
7. Para Spot request fulfillment, faça o seguinte:
 - a. [Frota spot] Em Allocation strategy (Estratégia de alocação), escolha a estratégia que atende às suas necessidades. Para obter mais informações, consulte [Estratégia de alocação para Instâncias spot \(p. 299\)](#).
 - b. [Frota spot] Para 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.
 - c. (Opcional) Para criar uma solicitação que seja válida somente em um período específico, edite os valores em Request valid from (Solicitação válida de) e Request valid until (Solicitação válida até).
 - d. [Frota spot] Por padrão, encerramos as Instâncias spot quando a solicitação expira. Para mantê-las em execução depois que sua solicitação expirar, limpe Encerrar instâncias na expiração.
 8. (Opcional) Para registrar Instâncias spot em um load balancer, escolha Receive traffic from one or more load balancers (Receber tráfego de um ou mais load balancers) e selecione 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.

[Frota spot] O tipo da solicitação é `fleet`. Quando a solicitação for atendida, as solicitações do tipo `instance` serão adicionadas, onde o estado será `active` e o status será `fulfilled`.

[Bloco spot] O tipo de solicitação é `block` e o estado inicial é `open`. Quando a solicitação for atendida, o estado será `active` e o status será `fulfilled`.

Para criar uma solicitação de Instância spot (AWS CLI)

Use o seguinte 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 seguinte 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 spot \(p. 314\)](#). Se você fizer download de um arquivo de especificação de execução no console, use o comando `request-spot-fleet` (o console especifica uma solicitação spot usando uma Frota spot).

O Amazon EC2 executará sua 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. Use o seguinte comando [describe-spot-instance-requests](#) para monitorar a solicitação de Instância spot:

```
aws ec2 describe-spot-instance-requests --spot-instance-request-ids sir-08b93456
```

Como localizar 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 visualizar solicitações de Instância spot e 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

As solicitações de instâncias spot não são marcadas instantaneamente e por um período podem parecer estarem separadas das Spot Fleet Requests (SFR).

3. Como alternativa, no painel de navegação, escolha Instâncias. No canto superior direito, escolha Mostrar/ocultar e selecione Ciclo de vida. Para cada instância, o Ciclo de vida é normal, spot ou scheduled.

Para localizar Instâncias spot em execução (AWS CLI)

Para enumerar as Instâncias spot, use o comando [describe-spot-instance-requests](#) com a opção `--query`, da seguinte maneira:

```
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`, da seguinte maneira:

```
aws ec2 describe-instances --filters "Name=instance-lifecycle,Values=spot"
```

Marcação de solicitações de Instância spot

Para categorizar e gerenciar as solicitações de Instância spot, você pode marcá-las com os metadados de sua preferência. Para obter mais informações, consulte [Marcação dos seus recursos do Amazon EC2 \(p. 1003\)](#).

Você pode atribuir uma tag à solicitação de Instância spot depois de criá-la. As tags criadas para suas solicitações de Instância spots se aplicam somente às solicitações. Essas tags não são adicionadas automaticamente à Instância spot que o serviço spot executa para atender à solicitação. Você mesmo deve adicionar tags a uma Instância spot depois de Instância spot ser executada.

Para adicionar uma tag à solicitação de Instância spot ou a uma Instância spot usando a AWS CLI

Use o comando [create-tags](#) para marcar seus recursos:

```
aws ec2 create-tags --resources sir-08b93456 i-1234567890abcdef0 --tags  
Key=purpose,Value=test
```

Cancelamento de uma solicitação de Instância spot

Se você não quiser mais sua solicitação spot, poderá cancelá-la. Você só pode cancelar solicitações de instância spot `open` ou `active`. A solicitação spot é `open` quando sua requisição não ainda não tiver sido atendida e nenhuma instância tiver sido executada. A solicitação spot será `active` quando ela for atendida e as Instâncias spot forem executadas como resultado. Se a solicitação spot estiver `active` e tiver uma Instância spot associada em execução, o cancelamento da solicitação não encerrará a instância. Para obter mais informações sobre o encerramento de uma Instância spot, consulte a próxima seção.

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 spot.
3. Escolha Actions (Ações), Cancel spot request (Cancelar solicitação spot).
4. (Opcional) Ao terminar de trabalhar com as Instâncias spot associadas, você poderá encerrá-las. No painel de navegação, escolha Instances (Instâncias), selecione a instância e escolha Actions (Ações), Instance State (Estado da instância) e Terminate (Encerrar).

Para cancelar uma solicitação de Instância spot (AWS CLI)

- Use o seguinte comando [cancel-spot-instance-requests](#) para cancelar a solicitação spot especificada:

```
aws ec2 cancel-spot-instance-requests --spot-instance-request-ids sir-08b93456
```

Encerramento de uma Instância spot

Se a solicitação spot for `active` e tiver uma Instância spot associada em execução, o cancelamento da solicitação não encerrará a instância; você precisará encerrar a Instância spot em execução manualmente. Se você encerrar uma Instância spot em execução que foi executada por uma solicitação spot persistente, a solicitação spot retornará o estado `open` para que uma nova Instância spot possa ser executada. Para cancelar uma solicitação spot persistente e encerrar as Instâncias spot, você precisará cancelar a solicitação spot primeiro e depois encerrar as Instâncias spot. Caso contrário, a solicitação Spot persistente poderá executar uma nova instância. Para obter mais informações sobre como cancelar uma solicitação de Instância spot, consulte a seção anterior.

Para encerrar uma Instância spot manualmente (AWS CLI)

- Use o comando [terminate-instances](#) a seguir para encerrar a Instâncias spot manualmente:

```
aws ec2 terminate-instances --instance-ids i-1234567890abcdef0 i-0598c7d356eba48d7
```

Exemplo de especificações de execução de solicitações 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 [Criação da solicitação de Instância spot](#) (p. 309).

1. Executar Instâncias spot (p. 314)
2. Executar Instâncias spot na zona de disponibilidade especificada (p. 314)
3. Executar Instâncias spot na sub-rede especificada (p. 314)
4. Executar uma Instância spot dedicada (p. 315)

Exemplo 1: Executar Instâncias spot

O exemplo a seguir não inclui uma zona de disponibilidade ou 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"  
    }  
}
```

Solicitação de Frota spot

Para usar uma Frota spot, crie uma solicitação de Frota spot que inclua a capacidade de destino, uma parte opcional sob demanda, uma ou mais especificações de execução para as instâncias e o preço máximo que você está disposto a pagar. O Amazon EC2 tenta manter a capacidade de destino do Frota spot conforme os preços spot mudam. Para obter mais informações, consulte [Como Frota spot funciona \(p. 298\)](#).

Há dois tipos de solicitações de Frota spot: `request` e `maintain`. Você pode criar uma Frota spot para enviar uma solicitação única da capacidade desejada ou solicitar que ela mantenha uma capacidade de destino ao longo do tempo. Os dois tipos de solicitações se beneficiam com a estratégia de alocação da Frota spot.

Ao criar uma solicitação única, a Frota spot fará as solicitações necessárias, mas não tentará reabastecer Instâncias spot se a capacidade for reduzida. Se a capacidade não estiver disponível, a Frota spot não enviará solicitações em grupos spot alternativos.

Para manter uma capacidade de destino, a Frota spot fará as solicitações necessárias para cumprir a capacidade de destino e reabastecerá automaticamente todas as instâncias interrompidas.

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 poderá especificar se o cancelamento da solicitação de Frota spot encerrará ou não as Instâncias spot na Frota spot.

Cada especificação de execução inclui as informações de que o Amazon EC2 precisa para executar uma instância, como uma AMI, um tipo de instância, uma sub-rede ou uma zona de disponibilidade e um ou mais security groups.

Tópicos

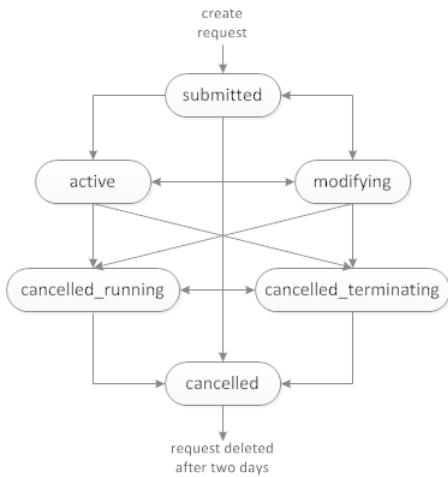
- [Estados das solicitações de Frota spots \(p. 316\)](#)
- [Pré-requisitos do Frota spot \(p. 317\)](#)
- [Usuários do Frota spot e IAM \(p. 317\)](#)
- [Verificações de integridade da Frota spot \(p. 318\)](#)
- [Planejamento de uma solicitação de Frota spot \(p. 319\)](#)
- [Função vinculada a serviço para solicitações de Frota spot \(p. 319\)](#)
- [Criação da solicitação de Frota spot \(p. 320\)](#)
- [Como monitorar um Frota spot \(p. 324\)](#)
- [Modificação da solicitação de Frota spot \(p. 324\)](#)
- [Cancelamento de uma solicitação de Frota spot \(p. 325\)](#)
- [Exemplos de configuração de Frota spot \(p. 326\)](#)

Estados das solicitações de Frota spots

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 de destino de Instâncias spot.
- **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 é 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 foi cancelada, e as Instâncias spot estão sendo encerradas. A solicitação permanece nesse estado até que todas as instâncias sejam encerradas.
- **cancelled** – a Frota spot foi 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.



Pré-requisitos do Frota spot

Se você usar o console do Amazon EC2 para criar uma Frota spot, ele criará uma função chamada aws-ec2-spot-fleet-tagging-role que concederá à Frota spot permissão para solicitar, executar, encerrar e marcar instâncias em seu nome. Essa função é selecionada quando você cria a solicitação de Frota spot. Se você usar a AWS CLI ou uma API em vez disso, deverá assegurar que essa função existe. Você pode usar o assistente de solicitação de Instâncias spot (a função é criada quando você avança para a segunda página do assistente) ou usar o console do IAM da maneira a seguir.

Para criar uma função do IAM para o Frota spot

1. Abra o console do IAM em <https://console.aws.amazon.com/iam/>.
 2. No painel de navegação, selecione Roles.
 3. Na página Select type of trusted entity (Selecionar tipo de entidade confiável), escolha AWS Service (Serviço da AWS), EC2, EC2 - Spot Fleet Tagging (EC2 - marcação de frota spot), Next: Permissions (Próximo: permissões).
 4. Na página Attached permissions policy, escolha Next: Review.
 5. Na página Review (Revisar), digite um nome para a função (por exemplo, **aws-ec2-spot-fleet-tagging-role**) e escolha Create role (Criar função).

Usuários do Frota spot e IAM

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 Create policy (Criar política), escolha JSON, substitua o texto pelo seguinte e escolha Review policy (Revisar política).

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",
```

```
        "Action": [
            "ec2:*"
        ],
        "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 spot 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`

4. Na página **Review policy** (Revisar política), digite um nome e uma descrição para a política e escolha **Create policy** (Criar política).
5. No painel de navegação, escolha **Users (Usuários)** e selecione o usuário.
6. Selecione **Permissions** e **Add permissions**.
7. Selecione **Attach existing policies directly**. Selecione a política que você criou anteriormente e escolha **Next: Review** (Próximo: Revisão).
8. Selecione **Add permissions**.

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`. Frota spot determina o status de integridade de uma instância usando as verificações de status fornecidas por Amazon EC2. Se o status da verificação de status da instância ou da verificação de status do sistema for `impaired` para três verificações de integridade consecutivas, o status de integridade da instância será `unhealthy`. Caso contrário, o status de integridade será `healthy`. Para obter mais informações, consulte [Verificações de status para suas instâncias](#) (p. 565).

Você pode configurar a Frota spot para substituir instâncias não íntegras. Depois de habilitar a substituição de verificação de integridade, uma instância é substituída após o status de integridade ser relatado como `unhealthy`. A Frota spot pode ficar abaixo de sua capacidade de destino por até alguns minutos enquanto uma instância não íntegra está sendo substituída.

Requisitos

- A substituição de verificação de integridade só tem suporte em Frotas spot que mantêm uma capacidade de destino, e não em Frotas spot únicas.
- 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`.

Planejamento de uma solicitação de Frota spot

Antes de criar uma solicitação de Frota spot, leia as [Melhores práticas 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 da instância da Frota spot \(p. 300\)](#).
- 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` no AWS CLI Command Reference. Para obter exemplos adicionais, consulte [Exemplos de configuração de Frota spot \(p. 326\)](#).

Função vinculada a serviço para solicitações de Frota spot

O Amazon EC2 cria uma função vinculada a serviço ao solicitar uma Frota spot. Uma função vinculada ao serviço inclui todas as permissões que o Amazon EC2 exige para chamar todos os outros serviços da AWS em seu nome. Para obter mais informações, consulte [Uso de funções vinculadas ao serviço](#) no Guia do usuário do IAM.

O Amazon EC2 usa a função vinculada a serviço chamada `AWSServiceRoleForEC2SpotFleet` para concluir as seguintes ações:

- `ec2:RequestSpotInstances` - Solicitar Instâncias spot
- `ec2:TerminateInstances` - Encerrar Instâncias spot
- `ec2:DescribeImages` - Descreva imagens de máquina da Amazon (AMI) para Instâncias spot
- `ec2:DescribeInstanceStatus` - Descreva o status das Instâncias spot
- `ec2:DescribeSubnets` - Descreva as sub-redes para Instâncias spot
- `ec2:CreateTags` – Adicionar tags de sistema a Instâncias spot

O Amazon EC2 também cria a função `AWSServiceRoleForEC2Spot` ao solicitar uma Frota spot. Para obter mais informações, consulte [Função vinculada a serviço para solicitações de Instância spot \(p. 309\)](#).

Se você tinha uma solicitação de Frota spot ativa antes de novembro de 2017, quando o Amazon EC2 começou a oferecer suporte a essa função vinculada a serviço, o Amazon EC2 criou a função

AWS*ServiceRoleForEC2SpotFleet* em sua conta da AWS. Para obter mais informações, consulte [Uma nova função apareceu na minha conta](#) no Guia do usuário do IAM.

Verifique se esta função está disponível antes de usar a AWS CLI ou uma API para criar uma Frota spot. Para criar a função, use o console do IAM da seguinte forma.

Para criar uma função do IAM para a Frota spot (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 Fleet (EC2 - frota spot), Next: Permissions (Próximo: permissões).
5. Na próxima página, escolha Next:Review (Próximo: revisar).
6. Na página Review (Revisar), selecione Create role (Criar função).

Se você não precisar mais usar Frota spot, é recomendável excluir a função *AWS*ServiceRoleForEC2SpotFleet**. Depois que essa função for excluída da sua conta, o Amazon EC2 criará a função novamente se você solicitar um Frota spot.

Criação da solicitação de Frota spot

Usando o Console de gerenciamento da AWS, crie rapidamente uma solicitação de Frota spot escolhendo apenas o aplicativo ou tarefa necessária e as especificações mínimas de computação. O Amazon EC2 configura uma frota que melhor atende às suas necessidades e segue a melhor prática do Spot. Para obter mais informações, consulte [Criar uma solicitação de Frota spot rapidamente \(console\) \(p. 320\)](#). Caso contrário, você pode modificar qualquer uma das configurações padrão. Para obter mais informações, consulte [Criar uma solicitação de Frota spot usando parâmetros definidos \(console\) \(p. 321\)](#).

[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 seu aplicativo ou tarefa), escolha Flexible workloads (Cargas de trabalho flexíveis), Load balancing workloads (Cargas de trabalho do balanceamento de carga), Big data workloads (Cargas de trabalho de big data) ou Defined duration workloads (Cargas de trabalho com duração definida).
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 o aplicativo 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 seu aplicativo 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 seu aplicativo ou tarefa), escolha Flexible workloads (Cargas de trabalho flexíveis), Load balancing workloads (Cargas de trabalho do balanceamento de carga), Big data workloads (Cargas de trabalho de big data) ou Defined duration workloads (Cargas de trabalho com duração definida).
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 o aplicativo 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. (Opcional) Em Network (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 adicionar armazenamento, especifique volumes de armazenamento de instâncias ou volumes do Amazon EBS adicionais, dependendo do tipo de instância.
- b. (Opcional) Para habilitar a otimização do Amazon EBS, em EBS-optimized (Otimizada para EBS), escolha Launch EBS-optimized instances (Executar instâncias otimizadas para EBS).
- c. (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).
- 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 CloudWatch).
- e. (Opcional) Para executar uma Instância spot dedicada, em Tenancy (Locação), selecione em Dedicated - run a dedicated instance (Dedicada – executar uma instância dedicada).
- f. (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.

- g. (Opcional) Para tornar as instâncias acessíveis na Internet, em Auto-assign IPv4 Public IP (Atribuir automaticamente IP público IPv4), escolha Enable (Habilitar).
 - h. (Opcional) Para executar as Instâncias spot com uma função do IAM, em IAM instance profile (Perfil de instância do IAM), escolha a função.
 - i. (Opcional) Para executar um script de startup, copie-o para User data.
 - j. (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.
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 que a Total target capacity (Capacidade total de destino). 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) Para substituir instâncias não íntegras em uma Frota spot Solicitar e manter, selecione Replace unhealthy instance (Substituir instâncias não íntegras).
- d. (Opcional) Por padrão, o serviço spot encerra Instâncias spot quando elas são interrompidas. Para manter a capacidade de destino, escolha Maintain target capacity (Manter a capacidade do 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.

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 seu aplicativo ou tarefa. Para alterar os tipos de instância ou a estratégia de alocação, desmarque **Apply recommendations** (Aplicar recomendações).
 - b. (Opcional) Para remover tipos de instância, em Fleet request (Solicitação de frota), escolha Remove (Remover). Para adicionar tipos de instância, escolha Select instance types (Selecionar tipos de instância).
 - c. (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 \(p. 299\)](#).
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 da 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`.

Para criar uma solicitação de Frota spot usando a AWS CLI

- Use o seguinte 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 \(p. 326\)](#).

A seguir está um exemplo de saída:

```
{  
    "SpotFleetRequestId": "sfr-73fb2ce-aa30-494c-8788-1cee4EXAMPLE"  
}
```

Como monitorar um Frotas spot

O Frotas 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 Frotas 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 Frotas spot. Para ver os detalhes da configuração, escolha Description (Descrição).
4. Para listar as Instâncias spot da Frotas spot, escolha Instances (Instâncias).
5. Para visualizar o histórico da Frotas spot, escolha a guia History (Histórico).

Para monitorar sua Frotas spot (AWS CLI)

Use o seguinte comando `describe-spot-fleet-requests` para descrever as solicitações de Frotas spot:

```
aws ec2 describe-spot-fleet-requests
```

Use o seguinte comando `describe-spot-fleet-instances` para descrever as Instâncias spot da Frotas spot especificada:

```
aws ec2 describe-spot-fleet-instances --spot-fleet-request-id sfr-73fdb2ce-  
aa30-494c-8788-1cee4EXAMPLE
```

Use o seguinte comando `describe-spot-fleet-request-history` para descrever o histórico da solicitação de Frotas spot especificada:

```
aws ec2 describe-spot-fleet-request-history --spot-fleet-request-id sfr-73fdb2ce-  
aa30-494c-8788-1cee4EXAMPLE --start-time 2015-05-18T00:00:00Z
```

Modificação da solicitação de Frotas spot

Você pode modificar uma solicitação de Frotas spot ativa para executar as seguintes tarefas:

- Aumentar a capacidade de destino
- Reduzir a capacidade de destino

Note

Você não pode modificar uma solicitação de Frotas spot única.

Você só pode modificar a parte da Instância spot de uma solicitação de Frotas spot. Você não pode modificar a parte da instância sob demanda de uma solicitação de Frotas spot.

Quando você aumenta a capacidade de destino, a Frotas spot executa as Instâncias spot adicionais de acordo com a estratégia de alocação da solicitação de Frotas spot. Se a estratégia de alocação for `lowestPrice`, a Frotas spot executará as instâncias do grupo de Instância spot com o menor preço na solicitação de Frotas spot. Se a estratégia de alocação for `diversified`, a Frotas spot distribuirá as instâncias pelos grupos na solicitação de Frotas spot.

Quando você diminui a capacidade de destino, a Frotas spot cancelará todas as solicitações abertas que excedem a nova capacidade de destino. Você pode solicitar que a Frotas spot encerre instâncias spot até

o tamanho da frota atingir a nova capacidade de destino. 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 Frota spot encerrará as instâncias entre os grupos. Como alternativa, você pode solicitar que a Frota spot mantenha seu tamanho atual, mas não substitua as instâncias spot que interrompidas ou encerradas manualmente.

Quando uma Frota spot encerra uma instância porque a capacidade de destino 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 a solicitação de Frota spot.
3. Escolha Actions (Ações) e Modify target capacity (Modificar capacidade de destino).
4. Em Modificar capacidade de destino, faça o seguinte:
 - a. Digite a nova capacidade de destino.
 - 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 seguinte comando `modify-spot-fleet-request` para atualizar a capacidade de destino 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
```

Cancelamento de uma solicitação de Frota spot

Ao terminar de usar a Frota spot, você poderá 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 suas 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 a 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 seguinte 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-73fb2ce-  
aa30-494c-8788-1cee4EXAMPLE --terminate-instances
```

A seguir está um exemplo de saída:

```
{  
    "SuccessfulFleetRequests": [  
        {  
            "SpotFleetRequestId": "sfr-73fb2ce-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-73fb2ce-  
aa30-494c-8788-1cee4EXAMPLE --no-terminate-instances
```

A seguir está um exemplo de saída:

```
{  
    "SuccessfulFleetRequests": [  
        {  
            "SpotFleetRequestId": "sfr-73fb2ce-aa30-494c-8788-1cee4EXAMPLE",  
            "CurrentSpotFleetRequestState": "cancelled_running",  
            "PreviousSpotFleetRequestState": "active"  
        }  
    ],  
    "UnsuccessfulFleetRequests": []  
}
```

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 [Criação da solicitação de Frota spot](#) (p. 320).

1. Executar Instâncias spot usando a zona de disponibilidade ou a sub-rede de menor preço da região (p. 327)
2. Executar Instâncias spot usando a zona de disponibilidade ou a sub-rede de menor preço de uma lista especificada (p. 327)
3. Executar Instâncias spot usando o tipo de instância de menor preço de uma lista especificada (p. 328)
4. Cancelar o preço da solicitação (p. 330)
5. Executar uma Frota spot usando a estratégia de alocação diversificada (p. 331)
6. Executar uma Frota spot usando o peso da instância (p. 333)
7. Executar uma Frota spot com capacidade sob demanda (p. 334)

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. O Frotas 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

O Frotas 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",  
            "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 (Zona de disponibilidade)

```
{  
    "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"  
        }  
    ]  
}
```

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 (Zona de disponibilidade)

```
{  
    "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 \(p. 299\)](#).

Availability Zone (Zona de disponibilidade)

```
{  
    "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"  
            }  
        }  
    ]  
}
```

Subnet (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"  
        }  
    ]  
}
```

```
        "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 as AZs. Para esse cenário, inclua cada AZ disponível 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 AZ diferente).

Availability Zone (Zona de disponibilidade)

```
{
    "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"
            }
        }
    ]
}
```

Subnet (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 da 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 da instância da Frota spot \(p. 300\)](#).

Availability Zone (Zona de disponibilidade)

```
{
    "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": 3
        }
    ]
}
```

Subnet (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 equilíbrio da capacidade de destino 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 disponíveis do Amazon EC2.

Para obter mais informações, consulte [Sob demanda na Frota spot \(p. 298\)](#).

```
{  
    "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-0dbb04d4a6cca5ad1",  
                "Version": "2"  
            },  
            "Overrides": [  
                {  
                    "InstanceType": "t2.medium",  
                    "WeightedCapacity": 1,  
                    "SubnetId": "subnet-d0dc51fb"  
                }  
            ]  
        }  
    ]  
}
```

Métricas do CloudWatch para Frota spot

O Amazon EC2 fornece métricas do Amazon CloudWatch que você pode usar para monitorar a Frota spot.

Important

Para garantir uma precisão, recomendamos que você habilite o monitoramento detalhado para usar essas métricas. Para obter mais informações, consulte [Habilitar e desabilitar o monitoramento detalhado para suas instâncias \(p. 575\)](#).

Para obter mais informações sobre as métricas do CloudWatch fornecidas pelo Amazon EC2, consulte [Monitoramento das suas instâncias usando o CloudWatch \(p. 575\)](#).

Métricas do 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 \(p. 577\)](#).

O namespace AWS/EC2Spot inclui as métricas a seguir.

Métrica	Descrição
AvailableInstancePoolsCount	Os grupos de Instância spot especificados na solicitação de Frota spot. Unidade: contagem
BidsSubmittedForCapacity	A capacidade para a qual Amazon EC2 enviou lances. Unidade: contagem
EligibleInstancePoolCount	Os grupos de Instância spot especificados na solicitação de Frota spot em que o Amazon EC2 pode atender a lances. O Amazon EC2 não atenderá a lances em grupos em que o preço do lance for menor que o preço spot, ou o preço spot for maior que o preço de Instâncias on-demand. Unidade: contagem
FulfilledCapacity	A capacidade preenchida pelo Amazon EC2. Unidade: contagem
MaxPercentCapacityAllocation	O valor máximo de PercentCapacityAllocation em todos os grupos de Frota spot especificados na solicitação de Frota spot. Unidade: percentual
PendingCapacity	A diferença entre TargetCapacity e FulfilledCapacity. Unidade: contagem
PercentCapacityAllocation	A capacidade alocada para o grupo de Instância spot para as dimensões especificadas. Para obter o valor máximo gravado em todos os grupos de Instância spot, use MaxPercentCapacityAllocation. Unidade: percentual
TargetCapacity	A capacidade de destino da solicitação de Frota spot. Unidade: contagem

Métrica	Descrição
TerminatingCapacity	A capacidade que está sendo encerrada, pois a capacidade provisionada é maior que a capacidade de destino. Unidade: contagem

Se a unidade de medida para uma métrica é Count, a estatística mais útil é Average.

Dimensões do 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.

Visualizar as métricas do CloudWatch para sua Frota spot

Você pode visualizar 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 de Frota spot ou grupos de métricas de Frota spot por ID de solicitação de Frota spot, tipo de instância ou zona de disponibilidade.

Para visualizar métricas da Frota spot

1. Abra o console do CloudWatch em <https://console.aws.amazon.com/cloudwatch/>.
2. No painel de navegação, em Métricas, escolha o namespace EC2 Spot.
3. (Opcional) Para filtrar as métricas por dimensão, selecione uma das seguintes ações:
 - Métricas de solicitação da frota — agrupar por solicitação de Frota spot
 - Por zona de disponibilidade — agrupar por solicitação de Frota spot e zona de disponibilidade
 - Por tipo de instância — agrupar por solicitação de Frota spot e tipo de instância
 - Por tipo de instância/zona de disponibilidade — agrupar por solicitação de Frota spot, zona de disponibilidade e tipo de instância
4. Para visualizar os dados de uma métrica, marque a caixa de seleção ao lado da métrica.

The screenshot shows the AWS CloudWatch Metrics interface. At the top, there's a search bar with 'EC2 Spot' and a 'Search Metrics' button. Below the search bar, there are navigation links: 'Fleet Request Metrics' (which is active), 'By Availability Zone', 'By Instance Type', and 'By Availability Zone/Instance Type'. A message says 'Showing all results (18) for EC2 Spot > Fleet Request Metrics. For more results expand your search to All EC2 Spot Metrics.' There are 'Select All' and 'Clear' buttons. The main area is titled 'EC2 Spot > Fleet Request Metrics' and shows a table with two columns: 'FleetRequestId' and 'Metric Name'. The table contains four rows, with the third row ('CPUUtilization') having a checked checkbox next to it.

FleetRequestId	Metric Name
sfr-4a707781-8fac-459b-a5ae-4701fceee47d7	AvailableInstancePoolsCount
sfr-4a707781-8fac-459b-a5ae-4701fceee47d7	BidsSubmittedForCapacity
<input checked="" type="checkbox"/> sfr-4a707781-8fac-459b-a5ae-4701fceee47d7	CPUUtilization
<input type="checkbox"/> sfr-4a707781-8fac-459b-a5ae-4701fceee47d7	DiskReadBytes

Escalabilidade automática da Frota spot

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) ou encerrar instâncias (reduzir a escala), no intervalo escolhido, em resposta a uma ou mais políticas de escalabilidade.

Se estiver usando peso de instância, 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 $12 * 0,2$ de 12 para obter 9,6 e o arredondará para 10, portanto, nenhuma ação de escalabilidade será executada.

Você também pode configurar o período do desaquecimento para uma política de escalabilidade. 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 seu aplicativo. 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.

O Frota spot oferece suporte aos seguintes tipos de escalabilidade automática:

- [Escalabilidade de rastreamento de destino \(p. 338\)](#)—Aumenta ou diminui a capacidade atual da frota com base em um valor de destino para uma métrica específica. Isso é semelhante à forma como o seu termostato mantém a temperatura da sua casa: você seleciona a temperatura e o termostato faz o resto.
- [Escalabilidade em etapas \(p. 339\)](#)—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 programada \(p. 341\)](#)—Aumenta ou diminui a capacidade atual da frota com base em data e hora.

Dimensionamento da Frota spot usando as políticas de rastreamento de destino

Com políticas de escalabilidade de rastreamento de destino, você seleciona uma métrica e define um valor de destino. O 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 escalabilidade de rastreamento de destino 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 cargas de trabalho de aplicativos.

Para garantir a disponibilidade do aplicativo, 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 de destino foi diminuída, a instância recebe um aviso de interrupção de Instância spot.

Não edite ou exclua os alarmes CloudWatch que o Frota spot gerencia para uma política de escalabilidade de rastreamento de destino. O Frota spot exclui os alarmes automaticamente quando você exclui a política de escalabilidade de rastreamento de destino.

Limites

- A solicitação de Frota spot deve ter o tipo de solicitação `maintain`. A escalabilidade automática não é compatível com solicitações únicas 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 Nome da política, digite um nome para a política.
7. Escolha uma Target metric.
8. Digite um Target value 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 Salvar.

Para configurar uma política de rastreamento de destino usando a AWS CLI

1. Registre a solicitação de Frota spot como um destino dimensionável usando o comando `register-scalable-target`.
2. Crie uma política de escalabilidade usando o comando `put-scaling-policy`.

Dimensionar uma 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 spot execute uma instância.

Quando uma Frota spot encerra uma instância porque a capacidade de destino foi diminuída, a instância recebe um aviso de interrupção de Instância spot.

Limits

- A solicitação de Frota spot deve ter o tipo de solicitação `maintain`. A escalabilidade automática não é compatível com solicitações únicas nem blocos spot.

Pré-requisitos

- Considere quais métricas do CloudWatch são importantes para seu aplicativo. 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 coleção de métricas do CloudWatch se o serviço que fornece as métricas não a habilitar por padrão.
- Se você usar o Console de gerenciamento da AWS para habilitar a escalabilidade automática para sua Frota spot, ele criará uma função denominada `aws-ec2-spot-fleet-autoscale-role` que concede ao Amazon EC2 Auto Scaling permissão para descrever os alarmes de suas políticas, monitorar a capacidade atual da frota e modificar a capacidade da frota. Se você configurar a escalabilidade automática usando a AWS CLI ou uma API, poderá usar essa função, se ela existir, ou criar manualmente sua própria função com essa finalidade.

Para criar uma função manualmente

1. Abra o console do IAM em <https://console.aws.amazon.com/iam/>.
2. No painel de navegação, escolha Roles (Funções) e Create role (Criar função).
3. Em Select type of trusted entity (Selecionar tipo de entidade confiável), escolha AWS service (Serviço da AWS).
4. Em Choose the service that will use this role (Selecionar o serviço que usará essa função), selecione EC2.
5. Para Select your use case (Selecionar caso de uso), selecione EC2 - Spot Fleet Auto Scaling (EC2 - Auto Scaling de frota spot) e Next: Permissions (Próximo: Permissões).

6. Para Attached permissions policy (Política de permissões anexadas), a política AmazonEC2SpotFleetAutoscaleRole aparecerá automaticamente. Selecione Next: Tags (Próximo: tags) e Next: Review (Próximo: revisar).
7. Para Review (Análise), digite um nome para a função e escolha Create role (Criar função).

Para 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. Escolha Create Alarm.
4. Em Métricas do CloudWatch por categoria, escolha uma categoria. Por exemplo, escolha Métricas spot do EC2, Métricas de solicitação de frota.
5. Selecione uma métrica e escolha Next (Avançar).
6. Em Limite do alarme, digite o nome e a descrição do alarme e defina o valor de limite e o número de períodos para o alarme.
7. (Opcional) Para receber uma notificação de um evento de escalabilidade, em Ações, escolha Nova lista e digite seu endereço de e-mail. Caso contrário, você poderá excluir a notificação agora e adicionar uma posteriormente, quando necessário.
8. Escolha Create Alarm.

Para configurar políticas de escalabilidade em etapas 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 Nome da política, digite um nome para a política.
 - b. Em Policy trigger (Gatilho de políticas), selecione um alarme existente ou escolha Create new alarm (Criar novo alarme) para abrir o console do Amazon CloudWatch e criar um alarme.
 - c. Em Modificar capacidade, selecione um tipo de ajuste de escalabilidade, um número e uma unidade.
 - d. (Opcional) Para executar a escalabilidade em etapas, escolha Definir etapas. Por padrão, uma política de adição tem um limite de -infinitude menor e um limite superior do limite de alarme. Por padrão, uma política de remoção tem um limite menor do limite de alarme e um limite maior de +infinitude. Para adicionar outra etapa, escolha Adicionar etapa.
 - e. (Opcional) Para modificar o valor padrão para o período do desaquecimento, selecione um número em Período de desaquecimento.
8. Escolha 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 dimensionável usando o comando [register-scalable-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](#).

Escalar o Frota spot usando a escalabilidade programada

A escalabilidade com base em uma programação permite que você dimensione seu aplicativo em resposta a alterações de demanda. Para usar a escalabilidade programada, crie ações programadas, que instruem o Frota spot a executar ações de escalabilidade em momentos específicos. Quando você cria uma ação programada, especifica o Frota spot, 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.

Limites

- A solicitação de Frota spot deve ter o tipo de solicitação `maintain`. A escalabilidade automática não é compatível com solicitações únicas 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 a solicitação de Frota spot e escolha Scheduled Scaling (Escalabilidade programada).
4. Escolha Create Scheduled Action (Criar ação programada).
5. Em Name (Nome), especifique um nome para a ação programada.
6. Digite 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 a solicitação de Frota spot e escolha Scheduled Scaling (Escalabilidade programada).
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 Eventos do Amazon CloudWatch.
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 a solicitação de Frota spot e escolha Scheduled Scaling (Escalabilidade programada).
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 a solicitação de Frota spot e escolha Scheduled Scaling (Escalabilidade programada).
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](#)

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.

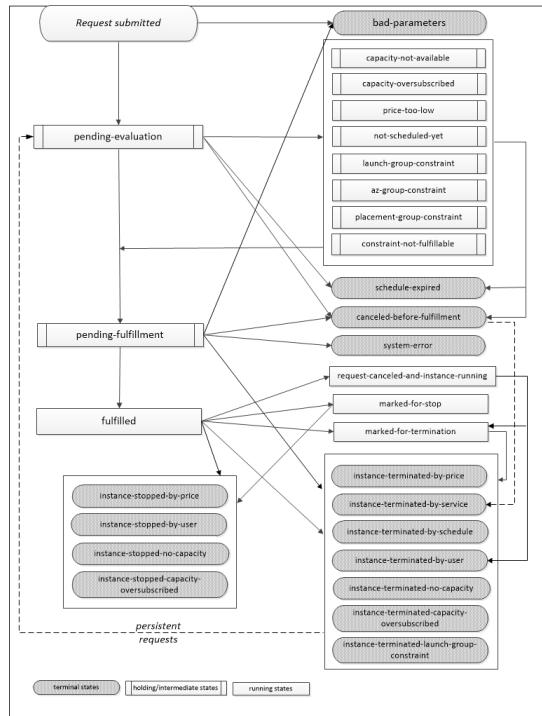
Em cada etapa do processo — também denominado ciclo de vida da solicitação spot, eventos específicos determinam estados sucessivos de solicitação.

Tópicos

- [Ciclo de vida de uma solicitação spot \(p. 342\)](#)
- [Como obter informações de status da solicitação \(p. 346\)](#)
- [Códigos de status das solicitações spot \(p. 346\)](#)

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 faz uma solicitação de Instância spot, ela entra no estado **pending-evaluation**, a menos que um ou mais parâmetros da solicitação não sejam válidos (**bad-parameters**).

Código de status	Estado da solicitação	Estado da instância
pending-evaluation	open	n/a
bad-parameters	closed	n/a

Em espera

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
capacity-oversubscribed	open	n/a

Código de status	Estado da solicitação	Estado da instância
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

Atendido

Quando todas as especificações das Instâncias spot forem cumpridas, a solicitação spot será atendida. O Amazon EC2 executa o 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

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. Por exemplo, se o preço for igual ao preço spot, mas não houver Instâncias spot disponíveis, o código de status será `instance-terminated-capacity-oversubscribed`. 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>closed</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-capacity-oversubscribed</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>
<code>instance-terminated-by-schedule</code>	<code>closed</code>	<code>terminated</code>
<code>instance-terminated-by-service</code>	<code>cancelled</code>	<code>terminated</code>
<code>instance-terminated-by-user†</code>	<code>closed ou cancelled *</code>	<code>terminated</code>
<code>instance-terminated-no-capacity</code>	<code>closed (única), open (persistente)</code>	<code>terminated</code>
<code>instance-terminated-capacity-oversubscribed</code>	<code>closed (única), open (persistente)</code>	<code>terminated</code>
<code>instance-terminated-launch-group-constraint</code>	<code>closed (única), open (persistente)</code>	<code>terminated</code>

† A Instância spot só pode obter esse estado se um usuário executar o comando de desativação a partir da instância. Não recomendamos que você faça isso, pois o serviço spot poderá reiniciar a instância.

* 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.

Como obter informações de status da solicitação

Você pode obter informações de status da solicitação usando o Console de gerenciamento da AWS 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, escolha Description (Descrição), 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 [Acessando o Amazon EC2 \(p. 3\)](#).

- `describe-spot-instance-requests` (AWS CLI)
- `Get-EC2SpotInstanceRequest` (AWS Tools para 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.

cancelled-before-fulfillment

O usuário cancelou a solicitação spot antes de ser atendida.

capacity-not-available

Não há capacidade suficiente disponível para as instâncias solicitadas.

capacity-oversubscribed

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 o Amazon EC2 está executando as instâncias spot.

instance-stopped-by-price

Sua instância foi interrompida porque o preço spot excedeu seu preço máximo.

instance-stopped-by-user

Sua instância foi interrompida porque um usuário executou o comando `shutdown -h` a partir da instância.

instance-stopped-capacity-oversubscribed

A instância foi interrompida porque o número de solicitações spot com preços máximos iguais ou superiores ao preço spot excedeu a capacidade disponível nesse grupo de Instância spot. O preço spot pode não ter sido alterado.

instance-stopped-no-capacity

Sua instância foi interrompida porque não havia capacidade spot suficiente disponível para ela.

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-capacity-oversubscribed

A instância foi encerrada porque o número de solicitações spot com preços máximos iguais ou superiores ao preço spot excedeu a capacidade disponível nesse grupo de Instância spot. O preço spot pode não ter sido alterado.

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 porque não há capacidade spot suficiente disponível para ela.

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 Referência geral do Amazon Web Services.

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.

Interrupções de Instância spots

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 possa ser interrompida. Portanto, você deve garantir que o aplicativo esteja preparado para uma interrupção de Instância spot.

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 – se não houver uma quantidade suficiente de instâncias do EC2 não utilizadas para atender à demanda por Instâncias spot, o Amazon EC2 interromperá as Instâncias spot. A ordem em que as instâncias são interrompidas é determinada pelo Amazon EC2.

- 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.

Um instância sob demanda especificado em uma Frota spot não pode ser interrompido.

Comportamento da interrupção

Você pode especificar se o Amazon EC2 deve colocar em hibernação, parar ou encerrar as Instâncias spot quando elas são interrompidas. Você pode escolher o comportamento de interrupção que melhor atende às suas necessidades. O padrão é encerrar as Instâncias spot quando elas são interrompidas. Para alterar o comportamento de interrupção, escolha uma opção em Interruption behavior no console ou `InstanceInterruptionBehavior` na configuração de execução ou no modelo de execução.

Como parar Instâncias spot interrompidas

Você pode alterar o comportamento de modo que o Amazon EC2 pare as Instâncias spot quando elas forem interrompidas, caso os seguintes requisitos sejam atendidos:

Requisitos

- Para uma solicitação de Instância spot, o tipo deve ser `persistent`, e não `one-time`. Você não pode especificar um grupo de execução na solicitação de Instância spot.
- Para uma solicitação de Frota spot, o tipo deve ser `maintain`, e não `request`.
- O volume raiz deve ser um volume do EBS, e não um volume de armazenamento de instâncias.

Depois que uma Instância spot é interrompida pelo serviço spot, somente o serviço spot poderá reiniciar o Instância spot, e a mesma especificação de execução deverá ser usada.

Para uma Instância spot executada por uma solicitação de `persistent` Instância spot, 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 uma Frota spot forem interrompidas e a Frota spot for do tipo `maintain`, o serviço spot executará instâncias de substituição para manter a capacidade desejada. O serviço spot localiza o(s) melhor(es) grupo(s) com base na estratégia de alocação especificada (`lowestPrice`, `diversified`, or `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 pode modificar alguns atributos de instância, mas não o tipo de instância. 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 spot 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 Frota spot, se houver muitas instâncias interrompidas, você poderá exceder o limite de número de volumes do EBS na sua conta.

Como colocar em hibernação Instâncias spot interrompidas

Você pode alterar o comportamento de modo que o Amazon EC2 coloque em hibernação as Instâncias spot quando elas forem interrompidas, caso os seguintes requisitos sejam atendidos:

Requisitos

- Para uma solicitação de Instância spot, o tipo deve ser `persistent`, e não `one-time`. Você não pode especificar um grupo de execução na solicitação de Instância spot.
- Para uma solicitação de Frota spot, o tipo deve ser `maintain`, e não `request`.
- O 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.
- As seguintes instâncias são compatíveis: C3, C4, C5, M4, M5, R3 e R4 com menos de 100 GB de memória.
- Os seguintes sistemas operacionais são compatíveis: Amazon Linux 2, Amazon Linux AMI, Ubuntu com um kernel Ubuntu sintonizado pela AWS (`linux-aws`) superior a 4.4.0-1041 e Windows Server 2008 R2 e versões posteriores.
- Instale o agente de hibernação em um sistema operacional suportado ou use uma das seguintes AMIs, que já incluem o agente:
 - 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
- Inicie o agente. Recomendamos que você use dados do usuário para iniciar o agente na inicialização da instância. Se preferir, você pode iniciar o agente manualmente.

Recomendação

- Recomendamos que você use um volume do 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. Se sua AMI não tiver um volume raiz criptografado, você poderá copiá-lo para uma nova AMI e solicitar a criptografia. Para obter mais informações, consulte [Amazon EBS Encryption \(p. 926\)](#) e [Cópia de uma AMI \(p. 154\)](#).

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 Frota spot, se houver muitas instâncias hibernadas, você poderá exceder o limite de número de volumes do EBS na sua conta.

O agente solicita hibernação ao sistema operacional quando a instância recebe um sinal do serviço spot. Se o agente não estiver instalado, o sistema operacional subjacente não oferecer suporte à hibernação ou não houver espaço de volume suficiente para salvar a memória da instância, a hibernação falhará e o serviço spot interromperá a instância.

Quando o serviço spot colocar uma Instância spot em hibernação, você receberá um aviso de interrupção, mas não terá dois minutos antes da interrupção da Instância spot. A hibernação começa imediatamente. Enquanto a instância estiver em processo de hibernação, as verificações de integridade da instância poderão falhar. Quando o processo de hibernação for concluído, o estado da instância será `stopped`.

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 [Preparação para hibernação de uma instância \(p. 351\)](#).

Como 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.
- Use avisos de interrupção de Instância spot para monitorar o status das instâncias spot.
- Embora nos esforcemos ao máximo para fornecer esse aviso o mais rápido possível, pode ser que a Instância spot seja encerrada antes que o aviso seja disponibilizado. Teste o aplicativo para ter a certeza de que ele tratará um encerramento de instância inesperado normalmente, mesmo se você estiver testando avisos de interrupção. Você pode fazer isso executando o aplicativo com uma instância sob demanda e, em seguida, encerrando a instância sob demanda por conta própria.

Preparação para 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 na inicialização 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 [Preparação 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:

```
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 spots

A melhor maneira de proteger-se contra a interrupção de Instância spots é arquitetar o aplicativo para que seja tolerante a falhas. Além disso, você pode aproveitar os avisos de interrupção da Instância spot, que enviam um aviso dois minutos antes do Amazon EC2 interromper ou encerrar a Instância spot. Recomendamos que você verifique esses avisos a cada cinco segundos.

Esse aviso é disponibilizado como um evento do CloudWatch e como um item nos [metadados de instância](#) (p. 516) no 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.

EC2 Instância spot Interruption Warning

Ao interromper o Amazon EC2, o Instância spot emite um evento que pode ser detectado pelo Eventos do Amazon CloudWatch. Para obter mais informações, consulte [Guia do usuário do Eventos do Amazon CloudWatch](#).

Este é um exemplo do evento de interrupção do 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. Caso contrário, não estará presente. Você pode recuperar `instance-action` da maneira a seguir.

```
[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 tempo em que essa instância será interrompida:

```
{"action": "stop", "time": "2017-09-18T08:22:00Z"}
```

O exemplo a seguir indica o tempo 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.

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.

```
[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 encerrar a instância, o status da solicitação será definido como `fulfilled`. O valor de `termination-time` permanece nos metadados da instância com o tempo aproximado original, que agora está no passado.

Feed de dados de Instância spots

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 suas 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 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.

Tópicos

- [Nome e formato do arquivo de feed de dados \(p. 354\)](#)
- [Requisitos do bucket do Amazon S3 \(p. 354\)](#)
- [Inscrever-se no seu feed de dados de Instância spot \(p. 355\)](#)
- [Exclusão de seu feed de dados de Instância spot \(p. 355\)](#)

Nome e formato do arquivo de 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 `myawsbucket` e o prefixo for `myprefix`, os nomes dos arquivos serão semelhantes ao seguinte:

```
myawsbucket.s3.amazonaws.com/myprefix/111122223333.2014-03-17-20.001.pwBdGTJG.gz
```

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. Nas instâncias spot <code>m1.small</code> , este campo é 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 para fornecer à conta de feed de dados da AWS a permissão **FULL_CONTROL**. A conta de feed de dados da AWS os 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 o 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.

Inscrever-se no seu feed de dados de Instância spot

Para assinar o feed de dados, use o seguinte comando [create-spot-datafeed-subscription](#):

```
aws ec2 create-spot-datafeed-subscription --bucket myawsbucket [--prefix myprefix]
```

A seguir está um exemplo de saída:

```
{  
    "SpotDatafeedSubscription": {  
        "OwnerId": "111122223333",  
        "Prefix": "myprefix",  
        "Bucket": "myawsbucket",  
        "State": "Active"  
    }  
}
```

Exclusão de seu feed de dados de Instância spot

Para excluir o feed de dados, use o seguinte comando [delete-spot-datafeed-subscription](#):

```
aws ec2 delete-spot-datafeed-subscription
```

Limites da Instância spot

As solicitações de Instância spots estão sujeitas aos limites a seguir:

Limites

- [Limites de solicitações spot \(p. 355\)](#)
- [Limites da Frota spot \(p. 356\)](#)
- [Instâncias T3 \(p. 356\)](#)
- [Instâncias T2 \(p. 356\)](#)

Limites de solicitações spot

Por padrão, há um limite de conta de 20 Instâncias spot por região. Se você encerrar a Instância spot, mas não cancelar a solicitação, a solicitação será contabilizada nesse limite até o Amazon EC2 detectar o encerramento e fechar a solicitação.

Os limites da Instância spot são dinâmicos. Quando sua conta é nova, o limite pode ser menor de 20 para começar, mas ele poderá aumentar com o tempo. Além disso, a conta pode ter limites para tipos de Instância spot específicos. Se enviar uma solicitação de Instância spot e receber o erro `Max spot instance count exceeded`, você poderá preencher o formulário [Create case](#) (Criar caso) do AWS Support Center para solicitar um aumento no limite de Instância spot. Em Limit type (Tipo de limite), selecione EC2 Spot Instances (Instâncias spot do EC2). Para obter mais informações, consulte [Limites de serviço do Amazon EC2 \(p. 1013\)](#).

Limites da Frota spot

Os limites comuns do Amazon EC2 aplicam-se a instâncias executadas por uma Frota spot ou uma Frota do EC2, como limites de solicitação spot, limites de instância e limites de volume. 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 especificações de execução por frota: 50
- O tamanho dos dados de usuário em uma especificação de execução: 16 KB
- A capacidade de destino por Frota spot ou Frota do EC2: 10.000
- A capacidade de destino em todas as Frotas spot e Frotas do EC2 de uma região: 100.000
- Uma solicitação de Frota spot ou de Frota do EC2 não pode abranger regiões.
- Uma solicitação de Frota spot ou de Frota do EC2 não pode abranger sub-redes diferentes na mesma zona de disponibilidade.

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.

Instâncias T3

Se você pretende usar T3 Instâncias spot imediatamente e por um curto período, sem tempo ocioso para acumular créditos de CPU, recomendamos executar T3 Instâncias spot no modo [standard \(p. 201\)](#) para evitar pagar custos mais altos.

Se você executar T3 Instâncias spot no modo [unlimited \(p. 193\)](#) e esgotar a CPU imediatamente, gastará os créditos excedentes por isso. Se você usar a instância por um curto período, a instância não terá tempo para acumular créditos de CPU para pagar os créditos excedentes, e você precisará pagar os créditos excedentes quando encerrar a instância.

O modo [Unlimited](#) para T3 Instâncias spot será adequado somente se a instância for executada por tempo suficiente para acumular créditos de CPU para intermitência. Caso contrário, o pagamento dos créditos excedentes deixa T3 Instâncias spot mais caro do que as instâncias M5 ou C5.

Instâncias T2

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 a [T2 ilimitada \(p. 193\)](#) ou usar um tipo de instância com CPU dedicada (por exemplo, `c4.large`).

Hosts dedicados

Um Host dedicado do Amazon EC2 é um servidor físico com a capacidade de instância do EC2 totalmente dedicada ao seu uso. O Hosts dedicados permite que você use suas licenças de software existentes

por soquete, por núcleo ou por VM, incluindo o Windows Server, Microsoft SQL Server, SUSE, Linux Enterprise Server e assim por diante.

Tópicos

- [Diferenças entre Hosts dedicados e Instâncias dedicadas \(p. 357\)](#)
- [Bring-Your-Own-License \(p. 357\)](#)
- [Capacidade da instância do Host dedicado \(p. 358\)](#)
- [Restrições e limitações de Hosts dedicados \(p. 358\)](#)
- [Definição de preço e cobrança \(p. 358\)](#)
- [Como trabalhar com Hosts dedicados \(p. 359\)](#)
- [Acompanhamento de alterações de configuração \(p. 369\)](#)

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 desempenho ou de segurança entre Instâncias dedicadas e instâncias em Hosts dedicados. A tabela a seguir destaca algumas das principais diferenças entre Hosts dedicados e Instâncias dedicadas:

	Host dedicado	Instâncias dedicadas
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
Recuperação automática de instâncias	Não suportado	Compatível
Traga sua própria licença (BYOL)	Compatível	Não suportado

Bring-Your-Own-License

O Hosts dedicados permite usar suas licenças de software por VM, por núcleo e por soquete existentes. Ao trazer sua própria licença, você será responsável por gerenciá-las, mas o Amazon EC2 tem recursos que ajudam a manter a conformidade das licenças, como afinidade de instância e colocação direcionada.

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 [Guia do usuário de VM Import/Export](#).
3. Depois de importar a imagem de máquina, você poderá executar instâncias dela em Hosts dedicados ativos em sua conta.
4. Ao executar essas instâncias, dependendo do sistema operacional, você pode ser solicitado a 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 [Acompanhamento de alterações de configuração \(p. 369\)](#).

Capacidade da instância do Host dedicado

Os Hosts dedicados são configurados para oferecer suporte a um único tipo de instância e capacidade de tamanho. O número de instâncias que podem ser executadas em um Host dedicado depende do tipo da instância para a qual o Host dedicado está configurado para oferecer suporte. Por exemplo, se você tiver alocado um Host dedicado c3.xlarge, terá o direito de executar até oito instâncias c3.xlarge no Host dedicado. Para determinar o número de tamanhos de tipos de instâncias que podem ser executadas em um Host dedicado específico, consulte [Definição de preço de Hosts dedicados do Amazon EC2](#).

Restrições e limitações de Hosts dedicados

Antes de alocar Hosts dedicados, observe as seguintes limitações e restrições:

- As AMIs do RHEL, SUSE Linux e Windows (oferecidas pela AWS ou no AWS Marketplace) não podem ser usadas com Hosts dedicados.
- Não há suporte para a recuperação de instâncias do Amazon EC2.
- 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.
- Os limites dos hosts são independentes dos limites das instâncias. As instâncias que você está executando em Hosts dedicados não contam para os limites da instância.
- Não há suporte para grupos do 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 há suporte para placement groups em Hosts dedicados.

Definição de preço e cobrança

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. Será cobrada uma taxa por hora pelo Host dedicado, independentemente da quantidade ou do tamanho das instâncias que você optar por executar nele. Em outras palavras, será feita a cobrança pelo Host dedicado inteiro e não por instâncias individuais que você optar por executar nele. Para obter mais informações sobre a definição de preços sob demanda, consulte [Definição de preços sob demanda de Hosts dedicados do Amazon EC2](#).

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 [Liberação de hosts dedicados \(p. 367\)](#).

Reservas de Host dedicados

As reservas de Host dedicado 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 o período de vigência de um ano somente.
- 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 abrange um único Host dedicado específico de sua conta. 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 da instância e a região 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](#).

Como trabalhar com Hosts dedicados

Para usar um Host dedicado, primeiro aloque os hosts a serem usados na sua conta. Em seguida, 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.

Tópicos

- [Noções básicas sobre posicionamento automático e afinidade \(p. 360\)](#)
- [Atribuição de Hosts dedicados \(p. 360\)](#)
- [Execução de instâncias em Hosts dedicados \(p. 361\)](#)
- [Modificação do posicionamento automático do Host dedicado \(p. 363\)](#)
- [Modificação da locação e da afinidade de instâncias \(p. 364\)](#)

- [Visualização de Hosts dedicados \(p. 365\)](#)
- [Marcação de Host dedicados \(p. 365\)](#)
- [Monitoramento do Hosts dedicados \(p. 366\)](#)
- [Liberação de hosts dedicados \(p. 367\)](#)
- [Compra de reservas de Host dedicado \(p. 368\)](#)
- [Visualização de reservas do Host dedicado \(p. 369\)](#)

Noções básicas sobre posicionamento automático e afinidade

O controle de posicionamento ocorre em nível de instância e de host.

Posicionamento automático

O posicionamento automático permite que você gerencie se as instâncias são executadas em um host específico ou em qualquer host disponível com configurações correspondentes. O posicionamento automático deve ser configurado no nível do host.

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 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).

Atribuição de Hosts dedicados

Para você começar a usar Hosts dedicados, primeiro eles precisam ser alocados para sua conta. Você pode atribuir Hosts dedicados à sua conta usando o console do Amazon EC2 ou as ferramentas de linha de comando.

Para alocar Hosts dedicados 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, Allocate Host dedicado (Alocar dh).
3. Configure as opções de Host dedicado a seguir:
 - a. Instance type (Tipo de instância) — o tipo de instância que deseja executar no Host dedicado.
 - b. Availability Zone (Zona de disponibilidade) — a zona de disponibilidade na qual o Host dedicado está localizado.
 - c. Allow instance auto-placement (Permitir posicionamento automático de instância) — escolha uma das seguintes configurações:

- Sim — o Host dedicado aceita execuções de instâncias não direcionadas que correspondem à sua configuração de tipo de instância.
- Não — o Host dedicado aceita execuções de instâncias de locação de host que especificuem somente seu ID de host exclusivo. Essa é a configuração padrão.

Para obter mais informações sobre posicionamento automático, consulte [Noções básicas sobre posicionamento automático e afinidade \(p. 360\)](#).

- d. Quantity (Quantidade) — o número de Hosts dedicados a serem alocados com essas opções.
4. (Opcional) Escolha Add Tag (Adicionar tag) e digite uma chave de tag e um valor de tag.
5. Escolha Allocate host (Alocar host).

Para atribuir Hosts dedicados usando as ferramentas de linha de comando

Use um dos seguintes comandos. 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` e aplicam uma tag com uma chave de `purpose` e um valor de `production`.

- [allocate-hosts](#) (AWS CLI)

```
aws ec2 allocate-hosts --instance-type "m4.large" --availability-zone "eu-west-1a"
--auto-placement "off" --quantity 1 --tag-specifications 'ResourceType=dedicated-
host,Tags=[{Key= purpose,Value= production}]'
```

- [New-EC2Host](#) (AWS Tools para Windows PowerShell)

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 Off -Quantity 1 -TagSpecification $tagspec
```

A capacidade do Host dedicado é disponibilizada em sua conta imediatamente.

Se você executar instâncias com locação de host, mas não tiver nenhum Host dedicado ativo em sua conta, ocorrerá um erro e a inicialização da instância falhará.

Execução de instâncias em Hosts dedicados

Depois de alocar um Host dedicado, você pode executar instâncias nele. Você não poderá 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 e limitações de Hosts dedicados \(p. 358\)](#).

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, escolha Actions (Ações), Launch Instance(s) onto Host (Executar instância(s) no host).
4. Selecione uma AMI na lista. AMIs do Windows, 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), mantenha o tipo de instância que foi selecionada por padrão e selecione Next: Configure Instance Details (Próximo: Configurar detalhes da instância).

O tipo de instância é determinado pelo host que você selecionou.

6. Na página Configure Instance Details (Configurar detalhes da instância), defina as configurações de instância para atender às suas necessidades. Em Affinity (Afinidade), escolha uma das seguintes opções:
 - Off (Desativado) — a instância é executada no host especificado, mas não é garantido que será reiniciada no mesmo Host dedicado se for interrompida.
 - Host — se for interrompida, a instância sempre será reiniciada nesse host específico.

Para obter mais informações sobre afinidade, consulte [Noções básicas sobre posicionamento automático e afinidade \(p. 360\)](#).

Note

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 Windows, 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 específicas do 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. Se os Hosts dedicados não forem compatíveis com o tipo de instância, eles estarão desabilitados na lista

- Afinidade — escolha uma das seguintes opções:
 - Off (Desativado) — a instância é executada no host especificado, mas não é garantido que será reiniciada nele se for interrompida.
 - Host — se for interrompida, a instância sempre será reiniciada no host especificado.

Para obter mais informações, consulte [Noções básicas sobre posicionamento automático e afinidade \(p. 360\)](#).

Note

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).

Para executar uma instância em um Host dedicado usando as ferramentas de linha de comando

Use um dos seguintes comandos e especifique a afinidade de instância, a locação e o host no parâmetro de solicitação Placement:

- [run-instances](#) (AWS CLI)
- [New-EC2Instance](#) (AWS Tools para Windows PowerShell)

Modificação do posicionamento automático do Host dedicado

Você pode modificar as configurações de posicionamento automático de um Host dedicado depois de alocá-lo à sua conta da AWS.

Para modificar o posicionamento automático de um Host dedicado usando o console do Amazon EC2

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. Escolha Hosts dedicados no painel de navegação.
3. Na página Hosts dedicados, selecione um host e escolha Actions (Ações) e, em seguida, escolha Modify Auto-Placement (Modificar posicionamento automático).
4. Na janela Modify Auto-Placement (Modificar posicionamento automático), em Allow instance auto-placement (Permitir posicionamento automático de instâncias), escolha Yes (Sim) para habilitar o posicionamento automático ou escolha No (Não) para desabilitar o posicionamento automático.
Para obter mais informações, consulte [Noções básicas sobre posicionamento automático e afinidade \(p. 360\)](#).
5. Escolha Salvar.

Para modificar o posicionamento automático de um Host dedicado usando as ferramentas de linha de comando

Use um dos seguintes comandos. Os seguintes exemplos habilitam o posicionamento automático para o Host dedicado especificado.

- [modify-hosts](#) (AWS CLI)

```
aws ec2 modify-hosts --auto-placement on --host-ids h-012a3456b7890cdef
```

- [Edit-EC2Host](#) (AWS Tools para Windows PowerShell)

```
PS C:\> Edit-EC2Host --AutoPlacement 1 --HostId h-012a3456b7890cdef
```

Modificação da 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.

Para modificar a locação e a afinidade de instâncias usando o console do Amazon EC2

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 Actions (Ações), Instance State (Estado da instância) e 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 [Instâncias dedicadas \(p. 371\)](#).
 - Launch the instance on a Host dedicado (Executar a instância em um dh) — executa a instância em um Host dedicado com afinidade configurável.
 - Affinity (Afinidade) — escolha uma das seguintes opções:
 - This instance can run on any one of my hosts (Esta instância pode ser executada em qualquer um dos meus hosts) — a instância é executada em qualquer Host dedicado disponível em uma conta que ofereça suporte ao seu tipo de instância.
 - This instance can only run on the selected host (Esta instância só pode ser executada no host selecionado) — a instância só pode ser executada no Host dedicado selecionado em Target Host (Host de destino).
 - Target Host (Host de destino) — selecione o Host dedicado no qual executar a instância. Se nenhum host de destino estiver listado, talvez não haja Hosts dedicados disponíveis e compatíveis em sua conta.

Para obter mais informações, consulte [Noções básicas sobre posicionamento automático e afinidade \(p. 360\)](#).

6. Escolha Salvar.

Para modificar a locação e a afinidade de instâncias usando as ferramentas de linha de comando

Use um dos seguintes comandos. Os exemplos a seguir alteram a afinidade da instância especificada de default para host e especifica o Host dedicado com o qual a instância tem afinidade.

- [modify-instance-placement](#) (AWS CLI)

```
aws ec2 modify-instance-placement --instance-id i-1234567890abcdef0 --affinity host --  
host-id h-012a3456b7890cdef
```

- [Edit-EC2InstancePlacement](#) (AWS Tools para Windows PowerShell)

```
PS C:\> Edit-EC2InstancePlacement -InstanceId i-1234567890abcdef0 -Affinity host -  
HostId h-012a3456b7890cdef
```

Visualização de Hosts dedicados

Você pode visualizar os detalhes de um Host dedicado e das Instâncias individuais existentes nele.

Para visualizar os detalhes de instâncias em um Host dedicado 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, selecione Hosts dedicados.
3. Na página Hosts dedicados, selecione o host para visualizar mais informações sobre ele.
4. Para obter informações sobre o host, escolha Description (Descrição). Para obter informações sobre as instâncias em execução no host, escolha Instances (Instâncias).

Para visualizar os detalhes de instâncias em um Host dedicado com as ferramentas de linha de comando

Use um dos seguintes comandos:

- [describe-hosts](#) (AWS CLI)

```
aws ec2 describe-hosts --host-id host_id
```

- [Get-EC2Host](#) (AWS Tools para Windows PowerShell)

```
PS C:\> Get-EC2Host -HostId host_id
```

Marcação de Host 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 você a localizar rapidamente um determinado Host dedicado com base nas 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 [Atribuição de Hosts dedicados \(p. 360\)](#).

Você só pode marcar um Host dedicado usando o console do Amazon EC2 e as ferramentas de linha de comando.

Para marcar 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, escolha Host 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 Salvar.

Para marcar um Host dedicado usando a linha de comando

Use um dos seguintes comandos:

- [create-tags](#) (AWS CLI)

O comando a seguir marca o Host dedicado especificado com Owner=TeamA.

```
aws ec2 create-tags --resources h-abc12345678909876 --tags Key=Owner,Value=TeamA
```

- [New-EC2Tag](#) (AWS Tools para Windows PowerShell)

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
```

Monitoramento do Hosts dedicados

O Amazon EC2 monitora constantemente o estado de seus Hosts dedicados. As atualizações são comunicadas no console do Amazon EC2. Você também pode obter informações sobre seus Hosts dedicados usando as ferramentas de linha de comando.

Para visualizar o estado de um Host dedicado 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, selecione Hosts dedicados.
3. Localize o Host dedicado na lista e revise o valor na coluna State (Estado).

Para visualizar o estado de um Host dedicado usando as ferramentas de linha de comando

Use um dos seguintes comandos e revise a propriedade state no elemento de resposta hostSet:

- [describe-hosts](#) (AWS CLI)

```
aws ec2 describe-hosts --host-id host_id
```

- [Get-EC2Host](#) (AWS Tools para Windows PowerShell)

```
PS C:\> Get-EC2Host -HostId host_id
```

A tabela a seguir explica os possíveis estados de um Host dedicado.

Estado	Descrição
<code>available</code>	A AWS não detectou nenhum problema com Host dedicado nenhuma manutenção ou reparo foram programados. As instâncias podem ser executadas neste host dedicado.
<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 Console de gerenciamento da AWS ou por e-mail. As instâncias não podem ser executadas em um Host dedicado neste estado.
<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 sendo 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 em 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.

Liberação de 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.

Para liberar um Host dedicado usando o console do Amazon EC2

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.

Para liberar um Host dedicado usando as ferramentas de linha de comando

Use um dos seguintes comandos:

- `release-hosts` (AWS CLI)

```
aws ec2 release-hosts --host-ids host_id
```

- `Remove-EC2Hosts` (AWS Tools para Windows PowerShell)

```
PS C:\> Remove-EC2Hosts -HostId host_id
```

Depois de liberar um Host dedicado, você não pode reutilizar o mesmo host ou ID de host, e não haverá mais taxas de faturamento sob demanda para ele. O estado do host dedicado será alterado para `released`, e você não poderá mais executar nenhuma instância nesse host.

Note

Se você tiver liberado recentemente Hosts dedicados, 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.

Compra de reservas de Host dedicado

Você pode comprar reservas usando o console do Amazon EC2 ou as ferramentas da linha de comando.

Para comprar reservas usando o console do Amazon EC2

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. Escolha Hosts dedicados, Host dedicado Reservations (Reservas de dh), Purchase Host dedicated Reservation (Comprar reserva de dh).
3. Na tela Purchase Host dedicated Reservation (Comprar reserva de dh), você pode 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. 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 escolha Purchase (Comprar).

Para comprar reservas usando as ferramentas de linha de comando

1. Use um dos seguintes comandos para listar as ofertas disponíveis que correspondam 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 prazo de um ano inclui 31.536.000 segundos e de três anos inclui 94.608.000 segundos.

- [describe-host-reservation-offerings \(AWS CLI\)](#)

```
aws ec2 describe-host-reservation-offerings --filter Name=instance-family,Values=m4  
--max-duration 31536000
```

- [Get-EC2HostReservationOffering \(AWS Tools para Windows PowerShell\)](#)

```
PS C:\> $filter = @{Name="instance-family"; Value="m4"}
```

```
PS C:\> Get-EC2HostReservationOffering -filter $filter -MaxDuration 31536000
```

Os dois comandos retornam uma lista de ofertas que correspondem aos seus critérios. Observe o `offeringId` da oferta a ser comprada.

2. Use um dos seguintes comandos para comprar a oferta e forneça o `offeringId` anotado na etapa anterior. Nos seguintes exemplos, é comprada a reserva especificada e ela é associada a um Host dedicado específico já atribuído à conta da AWS.

- [purchase-host-reservation \(AWS CLI\)](#)

```
aws ec2 purchase-host-reservation --offering-id hro-03f707bf363b6b324 --host-id-set h-013abcd2a00cbd123
```

- [New-EC2HostReservation \(AWS Tools para Windows PowerShell\)](#)

```
PS C:\> New-EC2HostReservation -OfferingId hro-03f707bf363b6b324 -HostIdSet h-013abcd2a00cbd123
```

Visualização de reservas do Host dedicado

Você pode visualizar informações sobre os Hosts dedicados associados à reserva, o prazo da reserva, a opção de pagamento selecionada e as datas de início e término da reserva.

Para visualizar os detalhes das reservas usando o console do Amazon EC2

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 dh) 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.

Para visualizar os detalhes das reservas com as ferramentas de linha de comando

Use um dos seguintes comandos:

- [describe-host-reservations \(AWS CLI\)](#)

```
aws ec2 describe-host-reservations
```

- [Get-EC2HostReservation \(AWS Tools para Windows PowerShell\)](#)

```
PS C:\> Get-EC2HostReservation
```

Acompanhamento de alterações de configuração

Você pode usar o AWS Config para gravar as alterações de configuração em Hosts dedicados e 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 as informações de configuração dos Hosts dedicados e das instâncias individualmente e cruza essas informações por meio de relações. Há três condições de geração de relatórios.

- AWS Config recording status (Status de gravação do CC) — 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

O 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 AMI (imagem de máquina da Amazon). 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 seus aplicativos. 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 este:

```
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 este:

```
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](#).

Para ativar o AWS Config usando a linha de comando ou a API

- Usando CLI da AWS, consulte [Visualização de detalhes de configuração \(CLI da AWS\)](#) no Guia do desenvolvedor do AWS Config.
- Usando a API do Amazon EC2, consulte [GetResourceConfigHistory](#).

Instâncias dedicadas

As Instâncias dedicadas são instâncias do Amazon EC2 que são executadas na 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. Além de disso, as Instâncias dedicadas que pertencem a contas da AWS vinculadas a uma única conta pagante também são isoladas fisicamente no nível de hardware. 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 [Hosts dedicados \(p. 356\)](#).

Conceitos básicos de Instâncias dedicadas

Cada instância em execução na VPC tem um atributo de locação. Esse atributo tem os valores a seguir.

Valor da locação	Descrição
default	Sua instância é executada em hardware compartilhado.
dedicated	Sua instância é executada no hardware de um único usuário.
host	Sua instância é executada em um Host dedicado, que é um servidor isolado com configurações que você pode controlar.

Após executar uma instância, há algumas restrições para alterar a sua locação.

- Você não pode alterar a locação de uma instância de default para dedicated ou host depois de executá-la.
- Você não pode alterar a locação de uma instância de dedicated ou host para default depois de executá-la.

Você pode alterar a locação de uma instância de **dedicated** para **host** ou de **host** para **dedicated** depois de executá-la. Para obter mais informações, consulte [Alteração da locação de uma instância \(p. 375\)](#).

Cada VPC tem um atributo de locação de instância relacionado. Esse atributo tem os valores a seguir.

Valor da locação	Descrição
default	Uma instância executada na VPC é executada em hardware compartilhado por padrão, a menos que você especifique explicitamente uma locação diferente durante a execução da instância.
dedicated	Uma instância executada na VPC é uma Instâncias dedicadas por padrão, a menos que você especifique explicitamente uma locação de host durante a execução da instância. Você não pode especificar uma locação de default durante a execução da instância.

Você pode alterar a locação da instância de uma VPC de **dedicated** para **default** depois de criá-la. Você não pode alterar a locação de instância de uma VPC para **dedicated**.

Para criar Instâncias dedicadas, você pode fazer o seguinte:

- Crie uma VPC com a locação da instância definida como **dedicated** (todas as instâncias executadas nessa VPC são Instâncias dedicadas).
- Criar a VPC com a locação da instância definida como **default** e especificar uma locação de **dedicated** para todas as instâncias quando você as executar.

Limitações de Instâncias dedicadas

Alguns serviços da AWS ou seus recursos não funcionarão com uma VPC com a locação de instância definida como **dedicated**. Verifique documentação do serviço para confirmar se há alguma limitação.

Alguns tipos de instância não podem ser executados em uma VPC com a locação da instância definida como **dedicated**. Para obter mais informações sobre os tipos de instância com suporte, consulte [Instâncias dedicadas do Amazon EC2](#).

Amazon EBS com Instâncias dedicadas

Quando você executa uma Instâncias dedicadas baseada em Amazon EBS, o volume EBS não é executado em hardware de único locatário.

Instâncias reservadas com locação dedicada

Para garantir que tem capacidade suficiente disponível para executar Instâncias dedicadas, você pode comprar Instâncias reservadas dedicadas. Para obter mais informações, consulte [Instâncias reservadas \(p. 253\)](#).

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. Contudo, se você adquirir uma Instância reservada com um valor de locação padrão, você não obterá uma Instância reservada dedicada se executar uma instância com a locação de instância **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 de Instâncias dedicadas

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 de Instâncias dedicadas

Você pode configurar a recuperação automática para um Instâncias dedicadas se ele for invalidado devido a uma falha de hardware subjacente ou a um problema que exija o envolvimento da AWS para repará-lo. Para obter mais informações, consulte [Recuperar sua instância](#) (p. 476).

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 [Como especificar a locação para suas Instâncias spot](#) (p. 308).

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. 373)
- [Executar Instâncias dedicadas em uma VPC](#) (p. 374)
- [Exibição de informações de locação](#) (p. 374)
- [Alteração da locação de uma instância](#) (p. 375)
- [Alterar a locação de uma VPC](#) (p. 376)

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).

Para criar uma VPC com uma locação de instância de dedicada (Assistente de VPC)

1. Abra o console de Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel, escolha Start VPC Wizard (Iniciar assistente de VPC).
3. Selecione uma configuração de VPC e escolha Select (Selecionar).
4. Na página seguinte do assistente, escolha Dedicated (Dedicada) na lista Hardware tenancy (Locação de hardware).
5. Escolha Criar VPC.

Para criar uma VPC com uma locação de instância de dedicada (caixa de diálogo Criar VPC)

1. Abra o console de 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 Yes, Create (Sim, criar).

Para configurar a opção de locação quando você cria uma VPC usando a linha de comando

- [create-vpc](#) (AWS CLI)
- [New-EC2Vpc](#) (AWS Tools para Windows PowerShell)

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.

Executar Instâncias dedicadas em uma VPC

Você pode executar uma Instâncias dedicadas usando o assistente de execução de instâncias do Amazon EC2.

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. Escolha Dedicated - Run a dedicated instance (Dedicada – Executar uma instância dedicada) na lista Tenancy (Locação) 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.

Para obter mais informações sobre a execução de uma instância com uma locação de host, consulte [Execução de instâncias em Hosts dedicados \(p. 361\)](#).

Para configurar a opção de locação para uma instância durante a execução usando a linha de comando

- [run-instances](#) (AWS CLI)
- [New-EC2Instance](#)

Exibição de informações de locação

Para exibir as informações da locação da VPC usando o console

1. Abra o console de 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 Tenancy (Locação) não for exibida, escolha Edit Table Columns (Editar colunas da tabela) (o ícone de engrenagem) e Tenancy (Locação) na caixa de diálogo Show/Hide Columns (Mostrar/ocultar colunas) e, em seguida, escolha Close (Fechar).

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 Show/Hide Columns (Mostrar/ocultar colunas) (o ícone de engrenagem) e Tenancy (Locação) na caixa de diálogo Show/Hide Columns (Mostrar/ocultar colunas) e, em seguida, Close (Fechar).
 - Selecione a instância. A guia Description (Descrição) no painel de detalhes exibe informações sobre a instância, incluindo sua locação.

Para descrever a locação da sua VPC usando a linha de comando

- [describe-vpcs](#) (AWS CLI)
- [Get-EC2Vpc](#) (AWS Tools para Windows PowerShell)

Para descrever a locação da sua instância usando a linha de comando

- [describe-instances](#) (AWS CLI)
- [Get-EC2Instance](#)

Para descrever o valor da locação de uma Instância reservada usando a linha de comando

- [describe-reserved-instances](#) (AWS CLI)
- [Get-EC2ReservedInstance](#) (AWS Tools para 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 para Windows PowerShell)

Alteração da locação de uma instância

Dependendo do tipo de instância e da plataforma, você pode alterar a locação de uma Instâncias dedicadas interrompida para host depois de executá-la. Na próxima vez que a instância for iniciada, ela será iniciada em um Host dedicado alocado para sua conta. Para obter mais informações sobre como alocar e trabalhar com Hosts dedicados, e os tipos de instâncias que podem ser usados com Hosts dedicados, consulte [Como trabalhar com Hosts dedicados \(p. 359\)](#). Da mesma forma, você pode alterar a locação de uma instância de Host dedicado interrompida para dedicated depois de executá-la. Na próxima vez que a instância for iniciada, ela será iniciada em hardware de locatário único controlado por nós.

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 Ações, Instance State, Parar.
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 Salvar.

Para modificar o valor da locação de uma instância usando a linha de comando

- [modify-instance-placement](#) (AWS CLI)
- [Edit-EC2InstancePlacement](#) (AWS Tools para Windows PowerShell)

Alterar a locação de uma VPC

Você pode alterar o atributo de locação da instância da VPC de `dedicated` para `default`. 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.

Você não pode alterar o atributo de locação da instância de uma VPC para `dedicated`.

Você só pode modificar o atributo de locação da instância de uma VPC usando a AWS CLI, um SDK da AWS ou a API do Amazon EC2.

Para modificar o atributo de locação da instância de uma VPC usando a AWS CLI

- Use o comando [modify-vpc-tenancy](#) para especificar 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
```

Reservas de capacidade sob demanda

O Reservas de capacidade sob demanda permite que você reserve capacidade para suas instâncias do Amazon EC2 por qualquer duração em uma determinada zona de disponibilidade. Isso oferece a você a capacidade de criar e gerenciar reservas de capacidade de forma independente dos descontos de faturamento oferecidos pela Instâncias reservadas (RI). Com a criação de Reservas de capacidade, você garante que sempre terá acesso à capacidade do EC2 sempre que necessário, pelo tempo que precisar. As Reservas de capacidade podem ser criadas a qualquer momento, sem estabelecer um compromisso de um ano ou três anos, e a capacidade está disponível imediatamente. Quando você não precisar mais da reserva, cancele a Reserva de capacidade para não incorrer em cobranças desnecessárias.

Quando você cria uma Reserva de capacidade, você especifica a zona de disponibilidade na qual deseja reservar a capacidade, o número de instâncias para as quais deseja reservar capacidade, e os atributos das instâncias, incluindo o tipo, a locação e a plataforma/SO das instâncias. As Reservas de capacidade podem ser usadas por instâncias que correspondem a 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, você pode usar suas RIs regionais com suas Reservas de capacidade para se beneficiar dos descontos de faturamento. Isso fornece a flexibilidade de adicionar reservas de capacidade seletivamente e ainda obter os descontos regionais de RI dessa utilização. A AWS aplica automaticamente o desconto de RI quando os atributos de uma Reserva de capacidade correspondem aos atributos de uma RI regional ativa.

Tópicos

- [Diferenças entre Reservas de capacidade e RIs \(p. 377\)](#)
- [Limites do Reserva de capacidade \(p. 377\)](#)
- [Restrições e limitações de Reserva de capacidade \(p. 377\)](#)
- [Definição de preço e faturamento de Reserva de capacidade \(p. 378\)](#)
- [Como trabalhar com Reservas de capacidade \(p. 379\)](#)

Diferenças entre Reservas de capacidade e RIs

A tabela a seguir destaca algumas das principais diferenças entre Reservas de capacidade e RIs:

	Reservas de capacidade	RIs de zona	RIs regionais
Prazo	Nenhum compromisso é necessário. Podem ser criadas e canceladas conforme necessário.	Exigem compromisso fixo de um ano ou três anos.	
Benefício da capacidade	Reservam capacidade em uma zona de disponibilidade específica.	Reservam capacidade em uma zona de disponibilidade específica.	Não reservam capacidade em uma zona de disponibilidade específica.
Desconto de faturamento	Sem desconto de faturamento. As instâncias executadas em uma Reserva de capacidade são cobradas por taxas sob demanda padrão. No entanto, as RIs regionais podem ser usadas com as Reservas de capacidade para obter um desconto de faturamento.	Fornecem desconto de faturamento.	
Limites de instâncias	Limitadas aos limites de instância sob demanda por região.	Limitadas a 20 por zona de disponibilidade. Um aumento do limite pode ser solicitado.	Limitadas a 20 por região. Um aumento do limite pode ser solicitado.

Limites do 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 de seus limites de instância sob demanda
- As Reservas de capacidade não podem ser compartilhadas entre contas da AWS
- As Reservas de capacidade não são transferíveis de uma conta da AWS para outra
- Os descontos de faturamento de RI 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 Host dedicados

Definição de preço e faturamento de Reserva de capacidade

Definição de preço

Quando a Reserva de capacidade está ativa, você é cobrado o equivalente à taxa sob demanda quer você execute as instâncias 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 você 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 e por 5 spots não utilizados na reserva.

Note

Os descontos de faturamento de RIs regionais se aplicam às Reservas de capacidade. A AWS aplica automaticamente suas RIs regionais ativas às Reservas de capacidade ativas e não utilizadas que têm atributos correspondentes. Para obter mais informações sobre RIs regionais, consulte [Instâncias reservadas \(p. 253\)](#).

Para obter mais informações sobre definição de preço do Amazon EC2, consulte [Definição de preço do Amazon EC2](#).

Faturamento

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 USD 0,10 por hora de uso. Neste exemplo, a Reserva de capacidade está ativa na conta por cinco horas. A Reserva de capacidade não é usada na primeira hora, portanto, é cobrada por uma hora não utilizada na taxa sob demanda padrão do tipo de instância m4.large. Das duas às cinco horas, a Reserva de capacidade é ocupada por uma instância m4.large. Durante esse período, a Reserva de capacidade não acumula cobranças e, em vez disso, a conta é cobrada pela instância m4.large que a está ocupando. Na sexta hora, a Reserva de capacidade é cancelada, e a instância m4.large é executada normalmente fora da capacidade reservada. Para essa hora, ela é cobrada pela taxa sob demanda do tipo de instância m4.large.

Hour	1	2	3	4	5	6
Unused Capacity Reservation	\$0.10	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00
On-demand Instance Usage	\$0.00	\$0.10	\$0.10	\$0.10	\$0.10	\$0.10
Hourly cost	\$0.10	\$0.10	\$0.10	\$0.10	\$0.10	\$0.10

Descontos de faturamento

Os descontos de faturamento de RIs regionais se aplicam às Reservas de capacidade. A AWS aplica automaticamente suas RIs regionais ativas às Reservas de capacidade ativas que têm atributos correspondentes. Para obter mais informações sobre RIs regionais, consulte [Instâncias reservadas \(p. 253\)](#).

Note

Os descontos de faturamento de RI de zona não se aplicam às Reservas de capacidade.

Quando suas horas de instância e horas de reserva combinadas excedem o total de horas de RI regional com desconto qualificado, os descontos são preferencialmente aplicados às horas de instância primeiro e em seguida às horas de reserva não utilizada.

Como visualizar sua fatura

Você encontrará mais informações sobre as cobranças e as taxas de sua conta visualizando 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 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 Guia do usuário do AWS Billing and Cost Management.

Como trabalhar com Reservas de capacidade

Para começar a usar as Reservas de capacidade, você precisa criar a reserva de capacidade na zona de disponibilidade necessária. Depois de criar uma Reserva de capacidade, você pode 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). Ou seja, as instâncias que têm atributos correspondentes executam automaticamente na capacidade da Reserva de capacidade. No entanto, você também pode destinar uma Reserva de capacidade para cargas de trabalho específicas. Isso permite que você controle explicitamente quais instâncias têm permissão para executar na capacidade reservada.

Tópicos

- [Criação de uma Reserva de capacidade \(p. 379\)](#)
- [Execução de uma instância em uma Reserva de capacidade existente \(p. 381\)](#)
- [Modificação de uma Reserva de capacidade \(p. 382\)](#)
- [Modificação das configurações de Reserva de capacidade de uma instância \(p. 383\)](#)
- [Visualização de uma Reserva de capacidade \(p. 384\)](#)
- [Cancelamento de uma Reserva de capacidade \(p. 384\)](#)

Criação de uma Reserva de capacidade

A criação de uma Reserva de capacidade em sua conta cria uma reserva de capacidade em uma determinada zona de disponibilidade. Depois de criada, você pode executar instâncias na capacidade reservada, conforme necessário.

Note

Sua solicitação para criar uma Reserva de capacidade poderá falhar se o Amazon EC2 não tiver capacidade suficiente para atender à solicitação. Se sua solicitação falhar devido a restrições de capacidade do Amazon EC2, tente novamente em um momento posterior, tente em uma zona de disponibilidade diferente ou solicite uma reserva de capacidade menor. Se seu aplicativo for flexível entre tipos e tamanhos de instâncias, tente criar uma Reserva de capacidade com diferentes atributos de instância.

Sua solicitação também poderá falhar se a quantidade solicitada exceder o limite de instância sob demanda para o tipo de instância selecionado. Se sua solicitação falhar devido a restrições de limite, aumente o limite de instância sob demanda para o tipo de instância necessário e tente novamente. Para obter mais informações sobre o aumento de seus limites de instância, consulte [Limites de serviço do Amazon EC2 \(p. 1013\)](#).

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 `open`, as novas instâncias e as instâncias existentes que têm atributos correspondentes executarão 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.

Você pode criar uma nova Reserva de capacidade usando o console do Amazon EC2 ou a AWS CLI.

Para criar 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 escolha 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):
 - a. Instance Type (Tipo de instância) especifique 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 \(p. 839\)](#).
 - c. Attach instance store at launch (Anexar armazenamento de instâncias na execução) indique 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) especifique o sistema operacional das instâncias pretendidas.
 - e. Availability Zone (Zona de disponibilidade) especifique a zona de disponibilidade na qual deseja reservar a capacidade.
 - f. Quantity (Quantidade) especifique 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 selecionada, 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 (Tempo específico) cancela a reserva de capacidade automaticamente. A reserva de capacidade é liberada automaticamente na data e hora especificadas. A Reserva de capacidade é cancelada em até uma hora da hora especificada. 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.

Note

Após o término da reserva, você não pode mais destinar instâncias na 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.

- 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, plataforma e uma zona de disponibilidade da instância) e estejam destinadas para reserva explicitamente.
5. Escolha Request reservation (Solicitar reserva).

Para criar uma Reserva de capacidade usando a AWS CLI

Use o comando [create-capacity-reservation](#).

```
$ aws ec2 create-capacity-reservation --instance-type instance_type --instance-platform platform_type --availability-zone az --instance-count quantity
```

Execução de uma instância em uma Reserva de capacidade existente

Você poderá executar uma instância em uma Reserva de capacidade se ela tiver atributos correspondentes (tipo, plataforma e zona de disponibilidade da instância) e capacidade suficiente. 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 da Reserva de capacidade disponível será reduzida em três.

Você pode executar uma instância em uma Reserva de capacidade que você criou anteriormente usando o console do Amazon EC2 ou a linha de comando.

Para executar uma instância em uma Reserva de capacidade existente usando o console

1. Abra o assistente para Executar instância procedendo da seguinte maneira:
 - Escolha Instances (Instâncias), Launch Instance (Executar instância).
 - Escolha Reservas de capacidade, Launch Instance (Executar instância).
2. Preencha os detalhes da instância para adequá-la a seus requisitos.
3. Na página Configure Instance Details (Configurar os detalhes da instância), em Reserva de capacidade, proceda de uma das seguintes maneiras:
 - Escolha Open (Aberta) para executar a instância em qualquer Reserva de capacidade open que tenha atributos correspondentes (tipo, plataforma e zona de disponibilidade da instância) e capacidade suficiente.

Note

Se você não tiver uma Reserva de capacidade open correspondente com capacidade suficiente, a instância será executada na capacidade sob demanda.

- Escolha None (Nenhuma) para impedir que a instância execute em uma Reserva de capacidade.
- Escolha a Reserva de capacidade específica na qual executar a instância.

Note

Se a Reserva de capacidade selecionada não tiver capacidade suficiente, a execução da instância falhará.

4. Escolha Review and Launch (Rever e executar), Launch (Executar).
5. Quando solicitado, selecione um par de chaves existente ou crie um novo e selecione Launch Instances (Executar instâncias).

Para executar uma instância em uma Reserva de capacidade existente usando a AWS CLI

Use o comando `run-instances` da `--capacity-reservation-specification` e especifique o parâmetro .

O exemplo a seguir executa uma instância `t2.micro` em qualquer Reserva de capacidade open que tenha atributos correspondentes e capacidade disponível:

```
$ aws ec2 run-instances --image-id ami-abc12345 --count 1 --instance-type t2.micro --key-name MyKeyPair --availability-zone us-east-1b --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 --availability-zone us-east-1b --capacity-reservation-specification CapacityReservationTarget=[{CapacityReservationId=cr-a1234567}]
```

Modificação de uma Reserva de capacidade

Você pode alterar os atributos de uma Reserva de capacidade ativa depois de tê-la criado. Não é possível modificar uma Reserva de capacidade depois que ela expirar ou depois de você a cancelar 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 um tipo de instância, otimização de EBS, configurações de armazenamento de instâncias, plataforma, zona de disponibilidade ou qualificação de instâncias da 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.

Você pode modificar uma Reserva de capacidade usando o console do Amazon EC2 e a AWS CLI.

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).

Note

Se você especificar uma nova quantidade que exceda seu limite de instância sob demanda restante para o tipo de instância selecionada, a atualização falhará.

Para modificar uma Reserva de capacidade usando a AWS CLI

Use o comando [modify-capacity-reservations](#):

```
$ aws ec2 modify-capacity-reservation --capacity-reservation-id reservation_id --instance-count quantity --end-date-type limited/unlimited --end-date expiration_date
```

Modificação das configurações de Reserva de capacidade de uma instância

Você pode modificar as configurações da Reserva de capacidade de uma instância existente a qualquer momento. Você pode modificar uma instância interrompida para fazer o seguinte:

- Destinar uma Reserva de capacidade específica. A instância não pode executar fora da Reserva de capacidade de destino.
- Execute em qualquer Reserva de capacidade que tenha atributos correspondentes (tipo de instância, plataforma e zona de disponibilidade) e capacidade disponível.
- Impedir a execução em uma Reserva de capacidade. A instância é impedida de executar em qualquer Reserva de capacidade, mesmo que a reserva seja aberta e tenha atributos correspondentes (tipo de instância, plataforma e zona de disponibilidade).

Note

Você só pode modificar as configurações da Reserva de capacidade de uma instância enquanto ela está parada.

Você pode modificar as configurações da Reserva de capacidade de uma instância usando o console do Amazon EC2 e a AWS CLI.

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), selecione a instância a ser modificada e escolha Actions (Ações), Modify Reserva de capacidade Settings (Modificar configurações da Reserva de capacidade).
3. Em Reserva de capacidade, execute um destes procedimentos:
 - Escolha Open (Aberta) para configurar a instância para execução em qualquer Reserva de capacidade open que tenha atributos correspondentes (tipo, plataforma e zona de disponibilidade da instância) e capacidade suficiente.

Note

Se você não tiver uma Reserva de capacidade open correspondente com capacidade suficiente, a instância será executada na capacidade sob demanda.

- Escolha None (Nenhuma) para impedir que a instância execute em uma .
- Escolha a Reserva de capacidade específica na qual a instância deve ser executada.

Note

Se os atributos da instância (tipo de instância, plataforma e zona de disponibilidade) não corresponderem aos da Reserva de capacidade selecionada, ou se a Reserva de capacidade selecionada não tiver capacidade suficiente, a execução da instância falhará.

Para modificar as configurações da Reserva de capacidade de uma instância usando a AWS CLI

Use o comando [modify-instance-capacity-reservation-attributes](#):

```
$ aws ec2 modify-instance-capacity-reservation-attributes --instance-id instance_id --  
capacity-reservation-specification 'CapacityReservationPreference=none|open'
```

Visualização de uma Reserva de capacidade

As Reservas de capacidade têm três estados possíveis:

- **active** — a Reserva de capacidade está ativa e 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** — a Reserva de capacidade foi cancelada manualmente. 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. As solicitações com falha são retidas por 60 minutos.

Você pode visualizar as Reservas de capacidade ativas usando o console do Amazon EC2 e a AWS CLI.

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](#):

```
$ aws ec2 describe-capacity-reservations
```

Cancelamento de 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 taxa padrão de instância sob demanda ou em uma tarifa com desconto se você tiver uma RI regional ativa 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, executem em uma Reserva de capacidade 'open (aberta)' com atributos correspondentes e capacidade suficiente, ou evitem a execução em uma Reserva de capacidade. Para obter mais informações, consulte [Modificação das configurações de Reserva de capacidade de uma instância](#) (p. 383).

Você pode cancelar uma Reserva de capacidade usando o console do Amazon EC2 e a AWS CLI.

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

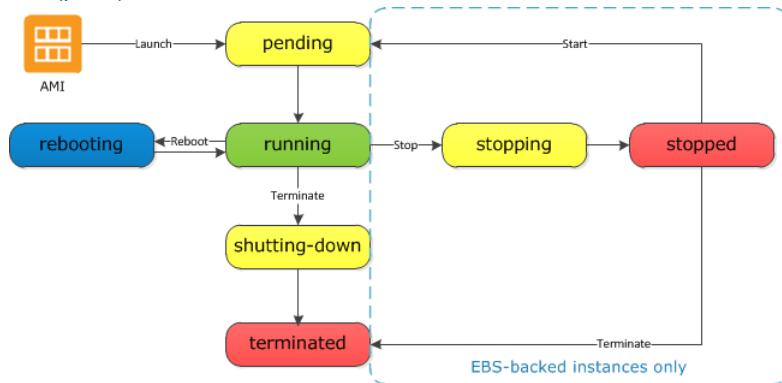
Use o comando [cancel-capacity-reservation](#):

```
$ aws ec2 cancel-capacity-reservation --capacity-reservation-id reservation_id
```

Ciclo de vida da instância

Trabalhando com o Amazon EC2 para gerenciar suas instâncias do momento em que você os executa até o encerramento, você garante que seus clientes tenham a melhor experiência possível com os aplicativos ou os sites que você hospeda nas suas instâncias.

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 \(p. 91\)](#).



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 [Como evitar cobranças inesperadas](#) no Guia do usuário do AWS Billing and Cost Management.

Estado da instância	Descrição	Faturamento para uso da instância
pending	A instância está se preparando para entrar	Não faturado

Estado da instância	Descrição	Faturamento para uso da instância
	no estado <code>running</code> . Uma instância entra no estado <code>pending</code> quando ela é executada pela primeira vez ou quando é reiniciada após estar no estado <code>stopped</code> .	
<code>running</code>	A instância está em execução e pronta para uso.	Faturado
<code>stopping</code>	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
<code>stopped</code>	A instância está desativada e não pode ser usada. A instância pode ser reiniciada a qualquer momento.	Não faturado
<code>shutting down</code>	A instância está se preparando para ser encerrada.	Não faturado
<code>terminated</code>	A instância foi permanentemente excluída e não pode ser reiniciada.	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 Instâncias reservadas (p. 253)

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 hora ou hora parcial do , 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 \(p. 390\)](#) e [Conecte-se à sua instância do Linux \(p. 439\)](#).

Parada e início de instância (somente instâncias baseadas em Amazon EBS)

Se sua instância falhar na verificação de status ou não estiver executando seus aplicativos 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.

Ao iniciar sua instância, ela entra no estado `pending` e, na maioria dos casos, nós movemos a instância para um novo computador host. (Sua instância pode permanecer no mesmo computador host se não houver problemas com o computador host.) 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.

Cada vez que você faz a transição de uma instância de `stopped` para `running`, nós cobramos por segundo quando a instância está em execução, com no mínimo um minuto sempre que a instância é reiniciada.

Para obter mais informações, consulte [Interrompa e inicie sua instância \(p. 458\)](#).

Hibernação de instância (somente instâncias baseadas em 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 reinicia 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 \(p. 387\)](#) 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 reinicia a instância em hibernação, ela entra no estado `pending` e, na maioria dos casos, nós movemos a instância para um novo computador host. Sua instância pode permanecer no mesmo computador host se não houver problemas com o computador host.

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 sua instância \(p. 461\)](#).

Reinicialização da instância

Você pode reinicializar sua instância usando o console do Amazon EC2, uma ferramenta de linha de comando e a API do Amazon EC2. Recomendamos que você use o Amazon EC2 para reinicializar sua instância em vez de executar o comando de reinicialização do sistema operacional pela sua instância.

A reinicialização de uma instância equivale a reinicialização de um sistema operacional. A instância permanece no mesmo computador host e mantém seu nome DNS público, endereço IP privado e todos os dados em seus volumes de armazenamento de instância. Normalmente demora alguns minutos para a reinicialização ser concluída, mas o tempo necessário para reinicialização depende da configuração da instância.

Reiniciar uma instância não inicia um novo faturamento de instância período; o faturamento por segundo continua sem a cobrança mínima de um segundo.

Para obter mais informações, consulte [Reinicialize sua instância \(p. 467\)](#).

Inativação 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 atingir sua data de inativação programada, ela será 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 [Inativação da instância \(p. 468\)](#).

Encerramento da instância

Ao perceber que não necessita mais de uma instância, pode encerrá-la. Assim que o estado de uma instância de mudar para `shutting-down` ou para `terminated`, não haverá mais custos para essa instância.

Se você ativou a proteção de encerramento, não poderá encerrar a instância usando o console, a CLI ou a API.

Depois de encerrar uma instância, ela permanecerá visível no console por um curto período, quando será automaticamente excluída. Você também pode descrever uma instância encerrada usando a CLI e a API. Recursos (como tags) são gradualmente dissociados da instância encerrada, portanto podem não ser visíveis na instância encerrada após um breve período. Você não pode se conectar nem recuperar uma instância encerrada.

Cada instância com Amazon EBS oferece suporte ao atributo `InstanceInitiatedShutdownBehavior`, que controla se instância é parada ou encerrada ao iniciar uma desativação de dentro da instância em si (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 [Encerre sua instância \(p. 470\)](#).

Diferenças entre reinicialização, parada, 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	Na maioria dos casos, nós movemos a instância para um novo computador host. Sua instância pode permanecer no mesmo computador host se não houver problemas com o computador host.	Na maioria dos casos, nós movemos a instância para um novo computador host. Sua instância pode permanecer no mesmo computador host se não houver problemas com o computador host.	Nenhum
Endereços IPv4 privados e públicos	Esses endereços permanecem iguais	A instância mantém seu endereço IPv4 privado. A instância obtém um endereço IPv4 público, a menos que tenha um endereço IP elástico, que não muda parada/inicialização.	A instância mantém seu endereço IPv4 privado. A instância obtém um endereço IPv4 público, a menos que tenha um endereço IP elástico, que não muda parada/inicialização.	Nenhum
Endereços IP elásticos (IPv4)	O endereço IP elástico permanece associado à instância	O endereço IP elástico permanece associado à instância	O endereço IP elástico permanece associado à instância	O endereço IP elástico está dissociado da instância
Endereço IPv6	O endereço permanece o mesmo	A instância mantém seu endereço IPv6	A instância mantém seu endereço IPv6	Nenhum
Volumes de armazenamento de instâncias	Os dados são preservados	Os dados são apagados	Os dados são apagados	Os dados são apagados
Volume do dispositivo raiz	O volume é preservado	O volume é preservado	O volume é preservado	O volume é excluído por padrão
RAM (conteúdo da memória)	A RAM é apagada	A RAM é apagada	A RAM é salva em um arquivo no volume raiz	A RAM é apagada
Faturamento	A hora de fatura da instância não é alterada.	As cobranças de uma instância são interrompidas assim	Você incorre em cobranças quando a instância está no	As cobranças de uma instância são interrompidas

Característica	Reiniciar	Parar/iniciar (somente instâncias com Amazon EBS)	Hibernação (somente instâncias baseadas em Amazon EBS)	Encerrar
		que o estado mudar para <code>stopping</code> . Cada vez que uma instância faz a transição de <code>stopped</code> para <code>running</code> , nós iniciamos um novo período de , faturando um mínimo de um minuto toda vez que você reinicia a instância.	estado <code>stopping</code> , mas não incorre em cobranças quando a instância está no estado <code>stopped</code> . Cada vez que uma instância faz a transição de <code>stopped</code> para <code>running</code> , nós iniciamos um novo período de , faturando um mínimo de um minuto toda vez que você reinicia a instância.	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 [Alteração do comportamento de desligamento iniciado da instância \(p. 473\)](#).

Executar sua instância

Uma instância é um servidor virtual na nuvem da AWS. Você executa uma instância a partir de uma imagem de máquina da Amazon (AMI). A AMI fornece o sistema operacional, o servidor de aplicativos e os aplicativos 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 executar e usar uma instância micro gratuitamente por 12 meses. 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 a [Definição de preços 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	Execução de uma instância usando o assistente de execução de instância (p. 391)
[Console do Amazon EC2] Crie um modelo de execução e execute a instância a partir desse modelo	Execução de uma instância a partir de um modelo de execução (p. 398)
[Console do Amazon EC2] Use uma instância existente como base	Execução de uma instância usando parâmetros de uma instância existente (p. 408)
[Console do Amazon EC2] Use um snapshot do Amazon EBS que você criou	Execução de uma instância do Linux a partir de um backup (p. 409)
[Console do Amazon EC2] Use uma AMI comprada do AWS Marketplace	Executar uma instância do AWS Marketplace (p. 410)

Método	Documentação
[AWS CLI] Use uma AMI selecionada	Uso do Amazon EC2 por meio da CLI da AWS
[AWS Tools para Windows PowerShell] Use uma AMI selecionada	Amazon EC2 do AWS Tools para Windows PowerShell
[AWS CLI] Use a frota do EC2 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.	Executar uma frota de EC2 (p. 412)

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. 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 \(p. 439\)](#).

Quando você tiver terminado com uma instância, encerre-a. Para obter mais informações, consulte [Encerre sua instância \(p. 470\)](#).

Execução de uma instância usando o assistente de execução de instância

Antes de executar a instância, verifique se está configurado. Para obter mais informações, consulte [Como configurar com o Amazon EC2 \(p. 21\)](#).

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.

Execução da sua instância a partir de uma AMI

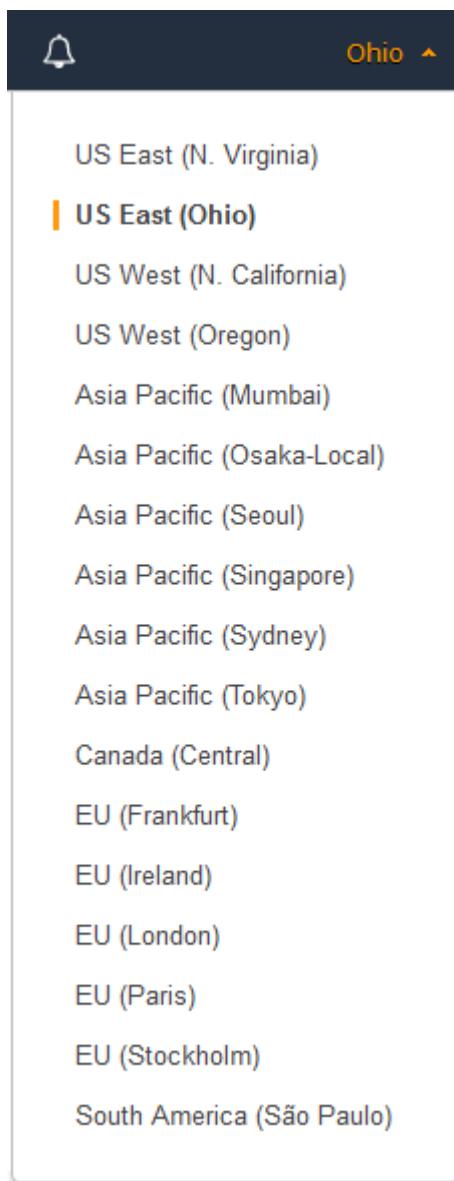
Quando você executa uma instância, deve selecionar uma configuração, conhecida como imagem de máquina da Amazon (AMI). A AMI contém as informações necessárias para criar uma nova instância. Por exemplo, um AMI pode conter o software necessário para atuar como servidor web: por exemplo, Linux, Apache e seu website.

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.

Inicie uma 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 é exibida. Selecione a região para a instância. Essa escolha é importante, pois alguns recursos do Amazon EC2 podem ser compartilhados entre regiões, enquanto outros não podem. Selecione a região que satisfaz suas necessidades. Para obter mais informações, consulte [Locais de recursos \(p. 992\)](#).



3. No painel do console do Amazon EC2, selecione Launch Instance (Iniciar instância).
4. Na página Escolher imagem de máquina da Amazon (AMI), escolha uma AMI da seguinte forma:
 - a. 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 ver 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 do AWS Marketplace \(p. 410\)](#).

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.

- b. 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 \(p. 91\)](#).
 - c. 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 \(p. 94\)](#).
 - d. Escolha a AMI que atenda às suas necessidades e marque Select (Selecionar).
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. Os tipos de instâncias maiores têm mais CPU e memória. Para obter mais informações, consulte [Tipos de instância \(p. 176\)](#).

Para permanecer elegível para o nível gratuito, escolha o tipo de instância t2.micro. Para obter mais informações, consulte [Instâncias de desempenho com capacidade de intermitência \(p. 189\)](#).

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).

6. 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.
 - (Opcional) Para ajudar a assegurar que você mantenha o número de instâncias para lidar com a demanda do aplicativo, escolha Launch into Auto Scaling Group (Executar no grupo de Auto Scaling) para criar uma configuração de execução e um grupo de Auto Scaling. O Auto Scaling escala o número de instâncias no grupo de acordo com suas especificações. Para mais informações, consulte o [Guia do usuário do Amazon EC2 Auto Scaling](#).
 - Purchasing option (Opção de compra): escolha Request Spot instances (Solicitar instâncias spot) para executar uma instância Spot. 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 [Criação da solicitação de Instância spot \(p. 309\)](#).
 - 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): selecione a sub-rede na qual executar sua instância. 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.
- 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 \(p. 724\)](#).
- 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.
- Reserva de capacidade: especifique se deseja executar a instância em capacidade compartilhada ou em uma Reserva de capacidade existente. Para obter mais informações, consulte [Execução de uma instância em uma Reserva de capacidade existente \(p. 381\)](#).
- 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 \(p. 712\)](#).
- 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 opções de CPU \(p. 495\)](#).
- Shutdown behavior (Comportamento de desativação): selecione se a instância deve parar ou encerrar quando desativada. Para obter mais informações, consulte [Alteração do comportamento de desligamento iniciado da instância \(p. 473\)](#).
- Enable termination protection (Permitir proteção de encerramento): para evitar o encerramento acidental, marque esta caixa de seleção. Para obter mais informações, consulte [Habilitação da proteção contra o encerramento de uma instância \(p. 472\)](#).
- 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 [Monitoramento das suas instâncias usando o CloudWatch \(p. 575\)](#).
- 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 for compatível com esse recurso, marque essa caixa de seleção para ativá-lo. Aplicam-se cobranças adicionais. Para obter mais informações, consulte [Amazon EBS – instâncias otimizadas \(p. 916\)](#).
- 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 [Instâncias dedicadas \(p. 371\)](#) e [Hosts dedicados \(p. 356\)](#).
- T2/T3 Unlimited (T2/T3 ilimitado): marque essa caixa de seleção para permitir que os aplicativos tenham intermitência acima da linha de base pelo tempo que for necessário. Podem se aplicar cobranças adicionais. Para obter mais informações, consulte [Instâncias de desempenho com capacidade de intermitência \(p. 189\)](#).
- 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 Auto-assign (Autoatribuir) permitir que a AWS escolha um para você.
- 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 \(p. 747\)](#). 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 [Como atribuir um endereço IPv4 público durante a execução da instância \(p. 728\)](#).

- 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.
 - 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 [Placement groups \(p. 793\)](#).
 - 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.
7. A AMI que você selecionou inclui um ou mais volumes de armazenamento, incluindo o volume de dispositivo raiz. Na página Add Storage (Adicionar storage), você pode especificar volumes adicionais para anexar à instância escolhendo Add New Volume (Adicionar novo volume). Você pode configurar as opções a seguir para cada volume:
- Type (Tipo): selecione os volumes de armazenamento de instâncias ou Amazon EBS para associar à instância. O tipo de volume disponível na lista depende do tipo de instância escolhido. Para obter mais informações, consulte [Armazenamento de instâncias do Amazon EC2 \(p. 958\)](#) e [Volumes do Amazon EBS \(p. 841\)](#).
 - 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 digitando texto no campo Snapshot. As descrições do snapshot diferenciam maiúsculas de minúsculas.
 - Size (Tamanho): para volumes baseados em Amazon EBS, você pode especificar um tamanho de armazenamento. Mesmo se você tiver selecionado uma AMI e uma instância qualificadas para o nível gratuito, para permanecer no nível gratuito, seu armazenamento total terá que ficar abaixo de 30 GiB.

Note

As AMIs do Linux requerem tabelas de partição GPT e GRUB 2 para volumes de inicialização de 2 TiB (2048 GiB) ou mais. Muitas AMIs do Linux usam hoje o esquema de particionamento MBR, que é compatível somente com volumes de inicialização de 2047

GiB. Se sua instância não for inicializada com um volume de inicialização de 2 TiB ou mais, a AMI que você está usando pode ser limitada a um tamanho de volume de inicialização de 2047 GiB. Volumes de não inicialização não têm essas limitações nas instâncias do Linux.

Note

Se você aumentar o tamanho do volume do dispositivo raiz nesse ponto (ou qualquer outro volume criado de um snapshot), precisará ampliar o sistema de arquivos naquele volume para usar o espaço extra. Para obter mais informações sobre estender seu sistema de arquivos após sua instância ter sido executada, consulte [Como modificar o tamanho, o desempenho ou o tipo de um volume do EBS \(p. 882\)](#).

- Volume Type (Tipo de volume): para volumes do Amazon EBS, selecione um volume Finalidade geral (SSD), Provisioned IOPS SSD ou Magnético. Para obter mais informações, consulte [Tipos de volume do Amazon EBS \(p. 844\)](#).

Note

Se você selecionar um volume de inicialização Magnético, será solicitado, ao concluir o assistente para fazer dos volumes do Finalidade geral (SSD) o volume de inicialização padrão para a instância e futuros lançamentos do console. Essa preferência persiste na sessão do navegador e não afeta as AMIs com volumes de inicialização Provisioned IOPS SSD. Recomendamos que você torne padrão os volumes do Finalidade geral (SSD), pois eles fornecem uma experiência muito mais rápida de inicialização e são o tipo ideal de volume para a maioria dos workloads. Para obter mais informações, consulte [Tipos de volume do Amazon EBS \(p. 844\)](#).

Note

Algumas contas da AWS criadas antes de 2012 podem ter acesso às Zonas de disponibilidade nas regiões us-west-1 ou ap-northeast-1 que não são compatíveis com volumes Provisioned IOPS SSD (io1). Caso não seja de criar um volume io1 (ou executar uma instância com um volume io1 no mapeamento de dispositivos do bloco) em uma dessas regiões, experimente uma zona de disponibilidade diferente na região. Você pode verificar se a zona de disponibilidade oferece suporte para volumes io1 ao criar um volume de io1 de 4 GiB naquela zona.

- IOPS: se você tiver selecionado o tipo de volume Provisioned IOPS SSD, poderá incorporar o número de operações de E/S por segundo (IOPS) que o volume é capaz de suportar.
- 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 [Preservação de volumes do Amazon EBS no encerramento da instância \(p. 474\)](#).
- Encrypted (Criptografado): selecione um valor nesse menu para configurar o estado de criptografia de novos volumes Amazon EBS. Se o valor padrão for Not encrypted (Não criptografado). As opções adicionais incluem usar sua chave mestra do cliente (CMK) gerenciada pela AWS ou uma CMK gerenciada pelo cliente criada por você. As chaves disponíveis estão listadas no menu. Você também pode passar o ponteiro do mouse sobre o campo e colar o Nome de recurso da Amazon (ARN) de uma chave diretamente na caixa de texto. Para obter mais informações sobre como criar CMKs gerenciadas pelo cliente, consulte [Guia do desenvolvedor do AWS Key Management Service](#).

Note

Os volumes criptografados só podem ser associados aos [tipos de instâncias selecionados \(p. 927\)](#).

Depois de configurar seus volumes, escolha Next: Add Tags (Próximo: Adicionar tags).

8. Na página Add Tags (Adicionar tags), especifique as [tags \(p. 1003\)](#) fornecendo combinações de chave e valor. Você pode marcar a instância, os volumes ou ambos com uma tag. Para Instâncias spot, você pode marcar a Instância spot como somente solicitação. Escolha Add another tag

(Adicionar outra tag) para adicionar mais de uma tag aos seus recursos. Escolha Next: Configure Security Group (Próximo: Configurar grupo de segurança) ao concluir.

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 \(p. 626\)](#).) Selecione ou crie um grupo de segurança da forma a seguir e escolha Review and Launch (Revisar e executar).
 - a. 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.

Note

(Opcional) Você não pode editar as regras de um grupo de segurança existente, mas você pode copiá-las a um novo grupo escolhendo Copy to new (Copiar para novo). Em seguida, você pode adicionar regras conforme descrito na próxima etapa.

- b. 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).
- c. 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.

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).

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, 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 executar uma instância, selecione a caixa de confirmação e escolha Launch Instances (Executar instâncias).

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.

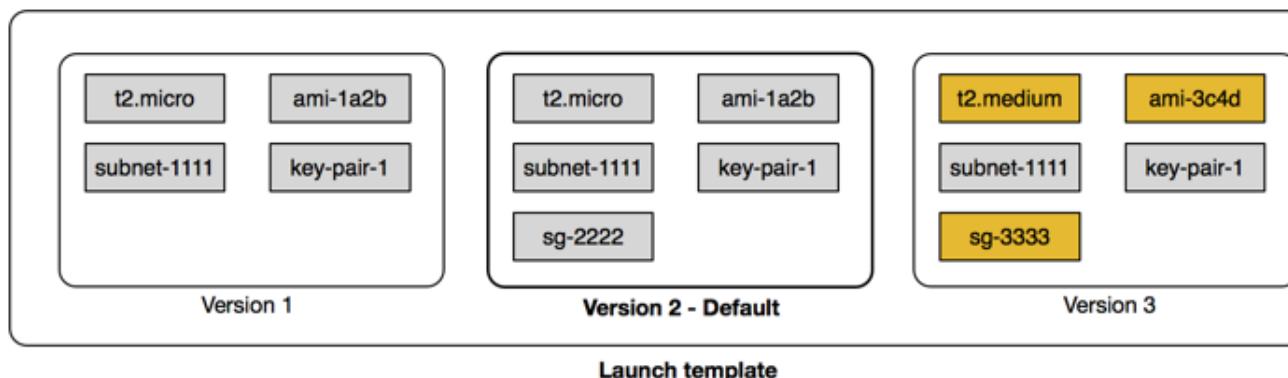
12. (Opcional) Você pode criar um alarme de verificação de status para a instância (taxas adicionais podem ser aplicadas). (Se você não tiver certeza, sempre pode adicionar um depois.) Na tela de confirmação, escolha Create status check alarms (Criar alarmes de verificação de status) e siga as instruções. Para obter mais informações, consulte [Criação e edição de alarmes de verificação de status \(p. 568\)](#).
13. Se a instância não executar ou o estado passar imediatamente para terminated, em vez de running, consulte [Solução de problemas de execução de instâncias \(p. 1026\)](#).

Execução de 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. Os modelos de execução permitem que você armazene parâmetros de execução de modo que não precise especificá-los cada vez que executar 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 AWS um 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 \(p. 398\)](#)
- [Uso de modelos de execução para controlar parâmetros de execução \(p. 399\)](#)
- [Controle do uso dos modelos de execução \(p. 399\)](#)
- [Criação de um modelo de execução \(p. 399\)](#)
- [Gerenciamento de versões de modelos de execução \(p. 404\)](#)
- [Execução de uma instância a partir de um modelo de execução \(p. 406\)](#)
- [Uso de modelos de execução com o Amazon EC2 Auto Scaling \(p. 407\)](#)
- [Uso de modelos de execução com o Frotas do EC2 \(p. 407\)](#)
- [Uso de modelos de execução com o Frotas spot \(p. 408\)](#)
- [Exclusão de um modelo de execução \(p. 408\)](#)

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 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 validados quando você cria o 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.
- 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`. Também devem ter permissões para criar ou usar recursos que são criados ou 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 do , consulte [Modelos de execução \(p. 697\)](#).

Controle do 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 [Permissões em nível do recurso compatíveis para ações da API do Amazon EC2 \(p. 653\)](#) e as seguintes políticas de exemplo: [Exemplo: trabalhar com modelos de execução \(p. 704\)](#).

Tenha cuidado ao conceder aos usuários permissões para usar as ações `ec2:CreateLaunchTemplate` e `ec2:CreateLaunchTemplateVersion`. Essas ações não oferecem suporte a permissões no nível do recurso que permitam 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.

Criação de 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.

Para criar um novo 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, selecione Launch Templates (Modelos de execução).
3. Escolha Create launch template (Criar modelo de execução) e forneça um nome e uma descrição.
4. Em Launch template contents (Conteúdo do modelo de execução), forneça as seguintes informações:
 - AMI ID (ID da 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 de sua propriedade ou [localizar uma AMI adequada \(p. 95\)](#).
 - 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 \(p. 176\)](#).
 - 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 \(p. 616\)](#).
 - Network type (Tipo de rede): se aplicável, se a instância deve ser executada em uma VPC ou no EC2-Classic. 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. Para obter mais informações, consulte [Grupos de segurança do Amazon EC2 para instâncias do Linux \(p. 626\)](#).
5. Em Network interfaces (Interfaces de rede), você pode especificar até duas [interfaces de rede \(p. 747\)](#) para a instância.
 - Device (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.
 - Security group ID (ID do grupo de segurança): o ID de um grupo de segurança na VPC ao qual associar a interface de rede.
 - Delete on termination (Excluir no encerramento): se a interface de rede deve ser excluída quando a instância for excluída.
6. Em Storage (Volumes) (Armazenamento - Volumes), especifique os volumes a serem anexados à instância, além dos volumes especificados pela AMI.
 - 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 \(p. 958\)](#) e [Volumes do Amazon EBS \(p. 841\)](#).

- 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 \(p. 844\)](#).
 - 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 [Preservação de volumes do Amazon EBS no encerramento da instância \(p. 474\)](#).
 - Encrypted (Criptografado): se criptografar novos volumes do Amazon EBS. Os volumes do Amazon EBS que são restaurados dos snapshots criptografados são criptografados automaticamente. Os volumes criptografados só podem ser associados aos [tipos de instâncias selecionados \(p. 927\)](#).
 - Key (Chave): para criptografar novos volumes do Amazon EBS, a chave mestra a ser usada ao criptografar os volumes. Digite a chave mestra padrão de sua conta ou qualquer chave mestra do cliente (CMK - customer master key) que tiver criado anteriormente usando o AWS Key Management Service. Você pode colar o ARN completo de qualquer chave à qual você tenha acesso. Para obter mais informações, consulte [.](#)
7. Em Tags, especifique as [tags \(p. 1003\)](#) fornecendo combinações de chave e valor. Você pode marcar a instância, os volumes ou ambos com uma tag.
 8. 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 Instâncias spot ao preço spot, limitado ao preço sob demanda, e escolha Customize Spot parameters (Personalizar parâmetros de Spot) 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 [Instâncias spot \(p. 293\)](#).
 - 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 \(p. 712\)](#).
 - Comportamento de desligamento: se a instância deve ser interrompida ou encerrada quando desligada. Para obter mais informações, consulte [Alteração do comportamento de desligamento iniciado da instância \(p. 473\)](#).
 - 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 sua instância \(p. 461\)](#).
 - Termination protection (Proteção contra encerramento): se encerramento acidental deve ser impedido. Para obter mais informações, consulte [Habilitação da proteção contra o encerramento de uma instância \(p. 472\)](#).
 - Monitoring (Monitoramento): se o monitoramento detalhado da instância deve ser habilitado usando o Amazon CloudWatch. Aplicam-se cobranças adicionais. Para obter mais informações, consulte [Monitoramento das suas instâncias usando o CloudWatch \(p. 575\)](#).
 - T2/T3 Unlimited (T2/T3 ilimitado): se permitir que os aplicativos tenham intermitência acima da linha de base pelo tempo que for necessário. Esse campo só é válido para instâncias T2 e T3. Podem se aplicar cobranças adicionais. Para obter mais informações, consulte [Instâncias de desempenho com capacidade de intermitência \(p. 189\)](#).
 - 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 [Placement groups \(p. 793\)](#).

- EBS-optimized instance (Instância otimizada para EBS): fornece capacidade dedicada adicional para E/S de Amazon EBS. Nem todos os tipos de instância são compatíveis com esse recurso, e cobranças adicionais são aplicáveis. Para obter mais informações, consulte [Amazon EBS – instâncias otimizadas \(p. 916\)](#).
- 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)). Podem se aplicar cobranças adicionais. Para obter mais informações, consulte [Instâncias dedicadas \(p. 371\)](#) e [Hosts dedicados \(p. 356\)](#). Se você especificar um Host dedicado, poderá escolher um host específico e a afinidade da instância.
- RAM disk ID (ID do disco RAM): o disco RAM da instância. Se tiver especificado um kernel, poderá ser necessário especificar um disco de RAM específico com os drivers compatíveis. Somente válido para AMIs paravirtuais (PV).
- Kernel ID (ID do kernel): o kernel da instância. Somente válido para AMIs paravirtuais (PV).
- 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 [Execução de comandos na instância do Linux na inicialização \(p. 510\)](#).

9. Escolha Create launch template (Criar modelo de execução).

Para criar um modelo de execução a partir de um modelo de execução existente (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. Escolha Create launch template (Criar modelo de execução). Forneça um nome e uma descrição para o modelo de execução.
4. Em Source template (Modelo de origem), escolha um modelo de execução no qual o novo modelo de execução se baseará.
5. 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.
6. Ajuste todos os parâmetros de execução quando necessário e escolha Create launch template (Criar modelo de execução).

Para criar um modelo de execução a partir de uma instância (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 e uma descrição 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 Template From Instance (Criar modelo a partir de instância).

Para criar um modelo de execução (AWS CLI)

- Use o comando `create-launch-template` (AWS CLI). O exemplo a seguir cria um modelo de execução que especifica o seguinte:

- 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 para a instância e cria uma tag para a instância (`Name=webserver`).

```
aws ec2 create-launch-template --launch-template-name TemplateForWebServer --version-description WebVersion1 --launch-template-data file://template-data.json
```

O seguinte é um arquivo `template-data.json` de exemplo:

```
{  
    "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"  
    }  
}
```

Para obter dados da instância de um modelo de execução (AWS CLI)

- Use o comando `get-launch-template-data` (AWS CLI) 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
```

Gerenciamento de versões de modelos de execução

Você pode criar versões de modelo de execução para um modelo de execução específico, definir uma versão padrão e excluir as versões que não são mais necessárias.

Tarefas

- [Criação de uma versão de modelo de execução \(p. 405\)](#)

- [Configuração da versão de modelo de execução padrão \(p. 405\)](#)
- [Exclusão de uma versão de modelo de execução \(p. 406\)](#)

Criação de 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 [Criação de um modelo de execução \(p. 399\)](#).

Para criar uma versão de 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. Escolha Create launch template (Criar modelo de execução).
4. Em What would you like to do (O que deseja de fazer), escolha Create a new template version (Criar uma nova versão do modelo)
5. Em Launch template name (Nome do modelo de execução), selecione o nome do modelo de execução atual na lista.
6. Em Template version description (Descrição da versão do modelo), digite uma descrição para a versão do modelo de execução.
7. (Opcional) Selecione uma versão do modelo de execução ou uma versão de um modelo de execução diferente para usar como uma base para a nova versão de modelo de execução. A nova versão de modelo de execução herdará os parâmetros de execução desta versão do modelo de execução.
8. Modifique os parâmetros de execução conforme necessário e escolha Create launch template (Criar modelo de execução).

Para criar uma versão de modelo de execução (AWS CLI)

- Use o comando `create-launch-template-version` (AWS CLI). 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"
```

Configuração da versão de 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.

Para definir a versão de modelo de execução padrão (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 Default version (Versão padrão), selecione o número de versão e escolha Set as default version (Definir como versão padrão).

Para definir a versão do modelo de execução (AWS CLI)

- Use o comando [modify-launch-template](#) (AWS CLI) e especifique a versão que deseja definir como padrão.

```
aws ec2 modify-launch-template --launch-template-id lt-0abcd290751193123 --default-version 2
```

Exclusão de 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.

Para excluir uma versão de 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 version (Excluir versão de modelo).
4. Selecione a versão a ser excluída e escolha Delete launch template version (Excluir versão do modelo de execução).

Para excluir uma versão de modelo de execução (AWS CLI)

- Use o comando [delete-launch-template-versions](#) (AWS CLI) e especifique os números de versão a serem excluídos.

```
aws ec2 delete-launch-template-versions --launch-template-id lt-0abcd290751193123 --versions 1
```

Execução de 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.

Para executar uma instância a partir de 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), Launch instance from template (Executar instância do modelo).
4. Selecione a versão de modelo de execução a ser usada.
5. (Opcional) Você pode substituir ou adicionar parâmetros de modelo de execução alterando e adicionando parâmetros na seção Instance details (Detalhes da instância).
6. Escolha Launch instance from template (Executar instância do modelo).

Para executar uma instância a partir de um modelo de execução (AWS CLI)

- Use o comando [run-instances](#) da AWS CLI 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 [Solução de problemas de execução de instâncias \(p. 1026\)](#).

Uso de 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.

Para criar ou atualizar um grupo do Amazon EC2 Auto Scaling com um modelo de execução (AWS CLI)

- Use o comando [create-auto-scaling-group](#) ou [update-auto-scaling-group](#) da AWS CLI e especifique o parâmetro `--launch-template`.

Uso de modelos de execução com a Frota do EC2

Você pode criar uma solicitação de um Frota do EC2 e especificar um modelo de execução na configuração da instância. Quando o Amazon EC2 atender à solicitação do Frota 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 [Como criar um Frota do EC2 \(p. 429\)](#).

Para criar uma Frota do EC2 com um modelo de execução (AWS CLI)

- Use o comando [create-fleet](#) da AWS CLI. Use o parâmetro `--launch-template-configs` para especificar o modelo de execução e quaisquer substituições para o modelo de execução.

Uso de modelos de execução com o Frota spot

Você pode criar uma solicitação de um Frota spot e especificar um modelo de execução na configuração da instância. Quando o Amazon EC2 atender à solicitação do 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 [Solicitação de Frota spot \(p. 315\)](#).

Para criar uma solicitação de Frota spot com um modelo de execução (AWS CLI)

- Use o comando [request-spot-fleet](#) da AWS CLI. Use o parâmetro `LaunchTemplateConfigs` para especificar o modelo de execução e quaisquer substituições para o modelo de execução.

Exclusão de 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.

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. Escolha Delete launch template (Excluir modelo de execução).

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
```

Execução de 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 este) 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 este) não clona sua instância selecionada; somente replica apenas 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 \(p. 398\)](#) 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 \(p. 724\)](#).
- 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 detalhes de configuração a seguir não são copiados da sua 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.

Para usar a instância atual como modelo

1. Na página Instâncias, selecione a instância que você deseja usar.
2. Selecione Actions (Ações) e Launch More Like This (Executar mais como este).
3. O assistente de execução abre na página Review Instance Launch (Revisar execução da instância). Você pode conferir os detalhes da sua instância e fazer todas as alterações necessárias clicando no link Edit (Editar) adequado.

Quando estiver pronto, escolha Launch (Executar) para selecionar um par de chaves e execute sua instância.

4. Se a instância não executar ou o estado passar imediatamente para terminated, em vez de running, consulte [Solução de problemas de execução de instâncias \(p. 1026\)](#).

Execução de uma instância do Linux a partir de um backup

Com uma instância do Linux baseada em Amazon EBS, você pode fazer backup do volume do dispositivo raiz da instância ao criar um snapshot. Quando tiver um snapshot do volume do dispositivo raiz de uma instância, você pode encerrar a instância e depois executar uma nova instância a partir do snapshot. Isso

pode ser útil se você não tiver a AMI original da qual executou uma instância, mas precisa poder executar uma instância usando a mesma imagem.

Algumas distribuições do Linux, como o Red Hat Enterprise Linux (RHEL) e o SUSE Linux Enterprise Server (SLES), usam o código de produto de faturamento associado a uma AMI para verificar o status da assinatura das atualizações de pacote. A criação de uma AMI a partir de um snapshot do EBS não mantém esse código de faturamento, e as instâncias subsequentes executadas dessa AMI não poderão se conectar à infraestrutura de atualização de pacote. Para manter os códigos de produto de faturamento, crie AMIs a partir da instância, não do snapshot. Para obter mais informações, consulte [Criação de uma AMI do Linux com Amazon EBS \(p. 111\)](#) ou [Criação de uma AMI em Linux com armazenamento de instâncias \(p. 115\)](#).

Use o procedimento a seguir para criar AMIs a partir do volume do dispositivo raiz da sua instância usando o console. Se você preferir, pode usar um dos comandos a seguir: [register-image](#) (AWS CLI) ou [Register-EC2Image](#) (AWS Tools para Windows PowerShell). Especifique o snapshot usando o mapeamento de dispositivos de blocos.

Para criar uma AMI a partir do volume do dispositivo raiz usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Elastic Block Store, Snapshots.
3. Selecione Criar snapshot.
4. Para Volumes, comece a digitar o nome ou o ID do volume do dispositivo raiz e selecione-o na lista de opções.
5. Selecione o snapshot que você acabou de criar, e escolha Actions (Ações), Create Image (Criar imagem).
6. Na caixa de diálogo Create Image from EBS Snapshot (Criar imagem a partir do snapshot do EBS), forneça as informações a seguir e selecione 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 [Nomenclatura de dispositivos nas instâncias do Linux \(p. 978\)](#).
 - 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 \(p. 94\)](#).
 - (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 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 [Como estender um sistema de arquivos Linux após um redimensionamento de volume \(p. 890\)](#).
7. No painel de navegação, selecione AMIs.
8. Selecione a AMI que acabou de criar e escolha Launch (Executar). Siga o assistente para executar sua instância. Para obter mais informações sobre como configurar cada etapa do assistente, consulte [Execução de uma instância usando o assistente de execução de instância \(p. 391\)](#).

Executar uma instância do AWS Marketplace

Você pode se inscrever em um produto do AWS Marketplace e executar uma instância a partir da AMI do produto usando o assistente de execução do Amazon EC2. Para obter mais informações sobre AMIs

pagas, consulte [AMIs pagas \(p. 107\)](#). Para cancelar sua assinatura depois do lançamento, primeiro encerre todas as instâncias sendo executadas a partir delas. Para obter mais informações, consulte [Gerenciamento de suas assinaturas do AWS Marketplace \(p. 111\)](#).

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 [Execução de uma instância usando o assistente de execução de instância \(p. 391\)](#). 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 acessem 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 (em execução), 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 \(p. 439\)](#).

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 [Gerenciamento de suas assinaturas do AWS Marketplace \(p. 111\)](#).

- Se a instância não executar ou o estado passar imediatamente para `terminated`, em vez de `running`, consulte [Solução de problemas de execução de instâncias \(p. 1026\)](#).

Execução de uma instância de AMI de AWS Marketplace usando a API e a CLI

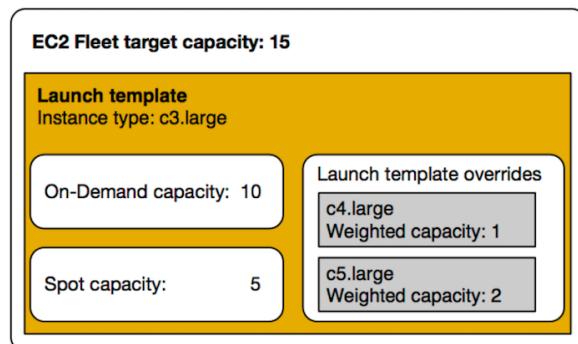
Para executar instâncias de produtos do AWS Marketplace usando a API ou as ferramentas de linha de comando, primeiro garanta que você esteja inscrito no produto. Você pode então executar uma instância com o ID da AMI do produto usando os seguintes métodos:

Método	Documentação
CLI da AWS	Use o comando <code>run-instances</code> ou consulte o tópico a seguir para obter mais informações: Execução de uma instância .
AWS Tools para Windows PowerShell	Use o comando <code>New-EC2Instance</code> ou consulte o tópico a seguir para obter mais informações: Executar uma instância do Amazon EC2 usando o Windows PowerShell
API de consulta	Use a solicitação <code>RunInstances</code> .

Executar uma frota de EC2

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 em conjunto. Ao usar Frota do EC2, você pode definir destinos de capacidade sob demanda e spot separados, especificar os tipos de instância que funcionam melhor para seus aplicativos e identificar a forma como o Amazon EC2 deve distribuir a capacidade da sua frota dentro de cada opção de compra.

A Frota do EC2 tenta executar o número de instâncias que são necessárias para atender à capacidade de destino especificada na sua solicitação. A frota também pode tentar manter a capacidade spot de destino se as Instâncias spot forem interrompidas devido a uma alteração nos preços spot ou na capacidade disponível. Para obter mais informações, consulte [Como as Instâncias spot funcionam \(p. 296\)](#).



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 executada.

Enquanto a frota está em execução, se o Amazon EC2 recuperar uma Instância spot devido a um aumento de preço ou uma falha na instância, a Frota do EC2 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 sua Instâncias reservadas. Por exemplo, se sua frota especificar instância sob demanda como `c4.1.large` e você tiver Instâncias reservadas para `c4.1.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 \(p. 413\)](#)
- [Limites da Frota do EC2 \(p. 413\)](#)
- [Estratégias de configuração da Frota do EC2 \(p. 414\)](#)
- [Gerenciar uma Frota do EC2 \(p. 422\)](#)

Limitações da Frota do EC2

As limitações a seguir se aplicam à Frota do EC2:

- A Frota do EC2 está disponível apenas por meio da API ou da AWS CLI.
- Uma solicitação de Frota do EC2 não pode abranger regiões. 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.

Limites da Frota do EC2

Os limites comuns do Amazon EC2 aplicam-se a instâncias executadas por uma Frota do EC2, como limites de solicitação spot, limites de instância e limites de volume. Além disso, os limites a seguir são aplicáveis:

- O número de Frotas do EC2 ativas por região: 1.000*
- O número de especificações de execução por frota: 50
- O tamanho dos dados de usuário em uma especificação de execução: 16 KB
- A capacidade de destino por Frota do EC2: 10.000
- A capacidade de destino em todas as Frotas do EC2 de uma região: 100.000*

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.

*Esses limites aplicam-se à Frotas do EC2 e Frotas spot.

Instâncias T3

Se você pretende usar T3 Instâncias spot imediatamente e por um curto período, sem tempo ocioso para acumular créditos de CPU, recomendamos executar T3 Instâncias spot no modo [standard \(p. 201\)](#) para evitar pagar custos mais altos.

Se você executar T3 Instâncias spot no modo [unlimited \(p. 193\)](#) e esgotar a CPU imediatamente, gastará os créditos excedentes por isso. Se você usar a instância por um curto período, a instância não terá tempo para acumular créditos de CPU para pagar os créditos excedentes, e você precisará pagar os créditos excedentes quando encerrar a instância.

O modo [Unlimited](#) para T3 Instâncias spot será adequado somente se a instância for executada por tempo suficiente para acumular créditos de CPU para intermitência. Caso contrário, o pagamento dos créditos excedentes deixa T3 Instâncias spot mais caro do que as instâncias M5 ou C5.

Instâncias T2

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 a [T2 ilimitada \(p. 193\)](#) ou usar um tipo de instância com CPU dedicada (por exemplo, `c4.large`).

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 on-demand e Instâncias spot para atender à capacidade desejada. A solicitação de Instâncias spot será atendida se o preço spot exceder o preço spot atual e se houver capacidade disponível. A frota também tentará manter a capacidade de destino se as Instâncias spot forem interrompidas devido a uma alteração nos preços spot ou na capacidade disponível.

Grupo de Instância spot é um conjunto de instâncias do EC2 não utilizadas com o mesmo tipo de instância, sistema operacional, zona de disponibilidade e plataforma de rede. 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 Instância spots 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 aplicativos 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. Ou você pode solicitar 1000 núcleos com um mínimo de 2 GB de RAM por núcleo. A frota determina a combinação de opções do Amazon EC2 para executar essa capacidade ao menor custo possível.

Use as estratégias de configuração apropriadas para criar uma Frota do EC2 que atenda às suas necessidades.

Tópicos

- [Planejar uma Frota do EC2 \(p. 415\)](#)
- [Tipos de solicitação de Frota do EC2 \(p. 415\)](#)
- [Estratégias de alocação para Instâncias spot \(p. 416\)](#)
- [Configurar a Frota do EC2 para backup sob demanda \(p. 417\)](#)
- [Sobreposições de preço máximo \(p. 417\)](#)
- [Peso da instância da Frota do EC2 \(p. 417\)](#)
- [Apresentação: Como usar a Frota do EC2 com o peso da instância \(p. 419\)](#)

- [Apresentação: Utilizar a Frota do EC2 com a opção sob demanda como a capacidade principal \(p. 421\)](#)

Planejar uma Frota do EC2

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 de Frota do EC2 \(p. 415\)](#).
- Determine os tipos de instâncias que atendem aos requisitos do aplicativo.
- 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 da instância da Frota do EC2 \(p. 417\)](#).
- 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.
- Leia as opções possíveis para sua Frota do EC2. Para mais informações, consulte o [Referência do arquivo de configuração JSON da Frota do EC2 \(p. 427\)](#). Para exemplos de configuração da Frota do EC2, consulte [Exemplos de configuração de Frota do EC2 \(p. 436\)](#).

Tipos de solicitação de 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.

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 spot, a frota não tentará reabastecer as Instâncias spot nem enviará solicitações em grupos de Instância spot alternativos se a capacidade estiver indisponível.

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.

Não é possível modificar a capacidade de destino de uma solicitação `instant` ou `request` do Frota do EC2 depois que ela é enviada. Para alterar a capacidade de destino de uma solicitação de frota `instant` ou `request`, exclua a frota e crie uma nova.

Todos os três tipos de solicitações se beneficiam com uma estratégia de alocação. Para obter mais informações, consulte [Estratégias de alocação para Instâncias spot \(p. 416\)](#).

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 possíveis de Instância spot representados por suas especificações de execução. Veja a seguir as estratégias de alocação que você pode especificar na sua frota:

`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.

`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`.

Como 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 Instância spot, uma Frota do EC2 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.

Configurar a Frota do EC2 para otimização de custos

Para otimizar os custos de uso de Instâncias spot, especifique a estratégia de alocação `lowestPrice` de modo que a Frota do EC2 implemente a combinação mais barata 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 (seja `lowestPrice` ou `diversified`) para Instâncias spot.

Configurar a Frota do EC2 para otimização de custos e diversificação

Para criar uma frota de Instâncias spot que seja barata e diversificada, use a estratégia de alocação `lowestPrice` em combinação com `InstancePoolsToUseCount`. O Frota do EC2 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 spot especificado. Esta combinação pode ser usada para evitar Instâncias spot mais caras.

Escolher a estratégia de alocação apropriada

Você pode otimizar a frota com base no seu caso de uso.

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 Instância 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 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 `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 executar um serviço da web, recomendamos que especifique um grande número de grupos spot (por exemplo, `InstancePoolsToUseCount=10`) para minimizar o impacto se um grupo de Instância spot ficar temporariamente indisponível.

Configurar a 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`.

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.

Peso da instância da Frota do EC2

Ao criar uma Frota do EC2, você poderá definir as unidades de capacidade com que cada tipo de instância contribuirá para o desempenho do aplicativo e poderá ajustar corretamente seu preço máximo para cada especificação de execução 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 seu preço por hora dividindo seu preço para um tipo de instância pelo número de unidades que ele representa. A Frota do EC2 calcula a quantidade de instâncias a ser executada, 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 (0,05 dividido por 2)
r3.8xlarge	8	10	2 (10 dividido por 8, resultado arredondado para cima)	0,10 USD	0,0125 (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 `lowestPrice`, 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.

Apresentação: Como usar a Frota do EC2 com o peso da instância

Esta apresentação usa uma empresa fictícia chamada Exemplo Corp para ilustrar o processo de solicitação de uma Frota do EC2 usando o peso da instância.

Objetivo

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.

Planejamento

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 um aplicativo 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 o aplicativo 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 seu aplicativo (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	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`.

Verificação de 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 do Frota do EC2 \(p. 423\)](#).

Criar a Frota do EC2

A Exemplo Corp cria um arquivo, `config.json`, com a seguinte configuração para sua Frota do EC2:

```
{  
    "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",  
                    "MaxPrice": "0.90",  
                    "SubnetId": "subnet-482e4972",  
                    "WeightedCapacity": 4  
                }  
            ]  
        }  
    ]  
}
```

```
        ]
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "DefaultTargetCapacityType": "spot"
    }
}
```

A Exemplo 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 [Como criar um Frota do EC2 \(p. 429\)](#).

Atendimento

A estratégia de alocação determina de quais grupos de Instância spot suas 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 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.

Apresentação: Utilizar a Frota do EC2 com a opção sob demanda como a capacidade principal

Esta apresentação 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).

Objetivo

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.

Planejamento

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 on-demand para garantir a acomodação do tráfego em períodos de pico.
- Capacidade de Instância spot – A ABC Online gostaria de aprimorar o desempenho, mas com preços mais baixos, com provisionamento de 5 Instâncias spot.

Verificação de 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 do Frota do EC2 \(p. 423\)](#).

Criar a Frota do EC2

A ABC Online cria um arquivo, `config.json`, com a seguinte configuração para sua Frota do EC2:

```
{  
    "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 [Como criar um Frota do EC2 \(p. 429\)](#).

Atendimento

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.

Gerenciar uma Frota 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 Frota do EC2 permanecerá ativa até que expire ou você a exclua. Ao excluir uma frota, você poderá especificar se a exclusão encerrará ou não as instâncias dessa frota.

Tópicos

- [Estados das solicitações de Frota do EC2 \(p. 423\)](#)
- [Pré-requisitos do Frota do EC2 \(p. 423\)](#)
- [Verificações de integridade da Frota do EC2 \(p. 425\)](#)
- [Gerar um arquivo de configuração JSON de Frota do EC2 \(p. 426\)](#)
- [Como criar um Frota do EC2 \(p. 429\)](#)
- [Marcando um Frota do EC2 \(p. 432\)](#)

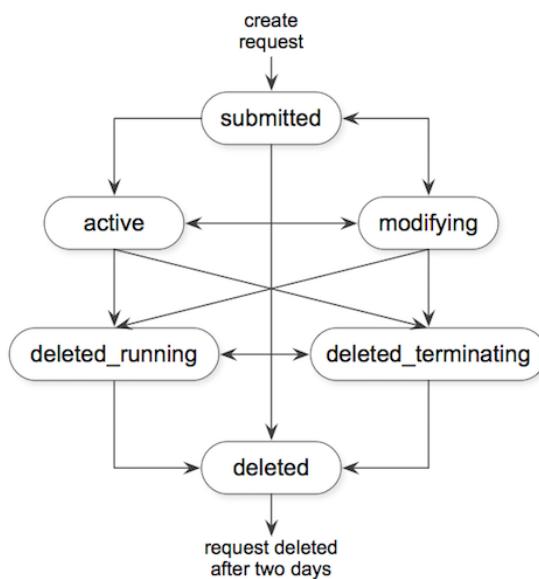
- [Como monitorar um Frotas do EC2 \(p. 422\)](#)
- [Modificar uma Frotas do EC2 \(p. 434\)](#)
- [Exclusão de uma Frotas do EC2 \(p. 435\)](#)
- [Exemplos de configuração de Frotas do EC2 \(p. 436\)](#)

Estados das solicitações de Frotas do EC2

Uma solicitação de Frotas do EC2 pode estar em um dos seguintes estados:

- **submitted** – A solicitação de Frotas do EC2 está sendo avaliada, e o Amazon EC2 está se preparando para executar o número de instâncias desejado, que pode incluir Instâncias on-demand, Instâncias spot ou ambas.
- **active** – A solicitação de Frotas 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 Frotas 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 de solicitação `maintain` pode ser modificado. Esse estado não se aplica a outros tipos de solicitação.
- **deleted_running** – A solicitação de Frotas 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.
- **deleted_terminating** – A solicitação de Frotas do EC2 foi excluída, e as instâncias estão sendo encerradas. A solicitação permanece nesse estado até que todas as instâncias sejam encerradas.
- **deleted** – A Frotas 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 Frotas do EC2. Se você exceder os limites da frotas, a solicitação será excluída imediatamente.



Pré-requisitos da Frotas do EC2

Para criar uma Frotas do EC2, observe os seguintes pré-requisitos.

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 [Execução de uma instância a partir de um modelo de execução \(p. 398\)](#).

Função vinculada ao serviço para Frota do EC2

A função `AWSServiceRoleForEC2Fleet` concede ao Frota do EC2 para solicitar, executar, encerrar e codificar instâncias em seu nome. O Amazon EC2 usa essa função vinculada ao serviço para realizar estas ações:

- `ec2:RequestSpotInstances` – Solicitação Instâncias spot.
- `ec2:TerminateInstances` – Encerrar Instâncias spot.
- `ec2:DescribeImages` – Descreva imagens de máquina da Amazon (AMI) para Instâncias spot.
- `ec2:DescribeInstanceStatus` – Descreva o status das Instâncias spot.
- `ec2:DescribeSubnets` – Descreva as sub-redes para Instâncias spot.
- `ec2:CreateTags` – Adicionar tags de sistema a Instâncias spot.

Verifique se esta função está disponível antes de usar a AWS CLI ou uma API para criar uma Frota do EC2. Para criar a função, use o console do IAM da seguinte forma.

Para criar uma função do IAM para o Frota do EC2

1. Abra o console do IAM em <https://console.aws.amazon.com/iam/>.
2. No painel de navegação, escolha Roles (Funções) e Create role (Criar função).
3. Em Select type of trusted entity (Selecionar tipo de entidade confiável), escolha AWS service (Serviço 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.

Usuários do Frota do EC2 e IAM

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

1. Abra o console do IAM em <https://console.aws.amazon.com/iam/>.
2. No painel de navegação, selecione Policies (Políticas).
3. Escolha Create policy (Criar política).
4. 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": [  
        "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 determina o status de integridade de uma instância usando as verificações de status fornecidas pelo Amazon EC2. Se o status da verificação de status da instância ou da verificação de status do sistema for `impaired` para três verificações de integridade consecutivas, o status de integridade da instância será `unhealthy`. Caso contrário, o status de integridade será `healthy`. Para obter mais informações, consulte [Verificações de status para suas instâncias \(p. 565\)](#).

Você pode configurar a Frota do EC2 para substituir instâncias não íntegras. Depois de habilitar a substituição de verificação de integridade, uma instância é substituída após o status de integridade ser relatado como `unhealthy`. A frota pode ficar abaixo de sua capacidade de destino por até alguns minutos enquanto uma instância não íntegra está sendo substituída.

Requisitos

- A substituição de verificação de integridade só tem suporte em Frotas do EC2 que mantêm uma capacidade de destino, e não em frotas únicas.
- 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`.

Gerar um arquivo de configuração JSON de 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 Frota do EC2:

```
aws ec2 create-fleet --generate-cli-skeleton
```

Os seguintes parâmetros de Frota do EC2 estão disponíveis:

```
{
    "DryRun": true,
    "ClientToken": "",
    "SpotOptions": {
        "AllocationStrategy": "lowestPrice",
        "InstanceInterruptionBehavior": "hibernate",
        "InstancePoolsToUseCount": 0
    },
    "OnDemandOptions": {
        "AllocationStrategy": "prioritized"
    },
    "ExcessCapacityTerminationPolicy": "termination",
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateId": "",
                "LaunchTemplateName": "",
                "Version": ""
            },
            "Overrides": [
                {
                    "InstanceType": "t2.micro",
                    "MaxPrice": "",
                    "SubnetId": "",
                    "AvailabilityZone": "",
                    "WeightedCapacity": null,
                    "Priority": null
                }
            ]
        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 0,
        "OnDemandTargetCapacity": 0,
        "SpotTargetCapacity": 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 de destino Instância spot em todos os grupos de Instância spot especificados pela Frota do EC2. Os valores válidos são `lowestPrice` e `diversified`. O padrão é `lowestPrice`. Especifique a estratégia de alocação que atende às suas necessidades. Para obter mais informações, consulte [Estratégias de alocação para Instâncias spot \(p. 416\)](#).

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 spot para os quais alocar sua capacidade spot de destino. Válido somente quando AllocationStrategy spot é definido como `lowestPrice`. A Frota do EC2 seleciona os grupos spot mais econômicos e aloca uniformemente sua capacidade spot de destino pelo número de grupos spot que você especificar.

AllocationStrategy (para OnDemandOptions)

A ordem das substituições do modelo de execução para utilização de modo a atender a capacidade sob demanda. Se você especificar `lowestPrice`, 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 `lowestPrice`.

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 do execução, consulte [Execução de uma instância a partir de um modelo de execução \(p. 398\)](#).

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 [Execução de uma instância a partir de um modelo de execução \(p. 398\)](#).

Versão

O número da versão do modelo de execução.

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. Se a AllocationStrategy estiver definida como prioritized, a Frota do EC2 usará a prioridade para determinar qual substituição de modelo de execução será usada primeiro para atender à capacidade sob demanda. A prioridade mais alta é executada primeiro. Os valores válidos são números inteiros começando em 0. Quanto menor o número, maior a prioridade. Se nenhum número for definido, a substituição terá a menor prioridade.

TotalTargetCapacity

O número de instâncias a serem executadas. Você pode escolher instâncias ou características de desempenho que são importantes para a carga de trabalho de seu aplicativo, 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) Indica se a Frota do EC2 envia uma solicitação síncrona única da capacidade desejada (`instant`) ou uma solicitação assíncrona única da capacidade desejada, mas sem tentar manter a capacidade, ou envia solicitações em grupos de capacidade alternativos, se a capacidade estiver indisponível (`request`), ou envia uma solicitação assíncrona da capacidade desejada e continua a manter a capacidade desejada reabastecendo Instâncias spot interrompidas (`maintain`). Os valores válidos são `instant`, `request` e `maintain`. O valor padrão é `maintain`. Para obter mais informações, consulte [Tipos de solicitação de Frota do EC2 \(p. 415\)](#).

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 \(p. 399\)](#). Para obter informações sobre marcação após a execução, consulte [Marcação dos seus recursos \(p. 1004\)](#).

Como criar um 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 Frotas 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 Frotas do EC2 \(p. 427\)](#).

As Frotas do EC2 podem ser criadas somente com o uso da AWS CLI.

Para criar uma Frotas do EC2 (AWS CLI)

- Use o seguinte comando `create-fleet` (AWS CLI) para criar uma Frotas do EC2:

```
aws ec2 create-fleet --cli-input-json file://file_name.json
```

Para obter arquivos de configuração de exemplo, consulte [Exemplos de configuração de Frotas do EC2 \(p. 436\)](#).

O seguinte é um exemplo de saída de uma frotas do tipo `request` ou `maintain`:

```
{  
    "FleetId": "fleet-12a34b55-67cd-8ef9-ba9b-9208dEXAMPLE"  
}
```

O seguinte é um exemplo de saída de uma frotas 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",  
            "Platform": null  
        },  
        {  
            "LaunchTemplateAndOverrides": {  
                "LaunchTemplateSpecification": {  
                    "LaunchTemplateId": "lt-01234a567b8910abcEXAMPLE",  
                    "Version": "1"  
                },  
                "Overrides": {  
                    "InstanceType": "c4.large",  
                    "AvailabilityZone": "us-east-1a"  
                }  
            },  
            "Lifecycle": "on-demand",  
            "InstanceIds": [  
                "i-5678901234abcdef0",  
                "i-1234567890abcdef1"  
            ]  
        }  
    ]  
}
```

```
        "i-5432109876abcdef9"
    ],
    "InstanceType": "c4.large",
    "Platform": null
},
]
```

O seguinte é 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
        },
    ]
}
```

O seguinte é 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": []
}
```

Marcando um Frota do EC2

Para categorizar e gerenciar as solicitações de Frota do EC2, você pode marcá-las com metadados personalizados. Para obter mais informações, consulte [Marcação dos seus recursos do Amazon EC2 \(p. 1003\)](#).

Você pode atribuir uma tag a uma solicitação de Frota do EC2 ao criá-la ou posteriormente. As tags atribuídas à solicitação de frota não são atribuídas às instâncias executadas pela frota.

Para marcar uma nova solicitação de frota EC2

Para marcar uma solicitação de Frota do EC2 ao criá-la, especifique o par de valor-chave no [arquivo JSON \(p. 426\)](#) usado para criar a frota. O valor de ResourceType deve ser fleet. Se você especificar outro valor, ocorrerá falha na frota.

Para marcar instâncias executadas por um Frota do EC2

Para marcar instâncias ao serem executadas pela frota, especifique as tags no [modelo de execução \(p. 399\)](#) mencionado na solicitação de Frota do EC2.

Para marcar uma instância e solicitação de Frota do EC2 existente (AWS CLI)

Use o comando [create-tags](#) a seguir para marcar os recursos existentes:

```
aws ec2 create-tags --resources fleet-12a34b55-67cd-8ef9-
ba9b-9208dEXAMPLE i-1234567890abcdef0 --tags Key=purpose,Value=test
```

Como monitorar um Frotas do EC2

A Frotas 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 sua Frotas do EC2 (AWS CLI)

Use o seguinte 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": "lowestPrice"
            },
            "FleetState": "active",
            "ExcessCapacityTerminationPolicy": "termination",
            "CreateTime": "2018-04-10T16:46:03.000Z"
        }
    ]
}
```

Use o seguinte comando [describe-fleet-instances](#) para descrever as instâncias da Frotas do EC2 especificada:

```
aws ec2 describe-fleet-instances --fleet-id fleet-73fb2ce-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-73fb2ce-aa30-494c-8788-1cee4EXAMPLE"
}
```

Use o seguinte comando [describe-fleet-history](#) para descrever o histórico da Frota do EC2 especificada na hora especificada:

```
aws ec2 describe-fleet-history --fleet-request-id fleet-73fb2ce-aa30-494c-8788-1cee4EXAMPLE --start-time 2018-04-10T00:00:00Z
```

```
{
    "HistoryRecords": [],
    "FleetId": "fleet-73fb2ce-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`.

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`.

Note

Você só pode modificar uma Frota do EC2 que tenha `Type=maintain`.

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 `lowestPrice`, a frota executará as instâncias do grupo de Instância spot com 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 `lowestPrice`, 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 Frota do EC2 encerra uma Instância spot porque a capacidade de destino foi diminuída, a instância recebe um aviso de interrupção de Instância spot.

Para modificar uma Frota do EC2 (AWS CLI)

Use o seguinte comando [modify-fleet](#) para atualizar a capacidade de destino da Frota do EC2 especificada:

```
aws ec2 modify-fleet --fleet-id fleet-73fbcd2ce-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 seguinte maneira:

```
aws ec2 modify-fleet --fleet-id fleet-73fbcd2ce-aa30-494c-8788-1cee4EXAMPLE --target-capacity-specification TotalTargetCapacity=10 --excess-capacity-termination-policy no-termination
```

Exclusão de 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.

Você precisa especificar se a Frota do EC2 deverá encerrar suas respectivas 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.

Para excluir uma Frota do EC2 (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"  
        }  
    ]  
}
```

Você pode modificar o comando anterior usando o parâmetro `--no-terminate-instances` para excluir a Frota do EC2 sem encerrar as instâncias:

```
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-a4c6-3daf4c6b7dcEXAMPLE"  
        }  
    ]  
}
```

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 mais informações, consulte [Referência do arquivo de configuração JSON da Frota do EC2 \(p. 427\)](#).

1. Executar Instâncias spot como a opção de compra padrão ([p. 436](#))
2. Executar Instâncias on-demand como a opção de compra padrão ([p. 436](#))
3. Executar Instâncias on-demand como a capacidade principal ([p. 437](#))
4. Executar Instâncias spot usando a estratégia de alocação lowestPrice ([p. 437](#))

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": "ondemand"  
    }  
}
```

```
"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: Executar Instâncias spot usando a estratégia de alocação de preço mais baixo

Se a estratégia de alocação para Instâncias spot não for especificada, a estratégia de alocação padrão, `lowestPrice`, será usada. O exemplo a seguir usa a estratégia de alocação `lowestPrice`. 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": "t2.micro",
                "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"  
}  
}
```

Conecte-se à sua instância do Linux

Saiba como se conectar às instâncias do Linux que você executou e transfira arquivos entre seu computador local e sua instância.

Para se conectar a uma instância Windows, consulte [Conexão com sua instância Windows](#) no Guia do usuário do Amazon EC2 para instâncias do Windows.

Seu computador	Tópico
Linux ou Mac OS X	Conexão à sua instância do Linux utilizando SSH (p. 439)
Windows	Conexão da sua instância do Linux no Windows usando PuTTY (p. 444) Como se conectar à instância Linux no Windows usando o Subsistema do Windows para Linux (p. 451) Conexão à sua instância do Linux utilizando SSH (p. 439)
Todos	Conexão à sua instância do Linux usando o MindTerm (p. 456)

Depois de se conectar à sua instância, você pode tentar um de nossos tutoriais, como [Tutorial: Instalar um servidor web do LAMP com Amazon Linux AMI \(p. 46\)](#) ou [Tutorial: Hospedagem de um blog do WordPress com Amazon Linux \(p. 56\)](#).

Conexão à sua instância do Linux utilizando SSH

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 [Resolução de problemas para se conectar à sua instância \(p. 1028\)](#).

Depois que iniciar sua instância, você poderá conectá-la e usá-la da forma como usaria um computador bem na sua frente.

Note

Depois de iniciar uma instância, pode demorar alguns minutos para ela ficar pronta e que você possa se conectar a ela. Verifique se sua instância foi aprovada nas verificações de status. É possível ver essas informações na coluna Verificações de status da página Instâncias.

Pré-requisitos

Antes de você se conectar à sua instância do Linux, preencha os seguintes pré-requisitos:

- **Instalação de um cliente SSH**

Com o Windows 10 1709, você pode ativar o recurso "OpenSSH Client (Beta)". Com o Linux e o Mac OS X, o mais provável é que haja um cliente SSH instalado por padrão. Você pode verificar se existe um cliente SSH digitando ssh na linha de comando. Se o seu computador não reconhecer o comando, você pode instalar um cliente SSH. Para obter mais informações, consulte <http://www.openssh.com>.

- **Instale as ferramentas de AWS CLI**

(Opcional) Se você estiver usando AMI pública de terceiros, pode usar as ferramentas de linha de comando (CLI) para verificar a impressão digital. Para obter mais informações sobre como instalar a AWS CLI, consulte [Obter configurações](#) no Guia do usuário do AWS Command Line Interface.

- Obtenha a ID da instância

Você pode obter a ID de sua instância usando o console do Amazon EC2 (pela coluna ID da instância). Se preferir, pode usar [describe-instances](#) (AWS CLI) ou o comando [Get-EC2Instance](#) (AWS Tools para Windows PowerShell).

- Obtenha o nome do DNS público da instância

Você pode obter o DNS público para sua instância usando o console do Amazon EC2. Verifique a coluna Public DNS (IPv4) (DNS público – IPv4). Se essa coluna estiver oculta, selecione o ícone Show/Hide e selecione Public DNS (IPv4) (DNS público – IPv4). Se preferir, pode usar [describe-instances](#) (AWS CLI) ou o comando [Get-EC2Instance](#) (AWS Tools para Windows PowerShell).

- (Somente IPv6) Obtenha o endereço IPv6 da instância

Se você tiver atribuído um endereço IPv6 à sua instância, é possível também conectar-se à instância usando o endereço IPv6 em vez de um endereço IPv4 público ou um hostname DNS IPv4 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. Marque o campo IPv6 IPs (IPs IPv6). Se preferir, pode usar [describe-instances](#) (AWS CLI) ou o comando [Get-EC2Instance](#) (AWS Tools para Windows PowerShell). Para obter mais informações sobre IPv6, consulte [Endereços IPv6 \(p. 725\)](#).

- Encontrar a chave privada e verificar as permissões

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. Verifique se o arquivo `.pem` tem permissões de 0400, não 0777. Para obter mais informações, consulte [Erro: Arquivo de chave privada desprotegido \(p. 1033\)](#).

- Obtenha o nome de usuário padrão da AMI usada para executar a instância

- Para a AMI do Amazon Linux 2 ou do Amazon Linux, o nome de usuário é `ec2-user`.
- Para um AMI do CentOS, o nome de usuário é `centos`.
- Em uma AMI do Debian, o nome de usuário é `admin` ou `root`.
- Para a AMI do Fedora, o nome de usuário é `ec2-user` ou `fedora`.
- Para a AMI do RHEL, o nome de usuário é `ec2-user` ou `root`.
- Para a AMI do SUSE, o nome de usuário é `ec2-user` ou `root`.
- Para uma AMI do Ubuntu, o nome de usuário é `ubuntu`.
- Caso contrário, se `ec2-user` e `root` não funcionarem, verifique com o provedor de AMI.

- Permitir tráfego SSH de entrada do endereço IP à instância

Certifique-se de que o grupo de segurança associado à sua instância permita tráfego SSH de entrada do seu 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 permite o tráfego SSH por padrão. Para obter mais informações, consulte [Como autorizar tráfego de entrada em suas instâncias Linux \(p. 720\)](#).

Conexão com sua instância do Linux

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 [Resolução de problemas para se conectar à sua instância \(p. 1028\)](#).

Para se conectar à sua instância usando SSH

1. (Opcional) Você pode verificar a impressão digital da chave RSA na sua instância em execução usando um dos comandos a seguir no sistema local (não na instância). Isso será útil se você tiver executado sua instância a partir de AMI pública de terceiros. Encontre a seção `SSH HOST KEY FINGERPRINTS`, observe a impressão digital RSA (por exemplo,

1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f) e compare-a à impressão digital da instância.

- [get-console-output \(AWS CLI\)](#)

```
aws ec2 get-console-output --instance-id instance_id
```

Certifique-se de que a instância está no estado `running`, não no estado `pending`. A seção `SSH HOST KEY FINGERPRINTS` só estará disponível após a primeira inicialização da instância.

2. Em um shell da linha de comando, troque os diretórios para o local do arquivo de chave privada que você criou quando executou a instância.
3. Use o seguinte comando para definir as permissões do arquivo de chave privada para que somente você possa lê-lo.

```
chmod 400 /path/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 \(p. 1033\)](#).

4. Use o comando ssh para se conectar à instância. Você especifica o arquivo de chave privada (`.pem`) e `user_name@public_dns_name`. Por exemplo, se você usou o Amazon Linux 2 ou Amazon Linux AMI, o nome de usuário é `ec2-user`.

```
ssh -i /path/my-key-pair.pem ec2-user@ec2-198-51-100-1.compute-1.amazonaws.com
```

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)?
```

5. (Somente IPv6) Alternativamente, você pode 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. Por exemplo, se você usou o Amazon Linux 2 ou o Amazon Linux AMI, o nome de usuário é `ec2-user`.

```
ssh -i /path/my-key-pair.pem ec2-user@2001:db8:1234:1a00:9691:9503:25ad:1761
```

6. (Opcional) Verifique se a impressão digital no alerta de segurança corresponde à impressão digital que você obteve na etapa 1. Caso essas impressões digitais não correspondam, alguém pode estar tentando um ataque "man-in-the-middle". Se corresponderem, continue para a próxima etapa.
7. 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.
```

Transferência de 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.

Pré-requisitos

- 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 <http://www.openssh.org>.

- Obtenha a ID da instância

Você pode obter a ID de sua instância usando o console do Amazon EC2 (pela coluna ID da instância). Se preferir, pode usar [describe-instances](#) (AWS CLI) ou o comando [Get-EC2Instance](#) (AWS Tools para Windows PowerShell).

- Obtenha o nome do DNS público da instância

Você pode obter o DNS público para sua instância usando o console do Amazon EC2. Verifique a coluna Public DNS (IPv4) (DNS público – IPv4). Se essa coluna estiver oculta, selecione o ícone Show/Hide e selecione Public DNS (IPv4) (DNS público – IPv4). Se preferir, pode usar [describe-instances](#) (AWS CLI) ou o comando [Get-EC2Instance](#) (AWS Tools para Windows PowerShell).

- (Somente IPv6) Obtenha o endereço IPv6 da instância

Se você tiver atribuído um endereço IPv6 à sua instância, é possível também conectar-se à instância usando o endereço IPv6 em vez de um endereço IPv4 público ou um hostname DNS IPv4 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. Marque o campo IPv6 IPs (IPs IPv6). Se preferir, pode usar [describe-instances](#) (AWS CLI) ou o comando [Get-EC2Instance](#) (AWS Tools para Windows PowerShell). Para obter mais informações sobre IPv6, consulte [Endereços IPv6 \(p. 725\)](#).

- Encontrar a chave privada e verificar as permissões

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. Verifique se o arquivo `.pem` tem permissões de 0400, não 0777. Para obter mais informações, consulte [Erro: Arquivo de chave privada desprotegido \(p. 1033\)](#).

- Obtenha o nome de usuário padrão da AMI usada para executar a instância
 - Para a AMI do Amazon Linux 2 ou do Amazon Linux, o nome de usuário é `ec2-user`.
 - Para um AMI do CentOS, o nome de usuário é `centos`.
 - Em uma AMI do Debian, o nome de usuário é `admin` ou `root`.
 - Para a AMI do Fedora, o nome de usuário é `ec2-user` ou `fedora`.
 - Para a AMI do RHEL, o nome de usuário é `ec2-user` ou `root`.
 - Para a AMI do SUSE, o nome de usuário é `ec2-user` ou `root`.
 - Para uma AMI do Ubuntu, o nome de usuário é `ubuntu`.
 - Caso contrário, se `ec2-user` e `root` não funcionarem, verifique com o provedor de AMI.
- Permitir tráfego SSH de entrada do endereço IP à instância

Certifique-se de que o grupo de segurança associado à sua instância permita tráfego SSH de entrada do seu 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 permite o tráfego SSH por padrão. Para obter mais informações, consulte [Como autorizar tráfego de entrada em suas instâncias Linux \(p. 720\)](#).

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. (Opcional) Você pode verificar a impressão digital da chave RSA na sua instância usando um dos comandos a seguir no sistema local (não na instância). Isso será útil se você tiver executado sua instância a partir de AMI pública de terceiros. Encontre a seção **SSH HOST KEY FINGERPRINTS**, observe a impressão digital RSA (por exemplo, 1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f) e compare-a à impressão digital da instância.
 - [get-console-output \(AWS CLI\)](#)

```
aws ec2 get-console-output --instance-id instance_id
```

A seção **SSH HOST KEY FINGERPRINTS** só estará disponível após a primeira inicialização da instância.

2. Em um shell de comando, troque os diretórios para o local do arquivo de chave privada que você especificou quando executou a instância.
3. Use o comando chmod para assegurar-se que o arquivo de chave privada não está visível publicamente. Por exemplo, se o nome do arquivo de chave privada for **my-key-pair.pem**, use o seguinte comando:

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

4. 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 **ec2-user** e o nome DNS público da instância for **ec2-198-51-100-1.compute-1.amazonaws.com**, use o comando a seguir para copiar o arquivo para o diretório inicial **ec2-user**.

```
scp -i /path/my-key-pair.pem /path/SampleFile.txt ec2-
user@ec2-198-51-100-1.compute-1.amazonaws.com:~
```

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)?
```

5. (Somente IPv6) Como alternativa, é possível transferir um arquivo usando o endereço IPv6 para a instância. O endereço IPv6 deve vir entre colchetes ([]), que devem ser recuados ()�.

```
scp -i /path/my-key-pair.pem /path/SampleFile.txt ec2-user@
\[2001:db8:1234:1a00:9691:9503:25ad:1761\]:~
```

6. (Opcional) Verifique se a impressão digital no alerta de segurança corresponde à impressão digital que você obteve na etapa 1. Caso essas impressões digitais não correspondam, alguém pode estar tentando um ataque "man-in-the-middle". Se corresponderem, continue para a próxima etapa.
7. 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
```

8. 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 sua instância do EC2 de volta ao diretório inicial no seu computador local como `SampleFile2.txt`, use o comando a seguir no seu computador local:

```
scp -i /path/my-key-pair.pem ec2-user@ec2-198-51-100-1.compute-1.amazonaws.com:~/SampleFile.txt ~/SampleFile2.txt
```

9. (Somente IPv6) Alternativamente, você pode transferir arquivos na outra direção usando o endereço IPv6 da instância.

```
scp -i /path/my-key-pair.pem ec2-user@[2001:db8:1234:1a00:9691:9503:25ad:1761]:~/SampleFile.txt ~/SampleFile2.txt
```

Conexão da sua instância do Linux no Windows usando PuTTY

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 sua instância, consulte [Solução de problemas ao conectar-se à sua instância](#).

Depois que iniciar sua instância, você poderá conectá-la e usá-la da forma como usaria um computador bem na sua frente.

Note

Depois de iniciar uma instância, pode demorar alguns minutos para ela ficar pronta e que você possa se conectar a ela. Verifique se sua instância foi aprovada nas verificações de status. É possível ver essas informações na coluna Verificações de status da página Instâncias.

Pré-requisitos

Antes de você se conectar à sua instância do Linux usando o PuTTY, preencha os seguintes pré-requisitos:

- **Instalar PuTTY**
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.
- **Obtenha a ID da instância**

Você pode obter a ID de sua instância usando o console do Amazon EC2 (pela coluna ID da instância). Se preferir, pode usar [describe-instances](#) (AWS CLI) ou o comando [Get-EC2Instance](#) (AWS Tools para Windows PowerShell).

- Obtenha o nome do DNS público da instância

Você pode obter o DNS público para sua instância usando o console do Amazon EC2. Verifique a coluna Public DNS (IPv4) (DNS público – IPv4). Se essa coluna estiver oculta, selecione o ícone Show/Hide e selecione Public DNS (IPv4) (DNS público – IPv4). Se preferir, pode usar [describe-instances](#) (AWS CLI) ou o comando [Get-EC2Instance](#) (AWS Tools para Windows PowerShell).

- (Somente IPv6) Obtenha o endereço IPv6 da instância

Se você tiver atribuído um endereço IPv6 à sua instância, é possível também conectar-se à instância usando o endereço IPv6 em vez de um endereço IPv4 público ou um hostname DNS IPv4 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. Marque o campo IPv6 IPs (IPs IPv6). Se preferir, pode usar [describe-instances](#) (AWS CLI) ou o comando [Get-EC2Instance](#) (AWS Tools para Windows PowerShell). Para obter mais informações sobre IPv6, consulte [Endereços IPv6 \(p. 725\)](#).

- Encontre a key 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.

- Obtenha o nome de usuário padrão da AMI usada para executar a instância

- Para a AMI do Amazon Linux 2 ou do Amazon Linux, o nome de usuário é `ec2-user`.
- Para um AMI do CentOS, o nome de usuário é `centos`.
- Em uma AMI do Debian, o nome de usuário é `admin` ou `root`.
- Para a AMI do Fedora, o nome de usuário é `ec2-user` ou `fedora`.
- Para a AMI do RHEL, o nome de usuário é `ec2-user` ou `root`.
- Para a AMI do SUSE, o nome de usuário é `ec2-user` ou `root`.
- Para uma AMI do Ubuntu, o nome de usuário é `ubuntu`.
- Caso contrário, se `ec2-user` e `root` não funcionarem, verifique com o provedor de AMI.

- Permitir tráfego SSH de entrada do endereço IP à instância

Certifique-se de que o grupo de segurança associado à sua instância permita tráfego SSH de entrada do seu 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 permite o tráfego SSH por padrão. Para obter mais informações, consulte [Como autorizar tráfego de entrada em suas instâncias Linux \(p. 720\)](#).

Conversão da sua chave privada usando PuTTYgen

PuTTY não é originalmente compatível com o formato de chave privada (`.pem`) gerado pelo Amazon EC2. PuTTY tem uma ferramenta chamado PuTTYgen, que pode converter as chaves para o PuTTY formato necessário (`.ppk`). Você deve converter sua chave privada no formato (`.ppk`) antes de tentar se conectar à sua instância usando o PuTTY.

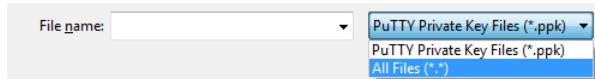
Para converter sua chave privada

1. Inicie o PuTTYgen (por exemplo, no menu Start (Iniciar), selecione All Programs (Todos os programas) > PuTTY > PuTTYgen).
2. Em Tipo de chave a ser gerada, escolha RSA.



Se você estiver usando uma versão mais antiga do PuTTYgen, escolha SSH-2 RSA.

3. Escolha Load (Carregar). Por padrão, o PuTTYgen exibe somente arquivos com a extensão .ppk. Para localizar o arquivo .pem, selecione 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 Abrir. Escolha OK para descartar a caixa de diálogo de confirmação.
5. Escolha Save private key para salvar a chave no formato que PuTTY pode usar. PuTTYgen exibe um aviso sobre salvar a chave sem uma senha. Escolha Sim.

Note

A frase secreta de uma chave privada é uma camada extra de proteção; por isso, mesmo se sua chave privada for descoberta, ela não poderá 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). 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.

Início de uma sessão do PuTTY

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. Se você receber um erro ao tentar se conectar à sua instância, consulte [Solução de problemas ao conectar-se à sua instância](#).

Para iniciar uma sessão do PuTTY

1. (Opcional) Você pode verificar a impressão digital da chave RSA na sua instância usando o comando `get-console-output` (AWS CLI) no seu sistema local (não na instância). Isso será útil se você tiver executado sua instância a partir de AMI pública de terceiros. Encontre a seção `SSH HOST KEY FINGERPRINTS`, observe a impressão digital RSA (por exemplo, `1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f`) e compare-a à impressão digital da instância.

```
aws ec2 get-console-output --instance-id instance_id
```

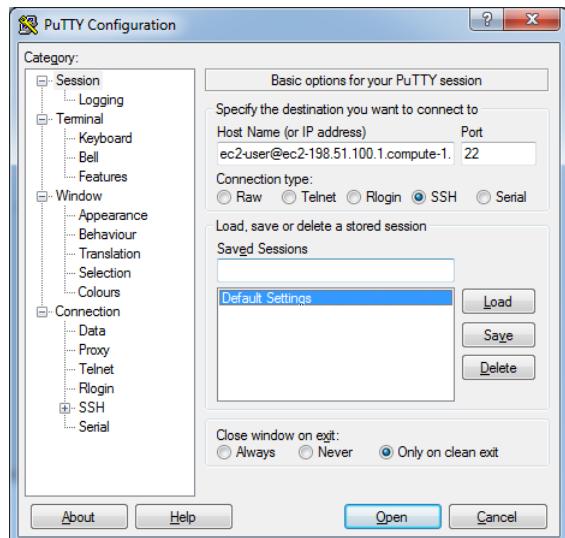
Veja um exemplo do que você deve procurar:

```
-----BEGIN SSH HOST KEY FINGERPRINTS-----  
... 1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f ...  
-----END SSH HOST KEY FINGERPRINTS-----
```

A seção `SSH HOST KEY FINGERPRINTS` só estará disponível após a primeira inicialização da instância.

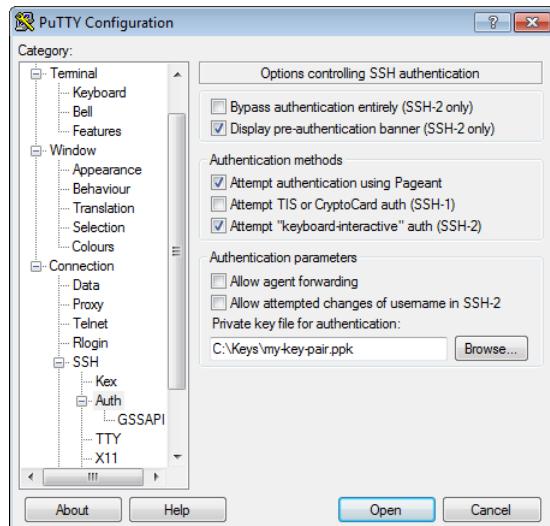
2. Inicie o PuTTY (no menu Iniciar, selecione Todos os programas > PuTTY > PuTTY).
3. No painel Categoria, selecione Sessão e preencha os seguintes campos:

- a. Na caixa Nome do host, entre em *user_name@public_dns_name*. Especifique o nome de usuário apropriado para sua AMI. Por exemplo:
 - Para a AMI do Amazon Linux 2 ou do Amazon Linux, o nome de usuário é `ec2-user`.
 - Para um AMI do CentOS, o nome de usuário é `centos`.
 - Em uma AMI do Debian, o nome de usuário é `admin` ou `root`.
 - Para a AMI do Fedora, o nome de usuário é `ec2-user` ou `fedora`.
 - Para a AMI do RHEL, o nome de usuário é `ec2-user` ou `root`.
 - Para a AMI do SUSE, o nome de usuário é `ec2-user` ou `root`.
 - Para uma AMI do Ubuntu, o nome de usuário é `ubuntu`.
 - Caso contrário, se `ec2-user` e `root` não funcionarem, verifique com o provedor de AMI.
- b. (Somente IPv6) Para se conectar usando o endereço IPv6 da sua instância, digite *user_name@ipv6_address*. Especifique o nome de usuário apropriado para sua AMI. Por exemplo:
 - Para a AMI do Amazon Linux 2 ou do Amazon Linux, o nome de usuário é `ec2-user`.
 - Para um AMI do CentOS, o nome de usuário é `centos`.
 - Em uma AMI do Debian, o nome de usuário é `admin` ou `root`.
 - Para a AMI do Fedora, o nome de usuário é `ec2-user` ou `fedora`.
 - Para a AMI do RHEL, o nome de usuário é `ec2-user` ou `root`.
 - Para a AMI do SUSE, o nome de usuário é `ec2-user` ou `root`.
 - Para uma AMI do Ubuntu, o nome de usuário é `ubuntu`.
 - Caso contrário, se `ec2-user` e `root` não funcionarem, verifique com o provedor de AMI.
- c. Em Tipo de conexão, selecione SSH.
- d. Certifique-se de que a Porta é 22.



4. (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.
5. 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 Abrir.
- c. (Opcional) Se você planeja iniciar esta sessão novamente depois, pode salvar as informações para uso futuro. Selecione Sessão na árvore Categoria, digite um nome para a sessão em Sessões salvas e selecione Salvar.
- d. Escolha Abrir para começar a sessão do PuTTY.



6. 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.
7. (Opcional) Verifique se a impressão digital na caixa de diálogo do alerta de segurança corresponde à impressão digital que você obteve previamente na etapa 1. Caso essas impressões digitais não correspondam, alguém pode estar tentando um ataque "man-in-the-middle". Se corresponderem, continue para a próxima etapa.
8. 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 sua instância, consulte [Solução de problemas ao conectar-se à sua instância](#).

Transferência de arquivos da sua instância do Linux usando 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 [Transferência de arquivos para sua instância do Linux usando WinSCP \(p. 449\)](#).

Para usar o PSCP, você precisar da chave privada gerada em [Conversão da sua chave privada usando PuTTYgen \(p. 445\)](#). Você também precisa do endereço DNS público da sua instância do Linux.

O exemplo a seguir transfere o arquivo `Sample_file.txt` da unidade C:\ em um computador Windows para o diretório inicial `ec2-user` em uma instância do Amazon Linux:

```
pscp -i C:\\path\\my-key-pair.ppk C:\\path\\Sample_file.txt ec2-user@public_dns:/home/ec2-user/Sample_file.txt
```

(Somente IPv6) O exemplo a seguir transfere o arquivo `Sample_file.txt` usando o endereço IPv6 da instância. O endereço IPv6 deve estar entre colchetes ([]).

```
pscp -i C:\\path\\my-key-pair.ppk C:\\path\\Sample_file.txt ec2-user@[ipv6-address]:/home/ec2-user/Sample_file.txt
```

Transferência de arquivos para 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 da sua máquina Windows para sua instância do Linux ou sincronize estruturas inteiras de diretório entre os dois sistemas.

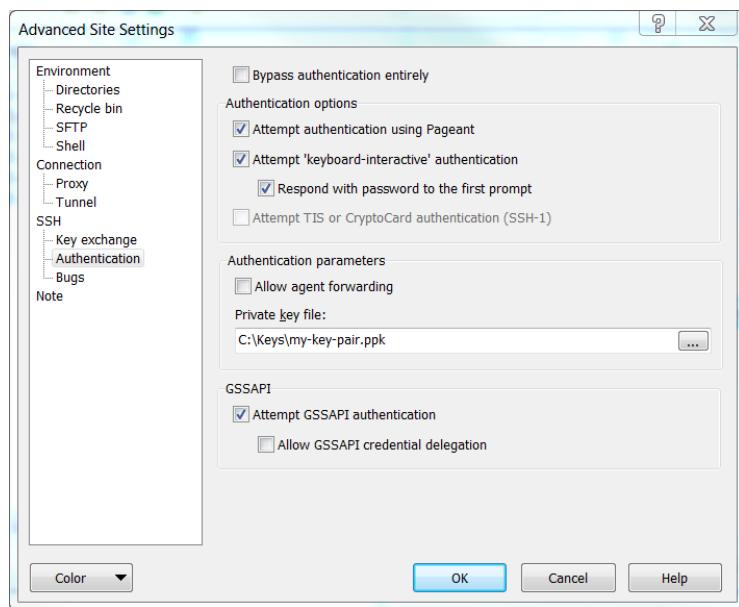
Para usar o WinSCP, você precisa da chave privada gerada em [Conversão da sua chave privada usando PuTTYgen \(p. 445\)](#). Você também precisa do endereço DNS público da sua instância do Linux.

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, para Nome do host, digite o hostname DNS público ou o endereço IPv4 público para sua instância.

(Somente IPv6) Para fazer login usando o endereço IPv6 da instância, digite o endereço IPv6 da sua instância.

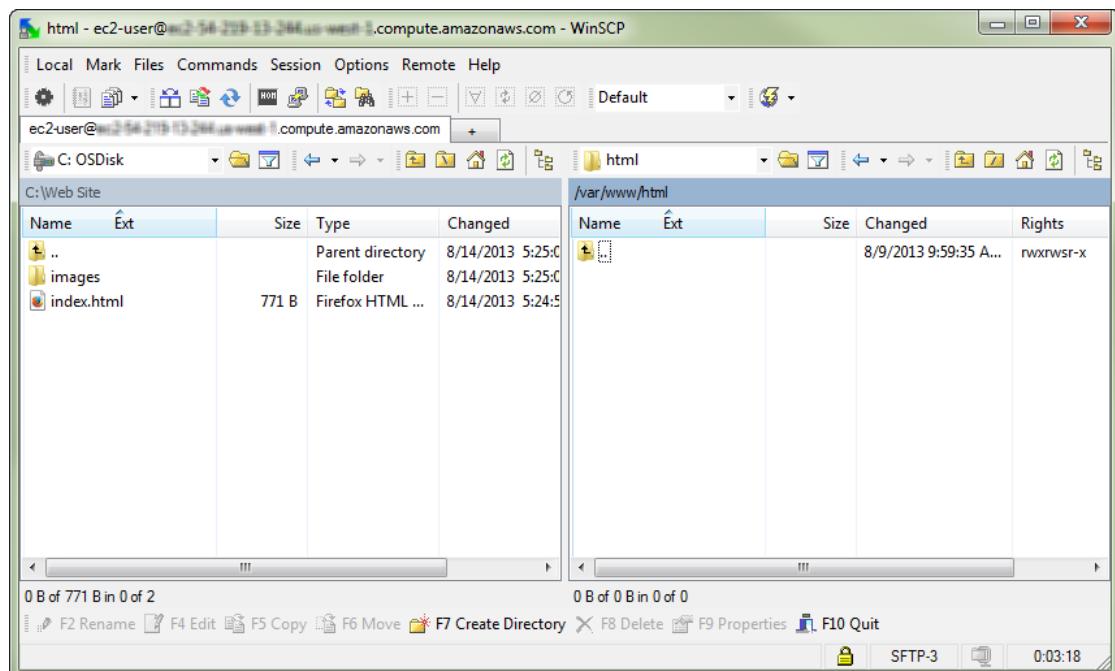
4. Para Nome de usuário, insira o nome de usuário padrão para sua AMI.
 - Para a AMI do Amazon Linux 2 ou do Amazon Linux, o nome de usuário é `ec2-user`.
 - Para um AMI do CentOS, o nome de usuário é `centos`.
 - Em uma AMI do Debian, o nome de usuário é `admin` ou `root`.
 - Para a AMI do Fedora, o nome de usuário é `ec2-user` ou `fedora`.
 - Para a AMI do RHEL, o nome de usuário é `ec2-user` ou `root`.
 - Para a AMI do SUSE, o nome de usuário é `ec2-user` ou `root`.
 - Para uma AMI do Ubuntu, o nome de usuário é `ubuntu`.
 - Caso contrário, se `ec2-user` e `root` não funcionarem, verifique com o provedor de 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 versões mais recentes do WinSCP, escolha Advanced para abrir as configurações avançadas do site e, em SSH, escolha Authentication para localizar a configuração Private key file.

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 [Conversão da sua chave privada usando PuTTYgen \(p. 445\)](#).

6. (Opcional) No painel esquerdo, escolha Diretórios e, em seguida, em Diretório remoto, digite o caminho para o diretório no qual você deseja acrescentar arquivos. Para versões mais recentes do WinSCP, escolha Advanced para abrir as configurações avançadas do site e, em Environment, escolha Directories para localizar a configuração Remote directory.
7. Escolha Login para se conectar e escolha Sim para adicionar a impressão digital do host ao cache do host.



8. Após a conexão ser estabelecida, na janela de conexão, sua instância do Linux está à direita e sua máquina local está à esquerda. Você pode arrastar e soltar arquivos diretamente no sistema

de arquivos remoto da sua máquina local. Para obter mais informações sobre WinSCP, consulte a documentação do projeto em <http://winscp.net/eng/docs/start>.

Se você receber o erro "Não é possível executar SCP para iniciar a transferência", primeiro deve instalar o 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
```

Como se conectar à instância Linux no Windows usando o Subsistema do Windows para Linux

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, na área de trabalho 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](#).

Depois que iniciar sua instância, você poderá conectá-la e usá-la da forma como usaria um computador bem na sua frente.

Note

Depois de iniciar uma instância, pode demorar alguns minutos para ela ficar pronta e que você possa se conectar a ela. Verifique se sua instância foi aprovada nas verificações de status. É possível ver essas informações na coluna Verificações de status da página Instâncias.

Se você receber um erro ao tentar se conectar à sua instância, consulte [Solução de problemas ao conectar-se à sua instância](#).

Tópicos

- [Pré-requisitos \(p. 439\)](#)
- [Como se conectar a uma instância do Linux usando o Subsistema do Windows para Linux \(p. 453\)](#)
- [Transferência de arquivos para instâncias do Linux usando SCP \(p. 454\)](#)
- [Desinstalação do Subsistema Windows para Linux \(p. 456\)](#)

Note

Ao instalar o WSL, todos os pré-requisitos e etapas são iguais aos descritos em [Conexão à sua instância do Linux utilizando SSH \(p. 439\)](#), e a experiência é exatamente igual a usar um Linux nativo.

Pré-requisitos

Antes de você se conectar à sua instância do Linux, preencha os seguintes pré-requisitos:

- Instalação do Subsistema Windows para Linux (WSL) e de uma distribuição do Linux

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.

- Instale as ferramentas de AWS CLI

(Opcional) Se você estiver usando AMI pública de terceiros, pode usar as ferramentas de linha de comando (CLI) para verificar a impressão digital. Para obter mais informações sobre como instalar a AWS CLI, consulte [Obter configurações](#) no Guia do usuário do AWS Command Line Interface.

- Obtenha a ID da instância

Você pode obter a ID de sua instância usando o console do Amazon EC2 (pela coluna ID da instância). Se preferir, pode usar [describe-instances](#) (AWS CLI) ou o comando [Get-EC2Instance](#) (AWS Tools para Windows PowerShell).

- Obtenha o nome do DNS público da instância

Você pode obter o DNS público para sua instância usando o console do Amazon EC2. Verifique a coluna Public DNS (IPv4) (DNS público – IPv4). Se essa coluna estiver oculta, selecione o ícone Show/Hide e selecione Public DNS (IPv4) (DNS público – IPv4). Se preferir, pode usar [describe-instances](#) (AWS CLI) ou o comando [Get-EC2Instance](#) (AWS Tools para Windows PowerShell).

- (Somente IPv6) Obtenha o endereço IPv6 da instância

Se você tiver atribuído um endereço IPv6 à sua instância, é possível também conectar-se à instância usando o endereço IPv6 em vez de um endereço IPv4 público ou um hostname DNS IPv4 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. Marque o campo IPv6 IPs (IPs IPv6). Se preferir, pode usar [describe-instances](#) (AWS CLI) ou o comando [Get-EC2Instance](#) (AWS Tools para Windows PowerShell). Para obter mais informações sobre IPv6, consulte [Endereços IPv6 \(p. 725\)](#).

- 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?](#).

```
cp /mnt/<Windows drive letter>/path/my-key-pair.pem ~/WSL-path/my-key-pair.pem
```

- Obtenha o nome de usuário padrão da AMI usada para executar a instância
 - Para a AMI do Amazon Linux 2 ou do Amazon Linux, o nome de usuário é `ec2-user`.
 - Para um AMI do CentOS, o nome de usuário é `centos`.
 - Em uma AMI do Debian, o nome de usuário é `admin` ou `root`.
 - Para a AMI do Fedora, o nome de usuário é `ec2-user` ou `fedora`.
 - Para a AMI do RHEL, o nome de usuário é `ec2-user` ou `root`.
 - Para a AMI do SUSE, o nome de usuário é `ec2-user` ou `root`.
 - Para uma AMI do Ubuntu, o nome de usuário é `ubuntu`.
 - Caso contrário, se `ec2-user` e `root` não funcionarem, verifique com o provedor de AMI.
- Permitir tráfego SSH de entrada do endereço IP à instância

Certifique-se de que o grupo de segurança associado à sua instância permita tráfego SSH de entrada do seu 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 permite o tráfego SSH por padrão. Para obter mais informações, consulte [Como autorizar tráfego de entrada em suas instâncias Linux \(p. 720\)](#).

Como se conectar a uma instância do Linux usando o Subsistema do Windows para Linux

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 sua instância, consulte [Solução de problemas ao conectar-se à sua instância](#).

Para se conectar à sua instância usando SSH

1. (Opcional) Você pode verificar a impressão digital da chave RSA na sua instância em execução usando um dos comandos a seguir no sistema local (não na instância). Isso será útil se você tiver executado sua instância a partir de AMI pública de terceiros. Encontre a seção `SSH HOST KEY FINGERPRINTS`, observe a impressão digital RSA (por exemplo, `1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f`) e compare-a à impressão digital da instância.
 - [get-console-output \(AWS CLI\)](#)

```
aws ec2 get-console-output --instance-id instance_id
```

Certifique-se de que a instância está no estado `running`, não no estado `pending`. A seção `SSH HOST KEY FINGERPRINTS` só estará disponível após a primeira inicialização da instância.

2. Em um shell da linha de comando, troque os diretórios para o local do arquivo de chave privada que você criou quando executou a instância.
3. Use o comando `chmod` para assegurar-se que o arquivo de chave privada não está visível publicamente. Por exemplo, se o nome do arquivo de chave privada for `my-key-pair.pem`, use o seguinte comando:

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

4. Use o comando `ssh` para se conectar à instância. Você especifica o arquivo de chave privada (`.pem`) e `user_name@public_dns_name`. Por exemplo, se você usou o Amazon Linux 2 ou Amazon Linux AMI, o nome de usuário é `ec2-user`.

```
sudo ssh -i /path/my-key-pair.pem ec2-user@ec2-198-51-100-1.compute-1.amazonaws.com
```

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)?
```

5. (Somente IPv6) Alternativamente, você pode 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. Por exemplo, se você usou o Amazon Linux 2 ou Amazon Linux AMI, o nome de usuário é `ec2-user`.

```
sudo ssh -i /path/my-key-pair.pem ec2-user@2001:db8:1234:1a00:9691:9503:25ad:1761
```

6. (Opcional) Verifique se a impressão digital no alerta de segurança corresponde à impressão digital que você obteve na etapa 1. Caso essas impressões digitais não correspondam, alguém pode estar tentando um ataque "man-in-the-middle". Se corresponderem, continue para a próxima etapa.
7. 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.
```

Transferência de 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.

Pré-requisitos

- 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 <http://www.openssh.org>.

- Obtenha a ID da instância

Você pode obter a ID de sua instância usando o console do Amazon EC2 (pela coluna ID da instância). Se preferir, pode usar [describe-instances](#) (AWS CLI) ou o comando [Get-EC2Instance](#) (AWS Tools para Windows PowerShell).

- Obtenha o nome do DNS público da instância

Você pode obter o DNS público para sua instância usando o console do Amazon EC2. Verifique a coluna Public DNS (IPv4) (DNS público – IPv4). Se essa coluna estiver oculta, selecione o ícone Show/Hide e selecione Public DNS (IPv4) (DNS público – IPv4). Se preferir, pode usar [describe-instances](#) (AWS CLI) ou o comando [Get-EC2Instance](#) (AWS Tools para Windows PowerShell).

- (Somente IPv6) Obtenha o endereço IPv6 da instância

Se você tiver atribuído um endereço IPv6 à sua instância, é possível também conectar-se à instância usando o endereço IPv6 em vez de um endereço IPv4 público ou um hostname DNS IPv4 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. Marque o campo IPv6 IPs (IPs IPv6). Se preferir, pode usar [describe-instances](#) (AWS CLI) ou o comando [Get-EC2Instance](#) (AWS Tools para Windows PowerShell). Para obter mais informações sobre IPv6, consulte [Endereços IPv6 \(p. 725\)](#).

- Encontrar a chave privada e verificar as permissões

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. Verifique se o arquivo `.pem` tem permissões de 0400, não 0777. Para obter mais informações, consulte [Erro: Arquivo de chave privada desprotegido \(p. 1033\)](#).

- Obtenha o nome de usuário padrão da AMI usada para executar a instância
 - Para a AMI do Amazon Linux 2 ou do Amazon Linux, o nome de usuário é `ec2-user`.
 - Para um AMI do CentOS, o nome de usuário é `centos`.
 - Em uma AMI do Debian, o nome de usuário é `admin` ou `root`.
 - Para a AMI do Fedora, o nome de usuário é `ec2-user` ou `fedora`.
 - Para a AMI do RHEL, o nome de usuário é `ec2-user` ou `root`.
 - Para a AMI do SUSE, o nome de usuário é `ec2-user` ou `root`.
 - Para uma AMI do Ubuntu, o nome de usuário é `ubuntu`.
 - Caso contrário, se `ec2-user` e `root` não funcionarem, verifique com o provedor de AMI.

- Permitir tráfego SSH de entrada do endereço IP à instância

Certifique-se de que o grupo de segurança associado à sua instância permita tráfego SSH de entrada do seu 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 permite o tráfego SSH por padrão. Para obter mais informações, consulte [Como autorizar tráfego de entrada em suas instâncias Linux \(p. 720\)](#).

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. (Opcional) Você pode verificar a impressão digital da chave RSA na sua instância usando um dos comandos a seguir no sistema local (não na instância). Isso será útil se você tiver executado sua instância a partir de AMI pública de terceiros. Encontre a seção **SSH HOST KEY FINGERPRINTS**, observe a impressão digital RSA (por exemplo, 1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f) e compare-a à impressão digital da instância.
 - [get-console-output \(AWS CLI\)](#)

```
aws ec2 get-console-output --instance-id instance_id
```

A seção **SSH HOST KEY FINGERPRINTS** só estará disponível após a primeira inicialização da instância.

2. Em um shell de comando, troque os diretórios para o local do arquivo de chave privada que você especificou quando executou a instância.
3. Use o comando chmod para assegurar-se que o arquivo de chave privada não está visível publicamente. Por exemplo, se o nome do arquivo de chave privada for `my-key-pair.pem`, use o seguinte comando:

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

4. 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 `ec2-user` e o nome DNS público da instância for `ec2-198-51-100-1.compute-1.amazonaws.com`, use o comando a seguir para copiar o arquivo para o diretório inicial `ec2-user`:

```
scp -i /path/my-key-pair.pem /path/SampleFile.txt ec2-
user@ec2-198-51-100-1.compute-1.amazonaws.com:~
```

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)?
```

5. (Somente IPv6) Como alternativa, é possível transferir um arquivo usando o endereço IPv6 para a instância. O endereço IPv6 deve vir entre colchetes ([]), que devem ser recuados (\).

```
scp -i /path/my-key-pair.pem /path/SampleFile.txt ec2-user@  
\[2001:db8:1234:1a00:9691:9503:25ad:1761\]:~
```

6. (Opcional) Verifique se a impressão digital no alerta de segurança corresponde à impressão digital que você obteve na etapa 1. Caso essas impressões digitais não correspondam, alguém pode estar tentando um ataque "man-in-the-middle". Se corresponderem, continue para a próxima etapa.
7. 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
```

8. 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 sua instância do EC2 de volta ao diretório inicial no seu computador local como `SampleFile2.txt`, use o comando a seguir no seu computador local:

```
scp -i /path/my-key-pair.pem ec2-user@ec2-198-51-100-1.compute-1.amazonaws.com:~/  
SampleFile.txt ~/SampleFile2.txt
```

9. (Somente IPv6) Alternativamente, você pode transferir arquivos na outra direção usando o endereço IPv6 da instância:

```
scp -i /path/my-key-pair.pem ec2-user@\[2001:db8:1234:1a00:9691:9503:25ad:1761\]:~/  
SampleFile.txt ~/SampleFile2.txt
```

Desinstalação do Subsistema Windows para Linux

Para obter informações sobre como desinstalar o Subsistema Windows para Linux, consulte [Como desinstalar o WSL Distribution?](#).

Conexão à sua instância do Linux usando o MindTerm

As instruções a seguir explicam como conectar-se à sua instância usando o MindTerm com o console do Amazon EC2. Se você receber um erro ao tentar se conectar à sua instância, consulte [Solução de problemas ao conectar-se à sua instância](#).

Depois que iniciar sua instância, você poderá conectá-la e usá-la da forma como usaria um computador bem na sua frente.

Note

Depois de iniciar uma instância, pode demorar alguns minutos para ela ficar pronta e que você possa se conectar a ela. Verifique se sua instância foi aprovada nas verificações de status. É possível ver essas informações na coluna Verificações de status da página Instâncias.

Pré-requisitos

- Verifique se seu navegador oferece suporte ao plug-in NPAPI

Se seu navegador não oferecer suporte ao plug-in NPAPI, ele não poderá executar o cliente MindTerm.

Important

O navegador Chrome não oferece suporte ao plug-in NPAPI. Para obter mais informações, consulte o [artigo de desaprovação de NPAPI no Chromium](#). O navegador FireFox não oferece suporte ao plug-in NPAPI. Para obter mais informações, consulte o [artigo de desaprovação de NPAPI no Java](#). O navegador Safari não oferece suporte ao plug-in NPAPI. Para obter mais informações, consulte o [artigo de desaprovação de NPAPI no Safari](#). Para obter informações sobre a desaprovação de NPAPI, consulte o artigo do [Wikipédia sobre NPAPI](#).

- Instalar Java

Seu computador Linux muito provavelmente inclui Java. Caso contrário, consulte [Como habilitar o Java no meu navegador?](#). Em um cliente Windows ou macOS, execute o navegador usando credenciais de administrador. Para Linux, podem ser necessárias etapas adicionais se você não fizer login como `root`.

- Habilite Java em seu navegador da

Para instruções, consulte https://java.com/en/download/help/enable_browser.xml.

- Encontrar a chave privada e verificar as permissões

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. Verifique se o arquivo `.pem` tem permissões de 0400, não 0777. Para obter mais informações, consulte [Erro: Arquivo de chave privada desprotegido \(p. 1033\)](#).

- Obtenha o nome de usuário padrão da AMI usada para executar a instância
 - Para a AMI do Amazon Linux 2 ou do Amazon Linux, o nome de usuário é `ec2-user`.
 - Para um AMI do CentOS, o nome de usuário é `centos`.
 - Em uma AMI do Debian, o nome de usuário é `admin` ou `root`.
 - Para a AMI do Fedora, o nome de usuário é `ec2-user` ou `fedora`.
 - Para a AMI do RHEL, o nome de usuário é `ec2-user` ou `root`.
 - Para a AMI do SUSE, o nome de usuário é `ec2-user` ou `root`.
 - Para uma AMI do Ubuntu, o nome de usuário é `ubuntu`.
 - Caso contrário, se `ec2-user` e `root` não funcionarem, verifique com o provedor de AMI.
- Permitir tráfego SSH de entrada do endereço IP à instância

Certifique-se de que o grupo de segurança associado à sua instância permita tráfego SSH de entrada do seu 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 permite o tráfego SSH por padrão. Para obter mais informações, consulte [Como autorizar tráfego de entrada em suas instâncias Linux \(p. 720\)](#).

Início do MindTerm

Para se conectar à sua instância usando um navegador com MindTerm.

1. No console do Amazon EC2, escolha Instâncias no painel de navegação.
2. Selecione a instância e escolha Conectar.
3. Selecione Um cliente Java SSH diretamente do meu navegador (Java obrigatório).

4. O Amazon EC2 detecta automaticamente o nome DNS público da sua instância e preenche o DNS público para você. Isso também detecta o nome do par de chaves que você especificou ao executar a instância. Preencha o seguinte e selecione Launch SSH Client.
 - a. Em User name, insira o nome do usuário para fazer login em sua instância.
 - Para a AMI do Amazon Linux 2 ou do Amazon Linux, o nome de usuário é `ec2-user`.
 - Para um AMI do CentOS, o nome de usuário é `centos`.
 - Em uma AMI do Debian, o nome de usuário é `admin` ou `root`.
 - Para a AMI do Fedora, o nome de usuário é `ec2-user` ou `fedora`.
 - Para a AMI do RHEL, o nome de usuário é `ec2-user` ou `root`.
 - Para a AMI do SUSE, o nome de usuário é `ec2-user` ou `root`.
 - Para uma AMI do Ubuntu, o nome de usuário é `ubuntu`.
 - Caso contrário, se `ec2-user` e `root` não funcionarem, verifique com o provedor de AMI.
 - b. Em Caminho da chave privada, insira o caminho totalmente qualificado para seu arquivo de chave privada (`.pem`), incluindo o nome do par de chaves; por exemplo:
`C:\KeyPairs\my-key-pair.pem`
- c. (Opcional) Selecione Armazenar no cache do navegador para armazenar o local da chave privada no cache do seu navegador. Isso permite que o Amazon EC2 detecte o local da chave privada nas sessões posteriores do navegador, até que você apague a memória cache do navegador.
5. Se necessário, selecione Sim para confiar no certificado e Executar para executar o cliente MindTerm.
6. Se essa for sua primeira vez executando o MindTerm, uma série de caixas de diálogo solicitarão que você aceite o acordo de licença, confirme a configuração do seu diretório inicial e confirme a configuração do diretório conhecido de hosts. Confirme essas configurações.
7. Um diálogo o alerta para adicionar o host ao seu conjunto de hosts conhecidos. Se você não quiser armazenar as informações da chave do host no computador local, selecione No.
8. Uma janela se abrirá e você estará conectado à sua instância.

Se você escolher Não na etapa anterior, verá a mensagem a seguir, que é esperada:

Verification of server key disabled in this session.

Interrompa e inicie sua instância

Você pode interromper e reiniciar sua instância se ela tiver um volume do Amazon EBS no dispositivo raiz. A instância retém o ID da instância, mas pode ser alterada conforme descrito na seção [Visão geral \(p. 459\)](#).

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. Sempre que você iniciar uma instância interrompida, nós cobraremos no mínimo 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.

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 [Encerre sua instância \(p. 470\)](#). Se você preferir hibernar a instância, consulte [Hibernar sua instância \(p. 461\)](#). Para obter mais informações, consulte [Diferenças entre reinicialização, parada, hibernação e encerramento \(p. 389\)](#).

Tópicos

- [Visão geral \(p. 459\)](#)
- [Interrupção e início das suas instâncias \(p. 460\)](#)
- [Modificação de uma instância interrompida \(p. 460\)](#)
- [Solução de problemas \(p. 461\)](#)

Visão geral

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 [Como determinar o tipo de dispositivo raiz da AMI \(p. 92\)](#).

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.
- A instância retém seus endereços IPv4 privados e todos os endereços IPv6 quando parada e reiniciada. Nós liberamos o endereço de público IPv4 e atribuímos um novo ao reiniciá-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 \(p. 804\)](#).
- 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 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 para 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 reiniciá-la. Para obter mais informações sobre ClassicLink, consulte [ClassicLink \(p. 812\)](#).

Para obter mais informações, consulte [Diferenças entre reinicialização, parada, hibernação e encerramento \(p. 389\)](#).

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`.

Interrupção e início das suas instâncias

Você pode iniciar e interromper sua instância com Amazon EBS usando o console ou a linha de comando.

Por padrão, ao iniciar a desativação de uma instância com Amazon EBS (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 [Alteração do comportamento de desligamento iniciado da instância \(p. 473\)](#).

Para parar e iniciar uma instância com Amazon EBS usando o console

1. No painel de navegação, selecione Instâncias e selecione a instância.
2. Escolha Ações, selecione Estado da instância e escolha Interromper. Se Parar estiver desabilitado, a instância já parou 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 de volumes do armazenamento de instâncias, certifique-se de fazer backup deles em um armazenamento persistente.

3. Na caixa de diálogo para confirmação, escolha Yes, parar. Pode demorar alguns minutos para que a instância pare.
4. Enquanto sua instância estiver interrompida, você poderá modificar determinados atributos de instância. Para obter mais informações, consulte [Modificação de uma instância interrompida \(p. 460\)](#).
5. Para reiniciar a instância interrompida, selecione a instância e escolha Actions, Instance State, Start.
6. 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 [Acessando o Amazon EC2 \(p. 3\)](#).

- `stop-instances` e `start-instances` (AWS CLI)
- `Stop-EC2Instance` e `Start-EC2Instance` (AWS Tools para Windows PowerShell)

Modificação de 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 Console de gerenciamento da AWS ou a interface da linha de comando. Você não pode usar o Console de gerenciamento da AWS 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 \(p. 247\)](#).

- Para alterar os dados do usuário para sua instância, consulte [Trabalhar com dados do usuário da instância \(p. 519\)](#).
- Para habilitar ou desabilitar a otimização do-EBS para sua instância, consulte [Modificação da otimização do-EBS \(p. 925\)](#).
- Para alterar o atributo `DeleteOnTermination` do volume do dispositivo raiz da sua instância, consulte [Atualização do mapeamento de dispositivos de blocos de uma instância em execução \(p. 987\)](#).

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 [Acessando o Amazon EC2 \(p. 3\)](#).

- `modify-instance-attribute` (AWS CLI)
- `Edit-EC2InstanceAttribute` (AWS Tools para Windows PowerShell)

Solução de problemas

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 da parada da sua instância \(p. 1035\)](#).

Hibernar sua instância

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 reinicia a instância, o volume raiz do Amazon EBS é restaurado para seu estado anterior, o conteúdo da RAM é recarregado, e os processos que estavam em execução na instância anteriormente 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 \(p. 464\)](#) e atender aos [pré-requisitos de hibernação \(p. 462\)](#). No momento, a hibernação só é compatível no Amazon Linux.

Se uma instância ou aplicativo levar muito tempo para inicializar e criar um espaço de memória para se tornar totalmente produtivo, você pode usar a hibernação para pré-aquecer a instância. Para "pré-aquecer" a instância, execute-a, coloque-a em um estado desejado e hiberne-a, pronta para ser retomada no mesmo estado conforme necessário.

Não cobramos pelo uso de uma instância em hibernação quando ela está no estado `stopped`. Cobramos pelo uso de instâncias quando elas estão no estado `stopping` (ao contrário de quando você [interrompe uma instância \(p. 458\)](#) sem hiberná-la) quando o conteúdo da RAM é transferido para o volume raiz do Amazon EBS. Não cobramos pelo uso de taxas de transferência de dados, mas cobramos pelo armazenamento de qualquer volume do Amazon EBS, incluindo armazenamento do conteúdo 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 [Encerre sua instância \(p. 470\)](#).

Important

A hibernação não é compatível atualmente em instâncias do Windows.

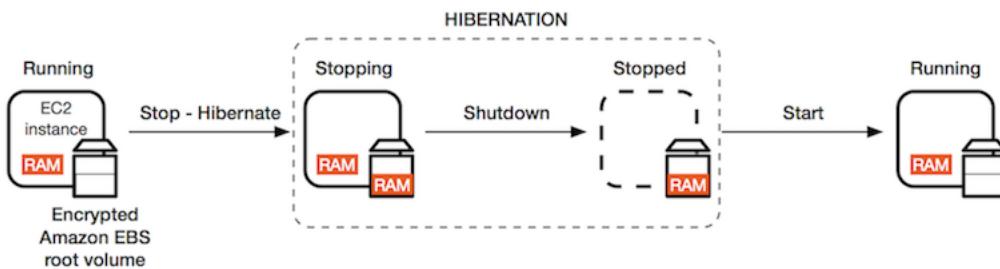
Tópicos

- [Visão geral da hibernação \(p. 462\)](#)
- [Pré-requisitos de hibernação \(p. 462\)](#)

- Limitações (p. 463)
- Configuração de uma AMI existente para oferecer suporte à hibernação (p. 464)
- Habilitar a hibernação para uma instância (p. 464)
- Hibernação de uma instância (p. 465)
- Reinício de uma instância em hibernação (p. 466)
- Solução de problemas de hibernação (p. 467)

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**. Sinalizamos ao sistema operacional para executar a hibernação (suspend-to-disk), o que congela todos os processos, salva o conteúdo da (RAM) no volume raiz do Amazon EBS e, em seguida, executa um desligamento normal.
- Quando o desligamento é concluído, a instância muda para o estado **stopped**.
- Todos os volumes do Amazon EBS permanecem associados à instância, e seus dados persistem, incluindo o conteúdo salvo da RAM.
- Na maioria dos casos, a instância é migrada para um novo host subjacente quando é reiniciada, o que é igual ao que acontece quando você interrompe e reinicia uma instância.
- Quando você reinicia a instância, a instância é reinicializada, e o sistema operacional lê o conteúdo da RAM no volume raiz do Amazon EBS antes de descongelar os processos para retomar seu estado.
- A instância retém seus endereços IPv4 privados e todos os endereços IPv6 quando é hibernada e reiniciada. Nós liberamos o endereço de público IPv4 e atribuímos um novo ao reiniciá-lo.
- 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 sua instância quando você o hiberna. Para obter mais informações, consulte [EC2-Classic \(p. 804\)](#).
- 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 reiniciá-la. Para obter mais informações, consulte [ClassicLink \(p. 812\)](#).

Para obter informações sobre como a hibernação difere da reinicialização, da interrupção e do encerramento, consulte [Diferenças entre reinicialização, parada, hibernação e encerramento \(p. 389\)](#).

Pré-requisitos de hibernação

Para hibernar uma instância, os seguintes pré-requisitos devem estar estabelecidos:

- Famílias de instâncias: as seguintes famílias instâncias são suportados: C3, C4, C5, M3, M4, M5, R3, R4 e R5, com menos de 150 GB de RAM. A hibernação não é compatível para instâncias *.metal.

- Tamanho de RAM da instância: o tamanho de RAM da instância deve ser menor que 150 GB.
- AMIs compatíveis: as seguintes AMIs oferecem suporte à hibernação: AMI do Amazon Linux 2018.03 liberado em 2018.11.16 ou posteriormente.

O suporte para o Amazon Linux 2 será disponibilizado em breve. Apenas AMIs HVM oferecem suporte à hibernação. Para configurar sua AMI para oferecer suporte à hibernação, consulte [Configuração de uma AMI existente para oferecer suporte à hibernação \(p. 464\)](#).

- Tipo de volume raiz: o volume raiz da instância deve ser um volume do Amazon EBS, não um volume de armazenamento da instância.
- Tamanho do volume raiz do Amazon EBS: o volume raiz deve ser grande o suficiente para armazenar o conteúdo da RAM e acomodar uso inesperado, por exemplo, sistema operacional ou aplicativos. Quando você habilita a hibernação, espaço é alocado no volume raiz na inicialização para armazenar a RAM.
- Criptografia do volume raiz do Amazon 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 Amazon EBS, eles sempre são criptografados. A criptografia do volume raiz é imposta na execução da instância. Para garantir que o volume raiz seja um volume do Amazon EBS criptografado, a AMI usada para executar a instância deve estar criptografada. Para obter mais informações, consulte [Como criar uma AMI com snapshot raiz criptografado de uma AMI não criptografada \(p. 148\)](#).
- Habilitar a hibernação na execução: na execução, habilita a hibernação usando o console do Amazon EC2 ou a AWS CLI. Não é possível habilitar a hibernação em uma instância existente (em execução ou parada). Para obter mais informações, consulte [Habilitar a hibernação para uma instância \(p. 464\)](#).
- Opções de compra: este recurso está disponível apenas para Instâncias on-demand e Instâncias reservadas. Para obter mais informações, consulte [Como colocar em hibernação Instâncias spot interrompidas \(p. 350\)](#).

Limitações

Não há suporte para as seguintes ações para hibernação:

- Alterar o tipo ou o tamanho de uma instância em hibernação
- Criar snapshots ou AMIs de instâncias para as quais a hibernação está habilitada
- Criar snapshots ou AMIs de instâncias em hibernação

Não é possível interromper ou hibernar instâncias com armazenamento de instâncias.*

Você não pode hibernar uma instância com mais de 150 GB de RAM.

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 Auto Scaling do Amazon EC2 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 de Auto Scaling](#) no Guia do usuário de Auto Scaling do Amazon EC2.

Não oferecemos suporte à manutenção de uma instância em hibernação por mais de 60 dias. Para manter a instância por mais que 60 dias, reinicie, interrompa e reinicialize 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 exigem uma reinicialização das instâncias em hibernação para que você possa executar um desligamento ou uma reinicialização para aplicar as atualizações e os patches de segurança necessários.

*Para instâncias C3 ou R3 que estão habilitadas para hibernação, não use volumes de armazenamento de instâncias.

Configuração de uma AMI existente para oferecer suporte à hibernação

Para hibernar uma instância que foi executada usando sua própria AMI, configure sua AMI para oferecer suporte à hibernação. Para obter mais informações, consulte [Atualização de software de instância \(p. 479\)](#).

Se você usar uma das [AMIs compatíveis \(p. 462\)](#) ou criar uma AMI com base em uma das [AMIs compatíveis \(p. 462\)](#), não será necessário configurá-la para oferecer suporte à hibernação. As AMIs compatíveis são fornecidas pré-configuradas para oferecer suporte à hibernação.

Para configurar uma AMI do Amazon Linux para oferecer suporte à hibernação (AWS CLI)

1. Atualize para o kernel mais recente, 4.14.77-70.59 ou posterior, usando o comando a seguir:

```
sudo yum update kernel
```

2. Instale o pacote ec2-hibinit-agent a partir dos repositórios usando o comando a seguir:

```
sudo yum install ec2-hibinit-agent
```

3. Reinicialize a instância.

4. Confirme se a versão do kernel está atualizada para a 4.14.77-70.59 ou superior usando o comando a seguir:

```
uname -a
```

5. Interrompa a instância e crie uma AMI. Para obter mais informações, consulte [Criação de uma AMI do Linux de uma instância \(p. 112\)](#).

Habilitar a hibernação para uma instância

Para hibernar uma instância, ela precisa primeiro ser habilitada para hibernação. Na inicialização, habilite a hibernação usando o console ou a linha de comando. Não é possível habilitar a hibernação para uma instância existente (em execução ou parada).

Para habilitar a hibernação (console)

1. Siga o procedimento do [Execução de uma instância usando o assistente de execução de instância \(p. 391\)](#).
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 \(p. 462\)](#).
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 \(p. 462\)](#).
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. 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 [Execução de uma instância usando o assistente de execução de instância \(p. 391\)](#).

Para habilitar a hibernação (AWS CLI)

- Use o comando `run-instances` para executar uma instância. Habilite a hibernação usando o parâmetro `--hibernation-options Configured=true`.

```
aws ec2 run-instances --image-id ami-abc12345 --count 1 --instance-type m5.large --key-name MyKeyPair --hibernation-options Configured=true
```

Para visualizar se uma instância está habilitada para hibernação (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.

Note

Não é possível habilitar ou desabilitar a hibernação após a execução.

Para visualizar se uma instância está habilitada para hibernação (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 --region us-east-1 ec2 describe-instances --filters "Name=hibernation-options.configured,Values=true"
```

O seguinte campo da saída indica que a instância está habilitada para hibernação:

```
"HibernationOptions": {  
    "Configured": true  
}
```

Hibernação de uma instância

É possível hibernar uma instância usando o console ou a linha de comando se ela estiver [habilitada para hibernação \(p. 464\)](#) e atender aos [pré-requisitos de hibernação \(p. 462\)](#). Se uma instância não puder hibernar com sucesso, ocorrerá um desligamento normal.

Para hibernar uma instância com suporte do Amazon EBS (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 \(p. 462\)](#).
4. Na caixa de diálogo de confirmação, escolha Yes, Stop - Hibernate (Sim, parar - hibernar). Pode demorar alguns minutos para que a instância hiberne. O Instance State (Estado da instância) é alterado para Stopping (Interromper), enquanto a instância está hibernando e Stopped (Interrompida) quando a instância está em hibernação.

Para hibernar uma instância com suporte do Amazon EBS (AWS CLI)

- Use o comando [stop-instances](#) e especifique o parâmetro `--hibernate`.

```
aws ec2 stop-instances --instance-ids i-1234567890abcdef0 --hibernate
```

Para visualizar se a hibernação foi iniciada em uma instância (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). Client.UserInitiatedHibernate: User initiated hibernate (Client.UserInitiatedHibernate: hibernação iniciada pelo usuário) indica que a hibernação foi iniciada na instância.

Para visualizar se a hibernação foi iniciada em uma instância (AWS CLI)

- Use o comando [describe-instances](#) e especifique o parâmetro `--filters "Name=state-reason-code,Values=Client.UserInitiatedHibernate"` para filtrar as instâncias nas quais a hibernação foi iniciada.

```
aws --region us-east-1 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  
}
```

Reinício de uma instância em hibernação

Reinic peace uma instância em hibernação iniciando-a da mesma maneira como inicia uma instância interrompida.

Para reiniciar uma instância em hibernação (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 \(p. 566\)](#) da instância mostram a instância em um estado de falha até que a instância seja reiniciada.

Para reiniciar um instância em hibernação (AWS CLI)

- Use o comando [start-instances](#).

Solução de 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 de `stopping` para o estado de `stopped`, e o estado da memória não é restaurado depois da execução, isso poderá 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 \(p. 439\)](#) 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 \(p. 462\)](#). Se tiver usado sua própria AMI, verifique se você seguiu as instruções de configuração para [Configuração de uma AMI existente para oferecer suporte à hibernação \(p. 464\)](#).

A instância está "presa" no estado `stopping`

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 da parada da sua instância \(p. 1035\)](#).

Reinicialize sua 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 permanece no mesmo host físico, para que sua instância mantenha seu nome DNS público (IPv4), o endereço IPv4 privado, endereço IPv6 (se aplicável) e quaisquer dados nos volumes de armazenamento de instância.

A reinicialização de uma instância não inicia uma nova de faturamento de instância (com uma cobrança mínima de um minuto), diferente do que acontece na interrupção e na reinicialização 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 suas instâncias \(p. 570\)](#).

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 até quatro minutos. Se você usar o AWS CloudTrail, usar o Amazon EC2 para reinicializar sua instância também criará um registro de API de quando a instância foi reinicializada.

Para reinicializar uma instância usando o console

1. Abra o console do Amazon 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.

Para reinicializar uma instância usando a linha de comando

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

- `reboot-instances` (AWS CLI)
- `Restart-EC2Instance` (AWS Tools para Windows PowerShell)

Inativação da instância

A instância está planejada ser inativada quando a AWS detectar uma falha irreparável do hardware subjacente que hospeda a instância. Quando uma instância atingir sua data de inativação programada, ela será 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 a migra 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.

Tópicos

- [Identificação de instâncias agendadas para desativação \(p. 468\)](#)
- [Como trabalhar com instâncias agendadas para desativação \(p. 469\)](#)

Para obter mais informações sobre os tipos de eventos de instância, consulte [Eventos programados para suas instâncias \(p. 570\)](#).

Identificação de instâncias agendadas para desativação

Se sua instância estiver programada para desativação, você receberá um e-mail antes do evento com o ID e a data de desativação da instância. Esse e-mail é enviado para o endereço que está associado à sua conta; o mesmo endereço de e-mail que você usa para fazer login no Console de gerenciamento da AWS. Se você usa uma conta de e-mail que não verifica regularmente, use o console do Amazon EC2 ou a linha de comando para determinar se alguma de suas instâncias estão agendadas para desativação. Para atualizar as informações de contato para sua conta, acesse a página [Configurações da conta](#).

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), você pode ver os eventos associados aos volumes e instâncias do Amazon EC2, organizados por região.

Scheduled Events



US East (N. Virginia):

1 instances have scheduled events

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 [Acessando o Amazon EC2 \(p. 3\)](#).

- [describe-instance-status](#) (AWS CLI)
- [Get-EC2InstanceState](#) (AWS Tools para Windows PowerShell)

Como trabalhar com instâncias agendadas para desativação

Há várias ações disponíveis para você quando sua instância está agendada para desativação. A ação que você realiza depende de se o dispositivo raiz da instância é um volume do Amazon EBS ou um volume de armazenamento de instâncias. Se você não souber qual é o tipo de dispositivo raiz da instância, você pode descobrir usando o console do Amazon EC2 ou a linha de comando.

Como determinar o tipo de dispositivo raiz de sua instância

Para determinar o tipo de dispositivo raiz de sua instância usando o console

1. No painel de navegação, selecione Events (Eventos). Use as listas de filtros para identificar as instâncias a serem desativadas, conforme demonstrado no procedimento acima, [Identificação de instâncias agendadas para desativação \(p. 468\)](#).
2. Na coluna Resource Id (ID do recurso), selecione o ID da instância para acessar a página Instances (Instâncias).
3. Selecione a instância e localize o campo Root device type (Tipo de dispositivo raiz) na guia Description (Descrição). Se o valor for ebs, sua instância é baseada em EBS. Se o valor for instance-store, sua instância é com armazenamento de instâncias.

Para determinar o tipo de dispositivo raiz de sua 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 [Acessando o Amazon EC2 \(p. 3\)](#).

- [describe-instances](#) (AWS CLI)
- [Get-EC2Instance](#)

Gerenciamento de instâncias agendadas para desativação

Você pode executar uma das ações listadas abaixo para preservar os dados em sua instância a ser desativada. 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 com 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 eles estejam anexados a uma instância baseada no EBS.

Tipo de dispositivo raiz da instância	Ação
EBS	Crie uma AMI baseada em EBS em sua instância para que você tenha um backup. Espere a data de desativação agendada – quando a instância é interrompida – ou interrompa a instância por conta própria antes da data de desativação. Você pode iniciar a instância novamente a qualquer momento. Para obter mais informações sobre como interromper e iniciar sua instância e o que esperar quando sua instância é interrompida, como o efeito em endereços IP elásticos, públicos e privados associados à instância, consulte Interrompa e inicie sua instância (p. 458) .
EBS	Crie uma AMI baseada no EBS de sua instância e execute uma instância de substituição. Para obter mais informações, consulte Criação de uma AMI do Linux com Amazon EBS (p. 111) .
Armazenamento de instâncias	Crie uma AMI com armazenamento de instâncias de sua instância usando as ferramentas da AMI e execute uma instância de substituição. Para obter mais informações, consulte Criação de uma AMI em Linux com armazenamento de instâncias (p. 115) .
Armazenamento de instâncias	Converta sua instância em uma instância baseada no EBS transferindo seus dados para um volume do EBS, tirando um snapshot do volume e, em seguida, criando uma AMI do snapshot. Você pode executar uma instância de substituição a partir da nova AMI. Para obter mais informações, consulte Conversão de uma AMI com armazenamento de instâncias em uma AMI com Amazon EBS (p. 127) .

Encerre sua 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.

Você não pode se conectar com uma instância ou reiniciá-la depois de tê-la encerrado. No entanto, você pode iniciar instâncias adicionais usando a mesma AMI. Se você preferir interromper e reiniciar a instância ou hiberná-la, consulte [Interrompa e inicie sua instância \(p. 458\)](#) ou [Hibernar sua instância \(p. 461\)](#). Para obter mais informações, consulte [Diferenças entre reinicialização, parada, hibernação e encerramento \(p. 389\)](#).

Tópicos

- [Encerramento da instância \(p. 471\)](#)

- [Como encerrar uma instância \(p. 472\)](#)
- [Habilitação da proteção contra o encerramento de uma instância \(p. 472\)](#)
- [Alteração do comportamento de desligamento iniciado da instância \(p. 473\)](#)
- [Preservação de volumes do Amazon EBS no encerramento da instância \(p. 474\)](#)
- [Solução de problemas \(p. 476\)](#)

Encerramento da 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 encerrada, recursos como tags e volumes são gradualmente dissociados da instância, portanto podem não ficar visíveis na instância encerrada 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 [Preservação de volumes do Amazon EBS no encerramento da instância \(p. 474\)](#).

Você pode impedir que uma instância seja encerrada acidentalmente por alguém usando o Console de gerenciamento da AWS, 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 [Habilitação da proteção contra o encerramento de uma instância \(p. 472\)](#).

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 [Alteração do comportamento de desligamento iniciado da instância \(p. 473\)](#).

Se você executar um script no encerramento da instância, sua instância 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 os scripts de desativação do sistema. No entanto, determinados eventos (como falha de hardware) podem impedir que esses scripts de desativação do sistema sejam executados.

O que acontece quando você encerra uma instância (API)

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. Isso é válido tanto para a interrupção quanto para o encerramento. 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 Console de gerenciamento da AWS ou a linha de comando.

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 de instâncias para 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 [Acessando o Amazon EC2 \(p. 3\)](#).

- [terminate-instances](#) (AWS CLI)
- [Stop-EC2Instance](#) (AWS Tools para Windows PowerShell)

Habilitação da proteção contra o encerramento de uma instância

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 encerrada accidentalmente usando o Amazon EC2, pode habilitar a proteção contra encerramento para a instância. O atributo `DisableApiTermination` define se a instância pode ser encerrada usando o console, a CLI ou a API. Por padrão, a proteção contra encerramento está desabilitada para sua instância. Você pode definir o valor desse atributo ao executar a instância, enquanto a instância estiver em execução ou quando a instância for interrompida (para instâncias baseadas no Amazon EBS).

O atributo `DisableApiTermination` não impede que você encerre uma instância iniciando o desligamento da instância (usando um comando do sistema operacional para o desligamento do sistema) quando o atributo `InstanceStateInitiatedShutdownBehavior` é definido. Para obter mais informações, consulte [Alteração do comportamento de desligamento iniciado da instância \(p. 473\)](#).

Limites

Você não pode habilitar a proteção contra encerramento de instâncias spot — uma instância spot é encerrada quando o preço spot excede sua sugestão de preço. No entanto, você pode preparar seu aplicativo para lidar com interrupções de instância spot. Para obter mais informações, consulte [Interrupções de Instância spots \(p. 348\)](#).

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, em seguida, selecione Change Termination Protection (Alterar proteção contra encerramento).
2. Selecione 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, em seguida, selecione Change Termination Protection (Alterar proteção contra encerramento).
2. Selecione 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 [Acessando o Amazon EC2 \(p. 3\)](#).

- [modify-instance-attribute](#) (AWS CLI)
- [Edit-EC2InstanceAttribute](#) (AWS Tools para Windows PowerShell)

Alteração do comportamento de desligamento iniciado da instância

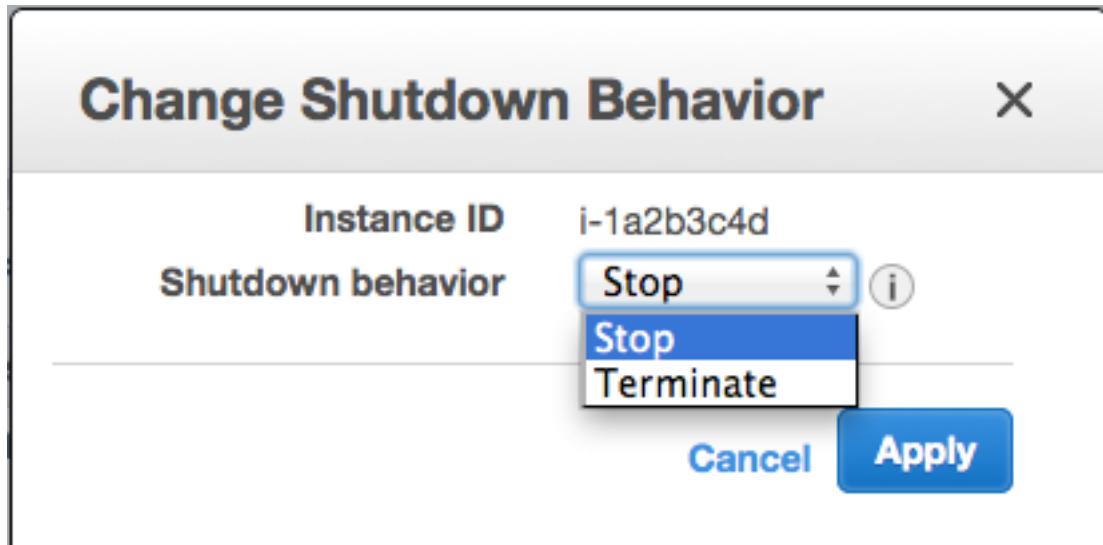
Por padrão, quando você inicia um desligamento em uma instância baseada no Amazon EBS (usando um comando como shutdown ou poweroff), a instância é interrompida (observe que halt não emite um comando poweroff e, se usado, a instância não será encerrada. Em vez disso, ela colocará a CPU em HLT e a instância 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, selecione Actions (Ações), Instance Settings (Configurações da instância) e, em seguida, selecione Change Shutdown Behavior (Alterar comportamento do desativação). O comportamento atual já está selecionado.
4. Para alterar o comportamento, selecione uma opção na lista Shutdown behavior (Comportamento de desativação) e, em seguida, selecione 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 [Acessando o Amazon EC2 \(p. 3\)](#).

- [modify-instance-attribute](#) (AWS CLI)
- [Edit-EC2InstanceAttribute](#) (AWS Tools para Windows PowerShell)

Preservação de 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.

Por padrão, o atributo `DeletionOnTermination` para o volume raiz de uma instância é definido como `true`. Portanto, o padrão é excluir o volume raiz de uma instância quando a instância é encerrada.

Por padrão, ao anexar um volume do EBS a uma instância, 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.

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 [Visualização dos volumes do EBS em um mapeamento de dispositivo de blocos da instância \(p. 987\)](#).

Você pode alterar o valor do atributo `DeleteOnTermination` de um volume quando executar a instância ou enquanto a instância estiver sendo executada.

Exemplos

- [Alteração do volume raiz a ser mantido na execução usando o console \(p. 475\)](#)

- [Alteração do volume raiz a ser mantido na execução usando a linha de comando \(p. 475\)](#)
- [Alteração do volume raiz de uma instância em execução a ser mantido usando a linha de comando \(p. 476\)](#)

Alteração do 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).

Você pode verificar a configuração exibindo detalhes do volume do dispositivo raiz no painel de detalhes da instância. Ao lado de Block devices (Dispositivos de blocos), clique na entrada do volume do dispositivo raiz. Por padrão, Delete on termination é `True`. Se você alterar o comportamento padrão, Delete on termination será `False`.

Alteração do 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 [Acessando o Amazon EC2 \(p. 3\)](#).

- [run-instances](#) (AWS CLI)
- [New-EC2Instance](#)

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"  
    }  
  }  
]
```

Alteração do 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 [Acessando o Amazon EC2 \(p. 3\)](#).

- [modify-instance-attribute](#) (AWS CLI)
- [Edit-EC2InstanceAttribute](#) (AWS Tools para 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  
    }  
  }  
]
```

Solução de problemas

Se sua instância permanecer no estado `shutting-down` por mais tempo do que o normal, ela será por fim removida (encerrada) por processos automatizados no serviço do Amazon EC2. Para obter mais informações, consulte [Solução de problemas de encerramento \(desativação\) da sua instância \(p. 1037\)](#).

Recuperar sua 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 danificada estiver em um placement group, a instância recuperada será executada no placement group. Para obter mais informações sobre como usar alarmes do Amazon CloudWatch para recuperar uma instância, consulte [Crie alarmes para parar, encerrar, reiniciar ou recuperar uma instância \(p. 595\)](#). Para solucionar problemas com falhas de recuperação de instância, consulte [Solução de problemas de falhas de recuperação de instâncias](#).

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

A ação de recuperação também pode ser acionada quando uma instância é programada pela AWS para ser interrompida ou cancelada devido à degradação do hardware subjacente. Para obter mais informações sobre eventos programados, consulte [Eventos programados para suas instâncias \(p. 570\)](#).

A ação de recuperação é compatível somente nas instâncias com as seguintes características:

- Use um dos seguintes tipos de instância: A1, C3, C4, C5, C5n, M3, M4, M5, M5a, R3, R4, R5, R5a, T2, T3, X1 ou X1e
- Use uma locação de instância **default** ou **dedicated**
- Use somente volumes do EBS (não configure volumes de armazenamento de instâncias).

Se a sua instância tiver um endereço IPv4 público, ela reterá o endereço IPv4 público após a recuperação.

Configuração de 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 um aplicativo específico. A seguir, temos algumas tarefas comuns para ajudá-lo a começar.

Tópicos

- [Cenários de configuração comuns \(p. 477\)](#)
- [Gerenciamento de software em sua instância do Linux \(p. 478\)](#)
- [Gerenciamento de contas de usuário em sua instância do Linux \(p. 483\)](#)
- [Controle do estado do processo para sua instância do EC2 \(p. 485\)](#)
- [Definição da hora de sua instância do Linux \(p. 491\)](#)
- [Otimizar opções de CPU \(p. 495\)](#)
- [Alteração do nome do host de sua instância do Linux \(p. 506\)](#)
- [Configuração de um DNS dinâmico em sua instância do Linux \(p. 508\)](#)
- [Execução de comandos na instância do Linux na inicialização \(p. 510\)](#)
- [Metadados da instância e dados do usuário \(p. 516\)](#)

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 [Gerenciamento de software em sua instância do Linux \(p. 478\)](#).

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 [Gerenciamento de contas de usuário em sua instância do Linux \(p. 483\)](#).

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 [Definição da hora de sua instância do Linux \(p. 491\)](#).

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 [Alteração do nome do host de sua instância do Linux \(p. 506\)](#). Você pode configurar uma instância para usar um provedor de serviço DNS dinâmico. Para obter mais informações, consulte [Configuração de um DNS dinâmico em sua instância do Linux \(p. 508\)](#).

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 [Execução de comandos na instância do Linux na inicialização \(p. 510\)](#).

Gerenciamento de software em sua instância do Linux

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.

Tópicos

- [Atualização de software de instância \(p. 479\)](#)
- [Adição de repositórios \(p. 480\)](#)
- [Localização de pacotes de software \(p. 481\)](#)
- [Instalação de pacotes de software \(p. 482\)](#)
- [Preparar-se para compilar software \(p. 482\)](#)

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 [Atualização de software de instância \(p. 479\)](#).

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 [Adição de repositórios \(p. 480\)](#). Para obter ajuda para localizar pacotes nos repositórios habilitados, consulte [Localização de pacotes de software \(p. 481\)](#). Para obter informações sobre como instalar uma instância do Amazon Linux, consulte [Instalação de pacotes de software \(p. 482\)](#).

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 \(p. 482\)](#).

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.

Atualização de software de instância

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

Esses procedimentos são destinados para uso com Amazon Linux. Para obter mais 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 reiniciar 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 que você deseja atualizar.

```
[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 reiniciar 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.

Adição de repositórios

Por padrão, as instâncias do Amazon Linux são executadas com dois repositórios habilitados: `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.

Important

Esses procedimentos são destinados para uso com Amazon Linux. Para obter mais 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>.

Localização de pacotes de software

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

Esses procedimentos são destinados para uso com Amazon Linux. Para obter mais informações sobre outras distribuições, consulte a documentação específica.

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.

```
[ec2-user ~]$ sudo yum search "find"
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
```

Instalação de pacotes de software

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

Esses procedimentos são destinados para uso com Amazon Linux. Para obter mais informações sobre outras distribuições, consulte a documentação específica.

Para instalar um pacote de um repositório, use o comando `yum install package`, substituindo `pacote` 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
```

Você também pode usar `yum install` para instalar arquivos de pacotes de RPM que você obteve por download da Internet. Para fazer isso, basta adicionar 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
```

Preparar-se para compilar software

Há uma variedade de 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

Esses procedimentos são destinados para uso com Amazon Linux. Para obter mais 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.

Para recuperar o código-fonte para 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.

Gerenciamento de contas de usuário em sua instância do Linux

Cada tipo de instância do Linux é executada com uma conta de usuário do sistema Linux padrão. Para a AMI do Amazon Linux 2 ou do Amazon Linux, o nome de usuário é `ec2-user`. Para CentOS, o nome de usuário é `centos`. No Debian, o nome de usuário é `admin` ou `root`. Para Fedora, o nome de usuário é `ec2-user` ou `fedora`. Para RHEL, o nome de usuário é `ec2-user` ou `root`. Para SUSE, o nome de usuário é `ec2-user` ou `root`. Para Ubuntu, o nome de usuário é `ubuntu`. Caso contrário, se `ec2-user` e `root` não funcionarem, verifique com seu provedor de 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 e grupos do IAM](#) no Guia do usuário do IAM.

Tópicos

- [Melhor prática \(p. 483\)](#)
- [Criar uma conta de usuário \(p. 484\)](#)
- [Remover uma conta de usuário \(p. 485\)](#)

Melhor prática

É adequado usar a conta de usuário padrão para muitos aplicativos, mas você pode escolher adicionar contas de usuário para que as pessoas possam ter seus próprios arquivos e espaços de trabalho. 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](#).

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.

Pré-requisitos

- Crie um par de chaves ou use um existente.

Para obter mais informações, consulte [Criação de um par de chaves usando o Amazon EC2 \(p. 617\)](#).

- Recupere a chave pública do par de chaves.

Para obter mais informações, consulte [Recuperação da chave pública para seu par de chaves no Linux \(p. 619\)](#) ou [Recuperação da chave pública para seu par de chaves no Windows \(p. 620\)](#).

Para adicionar uma conta de usuário

1. Use o comando adduser para adicionar a conta de usuário 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 denominada como newuser.

```
[ec2-user ~]$ sudo adduser newuser
```

[Ubuntu] Ao adicionar um usuário a um sistema do Ubuntu, inclua o parâmetro --disabled-password com esse comando para evitar adicionar uma senha à conta.

```
[ubuntu ~]$ sudo adduser newuser --disabled-password
```

2. Mude para a nova conta, de modo que o diretório e o arquivo que você criar tenham a propriedade adequada.

```
[ec2-user ~]$ sudo su - newuser  
[newuser ~]$
```

Observe que o prompt é alterado de ec2-user para newuser para indicar que você mudou a sessão de shell para a nova conta.

3. 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, crie o arquivo de chave e, por fim, cole a chave pública no arquivo de chave.
 - 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 do par de chaves no arquivo e salve as alterações. Por exemplo:

```
ssh-rsa AAAAB3NzaC1yc2EAAAQABAAQClKsfkNkuSevGj3eYhCe53pcjqP3maAhDFcvBS706V  
hz2ItxCih+PnDSUaw+WNQn/mZphTk/a/gU8jEzoOWbkM4yxyb/wB96xbiFveSFJuOp/d6RJhJOI0iBXr  
lsLnBItnckij7FbtxJMXLvvwJryDUilBMTjYtWB+QhYXUMOzce5Pjz5/i8SeJtjnV3iAoG/cQk+0Fzz  
qaeJAAHco+CY/5WrUBkrHmFJr6HcXkvJdWPkYQs3xqC0+FmUzofz221Cb5IMucxXPkX4rWi+z7wB3Rb  
BQoQzd8v7yeb70z1PnW0yN0qFU0XA246RA8QFYiCNYwI3f05p6KLxEXAMPLE
```

Agora, o usuário deve poder se conectar à conta `newuser` em sua instância usando a chave privada correspondente à chave pública que você adicionou ao arquivo `authorized_keys`.

Remover uma conta de usuário

Se uma conta de usuário não for mais necessária, você poderá remover essa conta de modo que ela não poderá mais ser usada.

Para remover um usuário do sistema

- 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 sua 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 o desempenho desejado (na frequência da CPU) de um núcleo. Os P-states são numerados começando com P0 (a configuração de desempenho 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:

- Propósito geral: `m4.10xlarge` | `m4.16xlarge`
- Otimizadas para computação: `c4.8xlarge`
- Otimizado para memória: `r4.8xlarge` | `r4.16xlarge` | `x1.16xlarge` | `x1.32xlarge` | `x1e.8xlarge` | `x1e.16xlarge` | `x1e.32xlarge`
- Otimizada para armazenamento: `d2.8xlarge` | `i3.8xlarge` | `i3.16xlarge` | `h1.8xlarge` | `h1.16xlarge`

- Computação acelerada: `f1.16xlarge | g3.16xlarge | p2.16xlarge | p3.16xlarge`
- Bare metal: `i3.metal | u-6tb1.metal | u-9tb1.metal | u-12tb1.metal`

Os tipos de instâncias a seguir oferecem a capacidade de um sistema operacional de controlar C-states do processador:

- Finalidade geral: `m5.12xlarge | m5.24xlarge | m5d.12xlarge | m5d.24xlarge`
- Otimizadas para computação: `c5.9xlarge | c5.18xlarge | c5d.9xlarge | c5d.18xlarge`
- Otimizado para memória: `r5.12xlarge | r5.24xlarge | r5d.12xlarge | r5d.24xlarge | z1d.6xlarge | z1d.12xlarge`
- Computação acelerada: `p3dn.24xlarge`

Talvez você queira alterar as configurações de C-state ou P-state para aumentar a consistência de desempenho do processador, reduzir a latência ou ajustar sua instância para uma carga de trabalho específica. As configurações padrão de C-state e P-state proporcionam o desempenho máximo, que é o ideal para a maioria das cargas de trabalho. Contudo, se seu aplicativo se beneficiaria de latência reduzida ao custo de frequências superiores de single ou dual core, ou de um desempenho 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 carga de trabalho.

Se a saída não exibe informações do C-state, inclua a opção `--debug` no comando (`sudo turbostat --debug stress <options>`).

Tópicos

- [O mais alto desempenho com a frequência máxima de Turbo Boost \(p. 486\)](#)
- [Alto desempenho e baixa latência limitando os C-states mais profundos \(p. 487\)](#)
- [Desempenho de linha de base com menor variabilidade \(p. 489\)](#)

O mais alto desempenho 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 cargas de trabalho. Essa configuração fornece o mais alto desempenho 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  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, as 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. As 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  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
...

```

Alto desempenho 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 desempenho. 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 um aplicativo 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 ~]$ 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
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
  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.

Desempenho de linha de base com menor variabilidade

Você pode reduzir a variabilidade da frequência do processador com P-states. Os P-states controlam o desempenho desejado (na frequência da CPU) de um núcleo. A maioria das cargas de trabalho funcionam melhor em P0, o que exige Turbo Boost. No entanto, é possível ajustar seu sistema para obter um desempenho consistente em vez de um desempenho intermitente que pode acontecer quando as frequências Turbo Boost são habilitadas.

As cargas de trabalho 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 carga de trabalho 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 carga de trabalho 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 carga de trabalho 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  0.00
 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  0.00
 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  0.00
 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  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.

Definição da hora de 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 acontecem. Se você usar um SDK da AWS CLI ou da AWS para fazer solicitações de sua instância, essas ferramentas assinarão solicitações em seu nome. Se a data e a hora 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 você pode acessar na sua instância. Esse serviço utiliza uma frota de relógios atômicos de referência conectados via satélite em cada região para fornecer leituras de hora atuais e precisas do padrão global de Tempo Universal Coordenado (UTC) por meio do Network Time Protocol (NTP). O Amazon Time Sync Service suaviza automaticamente qualquer segundo bissexto adicionado ao UTC.

O Amazon Time Sync Service está disponível por meio do NTP no endereço IP 169.254.169.123 para todas as instâncias em execução em uma VPC. Sua instância não requer acesso à Internet, e você não precisa configurar suas regras de security group nem de network ACL para permitir o acesso. 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.

Configuração do Amazon Time Sync Service no Amazon Linux AMI

Note

No Amazon Linux 2, a configuração padrão chrony já está definida 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
```

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. Inicie o daemon chrony (chronyd).

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

Starting chronyd: [OK]

Note

No RHEL e no CentOS (até a versão 6), o nome do serviço é `chrony` em vez de `chronyd`.

- Use o comando `chkconfig` para configurar o `chronyd` 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
```

```
^? 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
```

Configuração do 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
```

3. Reinicie o serviço chrony.

```
ubuntu:~$ sudo /etc/init.d/chrony restart
```

```
[ ok ] 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
|| |----- | 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    12    +15us[ +57us] +/-  320us
^- tbag.heanet.ie          1   6    17    13   -3488us[-3446us] +/- 1779us
^- ec2-12-34-231-12.eu-west- 2   6    17    13    +893us[ +935us] +/- 7710us
^? 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] +/-    0ns

```

Na saída retornada, ^* indica a fonte de hora preferida.

5. 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

```

Configuração do 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
```

Se essa linha não estiver presente, adicione-a. Comente qualquer outro servidor ou linhas de consulta. Abra o yast e ative o serviço chrony.

Alteração do fuso horário no Amazon Linux

As instâncias do Amazon Linux são configuradas para o fuso horário UTC (Tempo Universal Coordenado) por padrão, mas você pode alterar o horário de uma instância para o horário local ou outro fuso horário na rede.

Important

Esses procedimentos são destinados para uso com Amazon Linux. Para obter mais 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       GMTO     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. Neste exemplo, você pode usar o arquivo de fuso horário para Los Angeles, `/usr/share/zoneinfo/America/Los_Angeles`.

- Atualize o arquivo `/etc/sysconfig/clock` com o novo fuso horário.
 - 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`.
 - Localize a entrada `ZONE` e a 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.

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

- Reinicialize o sistema para obter as informações do novo fuso horário em todos os serviços e aplicativos.

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

Otimizar 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 para instâncias T2.

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 cargas de trabalho. No entanto, você pode especificar as seguintes opções de CPU para otimizar a instância para cargas de trabalho 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 cargas de trabalho 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 cargas de trabalho, como cargas de trabalho 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 \(p. 496\)](#)
- [Núcleos de CPU e threads por núcleo de CPU por tipo de instância \(p. 496\)](#)
- [Especificar opções de CPU para a instância \(p. 503\)](#)
- [Visualizar as opções de CPU para a instância \(p. 505\)](#)

Regras para especificar opções de CPU

Para especificar as opções de CPU para a instância, lembre-se das seguintes regras:

- No momento, as opções de CPU são compatíveis usando o console do Amazon EC2, a AWS CLI, um SDK da AWS ou a API do Amazon EC2.
- 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 \(p. 503\)](#).
- 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 \(p. 496\)](#).
- Para desabilitar o multithreading, especifique um thread por núcleo.
- Quando você [altera o tipo de instância \(p. 247\)](#) 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. Para cada tipo, a tabela mostra o padrão e o número compatível de núcleos de CPU e threads por núcleo.

Instâncias computacionais aceleradas

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Número válido de núcleos de CPU	Número válido de threads por núcleo
f1.2xlarge	8	4	2	1, 2, 3, 4	1, 2
f1.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
f1.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
g3.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
g3.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 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
p2.xlarge	4	2	2	1, 2	1, 2
p2.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 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, 2, 3, 4	1, 2
p3.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 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,	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Número válido de núcleos de CPU	Número válido de threads por núcleo
				38, 40, 42, 44, 46, 48	

Instâncias otimizadas para computação

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Número válido de núcleos de CPU	Número válido de threads 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, 2, 3, 4	1, 2
c4.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
c4.8xlarge	36	18	2	2, 4, 6, 8, 10, 12, 14, 16, 18	1, 2
c5.large	2	1	2	1	1, 2
c5.xlarge	4	2	2	2	1, 2
c5.2xlarge	8	4	2	2, 4	1, 2
c5.4xlarge	16	8	2	2, 4, 6, 8	1, 2
c5.9xlarge	36	18	2	2, 4, 6, 8, 10, 12, 14, 16, 18	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
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.18xlarge	72	36	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36	1, 2
c5n.large	2	1	2	1	1, 2
c5n.xlarge	4	2	2	2	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Número válido de núcleos de CPU	Número válido de threads por núcleo
c5n.2xlarge	8	4	2	2, 4	1, 2
c5n.4xlarge	16	8	2	2, 4, 6, 8	1, 2
c5n.9xlarge	36	18	2	2, 4, 6, 8, 10, 12, 14, 16, 18	1, 2
c5n.18xlarge	72	36	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36	1, 2

Instâncias de uso geral

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Número válido de núcleos de CPU	Número válido de threads por núcleo
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
m5.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	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.12xlarge	48	24	2	6, 12, 18, 24	1, 2
m5a.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

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Número válido de núcleos de CPU	Número válido de threads por núcleo
m5d.4xlarge	16	8	2	2, 4, 6, 8	1, 2
m5d.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	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
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

Instâncias otimizadas para memória

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Número válido de núcleos de CPU	Número válido de threads por núcleo
r4.large	2	1	2	1	1, 2
r4.xlarge	4	2	2	1, 2	1, 2
r4.2xlarge	8	4	2	1, 2, 3, 4	1, 2
r4.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
r4.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
r4.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
r5.large	2	1	2	1	1, 2
r5.xlarge	4	2	2	2	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Número válido de núcleos de CPU	Número válido de threads por núcleo
r5.2xlarge	8	4	2	2, 4	1, 2
r5.4xlarge	16	8	2	2, 4, 6, 8	1, 2
r5.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
r5.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
r5a.large	2	1	2	1	1, 2
r5a.xlarge	4	2	2	2	1, 2
r5a.2xlarge	8	4	2	2, 4	1, 2
r5a.4xlarge	16	8	2	2, 4, 6, 8	1, 2
r5a.12xlarge	48	24	2	6, 12, 18, 24	1, 2
r5a.24xlarge	96	48	2	12, 18, 24, 36, 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.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	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
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

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Número válido de núcleos de CPU	Número válido de threads por núcleo
x1e.xlarge	4	2	2	1, 2	1, 2
x1e.2xlarge	8	4	2	1, 2, 3, 4	1, 2
x1e.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
x1e.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
x1e.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
x1e.32xlarge	128	64	2	4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48, 52, 56, 60, 64	1, 2
z1d.large	2	1	2	1	1, 2
z1d.xlarge	4	2	2	2	1, 2
z1d.2xlarge	8	4	2	2, 4	1, 2
z1d.3xlarge	12	6	2	2, 4, 6	1, 2
z1d.6xlarge	24	12	2	2, 4, 6, 8, 10, 12	1, 2
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	Número válido de núcleos de CPU	Número válido de threads por núcleo
d2.xlarge	4	2	2	1, 2	1, 2
d2.2xlarge	8	4	2	1, 2, 3, 4	1, 2
d2.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
d2.8xlarge	36	18	2	2, 4, 6, 8, 10, 12, 14, 16, 18	1, 2
h1.2xlarge	8	4	2	1, 2, 3, 4	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Número válido de núcleos de CPU	Número válido de threads por núcleo
h1.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
h1.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 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, 2, 3, 4	1, 2
i3.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
i3.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 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

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 \(p. 500\)](#):

- 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

Desabilitar 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 [Execução de uma instância usando o assistente de execução de instância \(p. 391\)](#).

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 [Execução de uma instância usando o assistente de execução de instância \(p. 391\)](#).

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
```

Especificação de 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 [Execução de uma instância usando o assistente de execução de instância \(p. 391\)](#).
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 [Execução de uma instância usando o assistente de execução de instância \(p. 391\)](#).

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.

1. 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
```

2. 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.

Como visualizar as opções de CPU de uma instância (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 Description (Descrição) e visualize o campo Number of vCPUs (Número de vCPUs).
4. Para visualizar a contagem de núcleos e de threads por núcleo, escolha o valor do campo Number of vCPUs (Número de vCPUs).

Para visualizar as opções de CPU de uma instância (AWS CLI)

- Use o comando [describe-instances](#) do AWS CLI.

```
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 AWS Config Developer Guide.

Alteração do nome do host de sua instância do 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

Esses procedimentos são destinados para uso com Amazon Linux. Para obter mais informações sobre outras distribuições, consulte a documentação específica.

Alteração do 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 alterar o nome do host do sistema para um nome DNS público

Siga este procedimento se você já tiver um nome DNS público registrado.

- 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, você pode reiniciar usando o console do Amazon EC2 (na página Instances, escolha Actions, Instance State, Reboot).

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, você pode reiniciar usando o console do Amazon EC2 (na página Instances, escolha Actions, Instance State, Reboot).

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
```

Alteração do 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.

Alteração do 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?](#)

Configuração de um DNS dinâmico em sua instância do Linux

Quando você executa uma instância do EC2, ela é atribuída a um endereço IP público e a um DNS (Domain Name System) 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

Esses procedimentos são destinados para uso com Amazon Linux. Para obter mais 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.

Execução de 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 [Guia do usuário do AWS CloudFormation](#) e o [AWS OpsWorks User Guide](#).

Para obter informações sobre a execução de comandos na instância do Windows durante a inicialização, consulte [Execução de comandos na sua instância Windows na inicialização](#) e [Gerenciamento da configuração de instâncias 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 \(p. 36\)](#) 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 de 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

- [Pré-requisitos \(p. 511\)](#)
- [Dados de usuário e scripts de shell \(p. 511\)](#)
- [Dados do usuário e console \(p. 512\)](#)
- [Diretivas de cloud-init e dados de usuário \(p. 513\)](#)
- [Dados do usuário e AWS CLI \(p. 514\)](#)

Pré-requisitos

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 \(p. 31\)](#). 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 [Como configurar com o Amazon EC2 \(p. 21\)](#).

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

By default, user data scripts and cloud-init directives run only during the first boot cycle when an instance is launched. However, you can configure your user data scripts and cloud-init directives to run every time the instance is restarted from a stopped state. For more information, see [How can I execute user data after the initial launch of my EC2 instance?](#) in the AWS Knowledge Center.

Os scripts de shell de dados de usuário devem ser iniciados pelos caracteres `#!` e pelo caminho para o intérprete que você deseja que leia o script (geralmente `/bin/bash`). Para ter uma ótima introdução a scripts de shell, consulte o [Manual de Programação BASH](#) no Projeto de Documentação do Linux (tldp.org).

Os scripts inseridos como dados de usuário são executados como o usuário `root`, então, 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`).

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 e executado a partir de um diretório `/var/lib/cloud`. O script não é excluído depois de ser executado. Certifique-se de excluir os scripts de dados do usuário de `/var/lib/cloud` antes de criar um AMI a partir da instância. Caso contrário, o script existirá nesse diretório em qualquer instância iniciada na AMI e será executada quando a instância for iniciada.

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.

Especifique os dados do usuário da instância na execução

Siga o procedimento para executar uma instância em [Execução da sua instância a partir de uma AMI \(p. 391\)](#), mas, ao acessar [Step 6 \(p. 393\)](#) 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 0644 {} \;
echo "<?php phpinfo(); ?>" > /var/www/html/phpinfo.php
```

Reserve tempo suficiente para executar a instância e execute os comandos do script. Depois, verifique para saber se o script concluiu as tarefas pretendidas.

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 [Como adicionar regras a um security group \(p. 632\)](#).

(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 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.

Warning

Quando você interrompe uma instância, os dados em todos os volumes de armazenamento de instâncias são apagados. Para manter dados de volumes do armazenamento de instâncias, certifique-se de fazer backup deles em um armazenamento persistente.

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). Não é possível alterar os dados do usuário se a instância estiver em execução, mas é possível visualizá-la.
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 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 \(p. 163\)](#).

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

By default, user data scripts and cloud-init directives run only during the first boot cycle when an instance is launched. However, you can configure your user data scripts and cloud-init directives to run every time the instance is restarted from a stopped state. For more information, see [How can I execute user data after the initial launch of my EC2 instance?](#) in the AWS Knowledge Center.

A versão do Amazon Linux de cloud-init não oferece suporte a todas as diretivas que estão disponíveis no pacote básico, e algumas diretivas foram renomeadas (como `repo_update` em vez de `apt-upgrade`).

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 [Execução da sua instância a partir de uma AMI \(p. 391\)](#), mas, ao acessar [Step 6 \(p. 393\)](#) nesse procedimento, digite o texto da diretiva de cloud-init no campo User data 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 para saber se as diretivas concluíram as tarefas pretendidas.

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 [Como adicionar regras a um security group \(p. 632\)](#).

- (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 \(p. 520\)](#).

No Windows, você pode usar o AWS Tools para Windows PowerShell em vez de usar a AWS CLI. Para obter mais informações, consulte [Dados do usuário e Tools para Windows PowerShell](#) no Guia do usuário do Amazon EC2 para instâncias do Windows.

Exemplo: Especifique 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: Modifique 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.

No Linux, use o comando `base64` para codificar os dados de usuário.

```
base64 my_script.txt >my_script_base64.txt
```

No 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: Exibir 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"
}
```

No Linux, use a opção `--query` para obter os dados de usuário codificados e o comando `base64` para decodificá-los.

```
aws ec2 describe-instance-attribute --instance-id i-1234567890abcdef0 --attribute userData  
--output text --query "UserData.Value" | base64 --decode
```

No 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 da instância são divididos em categorias. Para obter mais informações, consulte [Categorias de metadados da instância \(p. 523\)](#).

Important

Embora você só possa acessar os metadados da instância e os dados do usuário de dentro da própria instância, os dados não são protegidos por métodos de criptografia. Qualquer um que possa acessar a instância pode visualizar seus metadados. Portanto, você deve tomar as precauções adequadas para proteger dados confidenciais (como chaves de criptografia duradouras). Você não deve armazenar dados confidenciais, por exemplo, senhas, como dados do usuário.

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 sua instância ou anexar um script simples. Você também pode usar esses dados para criar AMIs mais genéricas que podem ser modificadas por arquivos de configuração fornecidos no momento da execução. Por exemplo, se você executar servidores web para várias empresas de pequeno porte, elas poderão usar a mesma AMI e recuperar o conteúdo do bucket do Amazon S3 que você especificar nos dados do usuário na execução. Para adicionar um novo cliente a qualquer momento, basta criar um bucket para o cliente, adicionar seu conteúdo e executar sua AMI. Se você executar mais de uma instância ao mesmo tempo, os dados do usuário estarão disponíveis para todas as instâncias nessa reserva.

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 \(p. 528\)](#).

Tópicos

- [Recuperação dos metadados da instância \(p. 517\)](#)
- [Trabalhar com dados do usuário da instância \(p. 519\)](#)
- [Recuperação dos dados dinâmicos \(p. 520\)](#)
- [Exemplo: Valor de índice de execução da AMI \(p. 520\)](#)
- [Categorias de metadados da instância \(p. 523\)](#)

- [Documentos de identidade de instância \(p. 529\)](#)

Recuperação dos 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 um aplicativo externo.

Para visualizar todas as categorias de metadados da instância de dentro de uma instância em execução, use o seguinte URI:

```
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.

Você pode usar uma ferramenta como o cURL ou, se sua instância oferecer suporte a ele, o comando GET, por exemplo:

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/
```

```
[ec2-user ~]$ GET http://169.254.169.254/latest/meta-data/
```

Você também pode fazer download da [ferramenta Instance Metadata Query](#), que permite consultar os metadados da instância sem precisar digitar o URI completo nem os nomes das categorias.

Todos os metadados da instância são retornados como texto (tipo de conteúdo `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).

Exemplos de recuperação de 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.

```
[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
```

Este exemplo obtém itens de metadados de nível superior. Para obter mais informações, consulte [Categorias de metadados da instância \(p. 523\)](#).

```
[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/
```

Estes exemplos obtêm um valor de alguns itens de metadados do exemplo anterior.

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/ami-id
ami-12345678
```

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/reservation-id
r-fea54097
```

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/local-hostname
ip-10-251-50-12.ec2.internal
```

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/public-hostname
ec2-203-0-113-25.compute-1.amazonaws.com
```

Este exemplo obtém uma lista de chaves públicas disponíveis.

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/public-keys/
0=my-public-key
```

Este exemplo mostra os formatos nos quais a chave pública 0 está disponível.

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/public-keys/0/
openssh-key
```

Este exemplo obtém a chave pública 0 (no formato de chave OpenSSH).

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
ssh-rsa MIICiTCCAFICCQD6m7oRw0uXOjANBgkqhkiG9w0BAQUFADCBiDELMAkGA1UEBhMC
VVmxCzAJBgNVBAgTAlDbMRawDgYDVQQHEwdTZWF0dGx1MQ8wDQYDVQQKEwZBbWF6
b24xFDASBgNVBASTC01bTSBDb25zb2x1MRIwEAYDVQQDEw1UZXN0Q21sYWMxHzAd
BgkqhkiG9w0BCQEWEVG5vb25lQGFTYXpbvi5jb20wHcNMTEwNDI1MjA0NTIxWhcN
MTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAlDbMRawDgYD
VQQHEwdTZWF0dGx1MQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBASTC01bTSBDb25z
b2x1MRIwEAYDVQQDEw1UZXN0Q21sYWMxHzAdBgkqhkiG9w0BCQEWEVG5vb25lQGFT
YXpbvi5jb20wgZ8wDQYJKoZIhvCNQEBBQADgY0AMIGJAOGBAMAk0dn+a4GmWIWJ
21uUSfwfEvySWtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
rDHudUZg3qX4waLG5M43q7Wgc/Mb0ITxOUSQv7c7ugFFDzQGBzzswY6786m86gpe
Ibb3OhjZnzcvQAARHhd1QWIMm2nrAgMBAAEwDQYJKoZIhvCNQEFBQADgYEAtCu4
nUhVVxYUnteD9+h8Mg9q6q+auNKyExzyLwax1Aoo7TJHidbtS4J5inMzgL0Fkb
FFBjvSfpJI1J00zbhNY5f6GuoEDmFJ10ZxBHjJnyp378OD8uTs7fLvjx79LjSTb
NYiytvBZPQU5Yaxu2jXnimvw3rrszlaEXAMPLE my-public-key
```

Este exemplo obtém o ID de sub-rede para uma instância.

```
[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

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 da instância para recuperar as credenciais de segurança da AWS, evite consultar as credenciais durante cada transação ou simultaneamente de 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 da instância, tente novamente a consulta com uma estratégia de recuo exponencial.

Trabalhar com dados do usuário da instância

Ao trabalhar com dados do usuário da instância, lembre-se do seguinte:

- Os dados do usuário são tratados como dados opacos: o que você fornece é o que receberá de volta. Cabe à instância interpretá-los.
- Os dados do usuário estão limitados a 16 KB. Esse limite se aplica aos dados na forma bruta, não à forma codificada por base64.
- 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 devem ser decodificados quando você os recupera. Os dados são decodificados quando você os recuperar usando metadados da instância e o console.
- 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.

Especifique os dados do usuário da instância na execução

Você pode especificar dados do usuário quando você executar uma instância. Para obter mais informações, consulte [Execução de uma instância usando o assistente de execução de instância \(p. 391\)](#) e [Execução de comandos na instância do Linux na inicialização \(p. 510\)](#).

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 \(p. 512\)](#).

Recuperar os dados do usuário da instância

Para recuperar os dados do usuário de dentro 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 de usuário que foram fornecidas como texto separado por vírgulas:

```
[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:

```
[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 para uma instância no seu computador, consulte [Dados do usuário e AWS CLI \(p. 514\)](#)

Recuperação dos dados dinâmicos

Para recuperar os dados dinâmicos de dentro de uma instância em execução, use o seguinte URI:

```
http://169.254.169.254/latest/dynamic/
```

Este exemplo mostra como recuperar as categorias de identidade de instância de alto nível:

```
[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 de instância \(p. 529\)](#).

Exemplo: Valor de índice de execução da AMI

Este exemplo demonstra como usar dados do usuário e metadados da instância para configurar suas instâncias.

Alice deseja executar quatro instâncias de sua AMI de banco de dados favorita, sendo a primeira atuando como mestra e as três restantes como réplicas. Ao executá-las, ela deseja adicionar dados do usuário sobre a estratégia de replicação para cada replicante. 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.

Veja a seguir os dados do usuário que Alice construiu:

```
replicate-every=1min | replicate-every=5min | replicate-every=10min
```

Os dados `replicate-every=1min` definem a configuração da primeira replicante, `replicate-every=5min` define a configuração da segunda replicante, 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`, especificando os dados do usuário:

```
aws ec2 run-instances --image-id ami-12345678 --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-12345678
- 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

Metadados	Valor
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` para essa instância para garantir que ela seja uma das replicantes:

```
[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:

```
[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:

```
[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:

```
[ec2-user ~]$ echo $user_data | cut -d"|" -f"$ami_launch_index"
```

replicate-every=5min

Categorias de metadados da instância

A tabela a seguir lista as categorias de metadados da instância.

Important

Os nomes das categorias que são formatados em texto vermelho são espaços reservados para os dados que são exclusivos da sua instância; por exemplo, *mac* representa o endereço MAC para a interface de rede. Você deve substituir os espaços reservados pelos valores reais.

Dados	Descrição	Versão introduzida
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> .	2007-10-10
block-device-mapping/ami	O dispositivo virtual que contém o sistema de arquivos de inicialização/raiz.	2007-12-15
block-device-mapping/ebs N	Os dispositivos virtuais associadas a volumes Amazon EBS, se presentes. Os volumes Amazon EBS estarão disponíveis somente em metadados se estiverem presentes no momento da inicialização ou quando a instância foi iniciada pela última vez. O N indica o índice do volume do Amazon EBS (como <i>ebs1</i> ou <i>ebs2</i>).	2007-12-15
block-device-mapping/eph emeral N	Os dispositivos virtuais associados a volumes de armazenamento de instância não NVMe, se houver algum presente. O N indica o índice de cada volume efêmero.	2007-12-15

Dados	Descrição	Versão introduzida
<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:) é associado à instância específica.	2007-12-15
<code>block-device-mapping/swap</code>	Os dispositivos virtuais associados a swap. Nem sempre presente.	2007-12-15
<code>elastic-gpus/associations/<i>elastic-gpu-id</i></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>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 Para visualizar o histórico de eventos sobre eventos concluídos ou cancelados (p. 572) .	17/08/2018
<code>events/maintenance/scheduled</code>	Se houver eventos de manutenção da instância ativos, contém uma string JSON com informações sobre os eventos. Para obter mais informações, consulte Visualização de eventos programados (p. 570) .	17/08/2018
<code>hostname</code>	O nome de host DNS IPv4 privado da instância. Em casos em que várias interfaces de rede estão presentes, isso se refere ao dispositivo eth0 (o dispositivo para o qual o número de dispositivo é 0).	1,0
<code>iam/info</code>	Se houver uma função do IAM associada à instância, conterá informações sobre a última vez que o perfil de instância foi atualizado, incluindo a data LastUpdated, InstanceProfileArn e InstanceProfileId. Caso contrário, não estará presente.	2012-01-12

Dados	Descrição	Versão introduzida
<code>iam/security-credentials/ role-name</code>	Se houver uma função do IAM associada à instância, <code>role-name</code> será o nome da função, e <code>role-name</code> conterá as credenciais de segurança temporárias associadas à função (para obter mais informações, consulte Como recuperar credenciais de segurança dos metadados da instância (p. 713)). Caso contrário, não estará presente.	2012-01-12
<code>identity-credentials/ec2/ info</code>	[Reservado somente para uso interno] Informações sobre as credenciais que a AWS usa para identificar uma instância para o resto da infraestrutura do Amazon EC2.	23/05/2018
<code>identity-credentials/ec2/ security-credentials/ec2- instance</code>	[Reservado somente para uso interno] As credenciais que a AWS usa para identificar uma instância para o resto da infraestrutura do Amazon EC2.	23/05/2018
<code>instance-action</code>	Notifica a instância que ela deve ser reinicializada em preparação para o empacotamento. Valores válidos: <code>none</code> <code>shutdown</code> <code>bundle-pending</code> .	2008-09-01
<code>instance-id</code>	O ID dessa instância.	1,0
<code>instance-type</code>	O tipo da instância. Para obter mais informações, consulte Tipos de instância (p. 176) .	2007-08-29
<code>kernel-id</code>	O ID do kernel executado com essa instância, se aplicável.	2008-02-01
<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).	2007-01-19
<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).	1,0
<code>mac</code>	O endereço Media Access Control (MAC) da instância. Em casos em que várias interfaces de rede estão presentes, isso se refere ao dispositivo eth0 (o dispositivo para o qual o número de dispositivo é 0).	01/01/2011

Dados	Descrição	Versão introduzida
<code>metrics/vhostmd</code>	Suspenso.	01/05/2011
<code>network/interfaces/macs/mac/device-number</code>	O número de dispositivo exclusivo associado a essa interface. O número do dispositivo corresponde ao nome do dispositivo; por exemplo, um <code>device-number</code> de 2 é para o dispositivo <code>eth2</code> . Essa categoria corresponde aos campos <code>DeviceIndex</code> e <code>device-index</code> que são usados pelos comandos da API do Amazon EC2 e do EC2 para a AWS CLI.	01/01/2011
<code>network/interfaces/macs/mac/interface-id</code>	O ID da interface de rede.	01/01/2011
<code>network/interfaces/macs/mac/ipv4-associations/public-ip</code>	Os endereços IPv4 privados que estão associados a cada endereço IP público e estão atribuídos a essa interface.	01/01/2011
<code>network/interfaces/macs/mac/ipv6s</code>	Os endereços IPv6 associados à interface. Retornados apenas para instâncias executadas em uma VPC.	2016-06-30
<code>network/interfaces/macs/mac/local-hostname</code>	O nome do host local da interface.	2011-01-01
<code>network/interfaces/macs/mac/local-ipv4s</code>	Os endereços IPv4 privados associados à interface.	2011-01-01
<code>network/interfaces/macs/mac/mac</code>	O endereço MAC da instância.	2011-01-01
<code>network/interfaces/macs/mac/owner-id</code>	O ID do proprietário da interface de rede. Em ambientes de várias interfaces, um terceiro pode anexar uma interface, como o Elastic Load Balancing. O tráfego em uma interface é sempre cobrado do proprietário da interface.	01/01/2011
<code>network/interfaces/macs/mac/public-hostname</code>	O DNS público da interface (IPv4). Essa categoria só será retornada se o atributo <code>enableDnsHostnames</code> for definido como <code>true</code> . Para obter mais informações, consulte Using DNS with Your VPC .	01/01/2011
<code>network/interfaces/macs/mac/public-ipv4s</code>	Os endereços IP público ou elástico 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

Dados	Descrição	Versão introduzida
<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.	2016-06-30
<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.	2016-06-30
<code>network/interfaces/macs/mac/vpc-ipv6-cidr-blocks</code>	O bloco CIDR IPv6 da VPC na qual a interface reside.	2016-06-30
<code>placement/availability-zone</code>	A zona de disponibilidade na qual a instância foi executada.	2008-02-01
<code>product-codes</code>	Os códigos de produto do Marketplace associados à instância, se houver.	2007-03-01
<code>public-hostname</code>	O DNS público da instância. Essa categoria só será retornada se o atributo <code>enableDnsHostnames</code> for definido como <code>true</code> . Para obter mais informações, consulte Usar DNS com a VPC , no Guia do usuário da Amazon VPC.	2007-01-19
<code>public-ipv4</code>	O endereço IPv4 público. Se um endereço IP elástico estiver associado à instância, o valor retornado será o endereço IP elástico.	2007-01-19
<code>public-keys/0/openssh-key</code>	Chave pública. Disponível somente se fornecido no momento da execução da instância.	1,0
<code>ramdisk-id</code>	O ID do disco de RAM no momento da execução, se aplicável.	2007-10-10
<code>reservation-id</code>	O ID da reserva.	1,0

Dados	Descrição	Versão introduzida
<code>security-groups</code>	<p>Os nomes dos security groups aplicados à instância.</p> <p>Após a execução, você só pode alterar os grupos de segurança das instâncias. Essas alterações estão refletidas aqui e em <code>network/interfaces/macs/<i>mac</i>/security-groups</code>.</p>	1,0
<code>services/domain</code>	O domínio dos recursos da AWS para a região.	2014-02-25
<code>services/partition</code>	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 <code>aws-<i>partitionname</i></code> . Por exemplo, a partição dos recursos na região da China (Beijing) é aws-cn.	2015-10-20
<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 instance-action (p. 352) .	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 termination-time (p. 353) .	2014-11-05

Categorias de dados dinâmicos

A tabela a seguir lista as categorias de dados dinâmicos.

Dados	Descrição	Versão introduzida
<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>	2009-04-04

Dados	Descrição	Versão introduzida
<code>instance-identity/document</code>	O JSON que contém os atributos da instância, como o ID da instância, o endereço IP privado, etc. Consulte Documentos de identidade de instância (p. 529) .	2009-04-04
<code>instance-identity/pkcs7</code>	Usado para verificar a autenticidade e o conteúdo do documentos em relação à assinatura. Consulte Documentos de identidade de instância (p. 529) .	2009-04-04
<code>instance-identity/signature</code>	Os dados que podem ser usados por outras partes para verificar suas origem e autenticidade. Consulte Documentos de identidade de instância (p. 529) .	2009-04-04

Documentos de identidade de instância

Um documento de identidade de instância é um arquivo JSON que descreve uma instância. O documento de identidade de instância é acompanhado de uma assinatura e uma assinatura PKCS7 que podem ser usadas para verificar a precisão, a origem e a autenticidade das informações fornecidas no documento.

O documento de identidade de instância é gerado quando a instância é executada e exposta à instância por meio dos [metadados de instância \(p. 516\)](#). Ele valida os atributos das instâncias, como o tamanho da instância, o tipo de instância, o sistema operacional e a AMI.

Important

Devido à natureza dinâmica dos documentos de identidade de instância e assinaturas, recomendamos recuperar o documento de identidade de instância e a assinatura regularmente.

Como obter o documento de identidade de instância e assinaturas

Para recuperar o documento de identidade de instância, use o seguinte comando de sua instância em execução:

```
[ec2-user ~]$ 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"
}
```

Para recuperar a assinatura de identidade de instância, use o seguinte comando de sua instância em execução:

```
[ec2-user ~]$ curl http://169.254.169.254/latest/dynamic/instance-identity/signature
```

A seguir está um exemplo de saída:

```
dExamplesjNQhhJan7pORLpLSr7lJEF4V2DhKGlyoYVB0UYrY9njyBCmhEayaGrhtS/AWY+LPx  
1VSQURF5n0gwPNCuO6ICT0fNrm5IH7w9ydyalexamplejJw8XvWPxbuRkcN0TAA1p4RtCAqm4ms  
x2oALjWSCBExample=
```

Para recuperar a assinatura PKCS7, use o seguinte comando de sua instância em execução:

```
[ec2-user ~]$ curl http://169.254.169.254/latest/dynamic/instance-identity/pkcs7
```

A seguir está um exemplo de saída:

```
MIICiTCCAFICCQD6m7oRw0uXOjANBgkqhkiG9w0BAQUFADCBiDELMAkGA1UEBhMC  
VVVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGx1Mq8wDQYDVQQKEwZBbWF6  
b24xFDASBgNVBAsTC01BTSBDb25zb2x1MRIwEAYDVQQDEwLUZXN0Q21sYWMMxHzAd  
BgkqhkiG9w0BCQEWEg5vb25lQGFtYXpvbi5jb20wHhcNMTEwNDI1MjA0NTIxWhcN  
MTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBhMCVVVMxCzAJBgNVBAgTAldBMRAwDgYD  
VQQHEwdTZWF0dGx1Mq8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC01BTSBDb25z  
b2x1MRIwEAYDVQQDEwLUZXN0Q21sYWMMxHzAdBgkqhkiG9w0BCQEWEg5vb25lQGFt  
YXpvbi5jb20wgZ8wDQYJKoZIhvCNQAEBBQADgY0AMIGJAOGBAMaK0dn+a4GmWIWJ  
21uUSfwfEvYSwtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEI03IyNoH/f0wYK8m9T  
rDHudUZg3qX4waLG5M43q7Wgc/MbqITxOUSQv7c7ugFFDzQGBzzswY678m86gpE  
Ibb3OhjZnzcvcQaRHhd1QWIMm2nrAgMBAAEwDQYJKoZIhvCNQEFBQADgYEAtCu4  
nUhVVxYUntneD9+h8Mg9q6q+auNkyExzyLwax1Ao0TJHidbtS4J5iNmZgXL0Fkb  
FFBjvSfpJI1J00zbhNY5f6GuoEDMfJ10ZxBHjNyp3780D8uTs7fLvjk79LjSTb  
NYiytVbZPQ0Q5Yaxu2jXnimvw3rrszlaEXAMPLE
```

Verificação da assinatura PKCS7

Você pode usar a assinatura PKCS7 para verificar sua instância validando-a com o certificado público da AWS apropriado.

O certificado público da AWS para as regiões fornecidas pela conta da AWS é o seguinte:

```
-----BEGIN CERTIFICATE-----  
MIIC7TCCAQ0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxZcAJBgNVBAYTA1VTMRkw  
FwYDVQQIExBXYXN0aW5ndG9uIFNOYXR1MRAwDgYDVQQHEwdTZWF0dGx1MSAwHgYD  
VQQKExdBbWF6b24gV2ViIFNlcnPzY2VzIExMqzaefw0xMjAxMDUxMjU2MTJaFw0z  
ODAxMDUxMjU2MTJaMFwxZcAJBgNVBAYTA1VTMRkwFwYDVQQIExBXYXN0aW5ndG9u  
IFNOYXR1MRAwDgYDVQQHEwdTZWF0dGx1MSAwHgYDVQQKExdBbWF6b24gV2ViIFNl  
cnZpY2VzIExMqzCCAbcwggEsBgcqhkjOOAQBMII1BHwKBgQCjkvcS2bb1VQ4yt/5e  
ih5006kK/n1Lz1lr7D8ZwtQP8f0Epp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3  
VyIQzK7wLc1nd/YozQNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P  
hviYt5JH/nY14hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nvvHwh6+ERYRAoGBAI1j  
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rActXau8Qe+MbcJ1/U  
hhy1KHVpCG19fueQ2s6IL0Ca0/buycU1CiYQk40KNHccHfNiZbd1x1E9rpUp7bnF  
lRa2v1ntMX3caRVDbtPEWmdzSCYsYFDk4mZrOLBA4GEAAkBgEbmeve5f8LIE/Gf  
MNmP9CM5ev0QGx5h08Wqd+aTebs+k2tn92BPqeZqpWRa5P/+jrdKml1qx411HW  
MXrs3IgIb6+hUIB+S8dz8/mm0bpz76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw  
vSeDCOUAMYQR7R9LINYwouHiziqQYMAkGBYqGSM44BAMDLwAwLAIUWXBlk40xTwSw  
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K  
-----END CERTIFICATE-----
```

O certificado público da AWS para a região AWS GovCloud (US-West) é o seguinte:

```
-----BEGIN CERTIFICATE-----  
MIICuzCCAQ0CCQDrSGn1RgvSazANBgkqhkiG9w0BAQUFADCBoTELMAkGA1UEBhMC  
VVVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGx1MRMwEQYDVQQKEwpBbWF6
```

```
b24uY29tMRYwFAYDVQQLEw1FQzIgQXV0aG9yaXR5MRowGAYDVQQDEXFFQzIgQU1J
IEF1dGhvcm10eTEqMCgGCSqGS1b3DQEJARYbZWMyLWluc3RhbmN1LWlpZEBhbWF6
b24uY29tMB4XDTeXMDgxMjE3MTgwNVoXDTIxMDgwOTE3MTgwNVowgaExCzAJBgNV
BAYTA1VTM0swCQYDVQQIEwJXQTEQMA4GA1UEBxMHU2VhdHRSZTETMBEGA1UEChMK
QW1hem9uLmNvbTEWMBQGA1UECxMNRRUMyIEF1dGhvcm10eTEaMBgGA1UEAxMRRUMy
IEFNSSBBdXRob3JpdHkxKjAoBgkqhkiG9w0BCQEWG2VjMi1pbnN0YW5jZS1paWRA
YW1hem9uLmNvbTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAAqaIcGFFTx/SO
1W5G91jHvyQdGP25n1Y91aXCuOWAUTvSvNGpxrI4AXNrQF+CmIOC4beBAsnHCx0
82jYudWBBL19Wiza0psYc9flrczSzVLmN8w/c78F/95NfiQdnUOPpvqgcMeJo82c
gHkLR7XoFWgMrZJqrcUK0gnsQcb6kakCAwEAATANBgkqhkiG9w0BAQQUFAAOBgQDF
VHO+UGZr1LCQ78PbBH0GreIDqMFfa+W8xASDYUzrMvY3kcIelkoIazvi4VtPO7Qc
yAiLr6nk69Tr/MITnmmsZJZPetsqBndRyL+DaTRnF0/xvBQXj5tEh+AmRjvGtp
6iS1rQoNanN8oEct2j4b48rmCmnDhRoBcFHwCYs/3w==

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

Para outras regiões, entre em contato com o [AWS Support](#) para obter o certificado público da AWS.

Para verificar a assinatura PKCS7

1. Na sua instância, crie um arquivo temporário para a assinatura PKCS7:

```
[ec2-user ~]$ PKCS7=$(mktemp)
```

2. Adicione o cabeçalho -----BEGIN PKCS7----- ao arquivo PKCS7 temporário:

```
[ec2-user ~]$ echo "-----BEGIN PKCS7-----" > $PKCS7
```

3. Adicione o conteúdo da assinatura PKCS7 dos metadados de instância, mais a nova linha:

```
[ec2-user ~]$ curl -s http://169.254.169.254/latest/dynamic/instance-identity/pkcs7 >> $PKCS7
[ec2-user ~]$ echo "" >> $PKCS7
```

4. Adicione rodapé -----END PKCS7-----:

```
[ec2-user ~]$ echo "-----END PKCS7-----" >> $PKCS7
```

5. Crie um arquivo temporário para o documento de identidade de instância:

```
[ec2-user ~]$ DOCUMENT=$(mktemp)
```

6. Adicione o conteúdo do documento dos metadados de instância ao arquivo de documento temporário:

```
[ec2-user ~]$ curl -s http://169.254.169.254/latest/dynamic/instance-identity/document
> $DOCUMENT
```

7. Abra um editor de texto e crie um arquivo chamado AWSpubkey. Copie e cole o conteúdo do certificado público da AWS acima ao arquivo e salve-o.

8. Use as ferramentas OpenSSL para verificar a assinatura da seguinte forma:

```
[ec2-user ~]$ openssl smime -verify -in $PKCS7 -inform PEM -content $DOCUMENT -certfile
AWSpubkey -noverify > /dev/null
Verification successful
```

Identifique as instâncias Linux do EC2

Seu aplicativo pode precisar determinar se está executando em uma instância do EC2.

Para obter informações sobre como identificar as instâncias Windows, consulte [Identificar instâncias Windows do EC2](#) no Guia do usuário do Amazon EC2 para instâncias do Windows.

Inspeção do 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. 529).

Inspeção do 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, as para as instâncias do EC2 que não estão usando o Amazon Linux, a implementação de distribuição do SMBIOS podem representar o UUID em formato little-endian e, portanto, os caracteres "EC2" não aparecem no início do UUID.

Example : Obtenha o UUID do hypervisor

Se existir `/sys/hypervisor/uuid`, você pode usar o seguinte comando:

```
[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
```

Example : Obtenha o UUID de DMI (somente instâncias HVM)

Somente nas instâncias HVM, você pode usar o Desktop Management Interface (DMI).

Você pode usar a ferramenta `dmidecode` para retornar ao UUID. No Amazon Linux, use o comando a seguir para instalar a ferramenta `dmidecode` se ela ainda não estiver instalada na sua instância:

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

Em seguida, execute o seguinte comando:

```
[ec2-user ~]$ sudo dmidecode --string system-uuid
```

Como alternativa, use os comandos a seguir:

```
[ec2-user ~]$ sudo cat /sys/devices/virtual/dmi/id/product_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-FD21-01234ABCDEF
```

No exemplo de saída a seguir, o UUID é representado no formato little-endian.

```
45E12AEC-DCD1-B213-94ED-01234ABCDEF
```

Em instâncias Nitro, o comando a seguir pode ser usado:

```
[ec2-user ~]$ cat /sys/devices/virtual/dmi/id/board_asset_tag
```

Isso retorna o ID da instância, que é exclusivo das instâncias do EC2:

```
i-0af01c0123456789a
```

Amazon Elastic Inference

O Amazon Elastic Inference (EI) é um recurso que você pode anexar a suas instâncias do Amazon EC2 para acelerar suas cargas de trabalho de inferência de deep learning (DL). Os aceleradores do Amazon EI são fornecidos em vários tamanhos e são um método econômico para criar recursos inteligentes em aplicativos que são executados em instâncias do Amazon EC2.

O Amazon EI acelera as operações definidas pelo TensorFlow, o Apache MXNet e o formato Open Neural Network Exchange (ONNX) em aceleradores de inferência de DL baseados em GPU de baixo custo. Os desenvolvedores que criam uma grande variedade de aplicativos em instâncias do Amazon EC2 com cargas de trabalho de inferência de machine learning podem se beneficiar da implantação mais ampla por meio da redução de custo habilitada pelo Amazon EI.

Tópicos

- [Conceitos básicos de Amazon EI \(p. 534\)](#)
- [Como trabalhar com o Amazon EI \(p. 537\)](#)
- [Uso das métricas do CloudWatch para monitorar o Amazon EI \(p. 557\)](#)
- [Solução de problemas \(p. 560\)](#)

Conceitos básicos de Amazon EI

Quando você configura uma instância para execução com um acelerador do Amazon EI, a AWS localiza a capacidade disponível do acelerador e estabelece uma conexão de rede entre a instância e o acelerador.

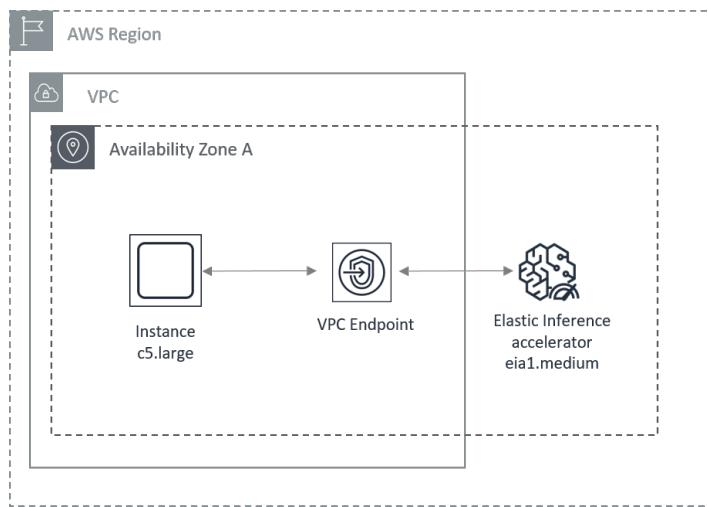
Os aceleradores do Amazon EI estão disponíveis para todos os tipos de instância do EC2.

Os tipos de acelerador do Amazon EI a seguir estão disponíveis. Você pode anexar qualquer tipo de acelerador do Amazon EI a qualquer tipo de instância.

Tipo de acelerador	Taxa de transferência para FP32 (TFLOPS)	Taxa de transferência para FP16 (TFLOPS)	Memória (GB)
eia1.medium	1	8	1
eia1.large	2	16	2
eia1.xlarge	4	32	4

Um acelerador do Amazon EI não faz parte do hardware de compõe a instância. Em vez disso, o acelerador é anexado por meio da rede usando um serviço de endpoint do AWS PrivateLink. O serviço de endpoint roteia o tráfego da instância para o acelerador do Amazon EI configurado com a instância.

Antes de executar uma instância com um acelerador do Amazon EI, crie um serviço de endpoint do AWS PrivateLink. Cada zona de disponibilidade exige apenas um serviço de endpoint para conectar instâncias com aceleradores do Amazon EI. Para obter mais informações, consulte [Serviços do VPC endpoint \(AWS PrivateLink\)](#).



Você pode usar o Amazon Elastic Inference habilitado para bibliotecas do TensorFlow, do TensorFlow Serving ou do Apache MXNet para carregar modelos e fazer chamadas de inferência. As versões modificadas dessas bibliotecas detectam automaticamente a presença de aceleradores do Amazon EI, distribuem de forma ideal as operações do modelo entre o acelerador do Amazon EI e a CPU da instância e controla com segurança o acesso a seus aceleradores usando políticas do IAM. As [AMIs do AWS Deep Learning](#) incluem as versões mais recentes do Amazon Elastic Inference habilitadas para TensorFlow Serving e MXNet. Se estiver usando AMIs personalizadas ou imagens de contêiner, você poderá fazer download e instalar as bibliotecas do [TensorFlow Serving do Amazon Elastic Inference](#) e do [Apache MXNet do Amazon Elastic Inference](#) no Amazon S3.

Note

Um acelerador do Amazon EI não é visível ou acessível por meio do gerenciador de dispositivos da instância.

O tráfego de rede do acelerador do Amazon EI usa o protocolo HTTPS (porta 443 do TCP). Verifique se o grupo de segurança da instância e do serviço de endpoint do AWS PrivateLink permite isso. Para obter mais informações, consulte [Configuração de seus grupos de segurança para o Amazon EI \(p. 538\)](#).

Definição de preço do Amazon EI

Você é cobrado por cada segundo que um acelerador do Amazon EI está anexado a uma instância no estado `running`. Você não é cobrado por um acelerador anexado a uma instância que esteja no estado `pending`, `stopping`, `stopped`, `shutting-down` ou `terminated`. Você também não é cobrado quando um acelerador do Amazon EI está no estado `unknown` ou `impaired`.

Você não é cobrado pelo AWS PrivateLink para VPC endpoints para o serviço Amazon EI quando tem aceleradores provisionados na sub-rede.

Para obter mais informações sobre a definição de preço por região do Amazon EI, consulte [Definição de preço do Amazon EI](#).

Considerações sobre o Amazon EI

Antes de começar a usar aceleradores do Amazon EI, esteja ciente das seguintes limitações:

- Você pode anexar um acelerador do Amazon EI a uma instância de cada vez e apenas durante a execução da instância.
- Não é possível compartilhar um acelerador do Amazon EI entre instâncias.

- Não é possível desanexar um acelerador do Amazon EI de uma instância ou transferi-lo para outra instância. Se você não precisar mais de um acelerador do Amazon EI, será necessário encerrar a instância. Para alterar o tipo de acelerador do Amazon EI, crie uma AMI a partir da instância, encerre-a e execute uma nova instância com uma especificação diferente do acelerador do Amazon EI.
- Atualmente, apenas as bibliotecas avançadas do MXNet para o Amazon Elastic Inference e do TensorFlow Serving para o Amazon Elastic Inference podem fazer chamadas de inferência para aceleradores do Amazon EI.
- Os aceleradores do Amazon EI podem ser anexados apenas a instâncias em uma VPC.
- A definição de preço de aceleradores do Amazon EI está disponível apenas a taxas sob demanda. Você pode anexar um acelerador a uma Instância reservada, Instância reservada programada ou Instância spot. No entanto, o preço sob demanda do acelerador do Amazon EI é aplicado. Você não pode reservar ou programar capacidade para o acelerador do Amazon EI.

Escolha de uma instância e de um tipo de acelerador para seu modelo

As demandas por recursos de computação da CPU, memória da CPU, aceleração baseada em GPU e memória da GPU variam significativamente entre diferentes tipos de modelos de deep learning. Os requisitos de latência e de taxa de transferência do aplicativo também determinam a quantidade de computação da instância e de aceleração do Amazon EI de que você precisa. Considere os fatores a seguir ao escolher uma combinação de instância e tipo de acelerador para seu modelo:

- Antes de avaliar a combinação certa de recursos para seu modelo ou aplicativo, determine as necessidades de latência de destino e de taxa de transferência para a pilha geral do aplicativo, bem como todas as restrições que possam existir. Por exemplo, se o aplicativo precisar responder em 300 milissegundos (ms), e a recuperação de dados (incluindo qualquer autenticação) e o pré-processamento utilizarem 200 ms, você terá uma janela de 100 ms para trabalhar com a solicitação de inferência. Usando essa análise, você pode determinar a combinação de infraestrutura de menor custo que atenda a esses objetivos.
- Comece com uma combinação de recursos razoavelmente pequena. Por exemplo, um tipo de instância `c5.xlarge` junto com um tipo de acelerador `eia1.medium`. Essa combinação foi testada para trabalhar bem com várias cargas de trabalho de visão de computação (incluindo uma versão grande do ResNet: ResNet-200) e fornece desempenho comparável ou melhor que uma instância `p2.xlarge`. Em seguida, você pode dimensionar a instância ou o tipo de acelerador dependendo dos objetivos de latência.
- Como os aceleradores do Amazon EI são anexados por meio da rede, a transferência de dados de entrada e saída entre a instância e o acelerador também é adicionada à latência da inferência. Usar um tamanho maior para a instância ou para o acelerador ou para ambos pode reduzir o tempo de transferência dos dados e, portanto, reduzir a latência de inferência geral.
- Se você carregar vários modelos em seu acelerador (ou o mesmo modelo de vários processos de aplicativos na instância), poderá ser necessário um acelerador de tamanho maior para as necessidades de computação e de memória no acelerador.
- É possível converter o modelo para precisão mista, que utiliza o FP16 TFLOPS mais alto do Amazon EI (para um determinado tamanho), para fornecer latência mais baixa e desempenho mais alto.

Uso do Amazon Elastic Inference com Auto Scaling do EC2

Ao criar um grupo do Auto Scaling, você pode especificar as informações necessárias para configurar as instâncias do Amazon EC2, incluindo os aceleradores do Amazon EI. Para configurar instâncias do

Auto Scaling com aceleradores do Amazon EI, você pode especificar um modelo de execução com a configuração da instância, junto com o tipo do acelerador do Amazon EI.

Como trabalhar com o Amazon EI

Depois de configurar e iniciar sua instância do EC2 com o Amazon EI, você pode usar aceleradores de Amazon EI nas versões do TensorFlow, do TensorFlow Serving e do Apache MXNet habilitadas para EI, com poucas alterações em seu código.

Tópicos

- [Configuração para iniciar o Amazon EC2 com Amazon EI \(p. 537\)](#)
- [Uso de modelos do TensorFlow com o Amazon EI \(p. 542\)](#)
- [Uso de modelos do MXNet com o Amazon EI \(p. 552\)](#)

Configuração para iniciar o Amazon EC2 com Amazon EI

Para executar uma instância e associá-la a um acelerador do Amazon EI, primeiro configure seus grupos de segurança e os serviços de endpoint do AWS PrivateLink. Em seguida, configure uma função de instância com a política do Amazon EI.

Tópicos

- [Configuração dos serviços de endpoint do AWS PrivateLink \(p. 537\)](#)
- [Configuração de seus grupos de segurança para o Amazon EI \(p. 538\)](#)
- [Configuração de uma função de instância com uma política do Amazon EI \(p. 539\)](#)
- [Execução de uma instância com o Amazon EI \(p. 541\)](#)

Configuração dos serviços de endpoint do AWS PrivateLink

O Amazon EI usa [VPC endpoints](#) para conectar a instância em sua VPC de forma privada com o acelerador do Amazon EI associado. Você deve criar um VPC endpoint para o Amazon EI antes de executar instâncias com aceleradores. Isso precisa ser feito apenas uma vez por VPC. Para obter mais informações, consulte [VPC endpoints da interface \(AWS PrivateLink\)](#).

Para configurar um Serviço de endpoint do AWS PrivateLink (console)

1. Abra o console de Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação à esquerda, escolha Endpoints, Create Endpoint (Criar endpoint).
3. Para Service category (Categoria do serviço), escolha Find service by name (Localizar serviço por nome).
4. Em Service Name (Nome do serviço), selecione com.amazonaws.<*your-region*>elastic-inference.runtime.

Por exemplo, na região us-west-2, selecione com.amazonaws.us-west-2.elastic-inference.runtim.

5. Em Subnets (Sub-redes), selecione uma ou mais zonas de disponibilidade nas quais o endpoint deve ser criado. Quando planejar executar instâncias com aceleradores, você deve selecionar sub-redes para a zona de disponibilidade.
6. Habilite o nome DNS privado e insira o grupo de segurança de seu endpoint. Escolha Create endpoint (Criar endpoint). Anote o ID do VPC endpoint para uso posterior.

- O grupo de segurança para o endpoint deve permitir o tráfego de entrada para a porta 443.

Para configurar um serviço de endpoint do AWS PrivateLink (AWS CLI)

- Use o comando `create-vpc-endpoint` e especifique o ID da VPC, o tipo do VPC endpoint (interface), o nome do serviço, as sub-redes que usarão o endpoint e os grupos de segurança associados às interfaces de rede do endpoint. Para obter informações sobre como configurar um grupo de segurança para o VPC endpoint, consulte [the section called “Configuração de seus grupos de segurança para o Amazon EI” \(p. 538\)](#).

```
aws ec2 create-vpc-endpoint --vpc-id vpc-insert VPC ID --vpc-endpoint-type Interface  
--service-name com.amazonaws.us-west-2.elastic-inference.runtime --subnet-id  
subnet-insert subnet --security-group-id sg-insert security group ID
```

Configuração de seus grupos de segurança para o Amazon EI

Você precisa de dois grupos de segurança: um para tráfego de entrada e saída para o novo VPC endpoint do Amazon EI e outro para o tráfego de saída das instâncias do EC2 associadas que você executa.

Configurar grupos de segurança para o Amazon EI

Para configurar um grupo de segurança para um acelerador do Amazon EI (console)

- Abra o console de Amazon VPC em <https://console.aws.amazon.com/vpc/>.
- No painel de navegação à esquerda, escolha Security (Segurança), Security Groups (Grupos de segurança), Create a Security Group (Criar um grupo de segurança).
- Em Create Security Group (Criar grupo de segurança), digite os valores nos campos e escolha Create (Criar).
- Escolha Close (Fechar).
- Selecione a caixa ao lado do grupo de segurança e escolha Inbound Rules (Regras de entrada).
- Selecione Edit rules (Editar regras).
- Escolha Add rule (Adicionar regra).
- Para permitir tráfego apenas na porta 443 de qualquer origem, ou do grupo de segurança ao qual você planeja associar a instância, em Type (Tipo), selecione HTTPS.
- Escolha Add rule (Adicionar regra).
- Selecione Save rules (Salvar regras).
- Escolha Outbound Rules (Regras de saída). Para permitir tráfego da porta 443 para qualquer destino, em Type (Tipo), selecione HTTPS.

Escolha Add rule (Adicionar regra).

Para permitir tráfego da porta 22 para a instância do EC2, em Type (Tipo), selecione SSH.

Escolha Add rule (Adicionar regra).

- Selecione Save rules (Salvar regras).
- Adicione uma regra de saída que restrinja o tráfego para o grupo de segurança do endpoint que você criou na etapa anterior ou que permita tráfego para HTTPS (porta 443 do TCP) para qualquer destino.
- Escolha Salvar.

Para configurar um grupo de segurança para um acelerador do Amazon EI (AWS CLI)

- Crie um grupo de segurança usando o comando `create-security-group`:

```
aws ec2 create-security-group  
--description insert a description for the security group  
--group-name assign a name for the security group  
[--vpc-id enter the VPC ID]
```

- Crie uma regra de entrada usando o comando `authorize-security-group-ingress`:

```
aws ec2 authorize-security-group-ingress --group-id insert the security group ID --  
group-name insert the name of the security group --protocol tcp  
--port 443
```

- Use o comando `authorize-security-group-egress` para criar uma regra de saída:

```
aws ec2 authorize-security-group-egress --group-id insert the security group ID --  
protocol tcp --port 443 --port 22 --cidr 0.0.0.0/0
```

Configuração de uma função de instância com uma política do Amazon EI

Para executar uma instância com um acelerador do Amazon EI, forneça uma [função do IAM](#) que permita ações nos aceleradores do Amazon EI.

Para configurar uma função de instância com uma política do Amazon EI (console)

- Abra o console do IAM em <https://console.aws.amazon.com/iam/>.
- No painel de navegação à esquerda, escolha Policies (Políticas), Create Policy (Criar política).
- Escolha a guia JSON e cole a política a seguir:

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "elastic-inference:Connect",  
                "iam>List*",  
                "iam:Get*",  
                "ec2:Describe*",  
                "ec2:Get*"  
            ],  
            "Resource": "*"  
        }  
    ]  
}
```

```
        }  
    ]  
}
```

Note

Você pode receber uma mensagem de aviso informando que o serviço de inferência elástica não está sendo reconhecido. Esse é um problema conhecido e não bloqueia a criação da política.

4. Escolha Review policy (Rever política) e insira um nome para a política, como `ec2-role-trust-policy.json` e uma descrição.
5. Escolha Create policy (Criar política).
6. No painel de navegação à esquerda, escolha Roles (Funções), Create Role (Criar função).
7. Escolha AWS service (Serviço da AWS), EC2, Next: Permissions (Próximo: permissões).
8. Selecione o nome da política que você acabou de criar (`ec2-role-trust-policy.json`). Escolha Next: Tags (Próximo: tags).
9. Forneça um nome de função e escolha Create Role (Criar função).

Ao criar a instância, selecione a função em Configure Instance Details (Configurar detalhes da instância) no assistente de execução.

Para configurar uma função de instância com uma política do Amazon EI (AWS CLI)

- Para configurar uma função de instância com uma política do Amazon EI, siga as etapas em [Criação de uma função do IAM](#). Adicione a seguinte política à sua instância:

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "elastic-inference:Connect",  
                "iam>List*",  
                "iam:Get*",  
                "ec2:Describe*",  
                "ec2:Get*"  
            ],  
            "Resource": "*"  
        }  
    ]
```

}

Note

Você pode receber uma mensagem de aviso informando que o serviço de inferência elástica não está sendo reconhecido. Esse é um problema conhecido e não bloqueia a criação da política.

Execução de uma instância com o Amazon EI

Agora você pode configurar instâncias do EC2 com aceleradores para execução em sua sub-rede. Você pode escolher qualquer tipo de instância do Amazon EC2 compatível e tamanho de acelerador do Amazon EI. Os aceleradores do Amazon EI estão disponíveis para todos os tipos de instância de geração atual. Há três tamanhos de aceleradores do Amazon EI para escolher:

- `eia1.medium` com 1 GB de memória de acelerador
- `eia1.large` com 2 GB de memória de acelerador
- `eia1.xlarge` com 4 GB de memória de acelerador

Para executar uma instância com o Amazon EI (console)

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. Escolha Launch Instance (Executar instância).
3. Em Choose an Amazon Machine Image (Escolher uma imagem de máquina da Amazon), selecione uma AMI do Amazon Linux ou do Ubuntu. Recomendamos uma das AMIs do deep learning.
4. Em Choose an Instance Type (Escolher um tipo de instância), selecione a configuração de hardware de sua instância.
5. Escolha Next: Configure Instance Details.
6. Em Configure Instance Details (Configurar os detalhes da instância), marque as definições da configuração. Confirme se você está usando a VPC com os grupos de segurança para a instância e o acelerador do Amazon EI que você configurou anteriormente. Para obter mais informações, consulte [Configuração de seus grupos de segurança para o Amazon EI \(p. 538\)](#).
7. Em IAM role (Função do IAM), selecione a função que você criou no procedimento [Configuração de uma função de instância com uma política do Amazon EI \(p. 539\)](#).
8. Selecione Add an Amazon EI accelerator (Adicionar um acelerador do Amazon EI).
9. Selecione o tamanho do acelerador do Amazon EI. Suas opções são: `eia1.medium`, `eia1.large` e `eia1.xlarge`.
10. (Opcional) Você pode optar por adicionar armazenamento e tags escolhendo Next (Avançar) na parte inferior da página. Ou pode deixar que o assistente de instância conclua as etapas de configuração restantes para você.
11. Reveja a configuração de sua instância e escolha Launch (Executar).
12. Você recebe um prompt para escolher um par de chaves existente para a instância ou para criar um novo par de chaves. Para obter mais informações, consulte [Pares de chaves do Amazon EC2](#).

Warning

Não selecione a opção Proceed without a key pair (Continuar sem um par de chaves). Se você executar a instância sem um par de chaves, você não poderá conectá-la.

13. Depois de fazer a seleção do par de chaves, escolha Launch instances (Executar instâncias).
14. Uma página de confirmação informa que sua instância está sendo executada. Para fechar a página de confirmação e retornar ao console, escolha View Instances (Visualizar instâncias).

15. Em Instances (Instâncias), você pode visualizar o status da execução. Demora um pouco para executar uma instância. Ao executar uma instância, seu estado inicial é pending. Depois que a instância é iniciada, seu estado muda para running.
16. Pode levar alguns minutos até que a instância esteja pronta para que você possa se conectar a ela. Verifique se a instância passou nas verificações de status. Você pode visualizar essas informações na coluna Status Checks (Verificações de status).

Para executar uma instância com o Amazon EI (AWS CLI)

Para executar uma instância com o Amazon EI na linha de comando, você precisa do nome do par de chaves, do ID da sub-rede, do ID do grupo de segurança, do ID da AMI e do nome do perfil da instância criada na seção [Configuração de uma função de instância com uma política do Amazon EI \(p. 539\)](#). Para o ID do grupo de segurança, use um que você tenha criado para a instância que contém o endpoint do AWS PrivateLink. Para obter mais informações, consulte [Configuração de seus grupos de segurança para o Amazon EI \(p. 538\)](#)). Para obter mais informações sobre o ID da AMI, consulte [Localização de uma AMI do Linux](#).

1. Use o comando `run-instances` para executar a instância e o acelerador:

```
aws ec2 run-instances --image-id ami-insert image ID --instance-type for example, m5.large --subnet-id insert your subnet ID --elastic-inference-accelerator Type=for example, eia1.large --key-name enter your key pair name --security-group-ids sg-enter your security group ID --iam-instance-profile Name="enter the name of your accelerator profile"
```

2. Quando a operação `run-instances` é bem-sucedida, a saída é semelhante à seguinte. O `ElasticInferenceAcceleratorArn` identifica o acelerador do Amazon EI.

```
"ElasticInferenceAcceleratorAssociations": [  
    {  
        "ElasticInferenceAcceleratorArn": "arn:aws:elastic-  
        inference:us-west-2:204044812891:elastic-inference-accelerator/  
        eia-3e1de7c2f64a4de8b970c205e838af6b",  
        "ElasticInferenceAcceleratorAssociationId": "eia-assoc-031f6f53ddcd5f260",  
        "ElasticInferenceAcceleratorAssociationState": "associating",  
        "ElasticInferenceAcceleratorAssociationTime": "2018-10-05T17:22:20.000Z"  
    }  
,
```

Agora você está pronto para executar seus modelos usando o TensorFlow ou o MXNet na AMI fornecida.

Uso de modelos do TensorFlow com o Amazon EI

A versão do TensorFlow e do TensorFlow Serving habilitada para Amazon EI permite que você use aceleradores de Amazon EI com alterações mínimas em seu código do TensorFlow. Os pacotes habilitados para Amazon EI estão disponíveis no AWS Deep Learning AMI. Você também pode fazer download dos pacotes a partir do [Bucket do Amazon S3](#) para criá-los em suas próprias AMIs do Amazon Linux ou do Ubuntu ou em contêineres do Docker.

Com o TensorFlow Serving do Amazon EI, a interface do TensorFlow Serving padrão permanece inalterada. A única diferença é que o ponto de entrada é um binário diferente denominado amazonei_tensorflow_model_server.

Para obter mais informações, consulte [TensorFlow Serving](#).

Os pacotes do TensorFlow de Amazon EI para Python 2 e 3 fornecem uma API EIPredictor. Essa função de API fornece uma maneira flexível de executar modelos no EI como uma alternativa ao uso do TensorFlow Serving.

Esta versão do TensorFlow Serving do Amazon EI foi testada para executar bem e fornecer benefícios de economia de custo com os seguintes casos de uso de deep learning e arquiteturas de rede (e variantes semelhantes):

Caso de uso	Topologia de rede de exemplo
Reconhecimento de imagens	Inception, ResNet, MVCNN
Detecção de objetos	SSD, RCNN
Tradução neural de máquina	GNMT

Tópicos

- [Exemplo do TensorFlow Serving de Amazon EI \(p. 543\)](#)
- [TensorFlow Predictor de Amazon EI \(p. 546\)](#)
- [Exemplo do TensorFlow Predictor de Amazon EI \(p. 548\)](#)
- [Requisitos e considerações adicionais \(p. 552\)](#)

Exemplo do TensorFlow Serving de Amazon EI

Veja a seguir um exemplo que você pode experimentar para fornecer diferentes modelos, como o ResNet, usando um Single Shot Detector (SSD). Como regra geral, você precisa de um modelo que pode ser fornecido e scripts de cliente que já foram obtidos por download na DLAMI.

Ativar o ambiente de inferência elástica do TensorFlow

- Se você estiver usando a Deep Learning AMI da AWS, ative o ambiente de TensorFlow Python 2.7. Os scripts de exemplo não são compatíveis com Python 3.x.

```
source activate amazonei_tensorflow_p27
```

Atenda e teste a inferência com um modelo de início

1. Faça download do modelo.

```
curl -O https://s3-us-west-2.amazonaws.com/aws-tf-serving-ei-example/ssd_resnet.zip
```

2. Descompacte o modelo.

```
unzip ssd_resnet.zip -d /tmp
```

3. Faça download de uma imagem de três cachorros para seu diretório inicial.

```
curl -O https://raw.githubusercontent.com/awslabs/mxnet-model-server/master/docs/images/3dogs.jpg
```

4. Navegue até a pasta onde o AmazonEI_TensorFlow_Serving está instalado e execute o seguinte comando para executar o servidor. Observe que, "model_base_path" deve ser um caminho absoluto.

```
AmazonEI_TensorFlow_Serving_v1.12_v1 --model_name=ssdresnet --model_base_path=/tmp/ssd_resnet50_v1_coco --port=9000
```

5. Enquanto o servidor estiver em execução no primeiro plano, execute outra sessão de terminal. Abra um novo terminal e ative o ambiente do TensorFlow.

```
source activate amazonei_tensorflow_p27
```

6. Use o editor de texto de sua preferência para criar um script com o conteúdo a seguir. Chame-o de `ssd_resnet_client.py`. Esse script usará um nome de arquivo de imagem como um parâmetro e obterá o resultado da previsão do modelo pré-treinado.

```
from __future__ import print_function

import grpc

import tensorflow as tf

from PIL import Image

import numpy as np

import time

import os

from tensorflow_serving.apis import predict_pb2

from tensorflow_serving.apis import prediction_service_pb2_grpc


tf.app.flags.DEFINE_string('server', 'localhost:9000',
                           'PredictionService host:port')

tf.app.flags.DEFINE_string('image', '', 'path to image in JPEG format')

FLAGS = tf.app.flags.FLAGS

if(FLAGS.image == ''):

    print("Supply an Image using '--image [path/to/image]''")

    exit(1)


coco_classes_txt = "https://raw.githubusercontent.com/amikelive/coco-labels/master/coco-labels-paper.txt"

local_coco_classes_txt = "/tmp/coco-labels-paper.txt"

# Downloading coco labels
```

```
os.system("curl -o %s -O %s" % (local_coco_classes_txt, coco_classes_txt))

# Setting default number of predictions

NUM_PREDICTIONS = 20

# Reading coco labels to a list

with open(local_coco_classes_txt) as f:

    classes = ["No Class"] + [line.strip() for line in f.readlines()]

    # Iterating over the predictions. The first inference request can take several
    # seconds to complete

    for curpred in range(NUM_PREDICTIONS):

        if(curpred == 0):

            print("The first inference request loads the model into the accelerator and can
            take several seconds to complete. Please standby!")

        # Start the timer

        start_time = time.time()

        # Setting up the prediction request

        request = predict_pb2.PredictRequest()

        # Setting the model spec name

        request.model_spec.name = 'ssdresnet'

        # Setting up the inputs and tensors from image data

        request.inputs['inputs'].CopyFrom(
            tf.contrib.util.make_tensor_proto(data, shape=data.shape))

        # Making the prediction request

        response = stub.Predict(request, timeout=10)

        # Getting the prediction results

        predictions = response.outputs['outputs'].float_val

        # Iterating over the predictions

        for pred in predictions:
```

```
start = time.time()

# This is where the inference actually happens

result = stub.Predict(request, 60.0) # 10 secs timeout

print("Inference %d took %f seconds" % (curpred, time.time()-start))

# Extracting results from output

outputs = result.outputs

detection_classes = outputs["detection_classes"]

# Creating an ndarray from the output TensorProto

detection_classes = tf.make_ndarray(detection_classes)

# Getting the number of objects detected in the input image from the output of the predictor

num_detections = int(tf.make_ndarray(outputs["num_detections"])[0])

print("%d detection[s]" % (num_detections))

# Getting the class ids from the output and mapping the class ids to class names from the coco labels

class_label = [classes[int(x)]

                for x in detection_classes[0][:num_detections]]

print("SSD Prediction is ", class_label)

if __name__ == '__main__':
    tf.app.run()
```

7. Agora execute o script passando o local do servidor, a porta e o nome do arquivo da fotografia do cachorro como parâmetros.

```
python ssd_resnet_client.py --server=localhost:9000 --image 3dogs.jpg
```

TensorFlow Predictor de Amazon EI

A API EI Predictor fornece uma interface simples para realizar inferências repetidas em um modelo pré-treinado. O exemplo de código a seguir mostra os parâmetros disponíveis.

```
ei_predictor = EIPredictor(model_dir,
                            signature_def_key=None,
                            signature_def=None,
                            input_names=None,
```

```
        output_names=None,  
  
        tags=None,  
  
        graph=None,  
  
        config=None,  
  
        use_ei=True)  
  
output_dict = ei_predictor(feed_dict)
```

Assim, o uso do EI Predictor é semelhante ao do TensorFlow Predictor para um [modelo salvo](#). O EI Predictor pode ser usado das seguintes maneiras:

```
//EI Predictor class picks inputs and outputs from default serving signature def with tag  
"serve". (similar to TF predictor)  
  
ei_predictor = EIPredictor(model_dir)  
  
//EI Predictor class picks inputs and outputs from the signature def picked using the  
signtaure_def_key (similar to TF predictor)  
  
ei_predictor = EIPredictor(model_dir, signature_def_key='predict')  
  
// Signature_def can be provided directly (similar to TF predictor)  
  
ei_predictor = EIPredictor(model_dir, signature_def= sig_def)  
  
// You provide the input_names and output_names dict.  
// similar to TF predictor  
  
ei_predictor = EIPredictor(model_dir,  
                           input_names,  
                           output_names)  
  
// tag is used to get the correct signature def. (similar to TF predictor)  
ei_predictor = EIPredictor(model_dir, tags='serve')
```

A funcionalidade adicional do EI Predictor inclui:

- Suporte para modelos congelados.

```
// For Frozen graphs, model_dir takes a file name , input_names and output_names  
// input_names and output_names should be provided in this case.  
ei_predictor = EIPredictor(model_dir,
```

```
    input_names=None,  
  
    output_names )
```

- Capacidade de desativar o uso de EI usando o sinalizador `use_ei`, cujo padrão é `True`. Isso é útil para testar o EIPredictor em relação ao TensorFlow Predictor.
- Capacidade de criar o EIPredictor a partir de um TensorFlow Estimator. Considerando um Estimator treinado, você pode exportar primeiro um SavedModel. Consulte a [documentação SavedModel](#) para obter mais detalhes. Veja a seguir um exemplo de uso:

```
saved_model_dir = estimator.export_savedmodel(my_export_dir, serving_input_fn)  
  
ei_predictor = EIPredictor(export_dir=saved_model_dir)  
  
// Once the EIPredictor is created, inference is done using the following:  
  
output_dict = ei_predictor(feed_dict)
```

Exemplo do TensorFlow Predictor de Amazon EI

Como instalar o TensorFlow de Amazon EI

O TensorFlow habilitado para EI vem incluído nas Deep Learning AMIs. Você também pode fazer download do pip wheels para o Python 2 e 3 do bucket do S3 de Amazon EI. Siga estas instruções para fazer download e instalar o pacote pip:

Escolha o pip wheel para a versão Python e o sistema operacional de sua escolha no [bucket do S3](#). Copie o caminho para o pip wheel e execute o seguinte comando:

```
curl -O [URL of the pip wheel of your choice]
```

Para instalar o pip wheel:

```
pip install [path to downloaded wheel]
```

Tente o exemplo a seguir para fornecer diferentes modelos, como o ResNet, usando um SSD. Como regra geral, você precisa de um script de modelo e cliente que pode ser fornecido obtido por download na Deep Learning AMI (DLAMI) antes de prosseguir.

Fornecer e testar a inferência com um modelo de SSD

1. Faça download do modelo. Se você já fez o download do modelo no exemplo do Serving, ignore esta etapa.

```
curl -O https://s3-us-west-2.amazonaws.com/aws-tf-serving-ei-example/ssd_resnet.zip
```

2. Descompacte o modelo. Mais uma vez, você pode ignorar esta etapa se já tiver o modelo.

```
unzip ssd_resnet.zip -d /tmp
```

3. Faça download de uma imagem de três cachorros para seu diretório atual.

```
curl -O https://raw.githubusercontent.com/awslabs/mxnet-model-server/master/docs/images/3dogs.jpg
```

4. Abra um editor de texto, como o vim, e cole o script de inferência a seguir. Salve o arquivo como `ssd_resnet_predictor.py`.

```
from __future__ import absolute_import
from __future__ import division
from __future__ import print_function

import os
import sys
import numpy as np
import tensorflow as tf
import matplotlib.image as mpimg
import time

from tensorflow.contrib.ei.python.predictor.ei_predictor import EIPredictor

tf.app.flags.DEFINE_string('image', '', 'path to image in JPEG format')
FLAGS = tf.app.flags.FLAGS

if(FLAGS.image == ''):

    print("Supply an Image using '--image [path/to/image]'")
    exit(1)

coco_classes_txt = "https://raw.githubusercontent.com/amikelive/coco-labels/master/coco-labels-paper.txt"
local_coco_classes_txt = "/tmp/coco-labels-paper.txt"

# Downloading coco labels
os.system("curl -o %s -O %s" % (local_coco_classes_txt, coco_classes_txt))

# Setting default number of predictions
NUM_PREDICTIONS = 20

# Reading coco labels to a list
with open(local_coco_classes_txt) as f:

    classes = ["No Class"] + [line.strip() for line in f.readlines()]

def main(_):

    # Reading the test image given by the user
    img = mpimg.imread(FLAGS.image)
```

```
# Setting batch size to 1
img = np.expand_dims(img, axis=0)

# Setting up EIPredictor Input
ssd_resnet_input = {'inputs': img}

print('Running SSD Resnet on EIPredictor using specified input and outputs')

# This is the EIPredictor interface, using specified input and outputs

eia_predictor = EIPredictor(

    # Model directory where the saved model is located
    model_dir='/tmp/ssd_resnet50_v1_coco/1/',

    # Specifying the inputs to the Predictor
    input_names={"inputs": "image_tensor:0"},

    # Specifying the output names to tensor for Predictor
    output_names={"detection_classes": "detection_classes:0", "num_detections": "num_detections:0",

                  "detection_boxes": "detection_boxes:0"},

    )

pred = None

# Iterating over the predictions. The first inference request can take several
seconds to complete

for curpred in range(NUM_PREDICTIONS):

    if(curdet == 0):

        print("The first inference request loads the model into the accelerator and can
take several seconds to complete. Please standby!")

        # Start the timer
        start = time.time()

        # This is where the inference actually happens
        pred = eia_predictor(ssd_resnet_input)

        print("Inference %d took %f seconds" % (curpred, time.time()-start))

    # Getting the number of objects detected in the input image from the output of the
    predictor
    num_detections = int(pred["num_detections"])

    print("%d detection[s]" % (num_detections))
```

```
# Getting the class ids from the output
detection_classes = pred["detection_classes"][0][:num_detections]

# Mapping the class ids to class names from the coco labels
print([classes[int(i)] for i in detection_classes])

print('Running SSD Resnet on EIPredictor using default Signature Def')

# This is the EIPredictor interface using the default Signature Def
eia_predictor = EIPredictor(
    # Model directory where the saved model is located
    model_dir='/tmp/ssd_resnet50_v1_coco/1/',
)

# Iterating over the predictions. The first inference request can take several
seconds to complete
for curpred in range(NUM_PREDICTIONS):
    if(curpred == 0):
        print("The first inference request loads the model into the accelerator and can
take several seconds to complete. Please standby!")

        # Start the timer
        start = time.time()

        # This is where the inference actually happens
        pred = eia_predictor(ssd_resnet_input)

        print("Inference %d took %f seconds" % (curpred, time.time()-start))

    # Getting the number of objects detected in the input image from the output of the
predictor
    num_detections = int(pred["num_detections"])

    print("%d detection[s]" % (num_detections))

    # Getting the class ids from the output
    detection_classes = pred["detection_classes"][0][:num_detections]

    # Mapping the class ids to class names from the coco labels
    print([classes[int(i)] for i in detection_classes])
```

```
if __name__ == "__main__":
    tf.app.run()
```

5. Execute o script de inferência.

```
python ssd_resnet_predictor.py --image 3dogs.jpg
```

Para obter mais tutoriais e exemplos, consulte a [API do Python do TensorFlow](#).

Requisitos e considerações adicionais

Formatos de modelos compatíveis

O Amazon EI oferece suporte ao formato saved-model do TensorFlow por meio do TensorFlow Serving.

Requisito do OpenSSL

O TensorFlow Serving do Amazon EI exige o OpenSSL para autenticação do IAM. O OpenSSL é pré-instalado no AWS Deep Learning AMI. Se estiver criando sua própria AMI ou contêiner do Docker, instale o OpenSSL.

- Comando para instalar o OpenSSL para Ubuntu:

```
sudo apt-get install libssl-dev
```

- Comando para instalar o OpenSSL para Amazon Linux:

```
sudo yum install openssl-devel
```

Aquecimento

O TensorFlow Serving do Amazon EI fornece um recurso de [aquecimento](#) para pré-carregar modelos e reduzir o atraso que é normal na primeira solicitação de inferência. O TensorFlow Serving do Amazon Elastic Inference só oferece suporte ao aquecimento da definição de assinatura "fault-finders".

Definições de assinaturas

O uso de várias [definições de assinaturas](#) pode ter um efeito multiplicativo na quantidade de memória consumida do acelerador. Para exercitar mais de uma definição de assinatura para suas chamadas de inferência, teste estes cenários ao determinar o tipo de acelerador para seu aplicativo.

Para modelos grandes, o EI tende a ter uma sobrecarga de memória maior. Isso pode levar a um erro de falta de memória. Se você receber esse erro, tente mudar para um tipo de Acelerador EI superior.

Uso de modelos do MXNet com o Amazon EI

A versão do Apache MXNet habilitada para o Amazon Elastic Inference permite que você use o Amazon EI perfeitamente, com poucas alterações em seu código do MXNet. Você pode usar o Amazon EI com as seguintes operações da API do MXNet:

- API MXNet Python Symbol
- API MXNet Python Module

Tópicos

- [Instalar o Apache MXNet habilitado para Amazon EI \(p. 553\)](#)
- [Ativar o ambiente MXNet de Amazon EI \(p. 553\)](#)
- [Usar o Amazon EI com a API MXNet Symbol \(p. 553\)](#)
- [Usar o Amazon EI com a API MXNet Module \(p. 555\)](#)
- [Requisitos e considerações adicionais \(p. 557\)](#)

Instalar o Apache MXNet habilitado para Amazon EI

O Apache MXNet habilitado para Amazon EI está disponível no AWS Deep Learning AMI. Um pacote 'pip' também está disponível no [Amazon S3](#) para que você possa criá-lo em suas próprias AMIs do Amazon Linux ou do Ubuntu ou em contêineres do Docker.

Ativar o ambiente MXNet de Amazon EI

Se você estiver usando a Deep Learning AMI da AWS, ative o ambiente de Amazon EI do Python 3 MXNet ou o ambiente de Amazon EI do Python 2 MXNet, dependendo da sua versão do Python.

Para o Python 3:

```
source activate amazonei_mxnet_p36
```

Para o Python 2:

```
source activate amazonei_mxnet_p27
```

Usar o Amazon EI com a API MXNet Symbol

Passe `mx.eia()` como o contexto em uma chamada para os métodos `simple_bind()` ou `bind()`. Para obter mais informações, consulte [API Symbol](#).

O exemplo a seguir chama o método `simple_bind()`.

```
import mxnet as mx

data = mx.sym.var('data', shape=(1,))
sym = mx.sym.exp(data)

# Pass mx.eia() as context during simple bind operation

executor = sym.simple_bind(ctx=mx.eia(), grad_req='null')
for i in range(10):

    # Forward call is performed on remote accelerator
    executor.forward()

    print('Inference %d, output = %s' % (i, executor.outputs[0]))
```

O exemplo a seguir chama o método bind().

```
import mxnet as mx

a = mx.sym.Variable('a')

b = mx.sym.Variable('b')

c = 2 * a + b

# Even for execution of inference workloads on eia,
# context for input ndarrays to be mx.cpu()

a_data = mx.nd.array([1,2], ctx=mx.cpu())

b_data = mx.nd.array([2,3], ctx=mx.cpu())

# Then in the bind call, use the mx.eia() context

e = c.bind(mx.eia(), {'a': a_data, 'b': b_data})

# Forward call is performed on remote accelerator

e.forward()
```

O exemplo a seguir chama o método bind() em um modelo real pré-treinado (Resnet-50) da API Symbol:

```
import mxnet as mx

import numpy as np


path='http://data.mxnet.io/models/imagenet/'

[mx.test_utils.download(path+'resnet/50-layers/resnet-50-0000.params'),
mx.test_utils.download(path+'resnet/50-layers/resnet-50-symbol.json'),
mx.test_utils.download(path+'synset.txt')]

ctx = mx.eia()

with open('synset.txt', 'r') as f:

    labels = [l.rstrip() for l in f]

sym, args, aux = mx.model.load_checkpoint('resnet-50', 0)

fname = mx.test_utils.download('https://github.com/dmlc/web-data/blob/master/mxnet/doc/tutorials/python/predict_image/cat.jpg?raw=true')

img = mx.image.imread(fname)
```

```
# convert into format (batch, RGB, width, height)

img = mx.image.imresize(img, 224, 224) # resize

img = img.transpose((2, 0, 1)) # Channel first

img = img.expand_dims(axis=0) # batchify

img = img.astype(dtype='float32')

args['data'] = img


softmax = mx.nd.random_normal(shape=(1,))

args['softmax_label'] = softmax


exe = sym.bind(ctx=ctx, args=args, aux_states=aux, grad_req='null')


exe.forward()

prob = exe.outputs[0].asnumpy()

# print the top-5

prob = np.squeeze(prob)

a = np.argsort(prob)[::-1]

for i in a[0:5]:

    print('probability=%f, class=%s' %(prob[i], labels[i]))
```

Usar o Amazon EI com a API MXNet Module

Ao criar o objeto `Module`, passe `mx.eia()` como o contexto. Para obter mais informações, consulte [API Module](#).

Para usar a API MXNet Module, você pode usar os seguintes comandos:

```
# Load saved model

sym, arg_params, aux_params = mx.model.load_checkpoint(model_path, EPOCH_NUM)


# Pass mx.eia() as context while creating Module object

mod = mx.mod.Module(symbol=sym, context=mx.eia())


# Only for_training = False is supported for eia

mod.bind(for_training=False, data_shapes=data_shape)

mod.set_params(arg_params, aux_params)
```

```
# Forward call is performed on remote accelerator  
  
mod.forward(data_batch)
```

O exemplo a seguir usa o Amazon EI com a API Module em um modelo real pré-treinado (Resnet-152):

```
import mxnet as mx  
  
import numpy as np  
  
from collections import namedtuple  
  
Batch = namedtuple('Batch', ['data'])  
  
  
path='http://data.mxnet.io/models/imagenet/'  
  
[mx.test_utils.download(path+'resnet/152-layers/resnet-152-0000.params'),  
 mx.test_utils.download(path+'resnet/152-layers/resnet-152-symbol.json'),  
 mx.test_utils.download(path+'synset.txt')]  
  
  
ctx = mx.eia()  
  
  
sym, arg_params, aux_params = mx.model.load_checkpoint('resnet-152', 0)  
mod = mx.mod.Module(symbol=sym, context=ctx, label_names=None)  
mod.bind(for_training=False, data_shapes=[('data', (1,3,224,224))],  
         label_shapes=mod._label_shapes)  
mod.set_params(arg_params, aux_params, allow_missing=True)  
  
with open('synset.txt', 'r') as f:  
    labels = [l.rstrip() for l in f]  
  
  
fname = mx.test_utils.download('https://github.com/dmlc/web-data/blob/master/mxnet/doc/tutorials/python/predict_image/cat.jpg?raw=true')  
img = mx.image.imread(fname)  
  
  
# convert into format (batch, RGB, width, height)  
img = mx.image.imresize(img, 224, 224) # resize  
img = img.transpose((2, 0, 1)) # Channel first  
img = img.expand_dims(axis=0) # batchify
```

```
mod.forward(Batch([img]))  
  
prob = mod.get_outputs()[0].asnumpy()  
  
# print the top-5  
  
prob = np.squeeze(prob)  
  
a = np.argsort(prob)[::-1]  
  
for i in a[0:5]:  
  
    print('probability=%f, class=%s' %(prob[i], labels[i]))
```

Esta versão do Apache MXNet do Amazon EI foi testada para executar bem e fornecer benefícios de economia de custo com os seguintes casos de uso de deep learning e arquiteturas de rede (e variantes semelhantes):

Caso de uso	Topologia de rede de exemplo
Reconhecimento de imagens	Inception, ResNet, VGG, ResNext
Detecção de objetos	SSD
Texto para fala	WaveNet

Requisitos e considerações adicionais

- O Apache MXNet do Amazon EI é criado com o MKLDNN. Portanto, todas as operações são compatíveis ao usar o contexto `mx.cpu()`. O contexto `mx.gpu()` não é compatível, portanto, nenhuma operação pode ser executada na GPU local.
- No momento, o Amazon EI não tem suporte para o modo MXNet Imperative ou para a API MXNet Gluon.
- No momento, o `mx.eia()` não fornece a funcionalidade total de um contexto do MXNet. Não é possível alocar memória para NDArray no acelerador do Amazon EI gravando algo como: `x = mx.nd.array([[1, 2], [3, 4]], ctx=mx.eia())` Isso resulta em um erro. Em vez disso, você deve usar: `x = mx.nd.array([[1, 2], [3, 4]], ctx=mx.cpu())`. O MXNet transfere os dados automaticamente para o acelerador conforme necessário.
- Porque o Amazon EI só oferece suporte à inferência, ao método `backward()` ou às chamadas para `bind()` com `for_training=True`. Como o valor padrão de `for_training` é `True`, defina `for_training=False`.

Uso das métricas do CloudWatch para monitorar o Amazon EI

É possível monitorar os aceleradores do Amazon EI usando o Amazon CloudWatch que coleta métricas sobre uso e desempenho. Essas estatísticas são registradas por um período de duas semanas para que você possa acessar informações históricas e obter uma perspectiva melhor de como está o desempenho do serviço.

Por padrão, o Amazon EI envia dados de métrica ao CloudWatch em períodos de 5 minutos.

Para obter mais informações, consulte o [Guia do usuário do Amazon CloudWatch](#).

Tópicos

- [Métricas e dimensões do Amazon EI \(p. 558\)](#)
- [Criação de alarmes do CloudWatch para monitorar o Amazon EI \(p. 559\)](#)

Métricas e dimensões do Amazon EI

As métricas são agrupadas primeiro pelo namespace do serviço e, em seguida, por várias combinações de dimensão dentro de cada namespace. Você pode usar os procedimentos a seguir para visualizar as métricas para o Amazon EI.

Para visualizar as métricas 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 o Amazon EI reside. Para obter mais informações, consulte [Regiões e endpoints](#).
3. No painel de navegação, selecione Métricas.
4. Em All metrics, selecione uma categoria de métricas, em seguida role para visualizar a lista completa de métricas.

Para visualizar as métricas (AWS CLI)

- Em um prompt de comando, digite o seguinte comando:

```
aws cloudwatch list-metrics --namespace " AWS/ElasticInference "
```

O CloudWatch exibe as seguintes métricas para o Amazon EI.

Métrica	Descrição
AcceleratorHealthCheckFailed	Informa se o acelerador do Amazon EI passou em uma verificação de integridade de status no último minuto. Valor de zero (0) indica que a verificação de status passou. Um valor de um (1) uma falha na verificação de status. Unidade: contagem
ConnectivityCheckFailed	Informa se a conectividade com o acelerador do Amazon EI está ativa ou falhou no último minuto. Um valor de zero (0) indica que a conexão está ativa. Um valor de um (1) uma falha de conectividade. Unidade: contagem

Métrica	Descrição
AcceleratorMemoryUsage	A memória do acelerador do Amazon EI usada no último minuto. Unidade: bytes

Você pode filtrar os dados do Amazon EI usando as dimensões a seguir.

Dimensão	Descrição
ElasticInferenceAcceleratorId	Esta dimensão filtra os dados pelo acelerador do Amazon EI.
InstanceId	Esta dimensão filtra os dados pela instância à qual o acelerador do Amazon EI está anexado.

Criação de alarmes do CloudWatch para monitorar o Amazon EI

Você pode criar um alarme do CloudWatch que envia uma mensagem de Amazon SNS quando o alarme mudar de estado. Um alarme observa uma única métrica por um período tempo que você especifica. Ele envia uma notificação a um tópico do SNS com base no valor da métrica em relação a um limite especificado em um número de períodos.

Por exemplo, você pode criar um alarme que monitora a integridade de um acelerador do Amazon EI. Ele envia uma notificação quando o acelerador do Amazon EI falha em uma verificação de integridade por três períodos de cinco minutos consecutivos.

Para criar um alarme para o status de integridade de um acelerador do Amazon EI

1. Abra o console do CloudWatch em <https://console.aws.amazon.com/cloudwatch/>.
2. No painel de navegação, escolha Alarms, Create Alarm.
3. Escolha Amazon EI Metrics (Métricas do Amazon EI).
4. Selecione o Amazon EI e a métrica AcceleratorHealthCheckFailed e escolha Next (Avançar).
5. Siga as instruções a seguir para configurar o alarme e, em seguida, escolha Create Alarm (Criar alarme):
 - Em Alarm Threshold (Limite do alarme), insira um nome e uma descrição. Em Whenever (Sempre), escolha => e digite 1. Para os períodos consecutivos, digite 3.
 - Em Actions (Ações), selecione uma lista de notificações existente ou escolha New list (Nova lista).
 - Em Alarm Preview, selecione um período de 5 minutos.

Solução de problemas

Veja a seguir erros comuns e etapas de solução de problemas.

Tópicos

- [Problemas na execução de aceleradores \(p. 560\)](#)
- [Resolver problemas de configuração \(p. 560\)](#)
- [Resolução de problemas de conectividade \(p. 560\)](#)
- [Como resolver problemas de status não íntegro \(p. 560\)](#)
- [Parar e iniciar a instância \(p. 560\)](#)
- [Solução de problemas de desempenho de modelos \(p. 561\)](#)
- [Como enviar comentários \(p. 561\)](#)

Problemas na execução de aceleradores

Verifique se você está executando em uma região onde os aceleradores do Amazon EI estão disponíveis. Para obter mais informações, consulte a [Tabela de regiões](#).

Resolver problemas de configuração

Se você iniciou sua instância com a Deep Learning AMI (DLAMI), execute `python ~/anaconda3/bin/EISetupValidator.py` para verificar se a instância está configurada corretamente para usar o serviço do Amazon EI. Ou você pode fazer download do [script](#) e executar '`python EISetupValidator.py`'.

Resolução de problemas de conectividade

Se não for possível conectar-se com êxito aos aceleradores, verifique se você concluiu o seguinte:

- Configurou um VPC endpoint para o Amazon EI para a sub-rede na qual você executou a instância.
- Configurou grupos de segurança para a instância e os VPC endpoints com regras de saída que permitem comunicação por HTTPS (porta 443). Configurou o grupo de segurança do VPC endpoint com uma regra de saída que permite tráfego HTTPS.
- Adicionou uma função de instância do IAM com a permissão "elastic-inference:Connect" à instância da qual você está se conectando ao acelerador.
- Marcou o CloudWatch Logs para verificar se o acelerador está íntegro. Os detalhes da instância do EC2 no console do Amazon EC2 contêm um link para o CloudWatch que permite visualizar a integridade do acelerador associado.

Como resolver problemas de status não íntegro

Se o acelerador do Amazon EI estiver em um estado não íntegro, você poderá usar as etapas de solução de problemas a seguir para resolver o problema.

Parar e iniciar a instância

Se o acelerador do Amazon EI estiver em um estado não íntegro, parar a instância e iniciá-la novamente é a opção mais simples. Para obter mais informações, consulte [Interrupção e início das suas instâncias \(p. 460\)](#).

Warning

Quando você interrompe uma instância, os dados em todos os volumes de armazenamento de instâncias são apagados. Se você tiver dados para preservação em volumes de armazenamento de instância, faça backup deles em armazenamento persistente.

Solução de problemas de desempenho de modelos

O Amazon EI acelera operações definidas por estruturas, como o TensorFlow e o MXNet. Embora o Amazon EI acelere a maioria dos operadores de rede neural, matemática, manipulação de matrizes e fluxos de controle, há muitos operadores que o Amazon EI não acelera. Esses incluem os operadores relacionados a treinamento, operadores de entrada/saída e alguns operadores em contrib.

Quando um modelo contém operadores que o Amazon EI não acelera, a estrutura os executa na instância. A frequência e o local desses operadores em um gráfico de modelo podem ter um impacto no desempenho da inferência de modelos com aceleradores do Amazon EI. Se você souber que seu modelo se beneficia da aceleração de GPU, mas não desempenha bem no Amazon EI, entre em contato com o AWS Support ou com o amazon-ei-feedback@amazon.com.

Como enviar comentários

Entre em contato com o AWS Support ou envie comentários para: amazon-ei-feedback@amazon.com.

Monitoramento do Amazon EC2

O monitoramento é uma parte importante para manter a confiabilidade, a disponibilidade e o desempenho de suas instâncias do Amazon Elastic Compute Cloud (Amazon EC2) e outras soluções da AWS. Você deve coletar dados de monitoramento de todas as partes de suas soluções da AWS para ser mais fácil realizar 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 o desempenho normal do Amazon EC2 em seu ambiente. Você deve medir o desempenho do Amazon EC2 em vários momentos e em condições diferentes de carga. Ao monitorar o Amazon EC2, você deve armazenar um histórico de dados de monitoramento coletados. Você poderá comparar o desempenho atual do Amazon EC2 com esses dados históricos para ajudá-lo a identificar padrões de desempenho normais e anomalias de desempenho, 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 o desempenho estiver fora da linha de base estabelecida, talvez seja necessário reconfigurar ou otimizar a instância para reduzir a utilização da CPU, melhorar a E/S de disco ou reduzir o tráfego de rede.

Para estabelecer uma linha de base, é preciso, no mínimo, monitorar os seguintes itens:

Item a ser monitorado	Métrica do Amazon EC2	Monitoramento do agente/ CloudWatch Logs
Utilização da CPU	CPUUtilization (p. 577)	
Utilização da rede	NetworkIn (p. 577) NetworkOut (p. 577)	
Desempenho do disco	DiskReadOps (p. 577) DiskWriteOps (p. 577)	
Leituras/gravações de disco	DiskReadBytes (p. 577) DiskWriteBytes (p. 577)	
Utilização de memória, utilização de troca de disco, utilização de espaço em disco, utilização de arquivo de páginas, coleção de logs		[Instâncias Linux e Windows Server] Colecionar métricas e logs das instâncias do Amazon EC2 e servidores locais com o agente do CloudWatch [Migração de agentes anteriores do CloudWatch Logs em

Item a ser monitorado	Métrica do Amazon EC2	Monitoramento do agente/ CloudWatch Logs
		instâncias do Windows Server] Migrar coleção de logs da instância Windows Server para o agente do CloudWatch

Monitoramento automático e manual

A AWS fornece várias ferramentas que você pode usar para monitorar o Amazon EC2. Você pode configurar algumas dessas ferramentas para fazer o monitoramento em seu lugar, e, ao mesmo tempo, algumas das ferramentas exigem intervenção manual.

Tópicos

- [Ferramentas de monitoramento automatizadas \(p. 563\)](#)
- [Ferramentas de monitoramento manual \(p. 564\)](#)

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 sua instância a fim de garantir que eles estejam funcionando corretamente. Essas verificações detectam problemas com sua instância que exigem a participação da AWS para repará-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 suas instâncias \(p. 565\)](#).

- Instance Status Checks (Verificações do status da instância) – monitore o software e a configuração de rede de sua 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 da inicialização ou da rede
 - Memória exaurida
 - Sistema de arquivos corrompido
 - Kernel incompatível

Para obter mais informações, consulte [Verificações de status para suas instâncias \(p. 565\)](#).

- 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 um 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 alarmes invocam ações apenas para alterações de estado sustentado. 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 [Monitoramento das suas instâncias usando o CloudWatch \(p. 575\)](#).

- Eventos do Amazon CloudWatch – automatiza os serviços da AWS e responde automaticamente a eventos do sistema. Os eventos dos serviços da AWS são entregues ao Eventos do CloudWatch 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 Eventos do Amazon CloudWatch?](#)
- Amazon CloudWatch Logs – monitore, armazene e acesse seus arquivos de log de instâncias do Amazon EC2, do AWS CloudTrail ou de outras origens. Para obter mais informações, consulte [O que é o Amazon CloudWatch Logs?](#)
- Scripts de monitoramento do Amazon EC2 – scripts Perl que podem monitorar a memória, o disco e o uso de arquivos de troca em suas instâncias. Para obter mais informações, consulte [Monitoramento de métricas de memória e disco para instâncias Linux do Amazon EC2](#).
- 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 seus recursos da AWS. Para obter mais informações, consulte [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 de 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 alertas para ser notificado sobre problemas
- Consultar visões gerais rápidas de seus 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 de sua solução da AWS para ser mais fácil realizar 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.

Monitoramento do status de suas 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.

Você também pode ver o status de eventos específicos programados para suas instâncias. Os eventos fornecem informações sobre atividades futuras, como reinicialização ou retirada, que estão planejadas para suas instâncias, além da hora de início e fim programada de cada evento.

Tópicos

- [Verificações de status para suas instâncias \(p. 565\)](#)
- [Eventos programados para suas instâncias \(p. 570\)](#)

Verificações de status para suas instâncias

Com o monitoramento do status da instância, você pode determinar rapidamente se Amazon EC2 detectou problemas que podem impedir a execução de suas instâncias a partir de aplicativos. 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. Esses dados expandem as informações que o Amazon EC2 já fornece sobre o estado pretendido de cada instância (como pending, running, stopping), assim como 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. No entanto, você pode criar ou

excluir alarmes 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 [Criação e edição de alarmes de verificação de status \(p. 568\)](#).

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 sua instância \(p. 476\)](#).

Tópicos

- [Tipos de verificações de status \(p. 566\)](#)
- [Visualização de verificações de status \(p. 566\)](#)
- [Envio de feedback de status de instância \(p. 568\)](#)
- [Criação e edição de alarmes de verificação de status \(p. 568\)](#)

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

Monitore os sistemas da AWS nos quais sua instância é executada. Essas verificações detectam problemas subjacentes na instância que exigem o envolvimento da AWS para 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, você pode interrompê-las e iniciá-las por conta própria, fazendo com que, na maioria dos casos, elas migrem para um novo host. Para instâncias com armazenamento de instância, você pode encerrar e substituir a instância.

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

Verificações de status de instâncias

Monitore a configuração de software e rede de sua instância individual. O Amazon EC2 verifica a integridade da instância enviando uma solicitação de protocolo de resolução de endereço (ARP) para o ENI. 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, reiniciando 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

Visualização de verificações de status

O Amazon EC2 fornece várias formas de visualizar e trabalhar com verificações de status.

Visualização de status usando o console

Você pode visualizar verificações de status usando o Console de gerenciamento da AWS.

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 AWS Management Console interface for monitoring instance status. At the top, there are tabs: Description, Status Checks (which is selected and highlighted in yellow), Monitoring, and Tags. Below the tabs, a note states: "Status checks detect problems that may impair this instance from running your applications. [Learn more](#) about status checks." There are two main sections: "System Status Checks" and "Instance Status Checks". Under "System Status Checks", it says "These checks monitor the AWS systems required to use this instance and ensure they are functioning properly." and "System reachability check passed" (in green). Under "Instance Status Checks", it says "These checks monitor your software and network configuration for this instance." and "Instance reachability check failed at October 7, 2013 11:52:11 AM UTC+2 (16 minutes ago)". A link "Learn more about this issue" is provided. At the bottom, there's a note: "Submit feedback if our checks do not reflect your experience with this instance or if they do not detect the issues you are having. Please note that we will not respond to customer support issues reported via this form. Please post your issue on the [Developer Forums](#) or contact [AWS Support](#) if you need technical assistance with this instance."

5. Se houver uma instância com verificação de status com falha 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 \(p. 1038\)](#).

Visualização de status usando a linha de comando ou a API

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 seguinte comando:

```
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 seguinte comando:

```
aws ec2 describe-instance-status --instance-ids i-1234567890abcdef0
```

Como opção, use os seguintes comandos:

- [Get-EC2InstanceState](#) (AWS Tools para 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 \(p. 1038\)](#).

Envio de feedback de status de instância

Você pode fornecer comentários se estiver tendo problemas com uma instância cujo status não é mostrado como danificado. Ou talvez queira 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.

Envio de feedback de status usando o 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.

Envio de feedback de status usando a linha de comando ou a API

Use o seguinte 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 opção, use os seguintes comandos:

- `Send-EC2InstanceState` (AWS Tools para Windows PowerShell)
- `ReportInstanceState` (API de consulta do Amazon EC2)

Criação e edição de alarmes de verificação de status

Você pode criar alarmes de status de instância e status de sistema para notificá-lo quando uma instância tiver o status de verificação com falha.

Criação de um alarme de verificação de status usando o console

Você pode criar alarmes de verificação de status para uma instância existente para monitorar o status da instância ou o status do sistema. Você pode configurar o alarme para lhe enviar uma notificação por e-mail ou interromper, encerrar ou recuperar uma instância quando houver falha na [verificação de status da instância ou na verificação de status do sistema \(p. 566\)](#).

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.

Note

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.

Para editar 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 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.

Criação de 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 é `StatusCheckFailed`.

Para criar um alarme de verificação de status (AWS CLI)

1. Selecione um tópico de SNS existente ou crie um novo. Para obter mais informações, consulte [Uso da AWS CLI com o Amazon SNS](#) no Guia do usuário do 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 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
```

Observação

- `--period` é o intervalo de tempo, em segundos, no qual as métricas de Amazon CloudWatch são coletadas. Este exemplo usa 300, que são 60 segundos multiplicados por 5 minutos.
- `--evaluation-periods` é o número de períodos consecutivos pelo qual o valor da métrica deve ser comparado ao limite. Este exemplo usa 2.
- `--alarm-actions` é a lista de ações a serem executadas quando o alarme é disparado. Cada ação é especificada como um Nome de recurso da Amazon (ARN). Este exemplo configura o alarme para enviar um e-mail usando Amazon SNS.

Eventos programados para suas instâncias

A 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 está associado à sua conta da AWS antes do evento programado com detalhes sobre o evento, incluindo as datas de início e término. Dependendo do evento, você pode tomar providências para controlar sua duração.

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 \(p. 570\)](#)
- [Visualização de eventos programados \(p. 570\)](#)
- [Trabalhar com instâncias programadas para interrupção ou retirada \(p. 573\)](#)
- [Trabalhar com instâncias programadas para reinicialização \(p. 573\)](#)
- [Trabalhar com instâncias programadas para manutenção \(p. 574\)](#)

Tipos de eventos programados

O Amazon EC2 oferece suporte aos seguintes tipos de eventos programados para suas instâncias:

- Instance stop: a instância será 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): a instância será interrompida, se ela for baseada no Amazon EBS, ou encerrada, se for baseada no armazenamento de instâncias.
- Instance reboot (Reinicialização da instância): a instância será reiniciada.
- System reboot (Reinicialização do sistema): o host da instância será reiniciado.
- System maintenance: a instância pode ser temporariamente afetada pela manutenção de rede ou pela manutenção de energia.

Visualização de eventos programados

Além de receber a notificação de eventos programados por e-mail, você pode verificar se há eventos programados usando um dos métodos a seguir.

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/>.

- 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 Lambda console interface. At the top, there are three dropdown filters: 'All resource types' (selected), 'All event types' (selected), and 'Ongoing and scheduled'. Below the filters, there is a table with two columns: 'Resource Name' and 'Event Type'. The first row shows 'my-instance' under 'Resource Name' and 'instance-stop' under 'Event Type'. At the bottom of the table, it says 'Event: i-c3870335'. Below the table, detailed information about the event is provided:

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.

The screenshot shows the EC2 Dashboard. A header bar says 'Scheduled Events'. Below it, a section for 'US West (Oregon)' shows '1 instances have scheduled events'. There is a small orange warning icon with a white exclamation mark.

- Observe que 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.



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]"
```

A seguir, temos um exemplo de saída que mostra um evento de retirada de instância:

```
[{"Events": [{"Code": "instance-stop", "Description": "The instance is running on degraded hardware", "NotBefore": "2015-05-23T00:00:00.000Z"}]}
```

Para visualizar os eventos programados para suas instâncias usando a AWS Tools para Windows PowerShell

- Use o comando [Get-EC2InstanceState](#):

```
PS C:\> (Get-EC2InstanceStatus -InstanceId i-1234567890abcdef0).Events
```

A seguir, temos um exemplo de saída que mostra um evento de retirada de instância:

```
Code      : instance-stop
Description : The instance is running on degraded hardware
NotBefore : 5/23/2015 12:00:00 AM
```

Para visualizar os eventos programados para suas instâncias usando metadados de instância

- Você pode recuperar informações sobre eventos de manutenção ativos para suas instâncias dos [metadados de instância \(p. 516\)](#) conforme indicado a seguir:

```
[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" : "243450899",
    "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

- Você pode recuperar informações sobre eventos concluídos ou cancelados para suas instâncias dos [metadados de instância \(p. 516\)](#) conforme indicado a seguir:

```
[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" : "243450899",
    "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" : "243451013",
  }
]
```

```
    "NotAfter" : "29 Jan 2019 09:17:23 GMT",
    "State" : "completed"
}
```

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 [Inativação da instância \(p. 468\)](#).

Important

Qualquer dado armazenado nos volumes de armazenamento da instância será perdido quando a instância for interrompida 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 de armazenamento da instância que você precisará mais tarde antes que a instância seja interrompida 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 [Interrompa e inicie sua instância \(p. 458\)](#).

É possível automatizar uma interrupção e inicialização imediatas em resposta a um evento programado de interrupção de instância. Para obter mais informações, consulte [Automatizar ações para instâncias do EC2](#) no Guia do usuário do AWS Health.

Ações para instâncias com armazenamento de instâncias

Recomendamos que você inicie 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 de uma instância ou do host subjacente da instância. Sejam quais forem as instâncias existentes que estejam programadas para reinicialização, o lançamento de uma nova instância não exigirá reinicialização, pois as atualizações já foram aplicadas ao host subjacente.

Você pode determinar se o evento de reinicialização é a reinicialização de uma instância ou de um sistema.

Para visualizar o tipo de evento de reinicialização programado (console)

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Events.
3. Escolha Instance resources (Recursos de instâncias) na lista de filtros e selecione a instância.

4. No painel inferior, localize Event type. O valor é `system-reboot` ou `instance-reboot`.

Para visualizar o tipo de evento de reinicialização programado (AWS CLI)

- Use o comando `describe-instance-status`:

```
aws ec2 describe-instance-status --instance-ids i-1234567890abcdef0
```

Ações para reinicialização de instância

Você pode aguardar até que a reinicialização da instância ocorra dentro da janela de manutenção programada. Como alternativa, você pode reiniciar a instância por conta própria em um horário que seja conveniente para você. Para obter mais informações, consulte [Reiniciar sua instância \(p. 467\)](#).

Após a reinicialização da instância, o evento programado para isso será cancelado 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. Recomendamos que você aguarde até que a reinicialização do sistema ocorra durante a janela de manutenção programada. A reinicialização do sistema geralmente é concluída em questão de minutos. A instância retém seu endereço IP e nome DNS, e qualquer dado em volumes de armazenamento de instância local é preservado. Após a reinicialização do sistema, o evento programado para a instância é desmarcado, 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, você poderá 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 da instância local não seriam 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 [Automatizar ações para instâncias do EC2](#) no Guia do usuário do AWS Health.

No caso de uma instância baseada no armazenamento de instâncias, 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.

Trabalhar com instâncias programadas para manutenção

Quando a AWS precisa manter o host subjacente de uma instância, ele 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 será 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 o aplicativo está funcionando conforme o esperado. Nesse ponto, a instância não deve mais ter um evento associado a ela, ou a descrição do evento programado começa com [Completed]. Às vezes, leva até 1 hora para que o status da instância seja atualizado. 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 [Interrompa e inicie sua instância \(p. 458\)](#).

É possível automatizar uma interrupção e inicialização imediatas em resposta a um evento programado de manutenção. Para obter mais informações, consulte [Automatizar ações para instâncias do EC2](#) no Guia 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.

Monitoramento das suas 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 aplicativo 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 e desabilitar o monitoramento detalhado para suas instâncias \(p. 575\)](#).

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 [Guia do usuário do Amazon CloudWatch](#).

Tópicos

- [Habilitar e desabilitar o monitoramento detalhado para suas instâncias \(p. 575\)](#)
- [Liste as métricas disponíveis do CloudWatch para suas instâncias \(p. 577\)](#)
- [Obtenha estatísticas para as métricas das suas instâncias \(p. 586\)](#)
- [Represente graficamente métricas para suas instâncias \(p. 594\)](#)
- [Criar um alarme do CloudWatch para uma instância \(p. 594\)](#)
- [Crie alarmes para parar, encerrar, reiniciar ou recuperar uma instância \(p. 595\)](#)

Habilitar e desabilitar o monitoramento detalhado para suas 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. A tabela a seguir descreve o monitoramento básico e detalhado para instâncias.

Tipo de monitoramento	Descrição
Basic	Os dados são disponibilizados automaticamente em períodos de cinco minutos, sem custo adicional.
Detalhado	Os dados estão disponíveis em períodos de 1 minutos a um custo adicional. 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. Para obter mais informações sobre a definição de preço, consulte a página do produto Amazon CloudWatch .

Habilitação do 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 [Como monitorar volumes com o CloudWatch \(p. 868\)](#).

Para habilitar o monitoramento detalhado para uma instância existente (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), 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 Console de gerenciamento da AWS, selecione a caixa Monitoring (Monitoramento) na página Configure Instance Details (Configurar detalhes de instância).

Para habilitar o monitoramento detalhado para uma instância existente (AWS CLI)

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 (AWS CLI)

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...
```

Desabilitação o monitoramento detalhado

Você pode desabilitar o monitoramento detalhado em uma instância quando executá-la ou depois de a instância estar sendo executada ou ter sido interrompida.

Para desabilitar o monitoramento detalhado (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), 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).

Para desabilitar o monitoramento detalhado (AWS CLI)

Use o comando `unmonitor-instances` para desabilitar o monitoramento detalhado das instâncias especificadas.

```
aws ec2 unmonitor-instances --instance-ids i-1234567890abcdef0
```

Liste as métricas disponíveis do CloudWatch para suas instâncias

O Amazon EC2 envia métricas para o Amazon CloudWatch. Você pode usar o Console de gerenciamento da AWS, 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.

Para obter informações sobre a obtenção de estatísticas para essas métricas, consulte [Obtenha estatísticas para as métricas das suas instâncias \(p. 586\)](#).

Métricas de instância

O namespace AWS/EC2 inclui as seguintes métricas de crédito de CPU para suas [instâncias de desempenho com capacidade de intermitência \(p. 189\)](#).

Métrica	Descrição
CPUCreditUsage	<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 a uma frequência de apenas 5 minutos. Se você especificar um período de mais cinco minutos, use a estatística Sum em vez da estatística Average.</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 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 a uma frequência de apenas 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>Unidades: créditos (minutos de vCPU)</p>
CPUSurplusCreditsCharged	<p>O número de créditos excedentes gastos que não são pagos pelos créditos de CPU ganhos e que, portanto, incorrem em uma cobrança adicional.</p> <p>Os créditos excedentes gastos são cobrados quando uma das seguintes situações ocorre:</p> <ul style="list-style-type: none"> • Os créditos excedentes ultrapassaram o número máximo de créditos que a instância pode obter em um período de 24 horas. Os créditos excedentes gastos acima do limite máximo são cobrados no final da hora. • A instância é interrompida ou encerrada. • A instância é alterada de <code>unlimited</code> para <code>standard</code>. <p>Unidades: créditos (minutos de vCPU)</p>

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 a potência de processamento necessária para executar um aplicativo 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>Unidade: 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>Unidade: 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>Unidade: 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 o aplicativo lê do 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 (cinco minutos), divida esse número por 300 para encontrar o número de bytes/segundo. Se você estiver usando o monitoramento detalhado (um 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>Unidade: bytes</p>

Métrica	Descrição
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 o aplicativo 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 (cinco minutos), divida esse número por 300 para encontrar o número de bytes/segundo. Se você estiver usando o monitoramento detalhado (um 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>Unidade: bytes</p>
NetworkIn	<p>O número 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 (cinco minutos), divida esse número por 300 para encontrar o número de bytes/segundo. Se você estiver usando o monitoramento detalhado (um minuto), divida o número por 60.</p> <p>Unidade: bytes</p>
NetworkOut	<p>O número 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 (cinco minutos), divida esse número por 300 para encontrar o número de bytes/segundo. Se você estiver usando o monitoramento detalhado (um minuto), divida o número por 60.</p> <p>Unidade: bytes</p>
NetworkPacketsIn	<p>O número 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. Essa métrica está disponível somente para monitoramento básico.</p> <p>Unidade: contagem</p> <p>Estatísticas: mínimo, máximo, média</p>

Métrica	Descrição
<code>NetworkPacketsOut</code>	O número 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. Essa métrica está disponível somente para monitoramento básico. Unidade: contagem Estatísticas: mínimo, máximo, média

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 as verificações de status EC2, consulte [Verificações de status de suas instâncias](#).

Métrica	Descrição
<code>StatusCheckFailed</code>	Relata se a instância foi aprovada tanto na verificação do status da instância quanto na verificação do status do sistema no último minuto. Essa métrica pode ser 0 (passou) ou 1 (falhou). Por padrão, esta métrica está disponível a uma frequência de um minuto gratuitamente. Unidade: contagem
<code>StatusCheckFailed_Instance</code>	Informa se a instância foi aprovada na verificação de status de instância no último minuto. Essa métrica pode ser 0 (passou) ou 1 (falhou). Por padrão, esta métrica está disponível a uma frequência de um minuto gratuitamente. Unidade: contagem
<code>StatusCheckFailed_System</code>	Informa se a instância foi aprovada na verificação de status de sistema no último minuto. Essa métrica pode ser 0 (passou) ou 1 (falhou). Por padrão, esta métrica está disponível a uma frequência de um minuto gratuitamente. Unidade: contagem

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 baseadas em Nitro \(p. 179\)](#).

Note

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	<p>Operações de leitura concluídas de todos os volumes do Amazon EBS anexados à instância em um período especificado.</p> <p>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 (cinco minutos), divida esse número por 300 para calcular o IOPS de leitura. Se você estiver usando o monitoramento detalhado (um minuto), divida o número por 60.</p> <p>Unidade: contagem</p>
EBSWriteOps	<p>Operações de gravação concluídas para todos os volumes do EBS anexados à instância em um período especificado.</p> <p>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 (cinco minutos), divida esse número por 300 para calcular o IOPS de gravação. Se você estiver usando o monitoramento detalhado (um minuto), divida o número por 60.</p> <p>Unidade: contagem</p>
EBSReadBytes	<p>Bytes lidos de todos os volumes do EBS anexados à instância em um período especificado.</p> <p>O número relatado é o número de bytes lidos durante o período. Se você estiver usando o monitoramento básico (cinco minutos), divida esse número por 300 para encontrar o número de bytes lidos/segundo. Se você estiver usando o monitoramento detalhado (um minuto), divida o número por 60.</p> <p>Unidade: bytes</p>
EBSWriteBytes	<p>Bytes gravados em todos os volumes do EBS anexados à instância em um período especificado.</p> <p>O número relatado é o número de bytes gravados durante o período. Se você estiver usando o monitoramento básico (cinco minutos), divida esse número por 300 para encontrar o número de bytes gravados/segundo. Se você estiver usando o monitoramento detalhado (um minuto), divida o número por 60.</p>

Métrica	Descrição
	<p>bytes gravados/segundo. Se você estiver usando o monitoramento detalhado (um minuto), divida o número por 60.</p> <p>Unidade: bytes</p>
EBSIOBalance%	<p>Disponível somente para os tamanhos de instâncias menores. 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>A estatística Sum não é aplicável a essa métrica.</p> <p>Unidade: percentual</p>
EBSByteBalance%	<p>Disponível somente para os tamanhos de instâncias menores. Fornece informações sobre a porcentagem de créditos de transferência restantes no bucket de intermitência. Essa métrica está disponível somente para monitoramento básico.</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 \(p. 868\)](#). Para obter informações sobre as métricas fornecidas para suas frotas do Spot, consulte [Métricas do CloudWatch para Frotas spot \(p. 334\)](#).

Dimensões do Amazon EC2

Você pode usar as dimensões a seguir para refinar as métricas apresentadas para suas instâncias.

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

Dimensão	Descrição
	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 valor comercial para seu aplicativo. Disponível para instâncias com monitoramento detalhado habilitado.

Listagem de 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 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' (which is selected and highlighted in orange), 'Graphed metrics', and 'Graph options'. Below the tabs is a search bar with the placeholder text 'Search for any metric, dimension or resource id'. Underneath the search bar, the text '722 Metrics' is displayed. The page then lists various AWS services with their respective metric counts:

Service	Métricas
EBS	117 Metrics
EC2	316 Metrics
EFS	7 Metrics
ELB	210 Metrics
ElasticBeanstalk	8 Metrics
RDS	60 Metrics
S3	4 Metrics

4. Selecione uma dimensão de métrica (por exemplo, Per-Instance Metrics (Métricas por instância)).

103 Metrics

- [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).

	Instance Name (192)	InstanceId	Metric Name
<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

Listagem de métricas usando a 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
```

Obtenha estatísticas para as métricas das suas instâncias

Você pode obter estatísticas para as métricas do CloudWatch para suas instâncias.

Tópicos

- [Visão geral das estatísticas \(p. 587\)](#)
- [Obter estatísticas para uma instância específica \(p. 587\)](#)
- [Aregar estatísticas entre instâncias \(p. 590\)](#)
- [Estatísticas agregadas por grupo de Auto Scaling \(p. 592\)](#)
- [Aregar estatísticas por AMI \(p. 593\)](#)

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 o seu aplicativo.
Maximum	O valor mais alto observado durante o período especificado. Você pode usar esse valor para determinar altos volumes de atividade para o seu aplicativo.
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 Console de gerenciamento da AWS ou a AWS CLI para determinar a utilização horária de CPU de uma instância do EC2 específica.

Requisitos

- Você deve ter o ID da instância. É possível obter o ID da instância usando o Console de gerenciamento da AWS 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 e desabilitar o monitoramento detalhado para suas instâncias \(p. 575\)](#).

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 Métricas.
3. Escolha o namespace de métricas do EC2.

All metrics Graphed metrics Graph options

Search for any metric, dimension or resource id

722 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).

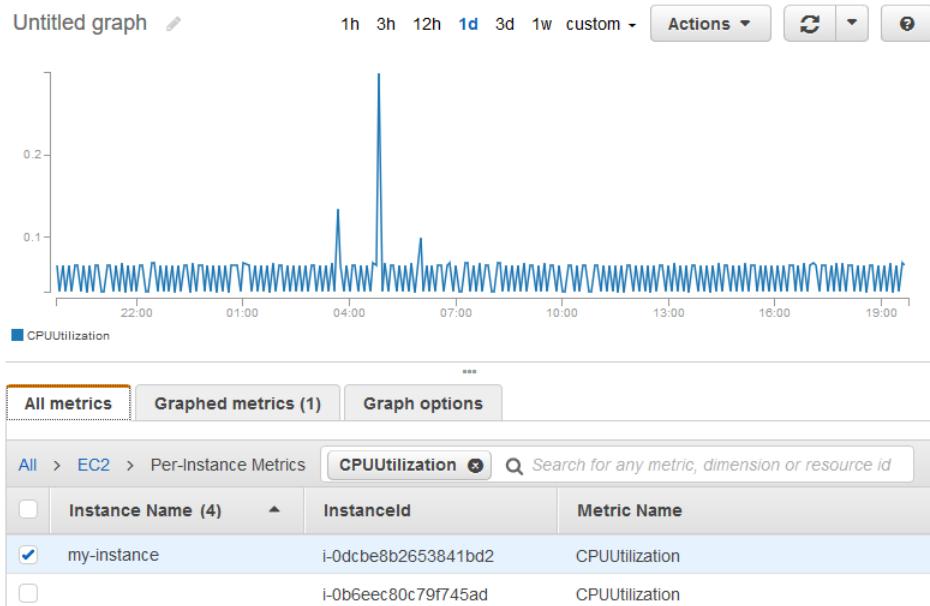
All metrics Graphed metrics Graph options

All > EC2 Search for any metric, dimension or resource id

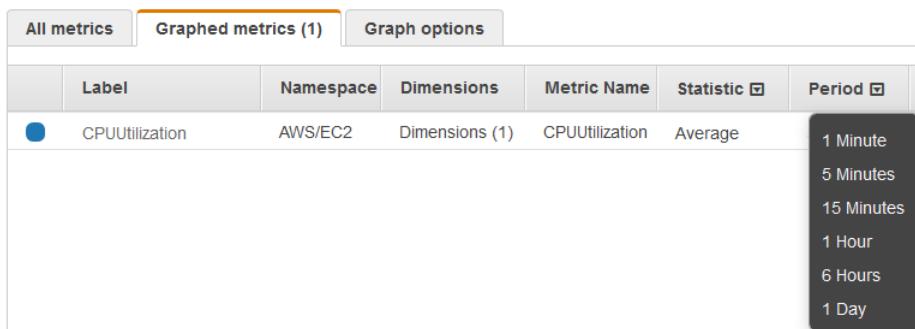
103 Metrics

By Auto Scaling Group 28 Metrics
By Image (AMI) Id 7 Metrics
Per-Instance Metrics 54 Metrics
Aggregated by Instance Type 7 Metrics
Across All Instances 7 Metrics

5. No campo de pesquisa, digite **CPUutilization** e pressione Enter. Escolha a linha da instância específica, que exibe um gráfico da métrica CPUUtilization para a instância. Para dar nome a um gráfico, selecione o ícone do lápis. Para alterar o período, selecione um dos valores predefinidos ou escolha custom (personalizado).



- Para alterar a estatística ou o período da métrica, selecione a guia Graphed metrics (Métricas em gráfico). Escolha o cabeçalho de coluna ou um valor individual e, em seguida, escolha um valor diferente.



Para obter a utilização de CPU para uma instância específica (AWS CLI)

Use o comando [get-metric-statistics](#) para obter a métrica CPUUtilization da instância específica usando o período e o intervalo de tempo especificados:

```
aws cloudwatch get-metric-statistics --namespace AWS/EC2 --metric-name CPUUtilization --period 3600 \
--statistics Maximum --dimensions Name=InstanceId,Value=i-1234567890abcdef0 \
--start-time 2016-10-18T23:18:00 --end-time 2016-10-19T23:18:00
```

A seguir está um exemplo de saída. Cada valor representa a porcentagem máxima de utilização da CPU para uma única instância do EC2.

```
{
  "Datapoints": [
    {
      "Timestamp": "2016-10-19T00:18:00Z",
      "Maximum": 0.33000000000000002,
      "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. Além disso, o Amazon CloudWatch não soma dados entre regiões. Portanto, as métricas são completamente separadas entre regiões. Antes que seja obter estatísticas agregadas em todas as instâncias, você deve habilitar o monitoramento detalhado (a uma cobrança adicional), que fornece dados em períodos 1 minuto.

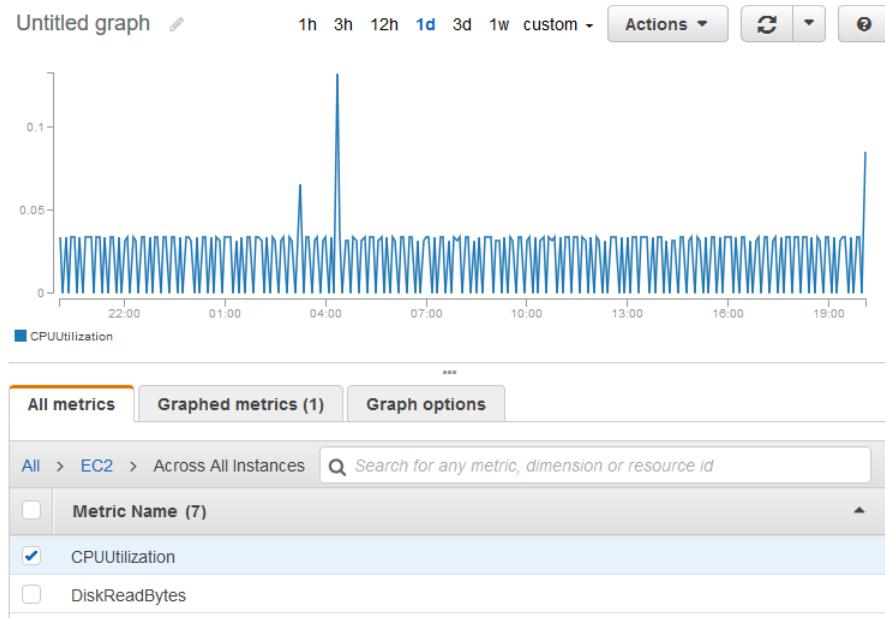
Este exemplo mostra a você como usar o monitoramento detalhado para obter uso médio de CPU para suas instâncias do EC2. Como nenhuma dimensão é especificada, o CloudWatch retorna estatísticas para todas as dimensões no namespace AWS/EC2.

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 Métricas.
3. Escolha o namespace EC2 e escolha Across All Instances (Em todas as instâncias).
4. Escolha a linha que contém CPUUtilization, que exibe um gráfico da métrica para todas as instâncias do EC2. Para dar nome a um gráfico, selecione o ícone do lápis. Para alterar o período, selecione um dos valores predefinidos ou escolha custom (personalizado).



5. Para alterar a estatística ou o período da métrica, selecione a guia Graphed metrics (Métricas em gráfico). Escolha o cabeçalho de coluna ou um valor individual e, em seguida, escolha um valor diferente.

Para obter a utilização média de CPU em suas instâncias (AWS CLI)

Use o comando [get-metric-statistics](#) da seguinte forma para obter a média da métrica CPUUtilization em todas as suas instâncias.

```
aws cloudwatch get-metric-statistics --namespace AWS/ECC --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": 0.1667083333333332,
      "Unit": "Percent"
    },
    {
      "SampleCount": 238.0,
      "Timestamp": "2016-10-11T23:18:00Z",
      "Average": 0.041596638655462197,
      "Unit": "Percent"
    },
    ...
  ],
}
```

```
        "Label": "CPUUtilization"
    }
```

Estatísticas agregadas 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. 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 um minuto para um intervalo de 24 horas em todas as instâncias do EC2 no grupo especificado do Auto Scaling.

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 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"
        }
    ],
    "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 são incluídas. O Amazon CloudWatch não pode agregar dados entre regiões. As métricas são completamente separadas entre regiões.

Antes que seja obter estatísticas agregadas em todas as instâncias, você deve habilitar o monitoramento detalhado (a uma cobrança adicional), que fornece dados em períodos 1 minuto. Para obter mais informações, consulte [Habilitar e desabilitar o monitoramento detalhado para suas instâncias \(p. 575\)](#).

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 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"
}
```

Represente graficamente métricas para suas instâncias

Após executar uma instância, você pode abrir o console do Amazon EC2 e ver os gráficos de monitoramento para uma 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 [Lista as métricas disponíveis do CloudWatch para suas instâncias \(p. 577\)](#).

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 serviços 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 para monitorar métricas do CloudWatch para 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.

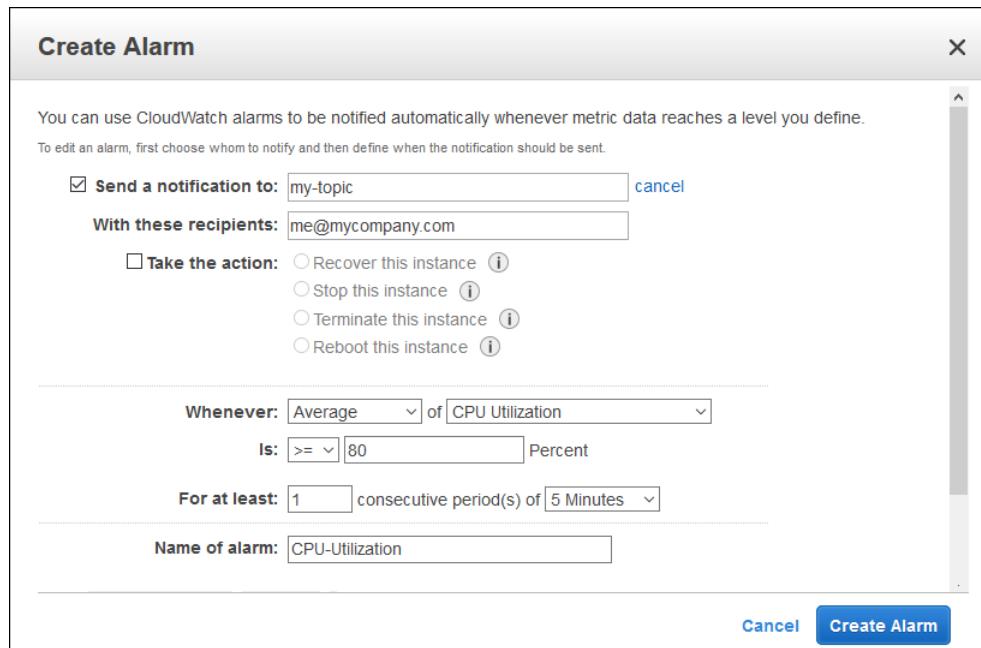
Para criar um alarme usando o console do CloudWatch

Para ver exemplos, consulte [Criação de alarmes do Amazon CloudWatch](#) no Guia do usuário do Amazon CloudWatch.

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, selecione Criar 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.



Crie alarmes para parar, 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 `AWSServiceRoleForCloudWatchEvents` ligado ao serviço permite que a AWS execute ações de alarme em seu nome. A primeira vez que criar um alarme no Console de gerenciamento da AWS, 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 você pode facilmente reiniciar 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 reiniciar 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.

Permissões

Se você for um usuário do AWS Identity and Access Management (IAM), deve ter as seguintes permissões para criar ou modificar um alarme:

- `iam:CreateServiceLinkedRole`, `iam:GetPolicy`, `iam:GetPolicyVersion` e `iam:GetRole` – para todos os alarmes com ações do Amazon EC2
- `ec2:DescribeInstanceStatus` e `ec2:DescribeInstances` – para todos os alarmes nas métricas de status das instâncias do Amazon EC2
- `ec2:StopInstances` – para alarmes com ações de interrupção
- `ec2:TerminateInstances` – para alarmes com ações de encerramento
- Nenhuma permissão específica é necessária para alarmes com ações de recuperação.

Se você tiver permissões de leitura/gravação para o Amazon CloudWatch, mas não para o Amazon EC2, ainda poderá criar um alarme, mas as ações de parar ou encerrar não serão executadas na instância do Amazon EC2. No entanto, se você receber permissão para usar as APIs associadas do Amazon EC2 mais tarde, as ações de alarme que você tiver criado anteriormente serão executadas. Para obter mais informações sobre permissões do IAM, consulte [Permissões e políticas](#) no Guia do usuário do IAM.

Tópicos

- [Inclusão de ações de parar em alarmes do Amazon CloudWatch \(p. 596\)](#)
- [Inclusão de ações de encerrar em alarmes do Amazon CloudWatch \(p. 597\)](#)
- [Inclusão de ações de reiniciar a alarmes do Amazon CloudWatch \(p. 598\)](#)
- [Inclusão de ações de recuperar em alarmes do Amazon CloudWatch \(p. 599\)](#)
- [Usar o console do Amazon CloudWatch para exibir o histórico do alarme e da ação \(p. 601\)](#)
- [Cenários de ação do alarme do Amazon CloudWatch \(p. 601\)](#)

Inclusão de ações de parar em 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.

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 deve 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.

Inclusão de ações de encerrar em 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 a ativação e a desativação da proteção contra encerramento de uma instância, consulte [Ativação da proteção contra encerramento de uma instância](#) no Guia do usuário do Amazon EC2 para instâncias do Linux.

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 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 deve 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.

Inclusão de ações de reiniciar 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 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 sua instância](#) no Guia do usuário do Amazon EC2 para instâncias do Linux.

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 [Como avaliar um alarme](#) em Guia do usuário do Amazon CloudWatch.

Para criar um alarme para reiniciar uma instância (console do Amazon EC2)

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância. Na guia Monitoramento, selecione Criar alarme.
4. Na caixa de diálogo Create Alarm (Criar alarme), faça o seguinte:
 - a. Para receber um e-mail quando o alarme for acionado, na caixa de diálogo Send a notification to (Enviar uma notificação para), escolha um tópico existente do Amazon SNS ou selecione Create topic (Criar tópico) para criar um tópico novo.

Para criar um novo tópico, em Send a notification to (Enviar notificação para), digite um nome para o tópico e, em With these recipients (Com estes destinatários), digite os endereços de e-mail dos destinatários (separados por vírgulas). Depois de criar o alarme, você receberá um e-mail de confirmação da inscrição que você deve aceitar antes de receber notificações para este tópico.
 - b. Selecione Take the action (Executar a ação), escolha Reboot this instance (Reiniciar a instância).
 - c. Para Sempre, escolha Falha na verificação de status (instância).
 - d. Em For at least (Durante pelo menos), especifique o período de avaliação do alarme. Neste exemplo, digite 3 períodos consecutivos de 1 minuto.
 - e. Para alterar o nome do alarme, em Name of alarm (Nome do alarme), digite um novo nome. Os nomes de alarme deve conter somente caracteres ASCII.
- f. Se você não digitar um nome para o alarme, o Amazon CloudWatch criará um automaticamente.
- f. Escolha Create Alarm.

Inclusão de ações de recuperar em 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 repará-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, C5n, M3, M4, M5, M5a, R3, R4, R5, R5a, T2, T3, X1 ou 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.

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.
- a. Selecione Take the action (Executar a ação), escolha Recover this instance (Recuperar a instância).
 - b. Para Sempre, escolha Falha na verificação de status (sistema).
 - c. Em For at least (Durante pelo menos), especifique o período de avaliação do alarme. Neste exemplo, digite 2 períodos consecutivos de 1 minuto.
 - d. Para alterar o nome do alarme, em Name of alarm (Nome do alarme), digite um novo nome. Os nomes de alarme deve 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 exibir o histórico do alarme e da ação

Você pode visualizar o histórico de ações e alarmes 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 Alarmes.
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.

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](#)

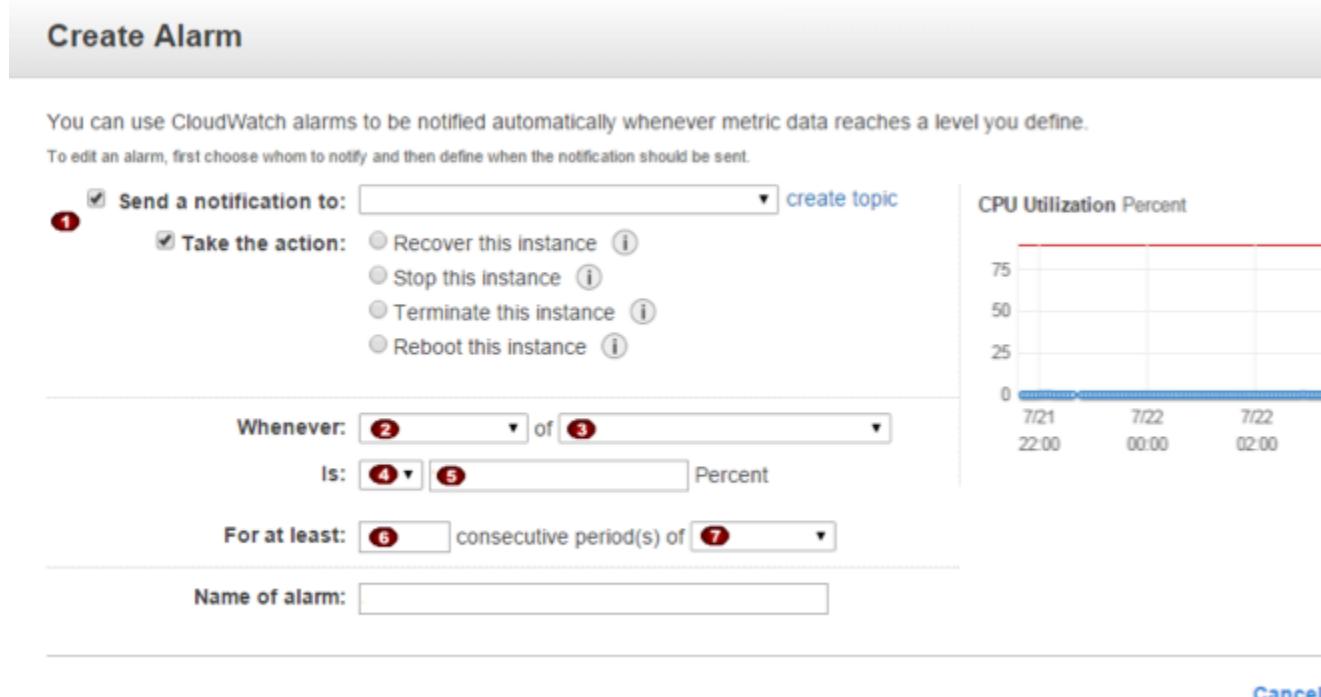
Take the action: Recover this instance [i](#)
 Stop this instance [i](#)
 Terminate this instance [i](#)
 Reboot this instance [i](#)

Whenever: of
Is: Percent

For at least: consecutive period(s) of

Name of alarm:

CPU Utilization Percent



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	CPUUtilization
4	<=
5	10%
6	60 minutos
7	1

Cenário 2: Interrompa 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	CPUUtilization
4	<=
5	5%
6	60 minutos
7	24

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	NetworkOut
4	>
5	10 GB
6	1 dia
7	1

Cenário 4: Pare servidores web com tráfego incomummente 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	NetworkOut
4	>
5	1 GB
6	1 hora
7	1

Cenário 5: Parar uma instância apresentando escape de memória

Crie um alarme que pare uma instância quando a utilização de memória alcançar ou exceder 90%, de forma que os logs do aplicativo sejam recuperados para a solução de problemas.

Note

A métrica MemoryUtilization é uma métrica personalizada. Para usar a métrica MemoryUtilization, você deve instalar o script Perl para instâncias do Linux. Para obter mais informações, consulte [Monitoramento de métricas de memória e disco para instâncias Linux do Amazon EC2](#).

Configuração	Valor
1	Interromper
2	Máximo
3	MemoryUtilization
4	>=
5	90%
6	1 minuto
7	1

Cenário 6: 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

Configuração	Valor
2	Média
3	StatusCheckFailed_System
4	>=
5	1
6	15 minutos
7	1

Cenário 7: Encerrar instâncias quando os jobs 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	NetworkOut
4	<=
5	100,000 bytes
6	5 minutos
7	1

Automatizar o Amazon EC2 com o Eventos do CloudWatch

O Eventos do Amazon CloudWatch permite que você automatize seus serviços da AWS e responda automaticamente aos eventos do sistema, como problemas de disponibilidade do aplicativo ou alterações de recursos. Os eventos dos serviços da AWS são entregues ao Eventos do CloudWatch 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 do tópico do Amazon SNS ou de uma fila do AWS SMS

Alguns exemplos de uso do Eventos do CloudWatch 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 serviço da AWS.

Para obter mais informações, consulte [Guia do usuário do Eventos do Amazon CloudWatch](#).

Monitoramento de métricas de memória e disco para instâncias em Linux do Amazon EC2

Novo agente do CloudWatch disponível

Um novo agente do CloudWatch de várias plataformas está disponível. Você pode usar um único agente para coletar métricas do sistema e arquivos de log das instâncias do Amazon EC2 e de servidores locais. O novo 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 novo agente em vez de os scripts de monitoramento mais antigos para coletar métricas e logs. Para obter mais informações sobre o agente do CloudWatch, 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.

O restante desta seção é informativo para clientes que ainda estão usando os scripts Perl mais antigos para monitoramento. Você pode fazer download desses [Scripts de monitoramento do Amazon CloudWatch para Linux](#) da biblioteca de códigos de exemplo da AWS.

Scripts de monitoramento do CloudWatch

As instâncias baseadas em Linux do Amazon CloudWatch Monitoring Scripts para Amazon Elastic Compute Cloud (Amazon EC2) demonstram como produzir e consumir métricas personalizadas do 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 suportados \(p. 605\)](#)
- [Conteúdo do pacote \(p. 606\)](#)
- [Pré-requisitos \(p. 606\)](#)
- [Conceitos básicos \(p. 608\)](#)
- [mon-put-instance-data.pl \(p. 609\)](#)
- [mon-get-instance-stats.pl \(p. 612\)](#)
- [Visualização de suas métricas personalizadas no console \(p. 613\)](#)
- [Solução de problemas \(p. 613\)](#)

Sistemas suportados

Esses scripts de monitoramento são destinados para uso com instâncias do Amazon EC2 executando Linux. Os scripts foram testados em instâncias usando as imagens de máquina da Amazon (AMI) a seguir, tanto na versão de 32 bits quanto na versão de 64 bits:

- Amazon Linux 2
- Amazon Linux AMI 2014.09.2 e posterior
- Red Hat Enterprise Linux 7.4 e 6.9
- SUSE Linux Enterprise Server 12
- Ubuntu Server 16.04 e 14.04

Note

Nos servidores executando o SUSE Linux Enterprise Server 12, talvez seja necessário primeiro fazer download do pacote perl-Switch. Faça download e instale 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
```

Você também pode monitorar as métricas de memória e disco nas instâncias do Amazon EC2 que executam o Windows por meio do envio desses dados ao CloudWatch Logs. Para obter mais informações, consulte [Envio de logs, eventos e contadores de desempenho ao Amazon CloudWatch](#) no Guia do usuário do Amazon EC2 para instâncias do Windows.

Conteúdo do pacote

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 do 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.

Pré-requisitos

Com algumas versões do Linux, você deve instalar módulos adicionais antes que os scripts de monitoramento funcionarem.

Amazon Linux 2 e Amazon Linux AMI

Para instalar os pacotes necessários

1. Iniciar a sessão na sua instância. Para obter mais informações, consulte [Conecte-se à sua instância do Linux \(p. 439\)](#).
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
```

Red Hat Enterprise Linux

Você deve instalar módulos Perl adicionais.

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 \(p. 439\)](#).
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 a 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 Red Hat Enterprise Linux 7.4

1. Iniciar a sessão na sua instância. Para obter mais informações, consulte [Conecte-se à sua instância do Linux \(p. 439\)](#).
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
```

SUSE Linux Enterprise Server

Você deve instalar módulos Perl adicionais.

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 \(p. 439\)](#).
2. Em um prompt de comando, instale pacotes da forma a seguir:

```
sudo zypper install perl-Switch perl-DateTime
sudo zypper install -y "perl(LWP::Protocol::https)"
```

Ubuntu Server

Você deve configurar seu servidor da forma a seguir.

Para 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 \(p. 439\)](#).
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
```

Conceitos básicos

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
```

3. Verifique se os scripts têm permissão para executar operações do CloudWatch usando uma das opções a seguir:

- Se você tiver associado uma função do IAM (perfil de instância) com sua instância, verifique se ela concede permissões para executar as seguintes operações:
 - cloudwatch:PutMetricData
 - cloudwatch:GetMetricStatistics
 - cloudwatch>ListMetrics
 - ec2:DescribeTags
- Especifique suas credenciais da AWS em um arquivo de credenciais. Primeiro, copie o arquivo `awscreds.template` incluído nos scripts de monitoramento para `awscreds.conf` da seguinte forma:

```
cp awscreds.template awscreds.conf
```

Adicione o conteúdo a seguir ao arquivo `awscreds.conf`:

```
AWSAccessKeyId = my-access-key-id
AWSSecretKey = my-secret-access-key
```

Para obter informações sobre como visualizar suas credenciais da AWS, consulte [Compreensão e obtenção de suas credenciais de segurança](#) no Referência geral do Amazon Web Services.

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.

Opções

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.
--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.

Nome	Descrição
--disk-space-used	<p>Coleta e envia a métrica DiskSpaceUsed para os discos selecionados. A métrica é relatada por padrão em gigabytes.</p> <p>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.</p>
--disk-space-avail	<p>Coleta e envia a métrica DiskSpaceAvailable para os discos selecionados. A métrica é relatada em gigabytes.</p> <p>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.</p>
--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	<p>Fornece a localização do arquivo que contém as credenciais da AWS.</p> <p>Esse parâmetro não pode ser usado com os parâmetros --aws-access-key-id e --aws-secret-key.</p>
--aws-access-key-id=VALUE	Especifica o ID da chave de acesso da AWS a ser usado para identificar o chamador. 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 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	<p>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.</p> <p>Não use esta opção com os parâmetros --aws-credential-file, --aws-access-key-id ou --aws-secret-key.</p>
--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.

Nome	Descrição
--auto-scaling[=only]	Adiciona métricas agregadas para o grupo de Auto Scaling. O valor <code>=only</code> é opcional; se especificado, o script relata somente métricas de Auto Scaling. A política do IAM associada à conta ou função do IAM que usa os scripts necessários para ter permissão para chamar a ação do EC2 <code>DescribeTags</code> .
--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.
--verbose	Exibe informações detalhadas sobre o que o script está fazendo.
--help	Exibe informações de uso.
--version	Exibe o número de versão do script.

Exemplos

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.

Para executar um teste simples sem postar dados no CloudWatch

```
./mon-put-instance-data.pl --mem-util --verify --verbose
```

Para coletar todas as métricas de memória disponíveis e enviá-las para o 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
```

Para definir um cronograma cron para métricas relatadas ao CloudWatch

1. Inicie a edição do crontab usando o comando a seguir:

```
crontab -e
```

2. 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, gravará a mensagem de erro no log do sistema.

Para coletar métricas agregadas para um grupo de Auto Scaling e enviá-las ao Amazon CloudWatch sem relatar métricas de instância individuais

```
./mon-put-instance-data.pl --mem-util --mem-used --mem-avail --auto-scaling=only
```

Para coletar métricas agregadas para o tipo de instância, ID da AMI e região, e enviá-las ao Amazon CloudWatch sem relatar métricas de instância individuais

```
./mon-put-instance-data.pl --mem-util --mem-used --mem-avail --aggregated=only
```

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.

Opções

Nome	Descrição
--recent-hours=N	Especifica o número de horas recentes para relatar, como representado por N, onde N é um inteiro.
--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 chamador. 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 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.

Exemplo

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%
```

Visualização de suas 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.

Solução de problemas

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 as chamadas à API do Amazon EC2 e do Amazon EBS com o AWS CloudTrail

O Amazon EC2 e o Amazon EBS estão integrados ao AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, uma função ou um serviço da AWS no Amazon EC2 e no Amazon EBS. O CloudTrail captura todas as chamadas às APIs do Amazon EC2 e do Amazon EBS como eventos, incluindo as chamadas do console e as chamadas de código às 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 não configurar uma trilha, você ainda poderá visualizar os eventos

mais recentes no console do CloudTrail em Event history. 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 CloudTrail, consulte o [AWS CloudTrail User Guide](#).

Informações sobre o Amazon EC2 e o Amazon EBS no CloudTrail

O CloudTrail está habilitado na sua conta da AWS ao criá-la. Quando ocorre uma atividade no Amazon EC2 e no Amazon EBS, ela é registrada em um evento do CloudTrail com outros eventos de serviços 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 [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 CloudTrail para fornecer 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. A trilha registra eventos de todas as regiões na partição da AWS e fornece os arquivos de log para o bucket do Amazon S3 que você especificar. Além disso, é possível configurar outros serviços da AWS para analisar mais profundamente e agir sobre os dados de evento coletados nos logs do CloudTrail. Para obter mais informações, consulte:

- Visão geral da criação de uma trilha
- CloudTrail Serviços compatíveis e integrações do
- 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 do Amazon EBS são registradas em log pelo CloudTrail e documentadas no [Amazon EC2 API Reference](#). 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 da 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 [Elemento userIdentity do CloudTrail](#).

Noções básicas sobre as entradas no arquivos de log do Amazon EC2 e do Amazon EBS

Uma trilha é uma configuração que permite a entrega de eventos como arquivos de log em um bucket do Amazon S3 que você especificar. 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 hora da ação, parâmetros de solicitação, e assim por diante. Arquivos de log do CloudTrail não são um rastreamento de pilha ordenada das chamadas da API pública. Assim, elas não são exibidas em nenhuma ordem específica.

Amazon Elastic Compute Cloud
User Guide for Linux Instances
Noções básicas sobre as entradas no arquivos
de log do Amazon EC2 e do Amazon EBS

O arquivo de log a seguir mostra que um usuário encerrou uma instância.

```
{  
    "Records": [  
        {  
            "eventVersion": "1.03",  
            "userIdentity": {  
                "type": "Root",  
                "principalId": "123456789012",  
                "arn": "arn:aws:iam::123456789012:root",  
                "accountId": "123456789012",  
                "accessKeyId": "AKIAIOSFODNN7EXAMPLE",  
                "userName": "user"  
            },  
            "eventTime": "2016-05-20T08:27:45Z",  
            "eventSource": "ec2.amazonaws.com",  
            "eventName": "TerminateInstances",  
            "awsRegion": "us-west-2",  
            "sourceIPAddress": "198.51.100.1",  
            "userAgent": "aws-cli/1.10.10 Python/2.7.9 Windows/7botocore/1.4.1",  
            "requestParameters": {  
                "instancesSet": {  
                    "items": [{  
                        "instanceId": "i-1a2b3c4d"  
                    }]  
                }  
            },  
            "responseElements": {  
                "instancesSet": {  
                    "items": [{  
                        "instanceId": "i-1a2b3c4d",  
                        "currentState": {  
                            "code": 32,  
                            "name": "shutting-down"  
                        },  
                        "previousState": {  
                            "code": 16,  
                            "name": "running"  
                        }  
                    }]  
                }  
            },  
            "requestID": "be112233-1ba5-4ae0-8e2b-1c302EXAMPLE",  
            "eventID": "6e12345-2a4e-417c-aa78-7594fEXAMPLE",  
            "eventType": "AwsApiCall",  
            "recipientAccountId": "123456789012"  
        }  
    ]  
}
```

Rede e segurança

O Amazon EC2 fornece os recursos de rede e segurança a seguir.

Recursos

- [Pares de chaves do Amazon EC2 \(p. 616\)](#)
- [Grupos de segurança do Amazon EC2 para instâncias do Linux \(p. 626\)](#)
- [Como controlar o acesso aos recursos do Amazon EC2 \(p. 641\)](#)
- [Endereçamento IP de instâncias do Amazon EC2 \(p. 723\)](#)
- [Traga seus próprios endereços IP \(BYOIP\) \(p. 738\)](#)
- [Endereços Elastic IP \(p. 742\)](#)
- [Interfaces de rede elástica \(p. 747\)](#)
- [Rede avançada no Linux \(p. 768\)](#)
- [Placement groups \(p. 793\)](#)
- [Unidade de transmissão máxima \(MTU\) de rede para sua instância do EC2 \(p. 801\)](#)
- [Virtual Private Clouds \(p. 804\)](#)
- [EC2-Classic \(p. 804\)](#)

Pares de chaves do Amazon EC2

O Amazon EC2 usa a criptografia de chave–pública para criptografar e descriptografar informações de login. A criptografia de chave–pública usa uma chave pública para criptografar uma parte dos dados, como uma senha e, em seguida, o destinatário usa a chave privada para descriptografar os dados. As chaves pública e privada são conhecidas como par de chaves.

Para fazer login na sua instância, você deve criar um par de chaves, especificar o nome do par de chaves ao executar a instância e fornecer a chave privada ao se conectar à instância. Em uma instância do Linux, o conteúdo da chave pública é posicionado em uma entrada dentro de `~/.ssh/authorized_keys`. Isso é feito no momento da inicialização e permite que você acesse com segurança sua instância usando a chave privada em vez de um password.

Criação de um par de chaves

Você pode usar o Amazon EC2 para criar seu par de chaves. Para obter mais informações, consulte [Criação de um par de chaves usando o Amazon EC2 \(p. 617\)](#).

Como alternativa, use uma ferramenta de terceiros e importe a chave pública para o Amazon EC2. Para obter mais informações, consulte [Importação da sua própria chave pública para o Amazon EC2 \(p. 618\)](#).

Cada par de chaves exige um nome. Certifique-se de escolher um nome que seja fácil de lembrar. Amazon EC2 associa a chave pública ao nome que você especifica como o nome da chave.

O Amazon EC2 armazena somente a chave pública, e você armazena a chave privada. Qualquer um com sua chave privada pode descriptografar suas informações de login, por isso é importante que você armazene as chaves privadas em um lugar seguro.

As chaves que o Amazon EC2 usa são chaves SSH-2 RSA de 2048 bits. É possível ter até cinco mil pares de chaves por região.

Execução e conexão à sua instância

Quando você executa uma instância, deve especificar o nome do par de chaves que planeja usar para conectar-se à instância. Se você não especificar o nome do par de chaves existente ao executar uma instância, não poderá se conectar à instância. Ao se conectar à instância, é preciso especificar a chave privada correspondente ao par de chaves especificado ao executar a instância.

Note

O Amazon EC2 não mantém uma cópia da sua chave privada; portanto, se você perder a chave privada, não haverá maneira de recuperá-la. Se você perder a chave privada para uma instância com armazenamento de instâncias, não poderá acessar a instância; deverá encerrá-la e executar outra instância usando um novo par de chaves. Se você perder a chave privada de uma instância do Linux com EBS, poderá recobrar o acesso à sua instância. Para obter mais informações, consulte [Conexão à sua instância do Linux se você perder sua chave privada \(p. 623\)](#).

Pares de chaves para múltiplos usuários

Se você tiver vários usuários que exigem acesso a uma única instância, poderá adicionar contas de usuário à sua instância. Para obter mais informações, consulte [Gerenciamento de contas de usuário em sua instância do Linux \(p. 483\)](#). Você pode criar um par de chaves para cada usuário e adicionar informações de chave pública de cada par de chaves ao arquivo `.ssh/authorized_keys` para cada usuário da sua instância. Você pode, então, distribuir os arquivos de chave privada para seus usuários. Dessa forma, não tem de distribuir o mesmo arquivo de chave privada usado para a conta-raiz para múltiplos usuários.

Tópicos

- [Criação de um par de chaves usando o Amazon EC2 \(p. 617\)](#)
- [Importação da sua própria chave pública para o Amazon EC2 \(p. 618\)](#)
- [Recuperação da chave pública para seu par de chaves no Linux \(p. 619\)](#)
- [Recuperação da chave pública para seu par de chaves no Windows \(p. 620\)](#)
- [Recuperação da chave pública para seu par de chaves a partir da sua instância \(p. 620\)](#)
- [Verificação da impressão digital do seu par de chaves \(p. 621\)](#)
- [Excluir o par de chaves \(p. 621\)](#)
- [Adição ou substituição de um par de chaves para sua instância \(p. 622\)](#)
- [Conexão à sua instância do Linux se você perder sua chave privada \(p. 623\)](#)

Criação de um par de chaves usando o Amazon EC2

Você pode criar um par de chaves usando o console do Amazon EC2 ou a linha de comando. Após criar um par de chaves, você pode especificá-lo ao executar sua instância. Você também pode adicionar o par de chaves a uma instância em execução para permitir que outro usuário se conecte à instância. Para obter mais informações, consulte [Adição ou substituição de um par de chaves para sua instância \(p. 622\)](#).

Para criar seu par de chaves 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, em REDE E SEGURANÇA, escolha Pares de chaves.

Note

O painel de navegação fica do lado esquerdo do console do Amazon EC2. Se você não vir o painel, ele pode estar minimizado; selecione a seta para expandir o painel.

3. Escolha Criar par de chaves.

-
4. Para Key pair name (Nome do par de chaves), insira um nome para o novo par de chaves e escolha Create (Criar).
 5. O arquivo de chave privada é baixado automaticamente pelo navegador. O nome do arquivo base é o nome especificado como sendo o nome do par de chaves e a extensão do nome do arquivo é .pem. Salve o arquivo de chave privada em um lugar seguro.

Important

Esta é a única chance de você salvar o arquivo de chave privada. Você precisará fornecer o nome do par de chaves ao iniciar uma instância e a chave privada correspondente sempre que se conectar à instância.

6. Se você usar um cliente de SSH em um computador Mac ou Linux para se conectar 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 \(p. 1033\)](#).

Para criar seu par de chaves 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 [Acessando o Amazon EC2 \(p. 3\)](#).

- [create-key-pair](#) (AWS CLI)
- [New-EC2KeyPair](#) (AWS Tools para Windows PowerShell)

Importação da sua própria 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 usando uma ferramenta de terceiros e, então, importar a chave pública para o Amazon EC2. Por exemplo, você pode usar ssh-keygen (uma ferramenta que vem com a instalação padrão de OpenSSH) para criar um par de chaves. 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.

Requisitos

- Os seguintes formatos são compatíveis:
 - Formato de chave pública de OpenSSH (o formato em ~/.ssh/authorized_keys)
 - Formato DER codificado em Base64
 - Formato de arquivo de chave pública SSH, conforme especificado em [RFC4716](#)
 - O formato do arquivo de chave privada SSH deve ser PEM (por exemplo, use `ssh-keygen -m PEM` para converter a chave OpenSSH no formato PEM)
- Crie uma chave RSA. O Amazon EC2 não aceita chaves DSA.
- Os tamanhos com suporte são 1024, 2048 e 4096.

Para criar um par de chaves usando uma ferramenta de terceiros

1. Gere um par de chaves com uma ferramenta de terceiros de sua escolha.

2. Salve a chave pública em um arquivo local. Por exemplo, `~/.ssh/my-key-pair.pub` (Linux) ou `C:\keys\my-key-pair.pub` (Windows). A extensão do nome de arquivo para esse arquivo não é importante.
3. Salve a chave privada em um arquivo local diferente que tenha a extensão `.pem`. Por exemplo, `~/.ssh/my-key-pair.pem` (Linux) ou `C:\keys\my-key-pair.pem` (Windows). Salve o arquivo de chave privada em um lugar seguro. Você precisará fornecer o nome do par de chaves ao iniciar uma instância e a chave privada correspondente sempre que se conectar à instância.

Use as etapas a seguir para importar seu par de chaves usando o console do Amazon EC2.

Para importar a chave pública

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, em REDE E SEGURANÇA, escolha Pares de chaves.
3. Selecione Importar par de chaves.
4. Na caixa de diálogo Importar par de chaves, escolha Explorar e selecione o arquivo de chave pública salvo previamente. Insira um nome para o par de chaves no campo Nome do par de chaves e selecione Importar.

Para importar a chave pública 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 [Acessando o Amazon EC2 \(p. 3\)](#).

- [import-key-pair](#) (AWS CLI)
- [Import-EC2KeyPair](#) (AWS Tools para Windows PowerShell)

Depois de o arquivo de chave pública ser importado, você pode verificar se par de chaves foi importado com êxito usando o console do Amazon EC2 da forma a seguir.

Para verificar se seu par de chaves foi importado

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. Na barra de navegação, selecione a região na qual você criou o par de chaves.
3. No painel de navegação, em REDE E SEGURANÇA, escolha Pares de chaves.
4. Verifique se o par de chaves que você importou está na lista exibida de pares de chaves.

Para ver seu par de chaves 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 [Acessando o Amazon EC2 \(p. 3\)](#).

- [describe-key-pairs](#) (AWS CLI)
- [Get-EC2KeyPair](#) (AWS Tools para Windows PowerShell)

Recuperação da chave pública para seu par de chaves no Linux

No seu computador Linux ou Mac local, você pode usar o comando `ssh-keygen` para recuperar a chave pública do 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. Por exemplo:

```
ssh-rsa AAAAB3NzaC1yc2EAAAQABAAQClKsfkNkuSevGj3eYhCe53pcjqP3maAhDFcvBS706V  
hz2ItxCih+PnDSUaw+WNQn/mZphTk/a/gU8jEzoOWbkM4yxyb/wB96xbiFveSFJuOp/d6RJhJOI0iBXr  
lsLnB1tntckij7FbtXJMxLvvwJryDUilBMTjYtwB+QhYXUMOzce5Pjz5/i8SeJtjnV3iAoG/cQk+0Fzz  
qaeJAAHco+CY/5WrUBkrHmFJr6HcXkvJdWPkYQS3xqC0+FmUzofz221CBt5IMucxxPkJ4rWi+z7wB3Rb  
BQoQzd8v7yeb7Oz1PnWOyN0qFU0XA246RA8QFYiCNYwI3f05p6KLxEXAMPLE
```

Se o comando falhar, verifique se você alterou as permissões no arquivo de par de chaves de forma que somente você possa visualizá-lo ao executar o comando a seguir:

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

Recuperação da chave pública para seu par de chaves no Windows

Em seu computador Windows local, você pode usar o PuTTYgen para obter a chave pública do seu par de chaves.

Inicie o PuTTYgen, escolha Carregar e selecione o arquivo .ppk ou .pem. O PuTTYgen exibe a chave pública.

Recuperação da chave pública para seu par de chaves a partir da sua 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 executar a instância, use o comando a seguir a partir da sua instância:

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
```

```
ssh-rsa AAAAB3NzaC1yc2EAAAQABAAQClKsfkNkuSevGj3eYhCe53pcjqP3maAhDFcvBS706V  
hz2ItxCih+PnDSUaw+WNQn/mZphTk/a/gU8jEzoOWbkM4yxyb/wB96xbiFveSFJuOp/d6RJhJOI0iBXr  
lsLnB1tntckij7FbtXJMxLvvwJryDUilBMTjYtwB+QhYXUMOzce5Pjz5/i8SeJtjnV3iAoG/cQk+0Fzz  
qaeJAAHco+CY/5WrUBkrHmFJr6HcXkvJdWPkYQS3xqC0+FmUzofz221CBt5IMucxxPkJ4rWi+z7wB3Rb  
BQoQzd8v7yeb7Oz1PnWOyN0qFU0XA246RA8QFYiCNYwI3f05p6KLxEXAMPLE my-key-pair
```

Se você alterar o par de chaves que usa para se conectar à instância, não atualizaremos os metadados da instância para mostrar a nova chave pública; você continuará a visualizar a chave pública do par de chaves que especificou ao executar a instância nos metadados de instância.

Para obter mais informações, consulte [Recuperação dos metadados da instância \(p. 517\)](#).

Como alternativa, em uma instância do Linux, conteúdo da chave pública é posicionado em uma entrada dentro de `~/.ssh/authorized_keys`. Você pode abrir esse arquivo em um editor. A seguir está uma entrada de exemplo do par de chaves chamado de `my-key-pair`. Ela consiste de uma chave pública seguida pelo nome do par de chaves. Por exemplo:

```
ssh-rsa AAAAB3NzaC1yc2EAAAQABAAQClKsfkNkuSevGj3eYhCe53pcjqP3maAhDFcvBS706V  
hz2ItxCih+PnDSUaw+WNQn/mZphTk/a/gU8jEzoOWbkM4yxyb/wB96xbiFveSFJuOp/d6RJhJOI0iBXr  
lsLnB1tntckij7FbtXJMxLvvwJryDUilBMTjYtwB+QhYXUMOzce5Pjz5/i8SeJtjnV3iAoG/cQk+0Fzz
```

```
qaeJAAHco+CY/5WrUBkrHmFJr6HcXkvJdWPkYQS3xqC0+FmUZofz221CBt5IMucxXPkX4rWi+z7wB3Rb  
BQoQzd8v7yeb7OzlPnWOyN0qFU0XA246RA8QFYiCNYWI3f05p6KLxEXAMPLE my-key-pair
```

Verificação da impressão digital do seu 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. 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 você tiver criado seu par de chaves usando a AWS, pode usar as ferramentas OpenSSL para gerar uma impressão digital da seguinte forma:

```
$ 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 carregado a chave pública para a AWS, pode usar as ferramentas de 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 OpenSSH 7.8 ou posterior e carregado a chave pública para a AWS, você pode usar ssh-keygen para gerar a impressão digital da seguinte forma:

```
$ ssh-keygen -ef path_to_private_key -m PEM | openssl rsa -RSAPublicKey_in -outform DER |  
openssl md5 -c
```

Excluir o par de chaves

Ao excluir um par de chaves, você só exclui a cópia do Amazon EC2 da chave pública. A exclusão de um par de chaves não afeta a chave privada no seu computador nem a chave pública em nenhuma instância já executada usando esse par de chaves. Você não pode executar uma nova instância usando um par de chaves excluído, mas pode continuar a se conectar a quaisquer instâncias executadas usando um par de chaves excluído, desde que ainda tenha o arquivo de chaves privadas (.pem).

Note

Se você estiver usando um grupo Auto Scaling (por exemplo, em um ambiente Elastic Beanstalk), certifique-se de que o par de chaves que você está excluindo não esteja especificado na sua configuração de execução. O Amazon EC2 Auto Scaling executará uma instância de substituição se detectar uma instância não íntegra. No entanto, a execução da instância falhará se o par de chaves não for encontrado.

Você pode excluir um par de chaves usando o console do Amazon EC2 ou a linha de comando.

Para excluir seu par de chaves usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.

2. No painel de navegação, em **RÉDE E SEGURANÇA**, escolha Pares de chaves.
3. Selecione o par de chaves e escolha Excluir.
4. Quando solicitado, escolha Sim.

Para excluir seu par de chaves 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 [Acessando o Amazon EC2 \(p. 3\)](#).

- [delete-key-pair](#) (AWS CLI)
- [Remove-EC2KeyPair](#) (AWS Tools para Windows PowerShell)

Note

Se você criar uma AMI em Linux a partir de uma instância e usar a AMI para executar uma nova instância em uma região ou conta diferente, a nova instância incluirá a chave pública da instância original. Isso permite que você se conecte à nova instância usando o mesmo arquivo de chave privada que sua instância original. Você pode remover essa chave pública da sua instância removendo a entrada do arquivo `.ssh/authorized_keys` usando um editor de texto da sua escolha. Para obter mais informações sobre o gerenciamento de usuários na sua instância e fornecer acesso remoto usando um par de chaves específico, consulte [Gerenciamento de contas de usuário em sua instância do Linux \(p. 483\)](#).

Adição ou substituição de um par de chaves para sua instância

Você pode alterar o par de chaves usado para acessar a conta do sistema padrão da sua instância. Por exemplo, se um usuário da sua organização requisitar acesso à conta do usuário no sistema usando um par de chaves separado, você poderá adicionar esse par de chaves à sua instância. Ou, se alguém tiver uma cópia do arquivo `.pem` e você quiser impedir que ele se conecte à sua instância (por exemplo, se tiver saído da organização), poderá substituir o par de chaves por um novo.

Note

Esses procedimentos são para modificar o par de chaves para a conta do usuário padrão, como `ec2-user`. Para obter mais informações sobre como adicionar contas de usuário à sua instância, consulte [Gerenciamento de contas de usuário em sua instância do Linux \(p. 483\)](#).

Antes de começar, crie um novo par de chaves usando o [console do Amazon EC2 \(p. 617\)](#) ou uma [ferramenta de terceiros \(p. 618\)](#).

Para adicionar ou substituir um par de chaves

1. Recupere a chave pública do seu novo par de chaves. Para obter mais informações, consulte [Recuperação da chave pública para seu par de chaves no Linux \(p. 619\)](#) ou [Recuperação da chave pública para seu par de chaves no Windows \(p. 620\)](#).
2. Conecte-se à sua instância usando o arquivo de chave privada existente.
3. 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.
4. Desconecte-se da sua instância e teste se você pode se conectar à sua instância usando novo arquivo de chave privada.
5. (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 você estiver usando um grupo Auto Scaling (por exemplo, em um ambiente Elastic Beanstalk), certifique-se de que o par de chaves que você está substituindo não esteja especificado na sua configuração de execução. O Amazon EC2 Auto Scaling executará uma instância de substituição se detectar uma instância não íntegra. No entanto, a execução da instância falhará se o par de chaves não for encontrado.

Conexão à sua instância do Linux se você perder sua chave privada

Se você perder a chave privada de uma instância com EBS, poderá recobrar o acesso à sua instância. Você deve parar a instância, separar seu volume do dispositivo raiz e associá-lo a outra instância como volume de dados, modificar o arquivo `authorized_keys`, 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 \(p. 385\)](#).

Este procedimento não é compatível para instâncias baseadas em armazenamento de instâncias. 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`. Se o dispositivo raiz estiver em um volume de armazenamento de instâncias, você deve ter a chave privada para se conectar à instância.

Pré-requisitos

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 se conectar a uma instância com EBS com um par de chaves diferente

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 nos referiremos a isso como a instância original.)
3. Na guia Description (Descrição), salve as informações necessárias para concluir este procedimento.
 - Anote o ID da instância, o ID da AMI e a zona de disponibilidade da instância original.
 - No campo Dispositivo raiz, anote o nome do dispositivo para o volume do dispositivo raiz (por exemplo, `/dev/sda1` ou `/dev/xvda`). Escolha o link e anote o ID de volume no campo ID do EBS (`vol-xxxxxxxxxxxxxxxxxx`).
4. Escolha Ações, selecione Estado da instância e selecione Parar. Se Parar estiver desabilitado, a instância já parou 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 de volumes do armazenamento de instâncias, certifique-se de fazer backup deles em um armazenamento persistente.

5. Escolha 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 [Criação de uma AMI do Linux com Amazon EBS \(p. 111\)](#).
 - Na página Escolher um tipo de instância, deixe o tipo de instância padrão que o assistente seleciona para você.

- Na página Configurar detalhes da instância, especifique a mesma zona de disponibilidade que a instância à qual você deseja se conectar. 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. Crie um novo par de chaves, baixe-o para um local seguro no seu computador e escolha Executar instâncias.
6. 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.)
7. 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.

8. Conecte-se à instância temporária.
9. 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 na 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 em 4 caracteres, onde /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.
 - Amazon Linux, Ubuntu e Debian

```
[ec2-user ~]$ sudo mount /dev/xvdf1 /mnt/tempvol
```

-
- Amazon Linux 2, CentOS, SLES 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
```

10. 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 verificar as permissões no arquivo para verificar se você conseguirá 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 mudaram:

```
[ec2-user ~]$ sudo ls -l /mnt/tempvol/home/ec2-user/.ssh
```

Se o ID do usuário e do grupo tiverem mudado, use o comando a seguir para restaurá-los:

```
[ec2-user ~]$ sudo chown 222:500 /mnt/tempvol/home/ec2-user/.ssh/authorized_keys
```

11. 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
```

12. No console do Amazon EC2, selecione o volume com o ID de volume que você anotou, escolha Actions (Ações), Detach Volume (Desanexar volume) e selecione Yes, Detach (Sim, desanexar). Espere o estado do volume tornar-se available. (Você pode precisar escolher o ícone Atualizar.)
13. Com o volume ainda selecionado, escolha Ações, Associar um volume. Selecione o ID da instância original, especifique o nome do dispositivo anotado anteriormente para o anexo do dispositivo raiz original (/dev/sda1 ou /dev/xvda) e escolha Attach (Anexar).

Important

Se você não especificar o mesmo nome do dispositivo do anexo original, não poderá iniciar a instância original. Amazon EC2 espera o volume do dispositivo raiz em sda1 ou /dev/xvda.

14. Selecione a instância original, escolha Ações, selecione Estado da instância e escolha Iniciar. 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 em relação ao nome do par de chaves original, especifique o nome do novo arquivo de chave privada conectado à sua instância.

15. (Opcional) Você pode encerrar a instância temporária se não tiver utilização adicional para ela. Selecione a instância temporária, escolha Ações, selecione Estado da instância e escolha Encerrar.

Grupos de segurança do Amazon EC2 para instâncias do Linux

Um security group atua como um firewall virtual que controla o tráfego para uma ou mais instâncias. Ao executar uma instância, você pode especificar um ou mais grupos de segurança. Caso contrário, usaremos 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. Você pode modificar as regras para um security group a qualquer momento. As novas regras são aplicadas automaticamente a todas as instâncias associadas ao security group. Quando decidimos se devemos permitir que o tráfego atinja uma instância, avaliamos todas as regras de todos os security groups que estão 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 [Como 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 [Alteração do security group \(p. 762\)](#).

Se houver requisitos que não sejam atendidos pelos security groups, você pode manter seu próprio firewall em qualquer uma das instâncias além de usar security groups.

Se você precisar permitir tráfego para uma instância do Windows, consulte [Grupos de segurança do Amazon EC2 para instâncias Windows](#) no Guia do usuário do Amazon EC2 para instâncias do Windows.

Tópicos

- [Regras de security groups \(p. 627\)](#)
 - [Acompanhamento da conexão \(p. 628\)](#)
- [Security groups padrão \(p. 629\)](#)
- [Security groups personalizados \(p. 630\)](#)
- [Como trabalhar com security groups \(p. 630\)](#)

- Criar um grupo de segurança ([p. 630](#))
- Como descrever security groups ([p. 631](#))
- Como adicionar regras a um security group ([p. 632](#))
- Atualizar regras do security group ([p. 633](#))
- Como excluir regras de um security group ([p. 634](#))
- Excluir um grupo de segurança ([p. 634](#))
- Referência de regras de security groups ([p. 634](#))
 - Regras do Servidor da Web ([p. 635](#))
 - Regras do Servidor de Banco de Dados ([p. 635](#))
 - Regras para conectar à instâncias a partir do seu computador ([p. 637](#))
 - Regras para conectar-se à instâncias a partir de instâncias com o mesmo security group ([p. 637](#))
 - Regras do Path MTU Discovery ([p. 638](#))
 - Regras do Ping/ICMP ([p. 638](#))
 - Regras do Servidor DNS ([p. 639](#))
 - Regras Amazon EFS ([p. 639](#))
 - Regras Elastic Load Balancing ([p. 640](#))

Regras de security groups

As regras de um security group controlam o tráfego de entrada que tem permissão para atingir as instâncias associadas ao security group e o tráfego de saída que tem permissão para sair delas.

As seguintes são as características das regras de security groups:

- Por padrão, os security groups permitem todo o tráfego de saída.
- As regras do security group sempre são permissivas. Você não pode criar regras que negam o acesso.
- Os security groups são stateful — se você enviar uma solicitação de sua instância, o tráfego da resposta dessa solicitação terá permissão para fluir, independentemente das regras de entrada do security group. 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 [Acompanhamento da conexão \(p. 628\)](#).
- Você pode adicionar e remover regras a qualquer momento. As novas regras são aplicadas automaticamente a todas as instâncias associadas ao security group.

Note

O efeito de algumas alterações nas regras pode depender de como o tráfego é acompanhado. Para obter mais informações, consulte [Acompanhamento da conexão \(p. 628\)](#).

- Quando você associa vários security groups a uma instância, as regras de cada security group são efetivamente agregadas para criar um conjunto de regras. Usamos esse conjunto de regras para determinar se devemos permitir acesso.

Note

Você pode atribuir vários security groups 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.

Para cada regra, especifique o seguinte:

- 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, o tipo e o código do ICMP.
- 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.
- (VPO ID da lista de prefixes para o serviço da AWS, por exemplo, p1-1a2b3c4d. Para obter mais informações, consulte [VPC endpoints do gateway](#) no Guia do usuário da Amazon VPC.
- Outro security group. Isso permite que as instâncias associadas ao security group especificado acessem instâncias associadas ao security group. Isso não adiciona regras do security group de origem a esse security group. 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.
- Descrição (opcional): Você pode adicionar uma descrição à regra; por exemplo, para 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 especifica um security group como a origem ou o destino de uma regra, a regra afeta todas as instâncias associadas ao security group. 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 \(p. 723\)](#). 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, aplicaremos a regra mais permissiva. Por exemplo, se você tiver uma regra que permite acesso à porta TCP 22 (SSH) do endereço IP 203.0.113.1 e outra regra que permite acesso à porta TCP 22 de todos, todos terão acesso à porta TCP 22.

Acompanhamento da conexão

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. Isso permite que os security groups sejam stateful — as respostas ao tráfego de entrada têm permissão para sair da instância independentemente das regras do security group de saída e vice-versa. Por exemplo, se você iniciar um comando ICMP ping para a instância em seu computador residencial, e as regras do security group permitirem tráfego ICMP, as informações sobre a conexão (incluindo as informações de porta) serão acompanhadas. 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.

Nem todos os fluxos de tráfego são acompanhados. Se uma regra de security group permitir fluxos TCP ou UDP para todo o tráfego (0.0.0.0/0) e houver uma regra correspondente na outra direção que permite

todo o tráfego de resposta (`0.0.0.0/0`) para todas as portas (`0-65535`), o fluxo do tráfego não será acompanhado. 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.

No exemplo a seguir, o security group tem regras de entrada específicas para tráfego TCP e ICMP, e uma regra de saída que permite todo o tráfego de saída.

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
ICMP	Tudo	0.0.0.0/0

Regras de saída		
Tipo de protocolo	Número da porta	IP de destino
Tudo	Tudo	0.0.0.0/0

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`). O tráfego ICMP é sempre acompanhado, independentemente das regras. Se você remover a regra de saída do security group, todo o tráfego de e para a instância será rastreado, incluindo o tráfego na porta 80 (HTTP).

Um fluxo de tráfego existente que é acompanhado não pode ser interrompido quando você remove a regra do security group que permite o fluxo. Em vez disso, o fluxo é interrompido quando é parado por você ou por outro host por pelo menos alguns minutos (ou até 5 dias para conexões TCP estabelecidas). Para UDP, isso pode exigir ações de terminação no lado remoto do fluxo. Um fluxo de tráfego não acompanhado será interrompido imediatamente se a regra que permite o fluxo for removida ou alterada. Por exemplo, se você remover uma regra que permite todo o tráfego SSH de entrada para a instância, suas conexões SSH existentes com a instância serão interrompidas imediatamente.

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 security group, pois isso será considerado como tráfego de resposta.

Para garantir que o tráfego seja interrompido imediatamente quando você remover uma regra de security group, 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 — Network ACLs são stateless e, portanto, não permitem tráfego de resposta automaticamente. Para obter mais informações, consulte [Network ACLs](#) no Guia do usuário da Amazon VPC.

Security groups 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 security group padrão é denominado `default`, e tem um ID atribuído pela AWS. As seguintes são as regras padrão para cada security group padrão:

- Permite todo o tráfego de entrada de outras instâncias associadas ao security group padrão (o security group especifica a si mesmo como um security group de origem em suas regras de entrada)
- Permite todo o tráfego de saída da instância.

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.`

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 security group não pode começar com 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 [Referência de regras de security groups \(p. 634\)](#).

Como trabalhar com security groups

Você pode criar, visualizar, atualizar e excluir security groups e regras de security groups usando o console do Amazon EC2.

Tarefas

- [Criar um grupo de segurança \(p. 630\)](#)
- [Como descrever security groups \(p. 631\)](#)
- [Como adicionar regras a um security group \(p. 632\)](#)
- [Atualizar regras do security group \(p. 633\)](#)
- [Como excluir regras de um security group \(p. 634\)](#)
- [Excluir um grupo de segurança \(p. 634\)](#)

Criar um grupo de segurança

Você pode criar um security group personalizado usando o console Amazon EC2. Você deve especificar a VPC para a qual você está criando o grupo de segurança.

Para criar um security group novo usando o console

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 dq 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 [Como adicionar regras a um security group \(p. 632\)](#).

Para criar um security group usando a linha de comando

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

O console do Amazon EC2 permite copiar as regras de um security group existente para um novo security group.

Para copiar um security group usando o console

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 dq VPC. Depois de concluir, escolha Create.

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 [Como alterar os grupos de segurança de uma instância](#) no Guia do usuário da Amazon VPC.

Como descrever security groups

Você pode visualizar informações sobre seus security groups usando o console do Amazon EC2 ou a linha de comando.

Para descrever seus grupos de segurança usando o console

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. Exibimos informações gerais na guia Description, regras de entrada na guia Inbound, regras de saída na guia Outbound e tags na aba Tags.

Para descrever um ou mais security groups usando a linha de comando

- [describe-security-groups](#) (AWS CLI)
- [Get-EC2SecurityGroup](#) (AWS Tools para Windows PowerShell)

Como adicionar regras a um security group

Quando você adiciona uma regra a um security group, a nova regra é aplicada automaticamente a todas as instâncias associadas ao security group após um breve período.

Para obter mais informações sobre como escolher regras de security groups para tipos específicos de acesso, consulte [Referência de regras de security groups \(p. 634\)](#).

Para adicionar regras a um security group usando o console

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.
 - 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 IPv4 0 . 0 . 0 . 0 /0. 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.

Note

Se o security group 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 [Referência de regras de security groups \(p. 634\)](#).

5. Escolha 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 IPv4 0 . 0 . 0 . 0 /0. Essa opção permite tráfego de saída para todos os endereços IP.

Note

Se o security group 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 Salvar.

Para adicionar uma ou mais regras a um security group usando a linha de comando

- [authorize-security-group-ingress](#) (AWS CLI)
- [Grant-EC2SecurityGroupIngress](#) (AWS Tools para Windows PowerShell)

Para adicionar uma ou mais regras de saída a um security group usando a linha de comando

- [authorize-security-group-egress](#) (AWS CLI)
- [Grant-EC2SecurityGroupEgress](#) (AWS Tools para Windows PowerShell)

Atualizar regras do security group

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.

Para atualizar uma regra do security group usando o console

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 a ser atualizado e escolha Inbound Rules, para atualizar uma regra para o tráfego de entrada, ou Outbound Rules, para atualizar uma regra para o tráfego de saída.
4. Selecione Edit. Modifique entrada de regra conforme necessário e escolha Save.

Para atualizar 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, não é possível modificar a regra. Em vez disso, você deve excluir a regra existente e adicionar uma regra nova. Para atualizar apenas a descrição da regra, você pode usar os comandos [update-security-group-rule-descriptions-ingress](#) e [update-security-group-rule-descriptions-egress](#).

Para atualizar a descrição da regra de entrada do security group usando a linha de comando

- [update-security-group-rule-descriptions-ingress](#) (AWS CLI)
- [Update-EC2SecurityGroupRuleIngressDescription](#) (AWS Tools para Windows PowerShell)

Para atualizar a descrição da regra de saída do security group usando a linha de comando

- [update-security-group-rule-descriptions-egress](#) (AWS CLI)
- [Update-EC2SecurityGroupRuleEgressDescription](#) (AWS Tools para Windows PowerShell)

Como excluir regras de um security group

Quando você excluir uma regra de um security group, a alteração é aplicada automaticamente a todas as instâncias associadas ao security group.

Para excluir uma regra do security group usando o console

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 Salvar.

Para remover uma ou mais regras de um security group usando a linha de comando

- [revoke-security-group-ingress](#) (AWS CLI)
- [Revoke-EC2SecurityGroupIngress](#) (AWS Tools para Windows PowerShell)

Para remover uma ou mais regras de saída de um security group usando a linha de comando

- [revoke-security-group-egress](#) (AWS CLI)
- [Revoke-EC2SecurityGroupEgress](#) (AWS Tools para Windows PowerShell)

Excluir um grupo de segurança

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.

Para excluir um security group usando o console

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.

Para excluir um security group usando a linha de comando

- [delete-security-group](#) (AWS CLI)
- [Remove-EC2SecurityGroup](#) (AWS Tools para Windows PowerShell)

Referência de regras de security groups

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 um servidor web precisa de regras de security group que permitam entrada HTTP e acesso HTTPS, e uma instância de banco de dados precisa

de regras que permitam 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 \(p. 635\)](#)
- [Regras do Servidor de Banco de Dados \(p. 635\)](#)
- [Regras para conectar à instâncias a partir do seu computador \(p. 637\)](#)
- [Regras para conectar-se à instâncias a partir de instâncias com o mesmo security group \(p. 637\)](#)
- [Regras do Path MTU Discovery \(p. 638\)](#)
- [Regras do Ping/ICMP \(p. 638\)](#)
- [Regras do Servidor DNS \(p. 639\)](#)
- [Regras Amazon EFS \(p. 639\)](#)
- [Regras Elastic Load Balancing \(p. 640\)](#)

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	Port	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 [Guia do usuário da Amazon RDS](#).

Para o IP de origem, especifique um dos seguintes:

- Um endereço IP específico ou intervalo de endereços IP na rede local
- Um ID de security group para um grupo de instâncias que acessa o banco de dados

Tipo de protocolo	Número do protocolo	Port	Observações
TCP	6	1433 (MS SQL)	A porta padrão para acessar um banco de dados Microsoft SQL Server, por exemplo, em uma instância do Amazon RDS
TCP	6	3306 (MySQL/Aurora)	A porta padrão para acessar um banco de dados MySQL ou Aurora, por exemplo, em uma instância do Amazon RDS
TCP	6	5439 (Redshift)	A porta padrão para acessar um banco de dados de cluster do Amazon Redshift.
TCP	6	5432 (PostgreSQL)	A porta padrão para acessar um banco de dados PostgreSQL, por exemplo, em uma instância do Amazon RDS
TCP	6	1521 (Oracle)	A porta padrão para acessar um banco de dados Oracle, por exemplo, em uma instância do Amazon RDS

Opcionalmente, é possível restringir o tráfego de saída de seus servidores de banco de dados, por exemplo, se você quiser permitir 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	Port	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

Tipo de protocolo	Número do protocolo	Port	IP de destino	Observações
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 à instâncias a partir do seu 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	Port	IP de origem
TCP	6	22 (SSH)	O endereço IPv4 público de seu computador ou um intervalo de endereços IP na rede local. Se a VPC estiver habilitada para IPv6 e sua instância tiver um endereço IPv6, você poderá digitar um endereço IPv6 ou um intervalo.
TCP	6	3389 (RDP)	O endereço IPv4 público de seu computador ou um intervalo de endereços IP na rede local. Se a VPC estiver habilitada para IPv6 e sua instância tiver um endereço IPv6, você poderá digitar um endereço IPv6 ou um intervalo.

Regras para conectar-se à instâncias a partir de instâncias com o mesmo security group

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 do Path MTU Discovery

A MTU do caminho é o tamanho de pacote máximo suportado no caminho entre o host de origem e o host de recepção. Se um host enviar um pacote que seja maior que a MTU do host de recebimento ou que seja maior que a MTU de um dispositivo ao longo do caminho, o host de recebimento retornará a seguinte mensagem ICMP:

Destination Unreachable: Fragmentation Needed and Don't Fragment was Set

Para garantir que sua instância possa receber essa mensagem e o pacote não seja eliminado, você deve adicionar uma regra ICMP às regras do security group.

Tipo de protocolo	Número do protocolo	Tipo ICMP	Código ICMP	IP de origem
ICMP	1	3 (destino inacessível)	4 (fragmentação necessária e Não fragmentado selecionado)	Os endereços IP dos hosts que se comunicam com a instância

Regras do 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 (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 (eco)	0	O endereço IPv6 público de seu computador ou

Tipo de protocolo	Número do protocolo	Tipo ICMP	Código ICMP	IP de origem
				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 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 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 security group.

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	Permite acesso SSH de entrada no computador local.

Tipo de protocolo	Número do protocolo	Portas	IP de origem	Observações
			endereços IP da rede.	

Regras Elastic Load Balancing

Se você estiver usando um load balancer, o security group associado ao load balancer deve ter regras que permitam comunicação com suas instâncias ou destinos.

Entrada				
Tipo de protocolo	Número do protocolo	Port	IP de origem	Observações
TCP	6	A porta do ouvinte	Para um load balancer voltado para a Internet: 0.0.0.0/0 (todos os endereços IPv4) Para um load balancer interno: o bloco CIDR IPv4 da VPC	Permitir todo o tráfego de entrada na porta do ouvinte do load balancer.
Saída				
Tipo de protocolo	Número do protocolo	Port	IP de destino	Observações
TCP	6	A porta do ouvinte da instância	O ID do security group da instância	Permitir tráfego de saída para instâncias na porta do ouvinte da instância.
TCP	6	A porta de verificação de integridade	O ID do security group da instância	Permitir tráfego de saída para instâncias na porta de verificação de integridade.

As regras do security group para suas instâncias devem permitir que o load balancer se comunique com as instâncias na porta do ouvinte e na porta de verificação de integridade.

Entrada				
Tipo de protocolo	Número do protocolo	Port	IP de origem	Observações
TCP	6	A porta do ouvinte da instância	O ID do load balancer do security group	Permitir tráfego do load balancer na

				porta do ouvinte da instância.
TCP	6	A porta de verificação de integridade	O ID do load balancer do security group	Permitir tráfego do load balancer na porta de verificação de integridade.

Para obter mais informações, consulte [Configurar grupos de segurança para seu Classic Load Balancer em Guia do usuário para Classic Load Balancers](#) e [Grupos de segurança para sua Balanceador de carga de aplicações](#) no Guia do usuário para Application Load Balancers.

Como controlar o acesso aos recursos do 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 aplicativos 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 security groups 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 \(p. 641\)](#)
- [Atributos de permissões do Amazon EC2 \(p. 641\)](#)
- [IAM e Amazon EC2 \(p. 642\)](#)
- [IAM Políticas do Amazon EC2 \(p. 643\)](#)
- [Funções do IAM para Amazon EC2 \(p. 712\)](#)
- [Como autorizar tráfego de entrada em suas instâncias Linux \(p. 720\)](#)

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 [Como autorizar tráfego de entrada em suas instâncias Linux \(p. 720\)](#).

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 em nível de conta da AWS somente. 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 [Transformação em AMI pública \(p. 100\)](#).

Cada snapshot do Amazon EBS tem um atributo `createVolumePermission` que controla quais contas da AWS podem usar o snapshot. Para obter mais informações, consulte [Compartilhamento de um snapshot do Amazon EBS \(p. 905\)](#).

IAM e Amazon EC2

O IAM permite que você:

- Crie 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?

Como criar um grupo e usuários no 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, digite um nome para o grupo e escolha Next Step.
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 da AWS pode atender às suas necessidades:
 - PowerUserAccess
 - ReadOnlyAccess
 - AmazonEC2FullAccess
 - AmazonEC2ReadOnlyAccess
5. Escolha Create Group.

O grupo novo é listado em Group Name.

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, digite um nome de usuário.
3. Em Access type, selecione Programmatic access e Console de gerenciamento da AWSaccess.
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 digitada 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:

- [IAM Políticas do Amazon EC2 \(p. 643\)](#)
- [Funções do IAM para Amazon EC2 \(p. 712\)](#)
- [AWS Identity and Access Management \(IAM\)](#)
- [Guia do usuário do IAM](#)

IAM Políticas do 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 que concedam aos usuários do permissão para usar os recursos específicos e as ações de API de que precisam e, então, anexar essas políticas aos usuários ou grupos do 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 ações de API do EC2, você não pode especificar para qual recurso um usuário tem permissão de trabalhar com essa ação. Em vez disso, você precisa permitir que os usuários trabalhem com todos os recursos dessa ação.

Tarefa	Tópico
Compreender a estrutura básica de uma política	Sintaxe da política (p. 644)
Definir ações em sua política	Ações do Amazon EC2 (p. 645)
Definir recursos específicos em sua política	Nomes de recursos da Amazon para o Amazon EC2 (p. 645)
Aplicar condições ao uso dos recursos	Chaves de condição do Amazon EC2 (p. 648)
Trabalhar com permissões disponíveis em nível de recurso para o Amazon EC2	Permissões em nível do recurso compatíveis para ações da API do Amazon EC2 (p. 653)
Testar a política	Como verificar se os usuários têm as permissões obrigatórias (p. 652)
Políticas de exemplo para uma CLI ou SDK	Políticas de exemplo para trabalhar com a AWS CLI ou um AWS SDK (p. 680)
Políticas de exemplo para o console do Amazon EC2	Políticas de exemplo para trabalhar no console do Amazon EC2 (p. 705)

Estrutura da política

Os tópicos a seguir explicam a estrutura de uma política do IAM.

Tópicos

- [Sintaxe da política \(p. 644\)](#)
- [Ações do Amazon EC2 \(p. 645\)](#)
- [Nomes de recursos da Amazon para o Amazon EC2 \(p. 645\)](#)
- [Chaves de condição do Amazon EC2 \(p. 648\)](#)
- [Como verificar se os usuários têm as permissões obrigatórias \(p. 652\)](#)

Sintaxe da política

A política do IAM é um documento JSON que consiste em uma ou mais declarações. Cada instrução é estruturada da seguinte maneira:

```
{  
  "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 \(p. 645\)](#).
- 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. Para especificar um recurso na declaração, você precisa usar o Amazon Resource Name (ARN – Nome de recurso da Amazon). Para obter mais informações sobre como especificar o valor do ARN, consulte [Nomes de recursos da Amazon para o Amazon EC2 \(p. 645\)](#). Para obter mais informações sobre quais ações de API dão suporte a quais ARNs, consulte [Permissões em nível do recurso compatíveis para ações da API do Amazon EC2 \(p. 653\)](#). Caso a ação da API não dê suporte a ARNs, use o curinga * para especificar que todos os recursos podem ser afetados pela ação.
- 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 \(p. 648\)](#).

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 \(p. 680\)](#).

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*"
```

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 no Amazon EC2 API Reference](#).

Nomes de recursos da Amazon para o Amazon EC2

Cada declaração de política do IAM se aplica aos recursos que você especifica usando os ARNs.

Important

Atualmente, nem todas as ações de API são compatíveis com ARNs individuais. Vamos adicionar suporte para ações de API e ARNs para recursos de Amazon EC2 adicionais posteriormente. Para obter informações sobre quais ARNs você pode usar com quais ações da API do Amazon EC2, bem como sobre as chaves de condição compatíveis para cada ARN, consulte [Permissões em nível do recurso compatíveis para ações da API do Amazon EC2 \(p. 653\)](#).

Um ARN tem a seguinte sintaxe geral:

```
arn:[aws]:[service]:[region]:[account]:resourceType/resourcePath
```

serviço

O serviço (por exemplo, ec2).

região

A região do recurso (por exemplo, us-east-1).

conta

A 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, você pode indicar uma instância específica (`i-1234567890abcdef0`) na declaração usando o ARN da seguinte forma:

```
"Resource": "arn:aws:ec2:us-east-1:123456789012:instance/i-1234567890abcdef0"
```

Você também pode especificar todas as instâncias pertencentes a uma conta específica usando o caractere curinga * da seguinte forma:

```
"Resource": "arn:aws:ec2:us-east-1:123456789012:instance/*"
```

Para especificar todos os recursos ou caso uma ação de API específica não dê suporte a ARNs, use o curinga * no elemento Resource da seguinte maneira:

```
"Resource": "*"
```

A tabela a seguir descreve os ARNs para cada tipo de recurso usado pelas ações da API do Amazon EC2.

Tipo de recurso	ARN
Todos os recursos do Amazon EC2	arn:aws:ec2:*
Todos os recursos do Amazon EC2 de propriedade da conta especificada, na região especificada	arn:aws:ec2:region:account:*

Tipo de recurso	ARN
Gateway do cliente	arn:aws:ec2:region:account:customer-gateway/cgw-id Em que cgw-id é cgw-xxxxxxxx
Conjunto de opções de DHCP	arn:aws:ec2:region:account:dhcp-options/dhcp-options-id Em que dhcp-options-id é dopt-xxxxxxxx
GPU elástica	arn:aws:ec2:region:account:elastic-gpu/*
Imagen	arn:aws:ec2:region::image/image-id Em que image-id é o ID da AMI, AKI ou ARI, e account não é usada
Instância	arn:aws:ec2:region:account:instance/instance-id Em que instance-id é i-xxxxxxxx ou i-xxxxxxxxxxxxxxxxx
Perfil da instância	arn:aws:iam::account:instance-profile/instance-profile-name Em que instance-profile-name é o nome do perfil da instância, e region não é usada
Gateway da Internet	arn:aws:ec2:region:account:internet-gateway/igw-id Em que igw-id é igw-xxxxxxxx
Par de chaves	arn:aws:ec2:region:account:key-pair/key-pair-name Em que key-pair-name é o nome do par de chaves (por exemplo, gsg-keypair)
Modelo de execução	arn:aws:ec2:region:account:launch-template/launch-template-id Em que launch-template-id é lt-xxxxxxxxxxxxxx
gateway NAT	arn:aws:ec2:region:account:natgateway/natgateway-id Onde natgateway-id é nat-xxxxxxxxxxxxxx
Conexão ACL	arn:aws:ec2:region:account:network-acl-nacl-id Em que nacl-id é acl-xxxxxxxx
Interface de rede	arn:aws:ec2:region:account:network-interface/eni-id Em que eni-id é eni-xxxxxxxx
Placement group	arn:aws:ec2:region:account:placement-group/placement-group-name Em que placement-group-name é o nome do placement group (por exemplo, my-cluster)
Instância reservada	arn:aws:ec2:region:account:reserved-instances/reservation-id Em que reservation-id é xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
Tabela de rotas	arn:aws:ec2:region:account:route-table/route-table-id Em que route-table-id é rtb-xxxxxxxx

Tipo de recurso	ARN
Grupo de segurança	arn:aws:ec2:region:account:security-group/security-group-id Em que security-group-id é sg-xxxxxxxx
Snapshot	arn:aws:ec2:region::snapshot/snapshot-id Em que snapshot-id é snap-xxxxxxxx ou snap-xxxxxxxxxxxxxxxxx, e account não é usada
Solicitação do Instância spot	arn:aws:ec2:region:account:spot-instances-request/spot-instance-request-id Em que spot-instance-request-id é sir-xxxxxxxx
Sub-rede	arn:aws:ec2:region:account:subnet/subnet-id Em que subnet-id é subnet-xxxxxxxx
Volume	arn:aws:ec2:region:account:volume/volume-id Em que volume-id é vol-xxxxxxxx ou vol-xxxxxxxxxxxxxxxxx
VPC	arn:aws:ec2:region:account:vpc/vpc-id Em que vpc-id é vpc-xxxxxxxx
Conexão de emparelhamento de VPC	arn:aws:ec2:region:account:vpc-peering-connection/vpc-peering-connection-id Em que vpc-peering connection-id é pcx-xxxxxxxx
conexão VPN	arn:aws:ec2:region:account:vpn-connection/vpn-connection-id Em que vpn-connection-id é vpn-xxxxxxxx
gateway VPN	arn:aws:ec2:region:account:vpn-gateway/vpn-gateway-id Em que vpn-gateway-id é vgw-xxxxxxxx

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 declaração, separe seus ARNs com vírgulas, como se segue:

```
"Resource": ["arn1", "arn2"]
```

Para obter mais informações gerais sobre ARNs, consulte [Nomes de recurso da Amazon \(ARN\) e namespaces de serviço da AWS](#) no Referência geral do Amazon Web Services. Para obter mais informações sobre os recursos criados ou modificados pelas ações do Amazon EC2, e sobre o ARN que você pode usar em suas declarações de políticas do IAM, consulte [Como conceder as permissões necessárias aos usuários do IAM para recursos do Amazon EC2](#) no Amazon EC2 API Reference.

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.

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 [Variáveis de política](#) 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.

O Amazon EC2 implementa as seguintes chaves de condição específicas ao serviço. Para obter informações sobre quais chaves de condição você pode usar com quais recursos do Amazon EC2, ação por ação, consulte [Permissões em nível do recurso compatíveis para ações da API do Amazon EC2 \(p. 653\)](#).

Chave de condição	Par de chave/valor	Tipos de avaliação
ec2:AccepterVpc	"ec2:AccepterVpc":"vpc-arn" Em que vpc-arn é o ARN da VPC para a VPC receptora em uma conexão de emparelhamento da VPC	ARN, nulo
ec2:AuthorizedService	"ec2:AuthorizedService":"service-principal" Em que service-principal é o principal do serviço (por exemplo, ecs.amazonaws.com)	Sequência, nula
ec2:AuthorizedUser	"ec2:AuthorizedUser":"principal-arn" Onde principal-arn é o ARN para o administrador (por exemplo, arn:aws:iam::123456789012:root)	ARN, nulo
ec2:AvailabilityZone	"ec2:AvailabilityZone":"az-api-name" Em que az-api-name é o nome da zona de disponibilidade (por exemplo, us-east-2a) Para listar as zonas de disponibilidade, use describe-availability-zones	Sequência, nula
ec2>CreateAction	"ec2:CreateAction":"api-name" Em que api-name é o nome da ação de criação de recurso (por exemplo, RunInstances)	Sequência, nula
ec2:EbsOptimized	"ec2:EbsOptimized":"optimized-flag"	Booliano, nulo

Chave de condição	Par de chave/valor	Tipos de avaliação
	Em que optimized-flag é true false (para uma instância)	
ec2:ElasticGpuType	"ec2:ElasticGpuType":"elastic-gpu-type" Onde elastic-gpu-type é o nome do tipo de GPU elástica	Sequência, nula
ec2:Encrypted	"ec2:Encrypted":"encrypted-flag" Em que encrypted-flag é true false (para um volume do EBS)	Booliano, nulo
ec2:ImageType	"ec2:ImageType":"image-type-api-name" Em que image-type-api-name é ami aki ari	Sequência, nula
ec2:InstanceMarketType	"ec2:InstanceMarketType":"market-type" Onde market-type é spot on-demand	Sequência, nula
ec2:InstanceProfile	"ec2:InstanceProfile":"instance-profile-arn" Em que instance-profile-arn é o ARN do perfil da instância	ARN, nulo
ec2:InstanceType	"ec2:InstanceType":"instance-type-api-name" Em que instance-type-api-name é o nome do tipo da instância.	Sequência, nula
ec2:IsLaunchTemplateResource	"ec2:IsLaunchTemplateResource":"launch-template-resource-flag" Em que launch-template-resource-flag é true false	Booliano, nulo
ec2:LaunchTemplate	"ec2:LaunchTemplate":"launch-template-arn" Em que launch-template-arn é o Nome de região da Amazon (ARN) do modelo de execução	ARN, nulo
ec2:Owner	"ec2:Owner":"account-id" Em que account-id é amazon aws-marketplace aws-account-id	Sequência, nula
ec2:ParentSnapshot	"ec2:ParentSnapshot":"snapshot-arn" Em que snapshot-arn é o ARN do snapshot	ARN, nulo
ec2:ParentVolume	"ec2:ParentVolume":"volume-arn" Em que volume-arn é o ARN do volume	ARN, nulo
ec2:Permission	"ec2:Permission":"permission" Onde permission é INSTANCE-ATTACH EIP-ASSOCIATE	Sequência, nula
ec2:PlacementGroup	"ec2:PlacementGroup":"placement-group-arn" Em que placement-group-arn é o ARN do placement group	ARN, nulo

Chave de condição	Par de chave/valor	Tipos de avaliação
ec2:PlacementGroup	"ec2:PlacementGroupStrategy":"placement-group-strategy" Em que placement-group-strategy é cluster spread	Sequência, nula
ec2:ProductCode	"ec2:ProductCode":"product-code" Em que product-code é o código do produto	Sequência, nula
ec2:Public	"ec2:Public":"public-flag" Em que public-flag é true false (para uma AMI)	Booliano, nulo
ec2:Region	"ec2:Region":"region-name" Em que region-name é o nome da região (por exemplo, us-east-2). Para listar as regiões, use describe-regions . Essa chave de condição pode ser usada com qualquer ação do Amazon EC2.	Sequência, nula
ec2:RequesterVpc	"ec2:RequesterVpc":"vpc-arn" Em que vpc-arn é o ARN da VPC para a VPC solicitante em uma conexão de emparelhamento da VPC	ARN, nulo
ec2:ReservedInstancesOfferingType	"ec2:ReservedInstancesOfferingType":"offering-type" Em que offering-type é No Upfront Partial Upfront All Upfront	Sequência, nula
ec2:ResourceTag	"/ec2:ResourceTag/tag-key":"tag-value" Em que tag-key e tag-value são o par de tag-chave	Sequência, nula
ec2:RootDeviceType	"ec2:RootDeviceType":"root-device-type-name" Em que root-device-type-name é ebs instance-store	Sequência, nula
ec2:SnapshotTime	"ec2:SnapshotTime":"time" Em que time é a hora da criação do snapshot (por exemplo, 2013-06-01T00: 00:00Z)	Data, nulo
ec2:Subnet	"ec2:Subnet":"subnet-arn" Em que subnet-arn é o ARN da sub-rede	ARN, nulo
ec2:Tenancy	"ec2:Tenancy":"tenancy-attribute" Em que tenancy-attribute é default dedicated host	Sequência, nula
ec2:VolumeIops	"ec2:VolumeIops":"volume-iops" Onde volume-iops é as operações de entrada/saída por segundo (IOPS). Para obter mais informações, consulte Tipos de volume do Amazon EBS (p. 844) .	Numérico, nulo
ec2:VolumeSize	"ec2:VolumeSize":"volume-size" Em que volume-size é o tamanho do volume, em GiB	Numérico, nulo

Chave de condição	Par de chave/valor	Tipos de avaliação
ec2:VolumeType	"ec2:VolumeType":"volume-type-name" Em que volume-type-name é gp2 para volumes do Finalidade geral (SSD), io1 para volumes do Provisioned IOPS SSD, st1 para volumes de Disco rígido com throughput otimizado, sc1 para volumes de Cold HDD ou standard para volumes Magnético.	Sequência, nula
ec2:Vpc	"ec2:Vpc":"vpc-arn" Em que vpc-arn é o ARN da VPC	ARN, nulo

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.

Todas as ações do Amazon EC2 oferecem suporte às chaves de condição `aws:RequestedRegion` e `ec2:Region`. Para obter mais informações, consulte [Exemplo: restrição de acesso a uma região específica \(p. 681\)](#).

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 exemplos de políticas, consulte [Permitir que uma instância do EC2 anexe ou desanexe volumes](#) e [Exemplo: permitir que uma instância específica visualize recursos em outros serviços da AWS \(p. 703\)](#). A chave `ec2:SourceInstanceARN` não pode ser usada como uma variável para preencher o ARN para o elemento `Resource` na instrução.

As chaves de condição da AWS a seguir foram introduzidas para o Amazon EC2 e têm suporte de um número limitado de serviços adicionais.

Chave de condição	Par de chave/valor	Tipos de avaliação
aws:RequestTag/tag-key	"aws:Request/tag-key":"tag-value" Em que tag-key e tag-value são o par de chave-valor da chave	Sequência, nula
aws:TagKeys	"aws:TagKeys":"tag-key" Em que tag-key é uma lista de chaves de tags (por exemplo, ["A","B"])	Sequência, nula

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 \(p. 680\)](#).

Como verificar se os usuários têm as permissões obrigatórias

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.

Caso a ação Amazon EC2 que você está testando criar ou modificar 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 concluirá a verificação da autorização, mas não concluirá 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 e [decode-authorization-message](#) no AWS CLI Command Reference.

Permissões em nível do recurso compatíveis para ações da API do Amazon EC2

Permissões no nível do recurso dizem respeito à capacidade de especificar em quais recursos os usuários têm permissões para executar ações. O Amazon EC2 oferece 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.

A tabela a seguir descreve as ações da API do Amazon EC2 que oferecem suporte no momento a permissões em nível de recurso, bem como os recursos com suporte (e os respectivos ARNs) e as chaves de condição de cada ação. Ao especificar um ARN, você pode usar o caractere curinga * em seus caminhos. Por exemplo, quando você não pode ou não deseja especificar IDs exatos de recursos. Para exemplos de como usar caracteres curinga, consulte [Políticas de exemplo para trabalhar com a AWS CLI ou um AWS SDK \(p. 680\)](#).

Important

Caso uma ação da API do Amazon EC2 não estiver listada nessa tabela, isso significa que ela não oferece suporte a permissões em nível de recurso. Se uma ação da API do Amazon EC2 não oferecer suporte a permissões em nível de recurso, você poderá conceder aos usuários permissões para usar a ação, mas precisará especificar um * para o elemento do recurso da declaração de política. Para ver um exemplo, consulte [Exemplo: acesso somente leitura \(p. 680\)](#). Para obter uma lista de ações da API do Amazon EC2 que não oferecem suporte a permissões em nível de recurso, consulte [Permissões em nível de recurso não compatíveis](#) no Amazon EC2 API Reference.

Ação API	Recursos	Chaves de condição
AcceptVpcPeeringConnection	Conexão de emparelhamento de VPC <code>arn:aws:ec2:region:account:vpc-peering-connection/*</code>	<code>ec2:AccepterVpc</code> <code>ec2:Region</code> <code>ec2:ResourceTag/tag-key</code>

Ação API	Recursos	Chaves de condição
	arn:aws:ec2:region:account:vpc-peering-connection/vpc-peering-connection-id	ec2:RequesterVpc
	VPC arn:aws:ec2:region:account:vpc/* arn:aws:ec2:region:account:vpc/vpc-id Em que vpc-id é uma VPC de propriedade do receptor.	ec2:ResourceTag/tag-key ec2:Region ec2:Tenancy
AssociateIamInstanceProfile	Instância arn:aws:ec2:region:account:instance/* arn:aws:ec2:region:account:instance/instance-id	ec2:AvailabilityZone ec2:EbsOptimized ec2:InstanceProfile ec2:InstanceType ec2:PlacementGroup ec2:Region ec2:ResourceTag/tag-key ec2:RootDeviceType ec2:Tenancy
AttachClassicLinkVpc	Instância arn:aws:ec2:region:account:instance/* arn:aws:ec2:region:account:instance/instance-id	ec2:AvailabilityZone ec2:EbsOptimized ec2:InstanceProfile ec2:InstanceType ec2:PlacementGroup ec2:Region ec2:ResourceTag/tag-key ec2:RootDeviceType ec2:Tenancy
	Grupo de segurança arn:aws:ec2:region:account:security-group/* arn:aws:ec2:region:account:security-group/security-group-id Onde o security group é o security group da VPC.	ec2:Region ec2:ResourceTag/tag-key ec2:Vpc

Ação API	Recursos	Chaves de condição
	VPC arn:aws:ec2:region:account:vpc/* arn:aws:ec2:region:account:vpc/vpc-id	ec2:Region ec2:ResourceTag/tag-key ec2:Tenancy
AttachVolume	Instância arn:aws:ec2:region:account:instance/* arn:aws:ec2:region:account:instance/instance-id	ec2:AvailabilityZone ec2:EbsOptimized ec2:InstanceProfile ec2:InstanceType ec2:PlacementGroup ec2:Region ec2:ResourceTag/tag-key ec2:RootDeviceType ec2:Tenancy
	Volume arn:aws:ec2:region:account:volume/* arn:aws:ec2:region:account:volume/volume-id	ec2:AvailabilityZone ec2:Encrypted ec2:ParentSnapshot ec2:Region ec2:ResourceTag/tag-key ec2:Volumelops ec2:VolumeSize ec2:VolumeType
AuthorizeSecurityGroupEgress	Esgo de segurança arn:aws:ec2:region:account:security-group/* arn:aws:ec2:region:account:security-group/security-group-id	ec2:Region ec2:ResourceTag/tag-key ec2:Vpc
	Esgo de segurança arn:aws:ec2:region:account:security-group/* arn:aws:ec2:region:account:security-group/security-group-id	ec2:Region ec2:ResourceTag/tag-key ec2:Vpc

Ação API	Recursos	Chaves de condição
CreateLaunchTemplateVersion	Modelo de execução arn:aws:ec2:region:account:launch-template/* arn:aws:ec2:region:account:launch-template/launch-template-id	ec2:Region ec2:ResourceTag/tag-key
CreateNetworkInterfacePermission	Interface de rede arn:aws:ec2:region:account:network-interface/* arn:aws:ec2:region:account:network-interface/eni-id	ec2:AuthorizedUser ec2:AvailabilityZone ec2:Permission ec2:Region ec2:ResourceTag/tag-key ec2:Subnet ec2:Vpc
CreateRoute	Tabela de rotas arn:aws:ec2:region:account:route-table/* arn:aws:ec2:region:account:route-table/route-table-id	ec2:Region ec2:ResourceTag/tag-key ec2:Vpc
CreateSnapshot	Snapshot	ec2:ParentVolume ec2:Region aws:RequestTag/tag-key aws:TagKeys
	Volume arn:aws:ec2:region:account:volume/* arn:aws:ec2:region:account:volume/volume-id	ec2:Encrypted ec2:Region ec2:VolumeLops ec2:VolumeSize ec2:VolumeType ec2:ResourceTag/tag-key
CreateTags	Amazon FPGA Image (AFI – Imagem FPGA da Amazon) arn:aws:ec2:region:account:fpga-image/* arn:aws:ec2:region:account:fpga-image/afi-id	ec2:CreateAction ec2:Region ec2:ResourceTag/tag-key
		aws:RequestTag/tag-key aws:TagKeys

Ação API	Recursos	Chaves de condição
	Conjunto de opções de DHCP arn:aws:ec2:region:account:dhcp-options/* arn:aws:ec2:region:account:dhcp-options/dhcp-options-id	ec2>CreateAction ec2:Region ec2:ResourceTag/tag-key aws:RequestTag/tag-key aws:TagKeys
	Imagem arn:aws:ec2:region::image/* arn:aws:ec2:region::image/image-id	ec2>CreateAction ec2:ImageType ec2:Owner ec2:Public ec2:Region ec2:ResourceTag/tag-key ec2:RootDeviceType aws:RequestTag/tag-key aws:TagKeys
	Instância arn:aws:ec2:region:account:instance/* arn:aws:ec2:region:account:instance/instance-id	ec2:AvailabilityZone ec2>CreateAction ec2:EbsOptimized ec2:InstanceProfile ec2:InstanceType ec2:PlacementGroup ec2:Region ec2:ResourceTag/tag-key ec2:RootDeviceType ec2:Tenancy aws:RequestTag/tag-key aws:TagKeys

Ação API	Recursos	Chaves de condição
	Gateway da Internet arn:aws:ec2:region:account:internet-gateway/* arn:aws:ec2:region:account:internet-gateway/igw-id	ec2>CreateAction ec2:Region ec2:ResourceTag/tag-key aws:RequestTag/tag-key aws:TagKeys
	Modelo de execução arn:aws:ec2:region:account:launch-template/* arn:aws:ec2:region:account:launch-template/launch-template-id	ec2>CreateAction ec2:Region ec2:ResourceTag/tag-key aws:RequestTag/tag-key aws:TagKeys
	gateway NAT arn:aws:ec2:region:account:natgateway/* arn:aws:ec2:region:account:natgateway/natgateway-id	ec2>CreateAction ec2:Region ec2:ResourceTag/tag-key aws:RequestTag/tag-key aws:TagKeys
	Conexão ACL arn:aws:ec2:region:account:network-acl/* arn:aws:ec2:region:account:network-acl/nacl-id	ec2>CreateAction ec2:Region ec2:ResourceTag/tag-key ec2:Vpc aws:RequestTag/tag-key aws:TagKeys
	Interface de rede arn:aws:ec2:region:account:network-interface/* arn:aws:ec2:region:account:network-interface/eni-id	ec2:AvailabilityZone ec2>CreateAction ec2:Region ec2:Subnet ec2:ResourceTag/tag-key ec2:Vpc aws:RequestTag/tag-key aws:TagKeys

Ação API	Recursos	Chaves de condição
	Instância reservada arn:aws:ec2:region:account:reserved-instances/* arn:aws:ec2:region:account:reserved-instances/reservation-id	ec2:AvailabilityZone ec2>CreateAction ec2:InstanceType ec2:ReservedInstancesOfferingType ec2:Region ec2:ResourceTag/tag-key ec2:Tenancy aws:RequestTag/tag-key aws:TagKeys
	Tabela de rotas arn:aws:ec2:region:account:route-table/* arn:aws:ec2:region:account:route-table/route-table-id	ec2>CreateAction ec2:Region ec2:ResourceTag/tag-key ec2:Vpc aws:RequestTag/tag-key aws:TagKeys
	Grupo de segurança arn:aws:ec2:region:account:security-group/* arn:aws:ec2:region:account:security-group/security-group-id	ec2>CreateAction ec2:Region ec2:ResourceTag/tag-key ec2:Vpc aws:RequestTag/tag-key aws:TagKeys
	Snapshot arn:aws:ec2:region::snapshot/* arn:aws:ec2:region::snapshot/snapshot-id	ec2>CreateAction ec2:Owner ec2:ParentVolume ec2:Region ec2:ResourceTag/tag-key ec2:SnapshotTime ec2:VolumeSize aws:RequestTag/tag-key aws:TagKeys

Ação API	Recursos	Chaves de condição
	Solicitação de instância Spot arn:aws:ec2:region:account:spot-instances-request/* arn:aws:ec2:region:account:spot-instances-request/spot-instance-request-id	ec2>CreateAction ec2:Region ec2:ResourceTag/tag-key aws:RequestTag/tag-key aws:TagKeys
	Sub-rede arn:aws:ec2:region:account:subnet/* arn:aws:ec2:region:account:subnet/subnet-id	ec2:AvailabilityZone ec2>CreateAction ec2:Region ec2:ResourceTag/tag-key ec2:Vpc aws:RequestTag/tag-key aws:TagKeys
	Volume arn:aws:ec2:region:account:volume/* arn:aws:ec2:region:account:volume/volume-id	ec2:AvailabilityZone ec2>CreateAction ec2:Encrypted ec2:ParentSnapshot ec2:Region ec2:ResourceTag/tag-key ec2:Volumelops ec2:VolumeSize ec2:VolumeType aws:RequestTag/tag-key aws:TagKeys
	VPC arn:aws:ec2:region:account:vpc/* arn:aws:ec2:region:account:vpc/vpc-id	ec2>CreateAction ec2:Region ec2:ResourceTag/tag-key ec2:Tenancy aws:RequestTag/tag-key aws:TagKeys

Ação API	Recursos	Chaves de condição
	Conexão VPN arn:aws:ec2:region:account:vpn-connection/* arn:aws:ec2:region:account:vpn-connection/vpn-connection-id	ec2>CreateAction ec2:Region ec2:ResourceTag/tag-key aws:RequestTag/tag-key aws:TagKeys
	gateway VPN arn:aws:ec2:region:account:vpn-gateway/* arn:aws:ec2:region:account:vpn-gateway/vpn-gateway-id	ec2>CreateAction ec2:Region ec2:ResourceTag/tag-key aws:RequestTag/tag-key aws:TagKeys
CreateVolume	Volume arn:aws:ec2:region:account:volume/*	ec2:AvailabilityZone ec2:Encrypted ec2:ParentSnapshot ec2:Region ec2:VolumeLops ec2:VolumeSize ec2:VolumeType aws:RequestTag/tag-key aws:TagKeys
CreateVpcPeeringConnection	VPC arn:aws:ec2:region:account:vpc/* arn:aws:ec2:region:account:vpc/vpc-id Em que vpc-id é uma VPC solicitante.	ec2:ResourceTag/tag-key ec2:Region ec2:Tenancy
	Conexão de emparelhamento de VPC arn:aws:ec2:region:account:vpc-peering-connection/*	ec2:AcceptorVpc ec2:Region ec2:RequesterVpc
DeleteCustomerGateway	Gateway do cliente arn:aws:ec2:region:account:customer-gateway/* arn:aws:ec2:region:account:customer-gateway/cgw-id	ec2:Region ec2:ResourceTag/tag-key

Ação API	Recursos	Chaves de condição
DeleteDhcpOptions	Conjunto de opções de DHCP arn:aws:ec2:region:account:dhcp-options/* arn:aws:ec2:region:account:dhcp-options/dhcp-options-id	ec2:Region ec2:ResourceTag/tag-key
DeleteInternetGateway	Gateway da Internet arn:aws:ec2:region:account:internet-gateway/* arn:aws:ec2:region:account:internet-gateway/igw-id	ec2:Region ec2:ResourceTag/tag-key
DeleteLaunchTemplate	Modelo de execução arn:aws:ec2:region:account:launch-template/* arn:aws:ec2:region:account:launch-template/launch-template-id	ec2:Region ec2:ResourceTag/tag-key
DeleteLaunchTemplateVersion	Modelo de execução arn:aws:ec2:region:account:launch-template/* arn:aws:ec2:region:account:launch-template/launch-template-id	ec2:Region ec2:ResourceTag/tag-key
DeleteNetworkAcl	Conexão ACL arn:aws:ec2:region:account:network-acl/* arn:aws:ec2:region:account:network-acl-nacl-id	ec2:Region ec2:ResourceTag/tag-key ec2:Vpc
DeleteNetworkAclEntry	Conexão ACL arn:aws:ec2:region:account:network-acl/* arn:aws:ec2:region:account:network-acl-nacl-id	ec2:Region ec2:ResourceTag/tag-key ec2:Vpc
DeleteRoute	Tabela de rotas arn:aws:ec2:region:account:route-table/* arn:aws:ec2:region:account:route-table/route-table-id	ec2:Region ec2:ResourceTag/tag-key ec2:Vpc
DeleteRouteTable	Tabela de rotas arn:aws:ec2:region:account:route-table/* arn:aws:ec2:region:account:route-table/route-table-id	ec2:Region ec2:ResourceTag/tag-key ec2:Vpc

Ação API	Recursos	Chaves de condição
DeleteSecurityGroup	Grupo de segurança arn:aws:ec2:region:account:security-group/security-group-id	ec2:Region ec2:ResourceTag/tag-key ec2:Vpc
DeleteSnapshot	Snapshot arn:aws:ec2:region::snapshot/* arn:aws:ec2:region::snapshot/snapshot-id	ec2:Owner ec2:ParentVolume ec2:Region ec2:SnapshotTime ec2:VolumeSize ec2:ResourceTag/tag-key
DeleteTags	Amazon FPGA Image (AFI – Imagem FPGA da Amazon) arn:aws:ec2:region:account:fpga-image/* arn:aws:ec2:region:account:fpga-image/afi-id	ec2:Region ec2:ResourceTag/tag-key aws:RequestTag/tag-key aws:TagKeys
	Conjunto de opções de DHCP arn:aws:ec2:region:account:dhcp-options/* arn:aws:ec2:region:account:dhcp-options/dhcp-options-id	ec2:Region ec2:ResourceTag/tag-key aws:RequestTag/tag-key aws:TagKeys
	Imagen arn:aws:ec2:region::image/* arn:aws:ec2:region::image/image-id	ec2:Region ec2:ResourceTag/tag-key aws:RequestTag/tag-key aws:TagKeys
	Instância arn:aws:ec2:region:account:instance/* arn:aws:ec2:region:account:instance/instance-id	ec2:Region ec2:ResourceTag/tag-key aws:RequestTag/tag-key aws:TagKeys
	Gateway da Internet arn:aws:ec2:region:account:internet-gateway/* arn:aws:ec2:region:account:internet-gateway/igw-id	ec2:Region ec2:ResourceTag/tag-key aws:RequestTag/tag-key aws:TagKeys

Ação API	Recursos	Chaves de condição
	Modelo de execução arn:aws:ec2:region:account:launch-template/* arn:aws:ec2:region:account:launch-template/launch-template-id	ec2:Region ec2:ResourceTag/tag-key aws:RequestTag/tag-key aws:TagKeys
	gateway NAT arn:aws:ec2:region:account:natgateway/* arn:aws:ec2:region:account:natgateway/natgateway-id	ec2:Region ec2:ResourceTag/tag-key aws:RequestTag/tag-key aws:TagKeys
	Conexão ACL arn:aws:ec2:region:account:network-acl/* arn:aws:ec2:region:account:network-acl-nacl-id	ec2:Region ec2:ResourceTag/tag-key aws:RequestTag/tag-key aws:TagKeys
	Interface de rede arn:aws:ec2:region:account:network-interface/* arn:aws:ec2:region:account:network-interface/eni-id	ec2:Region ec2:ResourceTag/tag-key aws:RequestTag/tag-key aws:TagKeys
	Instância reservada arn:aws:ec2:region:account:reserved-instances/* arn:aws:ec2:region:account:reserved-instances/reservation-id	ec2:Region ec2:ResourceTag/tag-key aws:RequestTag/tag-key aws:TagKeys
	Tabela de rotas arn:aws:ec2:region:account:route-table/* arn:aws:ec2:region:account:route-table/route-table-id	ec2:Region ec2:ResourceTag/tag-key aws:RequestTag/tag-key aws:TagKeys
	Grupo de segurança arn:aws:ec2:region:account:security-group/* arn:aws:ec2:region:account:security-group/security-group-id	ec2:Region ec2:ResourceTag/tag-key aws:RequestTag/tag-key aws:TagKeys

Ação API	Recursos	Chaves de condição
	Snapshot arn:aws:ec2:region::snapshot/* arn:aws:ec2:region::snapshot/snapshot-id	ec2:Region ec2:ResourceTag/tag-key aws:RequestTag/tag-key aws:TagKeys
	Solicitação de instância Spot arn:aws:ec2:region:account:spot-instances-request/* arn:aws:ec2:region:account:spot-instances-request/spot-instance-request-id	ec2:Region ec2:ResourceTag/tag-key aws:RequestTag/tag-key aws:TagKeys
	Sub-rede arn:aws:ec2:region:account:subnet/* arn:aws:ec2:region:account:subnet/subnet-id	ec2:Region ec2:ResourceTag/tag-key aws:RequestTag/tag-key aws:TagKeys
	Volume arn:aws:ec2:region:account:volume/* arn:aws:ec2:region:account:volume/volume-id	ec2:Region ec2:ResourceTag/tag-key aws:RequestTag/tag-key aws:TagKeys
	VPC arn:aws:ec2:region:account:vpc/* arn:aws:ec2:region:account:vpc/vpc-id	ec2:Region ec2:ResourceTag/tag-key aws:RequestTag/tag-key aws:TagKeys
	Conexão VPN arn:aws:ec2:region:account:vpn-connection/* arn:aws:ec2:region:account:vpn-connection/vpn-connection-id	ec2:Region ec2:ResourceTag/tag-key aws:RequestTag/tag-key aws:TagKeys
	gateway VPN arn:aws:ec2:region:account:vpn-gateway/* arn:aws:ec2:region:account:vpn-gateway/vpn-gateway-id	ec2:Region ec2:ResourceTag/tag-key aws:RequestTag/tag-key aws:TagKeys

Ação API	Recursos	Chaves de condição
DeleteVolume	Volume arn:aws:ec2:region:account:volume/* arn:aws:ec2:region:account:volume/volume-id	ec2:AvailabilityZone ec2:Encrypted ec2:ParentSnapshot ec2:Region ec2:ResourceTag/tag-key ec2:Volumelops ec2:VolumeSize ec2:VolumeType
DeleteVpcPeeringConnection	Conexão de emparelhamento de VPC arn:aws:ec2:region:account:vpc-peering-connection/* arn:aws:ec2:region:account:vpc-peering-connection/vpc-peering-connection-id	ec2:AcceptorVpc ec2:Region ec2:ResourceTag/tag-key ec2:RequesterVpc
DetachClassicLinkVpc	Instância arn:aws:ec2:region:account:instance/* arn:aws:ec2:region:account:instance/instance-id	ec2:AvailabilityZone ec2:EbsOptimized ec2:InstanceProfile ec2:InstanceType ec2:PlacementGroup ec2:Region ec2:ResourceTag/tag-key ec2:RootDeviceType ec2:Tenancy
	VPC arn:aws:ec2:region:account:vpc/* arn:aws:ec2:region:account:vpc/vpc-id	ec2:Region ec2:ResourceTag/tag-key ec2:Tenancy

Ação API	Recursos	Chaves de condição
DetachVolume	Instância arn:aws:ec2:region:account:instance/* arn:aws:ec2:region:account:instance/ instance-id	ec2:AvailabilityZone ec2:EbsOptimized ec2:InstanceProfile ec2:InstanceType ec2:PlacementGroup ec2:Region ec2:ResourceTag/tag-key ec2:RootDeviceType ec2:Tenancy
	Volume arn:aws:ec2:region:account:volume/* arn:aws:ec2:region:account:volume/ volume-id	ec2:AvailabilityZone ec2:Encrypted ec2:ParentSnapshot ec2:Region ec2:ResourceTag/tag-key ec2:Volumelops ec2:VolumeSize ec2:VolumeType
DisableVpcClassicLink	VPC arn:aws:ec2:region:account:vpc/* arn:aws:ec2:region:account:vpc/vpc-id	ec2:Region ec2:ResourceTag/tag-key ec2:Tenancy
DisassociateIamInstanceProfile	Instância arn:aws:ec2:region:account:instance/* arn:aws:ec2:region:account:instance/ instance-id	ec2:AvailabilityZone ec2:EbsOptimized ec2:InstanceProfile ec2:InstanceType ec2:PlacementGroup ec2:Region ec2:ResourceTag/tag-key ec2:RootDeviceType ec2:Tenancy

Ação API	Recursos	Chaves de condição
EnableVpcClassicLink	VPC arn:aws:ec2:region:account:vpc/* arn:aws:ec2:region:account:vpc/vpc-id	ec2:Region ec2:ResourceTag/tag-key ec2:Tenancy
GetConsoleScreenshot	Instância arn:aws:ec2:region:account:instance/* arn:aws:ec2:region:account:instance/instance-id	ec2:AvailabilityZone ec2:EbsOptimized ec2:InstanceProfile ec2:InstanceType ec2:PlacementGroup ec2:Region ec2:ResourceTag/tag-key ec2:RootDeviceType ec2:Tenancy
ModifyLaunchTemplate	Modelo de execução arn:aws:ec2:region:account:launch-template/* arn:aws:ec2:region:account:launch-template/launch-template-id	ec2:Region ec2:ResourceTag/tag-key
ModifySnapshotAttribute	Snapshot arn:aws:ec2:region::snapshot/* arn:aws:ec2:region::snapshot/snapshot-id	ec2:Owner ec2:ParentVolume ec2:Region ec2:SnapshotTime ec2:VolumeSize ec2:ResourceTag/tag-key

Ação API	Recursos	Chaves de condição
RebootInstances	Instância arn:aws:ec2:region:account:instance/* arn:aws:ec2:region:account:instance/ instance-id	ec2:AvailabilityZone ec2:EbsOptimized ec2:InstanceProfile ec2:InstanceType ec2:PlacementGroup ec2:Region ec2:ResourceTag/tag-key ec2:RootDeviceType ec2:Tenancy
RejectVpcPeeringConnection	Conexão de emparelhamento de VPC arn:aws:ec2:region:account:vpc-peering- connection/* arn:aws:ec2:region:account:vpc-peering- connection/vpc-peering-connection-id	ec2:AcceptorVpc ec2:Region ec2:ResourceTag/tag-key ec2:RequesterVpc
ReplaceIamInstanceProfile	Instância arn:aws:ec2:region:account:instance/* arn:aws:ec2:region:account:instance/ instance-id	ec2:AvailabilityZone ec2:EbsOptimized ec2:InstanceProfile ec2:InstanceType ec2:PlacementGroup ec2:Region ec2:ResourceTag/tag-key ec2:RootDeviceType ec2:Tenancy
ReplaceRoute	Tabela de rotas arn:aws:ec2:region:account:route-table/* arn:aws:ec2:region:account:route- table/route-table-id	ec2:Region ec2:ResourceTag/tag-key ec2:Vpc
RevokeSecurityGroupEgress	Grupo de segurança arn:aws:ec2:region:account:security- group/* arn:aws:ec2:region:account:security- group/security-group-id	ec2:Region ec2:ResourceTag/tag-key ec2:Vpc

Ação API	Recursos	Chaves de condição
RevokeSecurityGroupIngress	Grupo de segurança arn:aws:ec2:region:account:security-group/* arn:aws:ec2:region:account:security-group/security-group-id	ec2:Region ec2:ResourceTag/tag-key ec2:Vpc
RunInstances	GPU elástica arn:aws:ec2:region:account:elastic-gpu/*	ec2:ElasticGpuType ec2:IsLaunchTemplateResource ec2:LaunchTemplate ec2:Region
	Imagen arn:aws:ec2:region::image/* arn:aws:ec2:region::image/image-id	ec2:ImageType ec2:IsLaunchTemplateResource ec2:LaunchTemplate ec2:Owner ec2:Public ec2:Region ec2:RootDeviceType ec2:ResourceTag/tag-key
	Instância arn:aws:ec2:region:account:instance/*	ec2:AvailabilityZone ec2:EbsOptimized ec2:InstanceMarketType ec2:InstanceProfile ec2:InstanceType ec2:IsLaunchTemplateResource ec2:LaunchTemplate ec2:PlacementGroup ec2:Region ec2:RootDeviceType ec2:Tenancy aws:RequestTag/tag-key aws:TagKeys

Ação API	Recursos	Chaves de condição
	Par de chaves arn:aws:ec2:region:account:key-pair/* arn:aws:ec2:region:account:key-pair/key-pair-name	ec2:IsLaunchTemplateResource ec2:LaunchTemplate ec2:Region
	Modelo de execução arn:aws:ec2:region:account:launch-template/* arn:aws:ec2:region:account:launch-template/launch-template-id	ec2:IsLaunchTemplateResource ec2:LaunchTemplate ec2:Region
	Interface de rede arn:aws:ec2:region:account:network-interface/* arn:aws:ec2:region:account:network-interface/eni-id	ec2:AvailabilityZone ec2:IsLaunchTemplateResource ec2:LaunchTemplate ec2:Region ec2:Subnet ec2:ResourceTag/tag-key ec2:Vpc
	Placement group arn:aws:ec2:region:account:placement-group/* arn:aws:ec2:region:account:placement-group/placement-group-name	ec2:IsLaunchTemplateResource ec2:LaunchTemplate ec2:Region ec2:PlacementGroupStrategy
	Grupo de segurança arn:aws:ec2:region:account:security-group/* arn:aws:ec2:region:account:security-group/security-group-id	ec2:IsLaunchTemplateResource ec2:LaunchTemplate ec2:Region ec2:ResourceTag/tag-key ec2:Vpc

Ação API	Recursos	Chaves de condição
	Snapshot arn:aws:ec2:region::snapshot/* arn:aws:ec2:region::snapshot/snapshot-id	ec2:IsLaunchTemplateResource ec2:LaunchTemplate ec2:Owner ec2:ParentVolume ec2:Region ec2:SnapshotTime ec2:ResourceTag/tag-key ec2:VolumeSize
	Sub-rede arn:aws:ec2:region:account:subnet/* arn:aws:ec2:region:account:subnet/ subnet-id	ec2:AvailabilityZone ec2:IsLaunchTemplateResource ec2:LaunchTemplate ec2:Region ec2:ResourceTag/tag-key ec2:Vpc
	Volume arn:aws:ec2:region:account:volume/*	ec2:AvailabilityZone ec2:Encrypted ec2:IsLaunchTemplateResource ec2:LaunchTemplate ec2:ParentSnapshot ec2:Region ec2:VolumeLops ec2:VolumeSize ec2:VolumeType
		aws:RequestTag/tag-key aws:TagKeys

Ação API	Recursos	Chaves de condição
StartInstances	Instância arn:aws:ec2:region:account:instance/* arn:aws:ec2:region:account:instance/ instance-id	ec2:AvailabilityZone ec2:EbsOptimized ec2:InstanceProfile ec2:InstanceType ec2:PlacementGroup ec2:Region ec2:ResourceTag/tag-key ec2:RootDeviceType ec2:Tenancy
StopInstances	Instância arn:aws:ec2:region:account:instance/* arn:aws:ec2:region:account:instance/ instance-id	ec2:AvailabilityZone ec2:EbsOptimized ec2:InstanceProfile ec2:InstanceType ec2:PlacementGroup ec2:Region ec2:ResourceTag/tag-key ec2:RootDeviceType ec2:Tenancy
TerminateInstances	Instância arn:aws:ec2:region:account:instance/* arn:aws:ec2:region:account:instance/ instance-id	ec2:AvailabilityZone ec2:EbsOptimized ec2:InstanceProfile ec2:InstanceType ec2:PlacementGroup ec2:Region ec2:ResourceTag/tag-key ec2:RootDeviceType ec2:Tenancy

Ação API	Recursos	Chaves de condição
UpdateSecurityGroupRule	Descrição da regra de segurança arn:aws:ec2:region:account:security-group/* arn:aws:ec2:region:account:security-group/security-group-id	ec2:Region ec2:ResourceTag/tag-key ec2:Vpc
UpdateSecurityGroupRule	Descrição da regra de segurança arn:aws:ec2:region:account:security-group/* arn:aws:ec2:region:account:security-group/security-group-id	ec2:Region ec2:ResourceTag/tag-key ec2:Vpc

Permissões em nível de recurso para RunInstances

A ação da API [RunInstances](#) executa uma ou mais instâncias e cria vários recursos do Amazon EC2. A ação requer uma AMI e cria uma instância, e a instância deve ser associada a um security group. 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. O usuário deve ter permissões para usar esses recursos, portanto, eles devem ser especificados no elemento `Resource` de todas as políticas que usam permissões em nível de recurso para a ação `ec2:RunInstances`. Se não planejar usar permissões em nível de recurso com a ação `ec2:RunInstances`, você poderá especificar o caractere curinga * no elemento `Resource` de sua declaração, em vez de ARNs individuais.

Se estiver usando permissões em nível de recurso, a tabela a seguir descreve os recursos mínimos necessários para usar a ação `ec2:RunInstances`.

Tipo de inicialização	Recursos necessários	Chaves de condição
Iniciar usando uma AMI com armazenamento de instâncias	arn:aws:ec2:region:account:instance/*	ec2:AvailabilityZone ec2:EbsOptimized ec2:InstanceMarketType ec2:InstanceProfile ec2:InstanceType ec2:IsLaunchTemplateResource ec2:LaunchTemplate ec2:PlacementGroup ec2:Region ec2:RootDeviceType ec2:Tenancy
	arn:aws:ec2:region::image/* (ou um ID específico da AMI)	ec2:ImageType ec2:IsLaunchTemplateResource

Tipo de inicialização	Recursos necessários	Chaves de condição
		ec2:LaunchTemplate ec2:Owner ec2:Public ec2:Region ec2:RootDeviceType ec2:ResourceTag/tag-key
	arn:aws:ec2:region:account:securitygroup/* (ou um ID específico do grupo em segurança)	ec2:IsLaunchTemplateResource ec2:LaunchTemplate ec2:Region ec2:ResourceTag/tag-key ec2:Vpc
	arn:aws:ec2:region:account:networkinterface/* (ou um ID específico da interface de rede)	ec2:AvailabilityZone ec2:IsLaunchTemplateResource ec2:LaunchTemplate ec2:Region ec2:Subnet ec2:ResourceTag/tag-key ec2:Vpc
	arn:aws:ec2:region:account:subnet/* (ou um ID específico da sub-rede)	ec2:AvailabilityZone ec2:IsLaunchTemplateResource ec2:LaunchTemplate ec2:Region ec2:ResourceTag/tag-key ec2:Vpc

Tipo de inicialização	Recursos necessários	Chaves de condição
Iniciar usando uma AMI com Amazon EBS	arn:aws:ec2:region:account:instance/*	ec2:AvailabilityZone ec2:EbsOptimized ec2:InstanceMarketType ec2:InstanceProfile ec2:InstanceType ec2:IsLaunchTemplateResource ec2:LaunchTemplate ec2:PlacementGroup ec2:Region ec2:RootDeviceType ec2:Tenancy
	arn:aws:ec2:region::image/* (ou um ID específico da AMI)	ec2:ImageType ec2:IsLaunchTemplateResource ec2:LaunchTemplate ec2:Owner ec2:Public ec2:Region ec2:RootDeviceType ec2:ResourceTag/tag-key
	arn:aws:ec2:region:account:securitygroup/* (ou um ID específico do grupo em segurança)	ec2:IsLaunchTemplateResource ec2:LaunchTemplate ec2:Region ec2:ResourceTag/tag-key ec2:Vpc

Tipo de inicialização	Recursos necessários	Chaves de condição
	arn:aws:ec2:region:account:networkinterface/* (ou um ID específico da interface de rede)	ec2:AvailabilityZone ec2:IsLaunchTemplateResource ec2:LaunchTemplate ec2:Region ec2:Subnet ec2:ResourceTag/tag-key ec2:Vpc
	arn:aws:ec2:region:account:volume/*	ec2:Encrypted ec2:IsLaunchTemplateResource ec2:LaunchTemplate ec2:ParentSnapshot ec2:Region ec2:VolumeLops ec2:VolumeSize ec2:VolumeType
	arn:aws:ec2:region:account:subnet/* (ou um ID específico da sub-rede)	ec2:IsLaunchTemplateResource ec2:LaunchTemplate ec2:Region ec2:ResourceTag/tag-key ec2:Vpc

Recomendamos que você também especifique o recurso de par de chaves na política — embora não seja necessário executar uma instância, você não pode se conectar à instância sem um par de chaves. Para obter exemplos de como usar permissões em nível de recurso com a ação `ec2:RunInstances`, consulte [Executar instâncias \(RunInstances\) \(p. 689\)](#).

Para obter informações adicionais sobre as permissões em nível de recurso no Amazon EC2, consulte a seguinte postagem no Blog de segurança da AWS: [Desmistificação das permissões em nível de recurso do EC2](#).

[Permissões no nível de recurso para modelos de execução e RunInstances](#)

Você pode criar um [modelo de execução \(p. 398\)](#) que contenha o parâmetro para executar uma instância. Ao usar a ação `ec2:RunInstances`, os usuários podem especificar o modelo de execução a ser usado para executar as instâncias. Você pode aplicar ao recurso de modelo de execução permissões no nível

de recurso para a ação `ec2:RunInstances`. Por exemplo, você pode especificar que os usuários só podem executar instâncias usando um modelo de execução e que é necessário um modelo de execução específico. Você também pode controlar os parâmetros que os usuários podem ou não substituir no modelo de execução. Assim, você pode gerenciar os parâmetros para executar uma instância em um modelo de execução em vez de gerenciar uma política do IAM. Para obter exemplos de políticas do , consulte [Modelos de execução \(p. 697\)](#).

Permissões em nível de recursos para marcação

Algumas ações de resource-creating da API do Amazon EC2 permitem especificar tags quando você cria o recurso. Para obter mais informações, consulte [Marcação dos seus recursos \(p. 1004\)](#).

Para permitir que os usuários marquem recursos na criação, eles devem ter permissões para usar a ação que cria o recurso (por exemplo, `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`.

Para a ação `ec2:CreateTags`, você pode usar a chave de condição `ec2:CreateAction` para restringir a marcação das permissões para as ações resource-creating somente. Por exemplo, as seguintes políticas permitem que os usuários executem instâncias e apliquem quaisquer tags às instâncias e aos volumes durante a inicialização. 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 será avaliada se as tags forem fornecidas em um modelo de execução e esse modelo estiver especificado na ação `ec2:RunInstances`. Para ver um exemplo de política, consulte [Tags em um modelo de execução \(p. 696\)](#).

Você pode controlar as chaves e os valores das tags que são aplicados aos recursos usando as seguintes chaves de condição:

- `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 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 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. Para obter exemplos de políticas do IAM, consulte [Políticas de exemplo para trabalhar com a AWS CLI ou um AWS SDK](#) (p. 680).

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 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. 705). Para obter exemplos de políticas do IAM específicas à Amazon VPC, consulte [Como controlar o acesso aos recursos da Amazon VPC](#).

Exemplos

- [Exemplo: acesso somente leitura](#) (p. 680)
- [Exemplo: restrição de acesso a uma região específica](#) (p. 681)
- [Como trabalhar com instâncias](#) (p. 681)
- [Como trabalhar com volumes](#) (p. 683)
- [Como trabalhar com snapshots](#) (p. 685)
- [Executar instâncias \(RunInstances\)](#) (p. 689)
- [Exemplo: trabalhar com Instâncias reservadas](#) (p. 699)
- [Exemplo: marcação de recursos](#) (p. 700)
- [Exemplo: trabalhar com funções do IAM](#) (p. 702)
- [Exemplo: trabalhar com tabelas de rotas](#) (p. 703)
- [Exemplo: permitir que uma instância específica visualize recursos em outros serviços da AWS](#) (p. 703)
- [Exemplo: trabalhar com modelos de execução](#) (p. 704)

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 da API do Amazon EC2, consulte [Permissões em nível do recurso compatíveis para ações da API do Amazon EC2](#) (p. 653).

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: restrição de 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 UE (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"
                }
            }
        }
    ]
}
```

Como trabalhar com instâncias

Exemplos

- [Exemplo: descrever, executar, interromper, iniciar e encerrar todas as instâncias \(p. 681\)](#)
- [Exemplo: descrever todas as instâncias e interromper, iniciar e encerrar somente instâncias específicas \(p. 682\)](#)

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 da API do Amazon EC2, consulte [Permissões em nível do recurso compatíveis para ações da API do Amazon EC2 \(p. 653\)](#).

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 da API do Amazon EC2, consulte [Permissões em nível do recurso compatíveis para ações da API do Amazon EC2 \(p. 653\)](#).

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 declaração permite que os usuários encerrem todas as instâncias em Leste dos EUA (Norte da Virgínia) Região (us-east-1) que pertencem à conta da AWS especificada, mas somente quando a instância tem 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"  
            ],  
            "Condition": {"StringEquals": {"aws:RequestTag/purpose": "test"}  
        }  
    ]  
}
```

```
],
"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"
}
}
}
]
```

Como trabalhar com volumes

Exemplos

- [Exemplo: anexar e desanexar volumes \(p. 683\)](#)
- [Exemplo: criação de um volume \(p. 684\)](#)
- [Exemplo: criação de um volume com tags \(p. 684\)](#)

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 accessem 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: criação de um volume

A política a seguir permite que os usuários usem a ação da API [CreateVolume](#). O usuário terá permissão para criar um volume somente se o volume for criptografado e se seu tamanho for menor que 20 GiB.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateVolume"
            ],
            "Resource": "arn:aws:ec2:us-east-1:123456789012:volume/*",
            "Condition": {
                "NumericLessThan": {
                    "ec2:VolumeSize" : "20"
                },
                "Bool":{
                    "ec2:Encrypted" : "true"
                }
            }
        ]
    }
}
```

Exemplo: criação de 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 [Permissões em nível de recursos para marcação \(p. 678\)](#).

```
{
    "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"
                }
            }
        }
    ]
}
```

Como trabalhar com snapshots

Exemplos

- [Exemplo: criação de um snapshot \(p. 686\)](#)
- [Exemplo: criar um snapshot com tags \(p. 686\)](#)
- [Exemplo: modificar configurações de permissão para snapshots \(p. 689\)](#)

Exemplo: criação de um snapshot

A política a seguir permite que os clientes usem a ação da API [CreateSnapshot](#). O cliente poderá criar um snapshot 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 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 [Permissões no nível do recurso para marcação](#).

```
{  
    "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"  
                    ]  
                }  
            }  
        }  
    ]  
}
```

```
        "stack"
    ]
}
},
{
    "Effect": "Allow",
    "Action": "ec2:CreateTags",
    "Resource": "arn:aws:ec2:us-east-1::snapshot/*",
    "Condition": {
        "StringEquals": {
            "ec2:CreateAction": "CreateSnapshot"
        }
    }
}
]
```

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`. 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"
                }
            }
        }
    ]
}
```

As seguintes políticas só permitirão que um snapshot seja criado 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 adicionais 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 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"
                }
            }
        }
    ]
}
```

```
    ]  
}
```

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 de API [RunInstances](#) executa uma ou mais instâncias. A `RunInstances` requer uma AMI e cria uma instância, e 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 no nível de recursos que são necessárias para iniciar uma instância, consulte [Permissões em nível de recurso para RunInstances \(p. 674\)](#).

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 [Como trabalhar com instâncias \(p. 681\)](#).

Recursos

- [AMIs \(p. 690\)](#)
- [Tipos de instância \(p. 690\)](#)
- [Sub-redes \(p. 692\)](#)
- [Volumes do EC2 \(p. 693\)](#)
- [Tags \(p. 693\)](#)
- [Tags em um modelo de execução \(p. 696\)](#)
- [GPUs elásticas \(p. 697\)](#)
- [Modelos de execução \(p. 697\)](#)

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/*"  
        ]  
    }  
]
```

}

Sub-redes

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 EC2

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

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 [Permissões em nível de recursos para marcação \(p. 678\)](#).

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "ec2:RunInstances"  
            ],  
            "Resource": "*"  
        },  
        {  
            "Effect": "Allow",  
            "Action": [  
                "ec2:CreateTags"  
            ],  
            "Resource": "*"  
        }  
    ]  
}
```

```
    "Resource": "arn:aws:ec2:us-east-1:123456789012:instance/*",
    "Condition": {
        "StringEquals": {
            "ec2:CreateAction" : "RunInstances"
        }
    }
}
```

As política a seguir inclui a chave de condição `aws:RequestTag` que requer que os usuários marquem todas as instâncias e os volumes criados por `RunInstances` com as tags `environment=production` e `purpose=webserver`. A chave de condição `aws:TagKeys` usa o modificador `ForAllValues` para indicar que somente as chaves `environment` e `purpose` são permitidas na solicitação (nenhuma outra tag pode ser especificada). Se nenhuma tag for especificada na solicitação, haverá falha na solicitação.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:region::image/*",
                "arn:aws:ec2:region:account:subnet/*",
                "arn:aws:ec2:region:account:network-interface/*",
                "arn:aws:ec2:region:account:security-group/*",
                "arn:aws:ec2:region:account:key-pair/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:region:account:volume/*",
                "arn:aws:ec2:region:account:instance/*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/environment": "production" ,
                    "aws:RequestTag/purpose": "webserver"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": ["environment", "purpose"]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2>CreateTags"
            ],
            "Resource": "arn:aws:ec2:region:account:/*/*",
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction" : "RunInstances"
                }
            }
        }
    ]
}
```

}

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"  
                }  
            }  
        }  
    ]  
}
```

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"  
            ]  
        }  
    ]  
}
```

```
        "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"
        }
    }
}
]
```

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": {  
                    "arn:aws:ec2:region:us-east-2:instance/*/  
                }  
            }  
        }  
    ]  
}
```

```
        "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 alguns recursos do modelo de execução na solicitação `RunInstances`.

```
{  
    "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"  
                }  
            }  
        }  
    ]  
}
```

```
        "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"
                }
            }
        }
    ]
}
```

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 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: marcação de 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 `environment` 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/environment": ["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 \(p. 713\)](#).

```
{
    "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 excluam 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"  
                }  
            }  
        }  
    ]  
}
```

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, elas foram projetadas para solicitações feitas com a AWS CLI ou com um AWS SDK. O console usa ações de API adicionais para seus recursos, pois 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 mais informações, consulte o [AWS CloudTrail User Guide](#). 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 \(p. 705\)](#)
- [Exemplo: uso do Assistente de execução do EC2 \(p. 706\)](#)
- [Exemplo: trabalhar com volumes \(p. 708\)](#)
- [Exemplo: trabalhar com grupos de segurança \(p. 709\)](#)
- [Exemplo: trabalhar com endereços IP elásticos \(p. 711\)](#)
- [Exemplo: trabalhar com instâncias reservadas \(p. 712\)](#)

Para obter informações adicionais sobre como criar políticas para o console do Amazon EC2, consulte a seguinte postagem do Blog de segurança da AWS: [Como 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 \(p. 680\)](#). 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 da API do Amazon EC2, consulte [Permissões em nível do recurso compatíveis para ações da API do Amazon EC2 \(p. 653\)](#).

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: uso do 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:DescribeVpcs`: para ver as opções de rede disponíveis.
- `ec2:DescribeSubnets`: para visualizar todas as sub-redes disponíveis da VPC escolhida.
- `ec2:DescribeSecurityGroups`: para visualizar a página de security groups no assistente. Os usuários podem selecionar um security group existente.
- `ec2:DescribeKeyPairs` ou `ec2>CreateKeyPair`: para selecionar um par de chaves ou criar um novo par.

```
{  
    "Version": "2012-10-17",  
    "Statement": [{  
        "Effect": "Allow",  
        "Action": [  
            "ec2:DescribeImages",  
            "ec2:DescribeVpcs",  
            "ec2:DescribeSubnets",  
            "ec2:DescribeSecurityGroups",  
            "ec2:DescribeKeyPairs",  
            "ec2:CreateKeyPair"  
        ],  
        "Resource": "*"  
    }]  
}
```

```
    "Action": [
        "ec2:DescribeInstances", "ec2:DescribeImages",
        "ec2:DescribeKeyPairs", "ec2:DescribeVpcs", "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
    ],
    "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.
- `ec2>CreateSecurityGroup`: para criar um novo security group. Por exemplo, para criar o security group `launch-wizard-x` sugerido no assistente. No entanto, essa ação só cria um security group. Ela não adiciona ou modifica nenhuma regra. Para adicionar regras de entrada, os usuários devem receber a permissão para usar a ação de API `ec2:AuthorizeSecurityGroupIngress`. 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 [Permissões em nível de recursos para marcação \(p. 678\)](#). 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

Seja cuidadoso ao conceder permissão aos usuários para usarem a ação `ec2:CreateTags`. Isso limita a capacidade de usar a chave de condição `ec2:ResourceTag` para restringir o uso de outros recursos. Os usuários podem alterar a tag de um recurso para ignorar as restrições.

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 específico de instância, sub-rede e região

A política a seguir permite que os usuários executem instâncias `m1.small` usando AMIs de propriedade da Amazon e apenas em uma sub-rede específica (`subnet-1a2b3c4d`). Os usuários podem executar somente na região `sa-east-1`. Se os usuários selecionarem outra região ou selecionarem outro tipo de instância, AMI ou uma sub-rede no assistente de execução, a execução falhará.

A primeira declaração concede aos usuários permissão para visualizar as opções no assistente de execução, conforme demonstrado 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 \(RunInstances\) \(p. 689\)](#). 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 `m1.small`, e somente se a AMI for de propriedade da Amazon.

```
{  
    "Version": "2012-10-17",  
    "Statement": [{  
        "Effect": "Allow",  
        "Action": [  
            "ec2:DescribeInstances", "ec2:DescribeImages",  
            "ec2:DescribeKeyPairs", "ec2:DescribeVpcs", "ec2:DescribeSubnets",  
            "ec2:DescribeSecurityGroups"  
        ],  
        "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": "m1.small"  
            }  
        }  
    },  
    {  
        "Effect": "Allow",  
        "Action": "ec2:RunInstances",  
        "Resource": [  
            "arn:aws:ec2:sa-east-1::image/ami-*"  
        ],  
        "Condition": {  
            "StringEquals": {  
                "ec2:Owner": "amazon"  
            }  
        }  
    }  
}
```

Exemplo: trabalhar com volumes

A política a seguir concede aos usuários permissão para visualizar e criar volumes, e para anexar e desanexar volumes em instâncias específicas.

Os usuários podem anexar um volume às instâncias que tenham a tag "purpose=test" e também desanexar volumes dessas instâncias. Para anexar um volume usando o console do Amazon EC2, é útil que os usuários tenham permissão para usar a ação ec2:DescribeInstances, pois isso permite que eles selezionem uma instância de uma lista pré-preenchida na caixa de diálogo Attach Volume (Anexar volume). No entanto, isso também permite que os usuários visualizem todas as instâncias na página Instances no console, portanto, você pode omitir essa ação.

Na primeira instrução, a ação ec2:DescribeAvailabilityZones é necessária para garantir que um usuário possa selecionar uma zona de disponibilidade ao criar um volume.

Os usuários não podem marcar os volumes que criam (durante ou após a criação do volume).

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {"Effect": "Allow",  
         "Action": [  
             "ec2:DescribeVolumes",  
             "ec2:DescribeAvailabilityZones",  
             "ec2>CreateVolume",  
             "ec2:DescribeInstances"  
         ],  
         "Resource": "*"  
     },  
     {  
         "Effect": "Allow",  
         "Action": [  
             "ec2:AttachVolume",  
             "ec2:DetachVolume"  
         ],  
         "Resource": "arn:aws:ec2:region:111122223333:instance/*",  
         "Condition": {  
             "StringEquals": {  
                 "ec2:ResourceTag/purpose": "test"  
             }  
         }  
     },  
     {  
         "Effect": "Allow",  
         "Action": [  
             "ec2:AttachVolume",  
             "ec2:DetachVolume"  
         ],  
         "Resource": "arn:aws:ec2:region:111122223333:volume/*"  
     }  
    ]  
}
```

Exemplo: trabalhar com grupos de segurança

Visualizar grupos de segurança e adicionar e remover regras

A política a seguir concede aos usuários permissão para visualizar grupos de segurança no console do Amazon EC2 e para adicionar e remover regras de entrada e de saída para grupos de segurança que têm a tag 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:DescribeTags"  
         ],  
         "Resource": "*"  
     },  
     {  
         "Effect": "Allow",  
         "Action": [  
             "ec2:AuthorizeSecurityGroupIngress", "ec2:RevokeSecurityGroupIngress",  
             "ec2:AuthorizeSecurityGroupEgress", "ec2:RevokeSecurityGroupEgress"  
         ]  
     }  
    ]  
}
```

```
],
"Resource": [
    "arn:aws:ec2:region:111122223333:security-group/*"
],
"Condition": {
    "StringEquals": {
        "ec2:ResourceTag/Department": "Test"
    }
}
}
```

Como 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.

Atualmente, a ação de API `ec2:CreateSecurityGroup` não oferece suporte a permissões em nível de recurso. Contudo, é possível aplicar permissões em nível de recurso à ações `ec2:AuthorizeSecurityGroupIngress` e `ec2:AuthorizeSecurityGroupEgress` para controlar como os usuários podem criar regras.

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 Console de gerenciamento da AWS.

Essa política permite que os usuários visualizem todas as instâncias reservadas bem como instâncias sob demanda 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: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 em que 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.

Funções do IAM para Amazon EC2

Os aplicativos devem assinar suas solicitações de API com credenciais da AWS. Portanto, se você for um desenvolvedor de aplicativos, precisará de uma estratégia para gerenciar credenciais para seus aplicativos que executam em instâncias do EC2. Por exemplo, você pode distribuir de maneira segura suas credenciais da AWS para as instâncias, permitindo que os aplicativos 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 seus aplicativos possam fazer solicitações de API de suas instâncias de maneira segura, sem exigir que você gerencie as credenciais de segurança que os aplicativos 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 o aplicativo 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 o aplicativo recupere um conjunto de credenciais temporárias e use-as.

Por exemplo, você pode usar funções do IAM para conceder permissões a aplicativos em execução em suas instâncias que precisam usar um bucket no Amazon S3. Você pode especificar permissões para funções do IAM criando uma política em formato JSON. Essas são semelhantes às políticas que você cria para os usuários do IAM. Se você alterar uma função, a alteração será propagada para todas as instâncias.

Você não pode anexar várias funções do IAM a uma única instância, mas pode anexar uma única função do IAM a várias 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 em nível do recurso compatíveis para ações da API do Amazon EC2 \(p. 653\)](#) e o seguinte exemplo: [Exemplo: trabalhar com funções do IAM \(p. 702\)](#).

Tópicos

- [Perfis de instância \(p. 713\)](#)
- [Como recuperar credenciais de segurança dos metadados da instância \(p. 713\)](#)
- [Como conceder uma permissão de usuário do IAM para transmitir uma função do IAM para uma instância \(p. 714\)](#)
- [Como trabalhar com funções do IAM \(p. 715\)](#)

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 usando o console do 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.

Como recuperar credenciais de segurança dos metadados da instância

Um aplicativo na instância recupera as credenciais de segurança fornecidas pela função no item `iam/security-credentials/role-name` dos metadados da instância. O aplicativo 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.

```
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 aplicativos, AWS CLI e Tools para Windows PowerShell que são executados na instância, você não precisa obter as credenciais de segurança temporárias explicitamente — os AWS SDKs, a AWS CLI e o Tools para Windows PowerShell obtêm as credenciais do serviço de metadados da instância do EC2 e as usam automaticamente. 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 [Como usar credencias de segurança temporárias para solicitar acesso aos recursos da AWS](#) no Guia do usuário do IAM.

Para obter mais informações sobre os metadados da instância, consulte [Metadados da instância e dados do usuário \(p. 516\)](#).

Como conceder uma permissão de usuário do IAM para transmitir uma função do IAM para uma instância

Para permitir que um usuário do IAM execute uma instância com uma função do IAM ou para anexar ou substituir uma função do IAM para uma instância existente, você deve conceder ao usuário permissão para passar a função para a instância.

A política do IAM a seguir concede permissão aos usuários para executar instâncias (ec2:RunInstances) com uma função do IAM ou para anexar ou substituir uma função do IAM para uma instância existente (ec2:AssociateIamInstanceProfile e ec2:ReplaceIamInstanceProfileAssociation).

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "ec2:RunInstances",  
                "ec2:AssociateIamInstanceProfile",  
                "ec2:ReplaceIamInstanceProfileAssociation"  
            ],  
            "Resource": "*"  
        },  
        {  
            "Effect": "Allow",  
            "Action": "iam:PassRole",  
            "Resource": "*"  
        }  
    ]
```

}

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.

Como 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

- [Como criar uma função do IAM \(p. 715\)](#)
- [Como executar uma instância com uma função do IAM \(p. 717\)](#)
- [Como anexar uma função do IAM a uma instância \(p. 718\)](#)
- [Como substituir uma função do IAM \(p. 719\)](#)
- [Como desanexar uma função do IAM \(p. 719\)](#)

Como 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, digite um nome para a função e escolha Create role.

Como alternativa, você pode usar a AWS CLI para criar uma função do IAM.

Para criar uma função do IAM e um perfil de instância (AWS CLI)

- Crie uma função do IAM com uma política que permita que a função use um bucket do Amazon S3.
 - a. 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"  
        }  
    ]  
}
```

- b. Crie a função `s3access` e especifique a política de confiança que você criou.

```
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"
    }
}
```

- c. 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 aplicativos que executam na instância.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": ["s3:*"],
            "Resource": "*"
        }
    ]
}
```

- d. Anexe a política de acesso à função.

```
aws iam put-role-policy --role-name s3access --policy-name S3-Permissions --policy-document file://ec2-role-access-policy.json
```

- e. Crie um perfil de instância chamado `s3access-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"
    }
}
```

- f. 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
```

Para obter mais informações sobre esses comandos, consulte [create-role](#), [put-role-policy](#) e [create-instance-profile](#) no AWS CLI Command Reference.

Como alternativa, você pode usar os seguintes comandos do AWS Tools para Windows PowerShell:

- [New-IAMRole](#)
- [Register-IAMRolePolicy](#)
- [New-IAMInstanceProfile](#)

Como 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 Launch Instance.
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 seu aplicativo, recupere as credenciais de segurança da AWS disponibilizadas na instância e use-as para assinar as solicitações. O SDK da AWS cuida disso para você.

```
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 para Windows PowerShell.

2. Se você estiver usando as ações da API do Amazon EC2 em seu aplicativo, recupere as credenciais de segurança da AWS disponibilizadas na instância e use-as para assinar as solicitações. O SDK da AWS cuida disso para você.

```
curl http://169.254.169.254/latest/meta-data/iam/security-credentials/role_name
```

Como 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`.

Para anexar uma função do IAM a uma instância (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 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"  
        }  
    }  
}
```

Como alternativa, use os seguintes comandos do Tools para Windows PowerShell:

- [Get-EC2Instance](#)
- [Register-EC2IamInstanceProfile](#)

Como 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 pode fazer isso se quiser alterar a função do IAM para uma instância sem desanexar a existente primeiro. Por exemplo, para garantir que as ações da API executadas por aplicativos em execução na instância não sejam interrompidas.

Para substituir uma função do IAM para uma instância (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 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 para 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](#)

Como desanexar uma função do IAM

Você pode desanexar uma função do IAM de uma instância em execução ou parada.

Para desanexar uma função do IAM de uma instância (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 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](#)

Como autorizar tráfego de entrada em suas instâncias 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 o 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 security groups padrão e os security groups recentemente criados incluem regras padrão que não permitem que você acesse sua instância a partir da Internet. Para obter mais informações, consulte [Security groups padrão \(p. 629\)](#) e [Security groups personalizados \(p. 630\)](#). 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 apenas um endereço IP específico ou intervalo de endereços para acessar a instância.

Para obter mais informações sobre security groups, consulte [Grupos de segurança do Amazon EC2 para instâncias do Linux \(p. 626\)](#).

Como adicionar uma regra para o tráfego do SSH de entrada para 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 em seu endereço IP usando o SSH.

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 e, em seguida, escolha SSH na lista Type.
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 \(p. 721\)](#).
5. Escolha 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.

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 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 [Acessando 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 \(AWS Tools para Windows PowerShell\)](#)

```
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 para 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)
```

Como atribuir um security group 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 [Como alterar os grupos de segurança de uma instância](#) no Guia do usuário da Amazon VPC.

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. 723)
- [Endereços IPv4 públicos e nomes de host DNS externos](#) (p. 724)
- [Endereços IP elásticos \(IPv4\)](#) (p. 725)
- [Servidor DNS da Amazon](#) (p. 725)
- [Endereços IPv6](#) (p. 725)
- [Como trabalhar com endereços IP para a instância](#) (p. 726)
- [Vários endereços IP](#) (p. 730)

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`. Você pode usar o nome de host DNS interno para comunicação entre instâncias na mesma rede, mas não podemos resolver o nome de host DNS fora da rede em que a instância se encontra.

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 \(p. 730\)](#).

Um endereço IPv4 privado permanece associado à interface de rede quando a instância é interrompida e reiniciada e é liberada 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 rede da instância e como o endereço IPv4 privado da instância dentro da rede da instância. O endereço IP público é mapeado para o endereço IP privado primário por meio da conversão de endereço de rede (NAT). Para mais informações sobre a NAT, 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 à 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 [Como 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 [Como atribuir um endereço IPv4 público durante a execução da instância \(p. 728\)](#).

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 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 parada ou encerrada. A instância parada recebe um novo endereço IP público quando é reiniciada.
- 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 Elastic IP \(p. 742\)](#).

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. Você pode associá-lo a instâncias e de instâncias conforme necessário, e ele é alocado à sua conta até que você o libere. Para obter mais informações sobre endereços IP elásticos e como usá-los, consulte [Endereços Elastic IP \(p. 742\)](#).

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 sub-rede para IPv6
- Como associar um bloco CIDR IPv6 a sua VPC
- Como associar um bloco CIDR IPv6 a sua 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 [Como 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 para 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 \(p. 749\)](#).

Como trabalhar com endereços IP para a instância

Você pode visualizar os endereços IP atribuídos à instância, atribuir um endereço IPv4 público à instância durante a execução ou atribuir um endereço IPv6 à instância durante a execução.

Tópicos

- [Como determinar endereços IP públicos, privados ou elásticos \(p. 726\)](#)
- [Como determinar endereços IPv6 \(p. 728\)](#)
- [Como atribuir um endereço IPv4 público durante a execução da instância \(p. 728\)](#)
- [Atribuir um endereço IPv6 a uma instância \(p. 729\)](#)
- [Cancelar a atribuição de um endereço IPv6 de uma instância \(p. 730\)](#)

Como determinar endereços IP públicos, privados ou elásticos

Você pode usar o console do Amazon EC2 para determinar 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 \(p. 516\)](#).

Para determinar os endereços IPv4 privados 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 sua instância. No painel de detalhes, obtenha o endereço IPv4 privado no campo Private IPs e obtenha o nome do host DNS interno no campo Private DNS.
4. Se você tiver um ou mais endereços IPv4 privados secundários atribuídos às interfaces de rede que estão anexadas à instância, obtenha esse endereços IP no campo Secondary private IPs.
5. Como alternativa, no painel de navegação, escolha Network Interfaces e selecione a interface de rede associada à instância.
6. Obtenha o endereço IP privado primário no campo Primary private IPv4 IP e obtenha o nome do host DNS interno no campo Private DNS (IPv4).
7. Se você atribuiu endereços IP privados secundários à interface de rede, obtenha esses endereços no campo Secondary private IPv4 IPs.

Para determinar os endereços IPv4 públicos 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 sua instância. No painel de detalhes, obtenha o endereço IP público no campo IPv4 Public IP e obtenha o nome do host DNS externo no campo Public DNS (IPv4).
4. Se um ou mais endereços IP elásticos forem associados à instância, obtenha os endereços IP elásticos no campo Elastic IPs.

Note

Se a instância não tiver um endereço IPv4 público, mas tiver associado um endereço IP elástico a uma interface de rede para a instância, o campo IPv4 Public IP exibirá o endereço IP elástico.

5. Como alternativa, no painel de navegação, escolha Network Interfaces e selecione uma interface de rede associada à instância.
6. Obtenha o endereço IP público no campo IPv4 Public IP. Um asterisco (*) indica o endereço IPv4 público ou o endereço IP elástico que está mapeado para o endereço IPv4 privado primário.

Note

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, você pode usar os metadados da instância.

Para determinar os endereços IPv4 da instância usando os metadados

1. Conecte-se à sua instância.
2. Use o comando a seguir para acessar o endereço IP privado:

```
[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:

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/public-ipv4
```

Observe que se um endereço IP elástico estiver associado à instância, o valor retornado será o do endereço IP elástico.

Como determinar endereços IPv6

Você pode usar o console do Amazon EC2 para determinar os endereços IPv6 das instâncias.

Para determinar os endereços IPv6 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 sua instância. No painel de detalhes, obtenha os endereços IPv6 em IPv6 IPs.

Para determinar os endereços IPv6 da instância usando os metadados da instância

1. Conecte-se à sua instância.
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/>):

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/network/interfaces/macs/mac-address/ipv6s
```

Como 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.

Important

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 \(p. 724\)](#). 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 Elastic IP \(p. 742\)](#).

Para acessar o recurso de endereçamento IP público 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 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.

Important

Você não pode atribuir automaticamente um endereço IP público se especificar mais de uma interface de rede. Além disso, você não pode substituir a configuração da sub-rede usando o recurso de atribuição automática de endereço IP público, se especificar uma interface de rede existente para eth0.

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 [Execução de uma instância usando o assistente de execução de instância \(p. 391\)](#). 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.

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 Elastic IP \(p. 742\)](#). Você também pode modificar o comportamento do endereçamento IPv4 público da sub-rede. Para obter mais informações, consulte [Como modificar o atributo de endereçamento IPv4 público para a sub-rede](#).

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 [Acessando 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 para Windows PowerShell)

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.

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 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.

Como alternativa, você pode atribuir um endereço IPv6 à instância após a execução.

Para atribuir um endereço IPv6 à 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. Em Endereços IPv6, escolha Atribuir novo IP. 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 Salvar.

Note

Se você tiver executado a instância usando o Amazon Linux 2016.09.0 ou posterior ou o Windows Server 2008 R2 ou posterior, a instância será configurada para IPv6, e nenhuma etapa adicional será necessária para garantir que o endereço IPv6 seja reconhecido na instância. Se tiver executado a instância em uma AMI mais antiga, você poderá precisar configurar a instância manualmente. Para obter mais informações, consulte [Configurar o IPv6 em suas instâncias](#) no Guia do usuário da Amazon VPC.

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 [Acessando 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 para Windows PowerShell)
- `assign-ipv6-addresses` (AWS CLI)
- `Register-EC2Ipv6AddressList` (AWS Tools para Windows PowerShell)

Cancelar a atribuição de um endereço IPv6 de uma instância

Você pode cancelar a atribuição de um endereço IPv6 de uma instância usando o console do Amazon EC2.

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 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 [Acessando o Amazon EC2 \(p. 3\)](#).

- `unassign-ipv6-addresses` (AWS CLI)
- `Unregister-EC2Ipv6AddressList` (AWS Tools para 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 \(p. 749\)](#).

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 aplicativos 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 \(p. 731\)](#)
- [Como trabalhar com vários endereços IPv4 \(p. 732\)](#)
- [Como trabalhar com vários endereços IPv6 \(p. 735\)](#)

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 pode estar anexada ou desanexada da 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 o 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, e 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 quando ela é desanexada de uma instância ou anexada a outra instância.
- Embora não seja possível mover 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.
- Você pode mover qualquer interface de rede adicional de uma instância para outra.

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.

Como 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

- [Como atribuir um endereço IPv4 privado secundário \(p. 732\)](#)
- [Como configurar o sistema operacional na instância para reconhecer o endereço IPv4 privado secundário \(p. 734\)](#)
- [Como associar um endereço IP elástico ao endereço IPv4 privado secundário \(p. 734\)](#)
- [Como visualizar endereços IPv4 privados secundários \(p. 734\)](#)
- [Como cancelar a atribuição de um endereço IPv4 privado secundário \(p. 735\)](#)

Como 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 \(p. 732\)](#)
- [Para atribuir um endereço IPv4 secundário durante a execução usando a linha de comando \(p. 733\)](#)
- [Para atribuir um endereço IPv4 privado secundário a uma interface de rede \(p. 733\)](#)
- [Para atribuir um IPv4 privado secundário a uma instância existente usando a linha de comando \(p. 733\)](#)

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 \(p. 749\)](#).

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 [Como trabalhar com endereços IP elásticos \(p. 743\)](#).

- 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 [Como configurar o sistema operacional na instancia para reconhecer o endereço IPv4 privado secundário \(p. 734\)](#).

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 [Acessando 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 para 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 [Acessando o Amazon EC2 \(p. 3\)](#).

- [assign-private-ip-addresses](#) (AWS CLI)
- [Register-EC2PrivateIpAddress](#) (AWS Tools para Windows PowerShell)

Como configurar o sistema operacional na instância para reconhecer o endereço IPv4 privado secundário

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 as 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 li`. Se você precisar de controle manual sobre a configuração da rede, poderá remover o pacote ec2-net-utils. Para obter mais informações, consulte [Configuração da sua interface de rede usando ec2-net-utils \(p. 757\)](#).
- 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.

Como 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 [Acessando o Amazon EC2 \(p. 3\)](#).
 - [associate-address](#) (AWS CLI)
 - [Register-EC2Address](#) (AWS Tools para Windows PowerShell)

Como 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.

Como 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 [Acessando o Amazon EC2 \(p. 3\)](#).
 - [unassign-private-ip-addresses](#) (AWS CLI)
 - [Unregister-EC2PrivateIpAddress](#) (AWS Tools para Windows PowerShell)

Como 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

- [Como atribuir vários endereços IPv6 \(p. 736\)](#)
- [Como visualizar endereços IPv6 \(p. 737\)](#)
- [Cancelamento da atribuição de um endereço IPv6 \(p. 738\)](#)

Como 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 \(p. 176\)](#).
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 \(p. 749\)](#).
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 [Referência de regras de security groups \(p. 634\)](#). 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 [Acessando 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 para Windows PowerShell).
- Atribuir um endereço IPv6 a uma interface de rede:
 - [assign-ipv6-addresses](#) (AWS CLI)
 - [Register-EC2Ipv6AddressList](#) (AWS Tools para Windows PowerShell)

Como visualizar 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 [Acessando o Amazon EC2 \(p. 3\)](#).

- Visualizar endereços IPv6 de uma instância:
 - [describe-instances](#) (AWS CLI)
 - [Get-EC2Instance](#) AWS Tools para Windows PowerShell
- Para visualizar os endereços IPv6 de uma interface de rede:
 - [describe-network-interfaces](#) (AWS CLI)
 - [Get-EC2NetworkInterface](#) (AWS Tools para Windows PowerShell)

Cancelamento da 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 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 [Acessando o Amazon EC2 \(p. 3\)](#).

- [unassign-ipv6-addresses](#) (AWS CLI)
- [Unregister-EC2Ipv6AddressList](#) (AWS Tools para Windows PowerShell).

Traga seus próprios endereços IP (BYOIP)

Você pode trazer parte ou todo o seu intervalo de endereços IPv4 públicos da rede local para sua conta da AWS. Você continua a ter o intervalo de endereços, mas a AWS o anuncia na Internet. Depois de trazer o intervalo de endereços para a AWS, ele aparece em sua conta como um grupo de endereços. Você pode criar um endereço IP elástico em seu grupo de endereços e usá-lo com os recursos da AWS, como instâncias do EC2, gateways NAT e Network Load Balancers.

Important

O BYOIP não está disponível em todas as regiões. Para obter uma lista das regiões compatíveis, consulte [Perguntas frequentes sobre Traga seu próprio IP](#).

Requisitos

- 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). Ele deve ser registrado para uma empresa ou entidade institucional e não pode ser registrado para uma única pessoa.
- No ARIN, os tipos de rede suportados são "Alocação direta" e "Atribuição direta".
- No RIPE, os status de alocação suportados são "ALLOCATED PA", "LEGACY" e "ASSIGNED PI".
- O intervalo de endereços mais específico que pode ser especificado é /24.
- Você pode levar cada intervalo de endereços para uma região de cada vez.
- Você pode levar cinco intervalos de endereços por região para sua conta da AWS.
- 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 tem má reputação ou estiver associado a comportamentos mal-intencionados.

Preparar-se para levar seu intervalo de endereços para sua conta da AWS

Para garantir que apenas você possa levar seu intervalo de endereços para sua conta da AWS, você deve autorizar a Amazon para anunciar o intervalo de endereços e fornecer a prova de que você é o proprietário do intervalo de endereços.

Um Route Origin Authorization (ROA - Autorização de origem de rota) é um documento que você pode criar por meio de seu RIR. Ele contém o intervalo de endereços, os ASNs com permissão para anunciar o intervalo de endereços e uma data de expiração. Um ROA autoriza a Amazon a anunciar um intervalo de endereços em um número de AS específico. No entanto, ele não autoriza sua conta da AWS a levar seu intervalo de endereços para a AWS. Para autorizar sua conta da AWS a levar um intervalo de endereços para a AWS, você deve publicar um certificado X509 autoassinado nas observações de RDAP para o intervalo de endereços. O certificado contém uma chave pública, que a AWS usa para verificar a assinatura do contexto de autorização que você fornece. Você deve manter sua chave privada segura e usá-la para assinar a mensagem em contexto de autorização.

Os comandos no procedimento a seguir exigem a versão OpenSSL 1.0.2 ou posterior.

Para preparar-se para levar seu intervalo de endereços para sua conta da AWS

1. Crie um ROA para autorizar os Amazon ASNs 16509 e 14618 a anunciam seu intervalo de endereços, além dos ASNs atualmente autorizados a anunciar o intervalo de endereços. Você deve definir o tamanho máximo para 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:
 - ARIN — [Solicitações de ROA](#)
 - RIPE — [Gerenciamento de ROAs](#)
2. Gere um par de chaves RSA de 2048 bits da seguinte forma:

```
openssl genrsa -out private.key 2048
```

3. Crie um certificado X509 público a partir do par de chaves usando o seguinte comando. Neste exemplo, o certificado expira em 365 dias, após o qual ele não é mais confiável. Portanto, certifique-se de definir a expiração adequadamente. Quando solicitado por informações, você pode aceitar os valores padrão.

```
openssl req -new -x509 -key private.key -days 365 | tr -d "\n" > publickey.cer
```

4. Crie uma mensagem de autorização assinada para o prefixo e a conta da AWS. 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
```

O comando a seguir cria uma mensagem de autorização de texto sem formatação usando um número de conta de exemplo, intervalo de endereço e data de expiração e armazena-a em uma variável denominada `text_message`.

```
text_message="1|aws|123456789012|198.51.100.0/24|20191201|SHA256|RSAPSS"
```

O comando a seguir assina a mensagem de autorização em `text_message` usando o par de chaves que você criou e armazena-a em uma variável denominada `signed_message`:

```
signed_message=$(echo $text_message | tr -d "\n" | openssl dgst -sha256 -sigopt rsa_padding_mode:pss -sigopt rsa_pss_saltlen:-1 -sign private.key -keyform PEM | openssl base64 | tr -- '+=' '-_-' | tr -d "\n")
```

5. Atualize o registro de RDAP de seu RIR com o certificado X509. Certifique-se de copiar o ----- BEGIN CERTIFICATE----- e o -----END CERTIFICATE----- no certificado. Remova os caracteres de nova linha, se ainda não tiver feito isso, usando os comandos `tr -d "\n"` nas etapas anteriores. Para visualizar o certificado, execute o seguinte comando:

```
cat publickey.cer
```

No ARIN, adicione o certificado na seção "Public Comments (Comentários públicos) do intervalo de endereços.

No RIPE, adicione o certificado como um novo campo "desc" para o intervalo de endereços.

Provisionar o intervalo de endereços para uso com a 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-lo. Também verificamos se possui você o intervalo de endereços.

Para provisionar o intervalo de endereços, use o seguinte comando `provision-byoip-cidr`. O parâmetro `--cidr-authorization-context` usa as variáveis que você criou na seção anterior, não a mensagem da ROA.

```
aws ec2 provision-byoip-cidr --cidr address-range --cidr-authorization-context Message="$text_message",Signature="$signed_message"
```

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. Pode levar até cinco dias para concluir o processo de provisionamento. Para monitorar o status dos intervalos de endereços provisionados por você, use o seguinte comando [describe-byoip-cidrs](#):

```
aws ec2 describe-byoip-cidrs --max-results 5
```

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.

Recomendamos interromper o anúncio do intervalo de endereços em outros locais antes de anunciar por meio da AWS. Se você mantiver o anúncio de seu intervalo de endereços IP em outros locais, não poderemos oferecer suporte a ele ou solucionar problemas de forma confiável. Especificamente, não podemos garantir que o tráfego para o intervalo de endereços entre em nossa rede.

Para minimizar o tempo de inatividade, você pode configurar seus 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 [Como alocar um endereço IP elástico \(p. 743\)](#).

Para anunciar o intervalo de endereços, use o seguinte comando [advertise-byoip-cidr](#):

```
aws ec2 advertise-byoip-cidr --cidr address-range
```

Important

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.

Para interromper o anúncio do intervalo de endereços, use o seguinte comando [withdraw-byoip-cidr](#):

```
aws ec2 withdraw-byoip-cidr --cidr address-range
```

Important

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.

Desprovisionar o intervalo de endereços

Para parar de usar o intervalo de endereços com a AWS, libere todos os endereços IP elásticos ainda alocados no grupo de endereços, interrompa o anúncio do intervalo de endereços e desprovisione o intervalo de endereços.

Para liberar cada endereço IP elástico, use o seguinte comando [release-address](#):

```
aws ec2 release-address --allocation-id eipalloc-12345678
```

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
```

Endereços Elastic IP

Um Endereço IP elástico é um endereço IPv4 estático projetado para computação em nuvem dinâmica. Um endereço IP elástico está associado à conta da AWS. Com um endereço IP elástico, você pode mascarar a falha de uma instância ou software remapeando rapidamente o endereço para outra instância em sua conta.

Um endereço IP elástico é um endereço IPv4 público, que é acessível pela Internet. Se sua instância não tem um endereço IPv4 público, você pode associar um endereço IP elástico à instância para habilitar a comunicação com a Internet. Por exemplo, para conectar-se à instância de seu computador local.

No momento, não oferecemos suporte a endereços IP elásticos para IPv6.

Tópicos

- [Noções básicas sobre endereços IP elásticos \(p. 742\)](#)
- [Como trabalhar com endereços IP elásticos \(p. 743\)](#)
- [Como usar o DNS reverso para aplicativos de e-mail \(p. 747\)](#)
- [Limite de endereços IP elásticos \(p. 747\)](#)

Noções básicas sobre endereços IP elásticos

As seguintes são as características básicas de um endereço IP elástico:

- 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 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 \(p. 724\)](#).
- Você pode desassociar um endereço IP elástico de um recurso e reassociá-lo a outro recurso. As conexões abertas de uma instância continuarão funcionando por um tempo mesmo após desassociar o endereço IP elástico dele e reassociá-lo a outra instância. Recomendamos reabrir essas conexões usando o endereço IP elástico reassociado.
- Um endereço IP elástico desassociado permanece alocado à sua conta até você liberá-lo explicitamente.
- 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 as [informações de preço do Amazon EC2](#).
- Um endereço IP elástico deve ser usado apenas em uma região específica.
- 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.

- 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.

Como trabalhar com endereços IP elásticos

As seções a seguir descrevem como você pode trabalhar com endereços IP elásticos.

Tarefas

- [Como alocar um endereço IP elástico \(p. 743\)](#)
- [Como descrever endereços IP elásticos \(p. 744\)](#)
- [Marcar um endereço IP elástico \(p. 744\)](#)
- [Como associar um endereço IP elástico a uma instância em execução \(p. 745\)](#)
- [Desassociar um endereço IP elástico e reassociá-lo a outra instância \(p. 745\)](#)
- [Como liberar um endereço IP elástico \(p. 746\)](#)
- [Recuperar um endereço IP elástico \(p. 746\)](#)

Como 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 sua 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 \(BYOIP\) \(p. 738\)](#).

Você pode alocar um endereço IP elástico usando o console do Amazon EC2 ou a linha de comando.

Para alocar um endereço IP elástico no grupo de endereços IPv4 públicos da Amazon 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 (IPs elásticos).
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.

Para alocar um endereço IP elástico em um grupo de endereços IP de sua propriedade 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 (IPs elásticos).
3. Escolha Allocate new address.
4. Em IPv4 address pool (Grupo de endereços IPv4), escolha Owned by me (De minha propriedade) e selecione o grupo de endereços IP.

Para ver o intervalo de endereços IP do grupo de endereços selecionado e o número de endereços IP já alocados no grupo de endereços, consulte [Address range \(Intervalo de endereços\)](#).

5. Em IPv4 address (Endereço IPv4), siga um dos seguintes procedimentos:
 - Para permitir que o Amazon EC2 selecione um endereço IP do grupo de endereços, escolha No preference (Sem preferências).
 - Para selecionar um endereço IP específico do grupo de endereços, escolha Select an address (Selecionar um endereço) e, em seguida, digite o endereço IP.

6. Escolha Allocate (Alocar) e feche a tela de confirmação.

Para alocar 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 [Acessando o Amazon EC2 \(p. 3\)](#).

- [allocate-address](#) (AWS CLI)
- [New-EC2Address](#) (AWS Tools para Windows PowerShell)

Como descrever endereços IP elásticos

Você pode descrever um endereço IP elástico usando o Amazon EC2 ou a linha de comando.

Para descrever seus endereços IP elásticos 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. Selecione um filtro na lista de atributos de recursos para começar a pesquisar. Você pode usar vários filtros em uma única pesquisa.

Para descrever seus endereços IP elásticos 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 [Acessando o Amazon EC2 \(p. 3\)](#).

- [describe-addresses](#) (AWS CLI)
- [Get-EC2Address](#) (AWS Tools para Windows PowerShell)

Marcar 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.

Note

O rastreamento de alocação de custos usando tags de endereço IP elástico não é compatível.

Para marcar um endereço IP elástico 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. 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 Salvar.

Para marcar um endereço IP elástico usando a linha de comando

Use um dos seguintes comandos:

- [create-tags](#)

```
aws ec2 create-tags --resources eipalloc-12345678 --tags Key=Owner,Value=TeamA
```

- [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
```

Como associar um endereço IP elástico a uma instância em execução

Você pode associar um endereço IP elástico a uma instância usando o console do Amazon EC2 ou a linha de comando.

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.

Para associar um endereço IP elástico 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 IPs.
3. Selecione um endereço IP elástico e escolha Actions, Associate address.
4. Selecione a instância em Instance e selecione Associate.

Para associar 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 [Acessando o Amazon EC2 \(p. 3\)](#).

- [associate-address](#) (AWS CLI)
- [Register-EC2Address](#) (AWS Tools para Windows PowerShell)

Desassociar um endereço IP elástico e reassociá-lo a outra instância

Você pode desassociar um endereço IP elástico e, em seguida, reassociá-lo usando o console do Amazon EC2 ou a linha de comando.

Para desassociar e reassociar um endereço IP elástico 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. Selecione o endereço IP elástico e escolha Actions e, em seguida, selecione Disassociate address.
4. Escolha Disassociate address.
5. Selecione o endereço que você desassociou na etapa anterior. Em Actions, escolha Associate address.
6. Selecione a nova instância em Instance e escolha Associate.

Para dissociar 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 [Acessando o Amazon EC2 \(p. 3\)](#).

- [disassociate-address](#) (AWS CLI)
- [Unregister-EC2Address](#) (AWS Tools para Windows PowerShell)

Para associar 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 [Acessando o Amazon EC2 \(p. 3\)](#).

- [associate-address](#) (AWS CLI)
- [Register-EC2Address](#) (AWS Tools para Windows PowerShell)

Como liberar um endereço IP elástico

Quando não precisar mais de um endereço IP elástico, é recomendável liberá-lo (o endereço não deve estar associado a uma instância).

Para liberar um endereço IP elástico 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. Selecione o endereço IP elástico, escolha Actions e selecione Release addresses. Escolha Release quando solicitado.

Para liberar 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 [Acessando o Amazon EC2 \(p. 3\)](#).

- [release-address](#) (AWS CLI)
- [Remove-EC2Address](#) (AWS Tools para Windows PowerShell)

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.

Para recuperar um endereço IP elástico usando a linha de comando

- (AWS CLI) Use o comando [allocate-address](#) e especifique o endereço IP usando o parâmetro `--address`.

```
aws ec2 allocate-address --domain vpc --address 203.0.113.3
```

- (AWS Tools para Windows PowerShell) Use o comando [New-EC2Address](#) e especifique o endereço IP usando o parâmetro `-Address`.

```
PS C:\> New-EC2Address -Address 203.0.113.3 -Domain vpc -Region us-east-1
```

Como usar o DNS reverso para aplicativos de e-mail

Se você pretender enviar e-mail a terceiros a partir de uma instância, sugerimos provisionar um ou mais endereços IP elásticos e fornecer esses endereços para nós. A AWS trabalha com os ISPs e organizações antispam da Internet para reduzir a chance de que e-mails enviados desses endereços sejam sinalizados como spam.

Além disso, a atribuição de um registro DNS reverso estático ao endereço IP elástico usado para enviar e-mails pode ajudar a evitar que esses e-mails sejam sinalizados como spam por algumas organizações antispam. Observe que deve existir um registro DNS de encaminhamento correspondente (registro tipo A) apontando para o endereço IP elástico para que você possa criar o registro DNS reverso.

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.

Para remover os limites do envio de e-mail ou para nos fornecer os endereços IP elásticos e os registros de DNS reverso, vá para a página [Solicitar a remoção de limitações de envio de e-mail](#).

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.

Se você acredita que sua arquitetura justifica endereços IP elásticos adicionais, preencha o [Formulário de solicitação de endereço IP elástico do Amazon EC2](#). Descreva seu caso de uso para entendermos sua necessidade de endereços adicionais.

Interfaces de rede elástica

Uma interface de rede elástica (chamada interface de rede nesta documentação) é um componente lógico de redes em uma VPC que representa uma cartão de rede virtual.

Uma interface de rede 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

É possível criar e configurar interfaces de rede em sua conta e anexá-las a instâncias em sua VPC. 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 \(p. 767\)](#).

Todas as interfaces de rede têm o identificador de recursos eni-xxxxxxxx.

Important

O termo “interface de rede elástica” é abreviado às vezes como “ENI”. Esta não é a mesma coisa que o adaptador de rede elástica (ENA), que é uma interface personalizada que aperfeiçoa o desempenho da rede em alguns tipos de instância. Para obter mais informações, consulte [Rede avançada no Linux \(p. 768\)](#).

Tópicos

- [Informações básicas de interfaces de rede \(p. 748\)](#)
- [Endereços IP por interface de rede por tipo de instância \(p. 749\)](#)
- [Cenários para interfaces de rede \(p. 755\)](#)
- [Práticas recomendadas para configurar interfaces de rede \(p. 757\)](#)
- [Trabalho com interfaces de rede \(p. 758\)](#)
- [Interfaces de rede gerenciadas pelo solicitante \(p. 767\)](#)

Informações básicas de interfaces 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.

Você também pode modificar os atributos da interface de rede, incluindo a alteração dos security groups, e gerenciar seus endereços IP.

Cada instância em uma VPC tem uma interface de rede padrão, chamada interface de rede primária (eth0). 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 \(p. 749\)](#).

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 primária de rede (eth0) 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 para eth0, o atributo de endereçamento IPv4 público será determinado pela interface de rede.

Para obter mais informações, consulte [Endereços IPv4 públicos e nomes de host DNS externos \(p. 724\)](#).

Endereços IPv6 públicos para interfaces de rede

Você pode associar um bloco CIDR de IPv6 com sua VPC e sua sub-rede e atribuir um ou mais endereços IPv6 do intervalo de sub-rede 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 primária de rede (eth0) criada.

Para obter mais informações, consulte [Endereços IPv6 \(p. 725\)](#).

Monitoramento do tráfego IP

Você pode ativar um log de fluxo de VPC na sua interface de rede para capturar informações sobre o tráfego IP que vai e volta da interface de rede. Depois que você tiver criado um log de fluxo, pode visualizar e recuperar esses dados no Amazon CloudWatch Logs. Para obter mais informações, consulte [Logs de fluxo da VPC](#) no Guia do usuário da Amazon VPC.

Endereços IP por interface de rede por tipo de instância

A tabela a seguir lista o número máximo de interfaces de rede por tipo de instância e o número máximo de endereços IPv4 privados e endereços IPv6 por interface de rede. O limite de endereços IPv6 é separado do limite para endereços IPv4 privados por interface de rede. Nem todos os tipos de instância são compatíveis com endereçamento IPv6. Interfaces de rede, múltiplos endereços IPv4 privados e endereços IPv6 só estão disponíveis para instâncias em execução em uma VPC. Para obter mais informações, consulte [Vários endereços IP \(p. 730\)](#). Para obter mais informações sobre IPv6 na VPC, consulte [Endereçamento IP na sua VPC](#) no Guia do usuário da Amazon VPC.

Tipo de instância	Interfaces de rede máximas	Endereços IPv4 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
c1.medium	2	6	IPv6 não compatível
c1.xlarge	4	15	IPv6 não compatível
c3.large	3	10	10
c3.xlarge	4	15	15
c3.2xlarge	4	15	15
c3.4xlarge	8	30	30

Tipo de instância	Interfaces de rede máximas	Endereços IPv4 por interface	Endereços IPv6 por interface
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
c5.18xlarge	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.18xlarge	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
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

Tipo de instância	Interfaces de rede máximas	Endereços IPv4 por interface	Endereços IPv6 por interface
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
h1.2xlarge	4	15	15
h1.4xlarge	8	30	30
h1.8xlarge	8	30	30
h1.16xlarge	15	50	50
hs1.8xlarge	8	30	IPv6 não compatível
i2.xlarge	4	15	15
i2.2xlarge	4	15	15
i2.4xlarge	8	30	30
i2.8xlarge	8	30	30
i3.large	3	10	10
i3.xlarge	4	15	15
i3.2xlarge	4	15	15
i3.4xlarge	8	30	30
i3.8xlarge	8	30	30
i3.16xlarge	15	50	50
i3.metal	15	50	50
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

Tipo de instância	Interfaces de rede máximas	Endereços IPv4 por interface	Endereços IPv6 por interface
m2.2xlarge	4	30	IPv6 não compatível
m2.4xlarge	8	30	IPv6 não compatível
m3.medium	2	6	IPv6 não compatível
m3.large	3	10	IPv6 não compatível
m3.xlarge	4	15	IPv6 não compatível
m3.2xlarge	4	30	IPv6 não compatível
m4.large	2	10	10
m4.xlarge	4	15	15
m4.2xlarge	4	15	15
m4.4xlarge	8	30	30
m4.10xlarge	8	30	30
m4.16xlarge	8	30	30
m5.large	3	10	10
m5.xlarge	4	15	15
m5.2xlarge	4	15	15
m5.4xlarge	8	30	30
m5.12xlarge	8	30	30
m5.24xlarge	15	50	50
m5a.large	3	10	10
m5a.xlarge	4	15	15
m5a.2xlarge	4	15	15
m5a.4xlarge	8	30	30
m5a.12xlarge	8	30	30
m5a.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.12xlarge	8	30	30
m5d.24xlarge	15	50	50

Tipo de instância	Interfaces de rede máximas	Endereços IPv4 por interface	Endereços IPv6 por interface
p2.xlarge	4	15	15
p2.8xlarge	8	30	30
p2.16xlarge	8	30	30
p3.2xlarge	4	15	15
p3.8xlarge	8	30	30
p3.16xlarge	8	30	30
p3dn.24xlarge	15	50	50
r3.large	3	10	10
r3.xlarge	4	15	15
r3.2xlarge	4	15	15
r3.4xlarge	8	30	30
r3.8xlarge	8	30	30
r4.large	3	10	10
r4.xlarge	4	15	15
r4.2xlarge	4	15	15
r4.4xlarge	8	30	30
r4.8xlarge	8	30	30
r4.16xlarge	15	50	50
r5.large	3	10	10
r5.xlarge	4	15	15
r5.2xlarge	4	15	15
r5.4xlarge	8	30	30
r5.12xlarge	8	30	30
r5.24xlarge	15	50	50
r5a.large	3	10	10
r5a.xlarge	4	15	15
r5a.2xlarge	4	15	15
r5a.4xlarge	8	30	30
r5a.12xlarge	8	30	30
r5a.24xlarge	15	50	50

Tipo de instância	Interfaces de rede máximas	Endereços IPv4 por interface	Endereços IPv6 por interface
r5d.large	3	10	10
r5d.xlarge	4	15	15
r5d.2xlarge	4	15	15
r5d.4xlarge	8	30	30
r5d.12xlarge	8	30	30
r5d.24xlarge	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
u-6tb1.metal	5	30	30
u-9tb1.metal	5	30	30
u-12tb1.metal	5	30	30
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

Tipo de instância	Interfaces de rede máximas	Endereços IPv4 por interface	Endereços IPv6 por interface
x1e.16xlarge	8	30	30
x1e.32xlarge	8	30	30
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

Note

Se as instâncias `f1.16xlarge`, `g3.16xlarge`, `h1.16xlarge`, `i3.16xlarge` e `r4.16xlarge` usarem mais que 31 endereços IPv4 ou IPv6 por interface, elas não poderão acessar os metadados da instância, o DNS da VPC e os serviços de sincronização de tempo do 32º endereço IP em diante. Se o acesso a esses serviços for necessário a partir de todos os endereços IP da interface, recomendamos usar um máximo de 31 endereços IP por interface.

Cenários para interfaces de rede

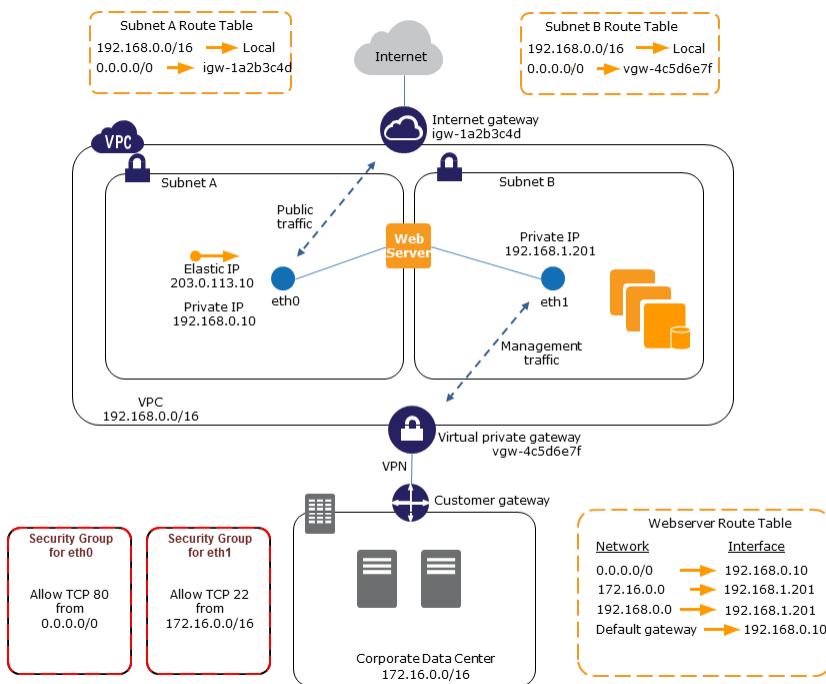
Associar várias interfaces de rede a uma instância é útil quando você deseja:

- Criar uma rede de gerenciamento.
- Usar dispositivos de rede e segurança na VPC.
- Criar instâncias dual-homed com cargas de trabalho/funções em sub-redes distintas.
- Criar uma solução de baixo orçamento e alta disponibilidade.

Criação de uma rede de gerenciamento

Você pode criar uma rede de gerenciamento usando interfaces de rede. Nesse cenário, a interface de rede primária (eth0) na instância lida com tráfego público e a interface de rede secundária (eth1) lida com o tráfego de gerenciamento de back-end e é conectada a uma sub-rede separada na sua VPC que tem controles de acesso mais restritivos. A interface voltada para o público, que pode ou não estar atrás de um load balancer, tem um grupo de segurança associado que permite acesso ao servidor da Internet (por exemplo, permite portas 80 e 443 do TCP de 0.0.0.0/0 ou do load balancer), enquanto a interface privada tem um grupo de segurança associado que permite acesso do SSH somente de um intervalo de endereços IP permitido de dentro da VPC ou da internet, de uma sub-rede privada dentro da VPC ou de 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 ferramentas de rede e segurança na sua 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 aplicativos e configurar interfaces adicionais com seus próprios endereços IP públicos e privados, security groups e verificação de origem/destino.

Criação de instâncias dual-homed com workloads/funções em sub-redes distintas

Você pode colocar uma interface de rede em cada um dos servidores web que se conecta a uma rede mid-tier na qual reside o servidor de aplicativos. O servidor de aplicativos também pode ser dual-homed para uma rede back-end (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 back-end e, então, envia solicitações aos servidores na rede back-end.

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.

Práticas recomendadas 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 anexar interfaces de rede secundárias (ethN) quando a instância estiver sendo executada ou interrompida. No entanto, você não pode separar a interface primária (eth0).
- Se você tiver várias sub-redes em uma zona de disponibilidade para a mesma VPC, poderá mover uma interface de rede de uma instância em uma dessas sub-redes para uma instância em outra dessas sub-redes.
- Ao executar uma instância da CLI ou da API, você pode especificar interfaces de rede para associar à instância para as interfaces de rede primárias (eth0) e 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, pode encontrar problemas de rede, como roteamento assimétrico. Se possível, use um endereço IPv4 privado secundário na interface de rede primária. Para obter mais informações, consulte [Como atribuir um endereço IPv4 privado secundário \(p. 732\)](#).

Configuração da sua 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 ifup padrão. Depois de o script reescrever os arquivos de configuração `ifcfg-ethN` e `route-ethN`, ele executará o ifup.

ec2ifdown ethN

Estende a funcionalidade de ifdown padrão. 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
```

Trabalho com interfaces de rede

Você pode trabalhar com interfaces de rede usando o console ou a linha de comando do Amazon EC2.

Tópicos

- [Criação de uma interface de rede \(p. 759\)](#)
- [Exclusão da interface de rede \(p. 759\)](#)
- [Visualização de detalhes sobre uma interface de rede \(p. 760\)](#)
- [Associação de uma interface de rede ao executar uma instância \(p. 760\)](#)
- [Associação de uma interface de rede a uma instância interrompida ou em execução \(p. 761\)](#)
- [Separação de uma interface de rede de uma instância \(p. 762\)](#)
- [Alteração do security group \(p. 762\)](#)
- [Alteração da verificação de origem ou do destino \(p. 763\)](#)
- [Associação de um endereço IP elástico \(IPv4\) \(p. 763\)](#)
- [Dissociação de um endereço IP elástico \(IPv4\) \(p. 764\)](#)
- [Atribuição de um endereço IPv6 \(p. 764\)](#)
- [Cancelamento da atribuição de um endereço IPv6 \(p. 765\)](#)
- [Alteração do comportamento de encerramento \(p. 765\)](#)

- [Adição ou edição de uma descrição \(p. 766\)](#)
- [Adição ou edição de tags \(p. 766\)](#)

Criação de uma interface de rede

Você pode criar uma interface de rede em uma sub-rede. A interface de rede não pode ser movida para outra sub-rede depois que for criada, e a interface somente pode ser associada a instâncias na mesma zona de disponibilidade.

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 Security groups, selecione um ou mais security groups.
9. 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 [Acessando o Amazon EC2 \(p. 3\)](#).

- [create-network-interface](#) (AWS CLI)
- [New-EC2NetworkInterface](#) (AWS Tools para Windows PowerShell)

Exclusão da interface de rede

Para excluir uma instância, você deve primeiro desacoplar a 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.

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 [Acessando o Amazon EC2 \(p. 3\)](#).

- [delete-network-interface](#) (AWS CLI)

- [Remove-EC2NetworkInterface](#) (AWS Tools para Windows PowerShell)

Visualização de detalhes sobre uma interface de rede

Você pode visualizar todas as interfaces de rede em sua conta.

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 [Acessando o Amazon EC2 \(p. 3\)](#).

- [describe-network-interfaces](#) (AWS CLI)
- [Get-EC2NetworkInterface](#) (AWS Tools para 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 [Acessando o Amazon EC2 \(p. 3\)](#).

- [describe-network-interface-attribute](#) (AWS CLI)
- [Get-EC2NetworkInterfaceAttribute](#) (AWS Tools para Windows PowerShell)

Associação de uma interface de rede ao executar uma instância

Você pode especificar uma interface de rede existente ou associar uma interface de rede adicional ao executar uma instância.

Note

Se ocorrer um erro ao acoplar uma interface de rede à sua instância, isso fará com que a execução da instância falhe.

Para associar uma interface de rede 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. Selecione uma AMI e um tipo de instância e escolha Próximo: Configurar detalhes da instância.
4. Na página Configurar detalhes da instância, selecione uma VPC para Rede e uma sub-rede para Sub-rede.
5. Na seção Interfaces de rede, o console permite que você especifique até duas interfaces de rede (nova, existente ou combinada) ao executar uma instância. Você também pode inserir um endereço IPv4 primário e um ou mais endereços IPv4 secundários para qualquer nova interface.

Você pode adicionar mais interfaces de rede à instância depois de executá-la. 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 \(p. 749\)](#).

Note

Se você especificar mais de um interface de rede, não poderá atribuir automaticamente um endereço IPv4 público à sua instância.

6. (Somente IPv6) Se você estiver executando uma instância em uma sub-rede com um bloco CIDR IPv6 associado, pode especificar endereços IPv6 para todas as interfaces de rede que associar. Em IPs IPv6, selecione Adicionar 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.
7. Escolha Next: Add Storage.
8. Na página Adicionar armazenamento, você pode especificar volumes para associar às instâncias além dos volumes especificados pela AMI (com o volume do dispositivo raiz); em seguida, selecione Próximo: Adicionar tags.
9. Na página Adicionar tags, especifique as tags da instância, como nome amigável, e selecione Próximo: Configurar security group.
10. Na página Configurar security group, você pode selecionar um security group ou criar um novo. Escolha Review and Launch.

Note

Se tiver especificado uma interface de rede existente na etapa 5, a instância estará associada ao security group dessa interface de rede, independentemente de qualquer opção que você selecionar nessa etapa.

11. Na página Revisar execução da instância, serão exibidos detalhes sobre a interface primária e adicional de rede. Revise as configurações e selecione Executar para escolher um par de chaves e executar sua instância. Se você é novo no Amazon EC2 e não ainda tiver criado nenhum par de chaves, o assistente solicitará que você crie um.

Para associar uma interface de rede ao executar 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 [Acessando o Amazon EC2 \(p. 3\)](#).

- `run-instances` (AWS CLI)
- `New-EC2Instance`

Associação de uma interface de rede a uma instância interrompida ou em execução

Você pode associar uma interface de rede a alguma das suas instâncias interrompidas ou em execução na sua VPC usando as páginas Instâncias ou Interfaces de rede do console do Amazon EC2.

Note

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 \(p. 724\)](#).

Para associar uma interface de rede a 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. Escolha Ações, Redes, Associar interface de rede.
4. Na caixa de diálogo Associar interface de rede, selecione a interface de rede e escolha Associar.

Para associar uma interface de rede a 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. Selecione a interface de rede e escolha Associar.
4. Na caixa de diálogo Associar interface de rede, selecione a instância e 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 [Acessando o Amazon EC2 \(p. 3\)](#).

- [attach-network-interface](#) (AWS CLI)
- [Add-EC2NetworkInterface](#) (AWS Tools para Windows PowerShell)

Separação de uma interface de rede de uma instância

Você pode separar uma interface de rede secundária a qualquer momento usando as páginas Instâncias ou Interfaces de rede do console do Amazon EC2.

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. Escolha Ações, Redes, Separar interface de rede.
4. Na caixa de diálogo Separar interface de rede, selecione a interface de rede e escolha Separar.

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. Selecione a interface de rede e escolha Separar.
4. Na caixa de diálogo Separar interface de rede, escolha Sim, separar. Se a interface de rede não conseguir se separar da instância, escolha Forçar separação e tente novamente.

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 [Acessando o Amazon EC2 \(p. 3\)](#).

- [detach-network-interface](#) (AWS CLI)
- [Dismount-EC2NetworkInterface](#) (AWS Tools para Windows PowerShell)

Alteração do security group

Você pode alterar os security groups associados a qualquer interface de rede. Ao criar o security group, não deixe de certificar a mesma VPC que a sub-rede para interface de rede.

Note

Para alterar a associação do security group para interfaces de propriedade de outros serviços, como Elastic Load Balancing, use o console ou a interface de linha de comando para esse serviço.

Para alterar o security group 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 e escolha Ações, Alterar security groups.
4. Na caixa de diálogo Alterar security groups, selecione os security groups a serem usados e escolha Salvar.

Para alterar o security group de 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 [Acessando o Amazon EC2 \(p. 3\)](#).

- [modify-network-interface-attribute](#) (AWS CLI)
- [Edit-EC2NetworkInterfaceAttribute](#) (AWS Tools para Windows PowerShell)

Alteração da verificação de origem ou do destino

O atributo de verificação de origem/destino controla se a verificação de origem/destino está ativada na instância. Desabilitar esse atributo permite que uma instância lide com o tráfego de rede que não é especificamente destinado para a instância. Por exemplo, instâncias que executam serviços como tradução de endereço de rede, roteamento ou firewall devem definir esse valor como disabled. O valor padrão é enabled.

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. Selecione a interface de rede e escolha Ações, Alterar verificação de origem/destino.
4. Na caixa de diálogo, escolha Habilitado (se estiver habilitando) ou Desabilitado (se estiver desabilitando), e Salvar.

Para alterar a verificação de origem/destino de 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 [Acessando o Amazon EC2 \(p. 3\)](#).

- [modify-network-interface-attribute](#) (AWS CLI)
- [Edit-EC2NetworkInterfaceAttribute](#) (AWS Tools para Windows PowerShell)

Associação de um endereço IP elástico (IPv4)

Se você tiver um endereço IP elástico (IPv4), pode associá-lo com um dos endereços IPv4 privados da interface de rede. Você pode associar um endereço IP elástico a cada endereço IPv4 privado.

Você pode associar um endereço IP elástico usando o console do Amazon EC2 ou a linha de comando.

Para associar um endereço IP elástico 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 escolha Ações, Associar endereço.
4. Na caixa de diálogo Associar endereço IP elástico, selecione o endereço IP elástico na lista Endereço.
5. Para Associar ao endereço IP privado, selecione o endereço IPv4 privado a ser associado ao endereço IP elástico.
6. Escolha Permitir reassociação para permitir que o endereço IP elástico seja associado com uma interface de rede especificada, se ela estiver associada no momento a outra instância ou interface de rede, e escolha Associar endereço.

Para associar 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 [Acessando o Amazon EC2 \(p. 3\)](#).

- [associate-address](#) (AWS CLI)
- [Register-EC2Address](#) (AWS Tools para Windows PowerShell)

Dissociação de um endereço IP elástico (IPv4)

Se a interface de rede tiver um endereço IP elástico (IPv4) associado, você pode dissociar o endereço e, então, associá-lo a outra interface de rede ou liberá-lo de volta ao pool de endereços. Esta é a única forma de associar um endereço IP elástico a uma instância em uma sub-rede diferente ou VPC usando uma interface de rede, pois as interfaces de rede são específicas de uma sub-rede específica.

Você pode dissociar um endereço IP elástico usando o console do Amazon EC2 ou a linha de comando.

Para dissociar um endereço IP elástico 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 escolha Ações, Dissociar o endereço.
4. Na caixa de diálogo Dissociar endereço IP, escolha Sim, dissociar.

Para dissociar 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 [Acessando o Amazon EC2 \(p. 3\)](#).

- [disassociate-address](#) (AWS CLI)
- [Unregister-EC2Address](#) (AWS Tools para Windows PowerShell)

Atribuição de um endereço IPv6

Você pode atribuir um ou mais endereços IPv6 a uma interface de rede. A interface de rede deve estar 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.

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.

2. No painel de navegação, selecione Interfaces de rede e selecione a interface de rede.
3. Escolha Ações, Gerenciar endereços IP.
4. Em Endereços IPv6, escolha Atribuir novo IP. Especifique um endereço IPv6 do intervalo da sub-rede. Para permitir que a AWS escolha um endereço para você, deixe o valor de Atribuir automaticamente.
5. Escolha Yes, Update.

Para atribuir um endereço IPv6 a 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 [Acessando o Amazon EC2 \(p. 3\)](#).
 - [assign-ipv6-addresses](#) (AWS CLI)
 - [Register-EC2Ipv6AddressList](#) (AWS Tools para Windows PowerShell)

Cancelamento da atribuição de um endereço IPv6

Você pode cancelar a atribuição de um endereço IPv6 de uma interface de rede 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 Interfaces de rede e selecione a interface de rede.
3. Escolha Ações, Gerenciar endereços IP.
4. Em Endereços IPv6, escolha Cancelar a atribuição para o endereço IPv6 fazer a remoção.
5. Escolha Yes, Update.

Para cancelar a atribuição de um endereço IPv6 de 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 [Acessando o Amazon EC2 \(p. 3\)](#).
 - [unassign-ipv6-addresses](#) (AWS CLI)
 - [Unregister-EC2Ipv6AddressList](#) (AWS Tools para Windows PowerShell).

Alteração do 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.

Você pode alterar o comportamento de encerramento para uma interface de rede usando o console do Amazon EC2 ou a linha de comando.

Para 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. Selecione a interface de rede e escolha Ações, Alterar comportamento de encerramento.
4. Na caixa de diálogo Change Termination Behavior, marque a caixa Delete on termination se você quiser que a interface de rede seja excluída quando encerrar uma instância.

Para alterar o comportamento de encerramento de 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 [Acessando o Amazon EC2 \(p. 3\)](#).

- [modify-network-interface-attribute](#) (AWS CLI)
- [Edit-EC2NetworkInterfaceAttribute](#) (AWS Tools para Windows PowerShell)

Adição ou edição de uma descrição

Você pode alterar a descrição de uma interface de rede usando o console do Amazon EC2 ou a linha de comando.

Para 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. Selecione a interface de rede e escolha Ações, Alterar descrição.
4. Na caixa de diálogo Alterar descrição, digite uma descrição para a interface de rede e escolha Salvar.

Para alterar a descrição de 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 [Acessando o Amazon EC2 \(p. 3\)](#).

- [modify-network-interface-attribute](#) (AWS CLI)
- [Edit-EC2NetworkInterfaceAttribute](#) (AWS Tools para Windows PowerShell)

Adição ou edição de 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 [Marcação dos seus recursos do Amazon EC2 \(p. 1003\)](#).

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 [Acessando o Amazon EC2 \(p. 3\)](#).

- [create-tags](#)
- [New-EC2Tag](#)

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 ser modificada ou desacoplada. Se você excluir o recurso que a interface de rede representa, o serviço da AWS desacopla e exclui a 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 [Adição ou edição de tags \(p. 766\)](#).

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 o administrador ou serviço que criou uma 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 AWS, o campo RequesterManaged exibe true.

```
{  
    "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 para Windows PowerShell.

Rede avançada no Linux

A rede avançada usa virtualização de E/S raiz (SR-IOV) para fornecer recursos de rede de alto desempenho em [tipos de instâncias com suporte \(p. 768\)](#). A SR-IOV é um método de virtualização de dispositivos que fornece desempenho 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, um desempenho melhor de pacotes por segundo (PPS) e latências entre instâncias consistentemente mais baixas. Não há nenhuma cobrança adicional pelo uso da rede avançada.

Tópicos

- [Tipos de rede avançada \(p. 768\)](#)
- [Como habilitar a rede avançada na instância \(p. 768\)](#)
- [Como habilitar a rede avançada com o Elastic Network Adapter \(ENA\) em instâncias do Linux compatíveis \(p. 769\)](#)
- [Como habilitar a rede avançada com a interface Intel 82599 VF nas instâncias do Linux \(p. 780\)](#)
- [Solução de problemas do Elastic Network Adapter \(ENA\) \(p. 786\)](#)

Tipos de rede avançada

Dependendo do tipo de instância, a rede avançada pode ser habilitada 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 A1, C5, C5d, C5n, F1, G3, H1, I3, m4.16xlarge, M5, M5a, M5d, P2, P3, R4, R5, R5a, R5d, T3, u-6tb1.metal, u-9tb1.metal, u-12tb1.metal, X1, X1e, and z1d usam o Elastic Network Adapter para redes avançadas.

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.

As instâncias C3, C4, D2, I2, M4 (exceto m4.16xlarge) e R3 usam a interface Intel 82599 VF para rede avançada.

Para obter mais informações sobre a velocidade de rede compatível com cada tipo de instância, consulte [Tipos de instância do Amazon EC2](#).

Como habilitar a rede avançada na instância

Se o seu tipo de instância for compatível com o Elastic Network Adapter para rede avançada, siga os procedimentos em [Como habilitar a rede avançada com o Elastic Network Adapter \(ENA\) em instâncias do Linux compatíveis \(p. 769\)](#).

Se o seu tipo de instância for compatível com a interface Intel 82599 VF para rede avançada, siga os procedimentos em [Como habilitar a rede avançada com a interface Intel 82599 VF nas instâncias do Linux \(p. 780\)](#).

Como habilitar a rede avançada com o Elastic Network Adapter (ENA) em instâncias do Linux compatíveis

O Amazon EC2 oferece recursos de rede avançada pelo Elastic Network Adapter (ENA).

Tópicos

- [Requisitos \(p. 769\)](#)
- [Como testar se a rede avançada está habilitada \(p. 769\)](#)
- [Como habilitar uma rede avançada no Amazon Linux AMI \(p. 771\)](#)
- [Como habilitar a rede avançada no Ubuntu \(p. 772\)](#)
- [Como habilitar a rede avançada no Linux \(p. 773\)](#)
- [Como habilitar a rede avançada com o Ubuntu com o DKMS \(p. 775\)](#)
- [Solução de problemas \(p. 777\)](#)
- [Otimizações do sistema operacional \(p. 777\)](#)

Requisitos

Para se preparar para a rede avançada com o ENA, configure a instância da seguinte forma:

- Selecione os seguintes tipos de instância disponíveis: A1, C5, C5d, C5n, F1, G3, H1, I3, `m4.16xlarge`, M5, M5a, M5d, P2, P3, R4, R5, R5a, R5d, T3, `u-6tb1.metal`, `u-9tb1.metal`, `u-12tb1.metal`, X1, X1e, and z1d.
- 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.
- Instale e configure a [AWS CLI](#) ou o [AWS Tools para Windows PowerShell](#) em qualquer computador de sua escolha, preferivelmente, em seu desktop ou notebook local. Para obter mais informações, consulte [Acessando o Amazon EC2 \(p. 3\)](#). 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 se isso ocorrer.

Como testar se a rede avançada está habilitada

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` da seguinte forma:

```
[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 [Como habilitar a rede avançada no Ubuntu \(p. 772\)](#).

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 ec2 describe-instances --instance-ids instance_id --query
"Reservations[].[Instances[]].EnaSupport"
```

- [Get-EC2Instance](#) Tools para 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 ec2 describe-images --image-id ami_id --query "Images[].[EnaSupport]"
```

- [Get-EC2Image](#) (Tools para 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 eth0.

```
[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
```

No caso acima, o módulo ena não está carregado porque o driver listado é vif.

```
[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
```

Nesse caso, o módulo ena está carregado e na versão mínima recomendada. Essa instância configurou a rede avançada corretamente.

Como habilitar uma rede avançada no Amazon Linux AMI

O Amazon Linux 2 e as versões mais recentes do Amazon Linux AMI têm o módulo necessário para a rede avançada instalado e também têm o atributo necessário `enaSupport` definido. 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 [Como testar se a rede avançada está habilitada \(p. 769\)](#).

Se você executou a instância usando uma Amazon Linux AMI 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 para 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 [Como testar se a rede avançada está habilitada \(p. 769\)](#).
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 para 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 \(instâncias compatíveis com o armazenamento de instâncias\) \(p. 772\)](#).

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 \(Tools para Windows PowerShell\)](#)

```
Edit-EC2InstanceAttribute -InstanceId instance_id -EnaSupport $true
```

7. (Opcional) Crie uma AMI na instância, conforme descrito em [Criação de uma AMI do Linux com Amazon EBS \(p. 111\)](#). 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 para 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 [Como testar se a rede avançada está habilitada \(p. 769\)](#).

Se não for possível conectar-se à instância depois de habilitar a rede avançada, consulte [Solução de problemas do Elastic Network Adapter \(ENA\) \(p. 786\)](#).

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 [Criação de uma AMI em Linux com armazenamento de instâncias \(p. 115\)](#), habilitando o atributo de rede avançada ao registrar a AMI.

- [register-image \(AWS CLI\)](#)

```
aws ec2 register-image --ena-support ...
```

- [Register-EC2Image \(AWS Tools para Windows PowerShell\)](#)

```
Register-EC2Image -EnaSupport $true ...
```

Como habilitar a rede avançada no Ubuntu

As AMIs HVM do Ubuntu mais recentes têm o módulo necessário para a rede avançada com ENA instalado e também têm o atributo necessário enaSupport definido. 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 [Como testar se a rede avançada está habilitada \(p. 769\)](#).

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)

Ubuntu 16.04 e 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.

- 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.

- [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 para 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. 773).
- 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 para Windows PowerShell)

```
Edit-EC2InstanceAttribute -InstanceId instance_id -EnaSupport $true
```

- (Opcional) Crie uma AMI na instância, conforme descrito em [Criação de uma AMI do Linux com Amazon EBS](#) (p. 111). 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.
- 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 para 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 [Criação de uma AMI em Linux com armazenamento de instâncias](#) (p. 115), habilitando o atributo de rede avançada ao registrar a AMI.

- [register-image](#) (AWS CLI)

```
aws ec2 register-image --ena-support ...
```

- [Register-EC2Image](#) (AWS Tools para Windows PowerShell)

```
Register-EC2Image -EnaSupport $true ...
```

Como habilitar a rede avançada no Linux

O procedimento a seguir fornece as etapas gerais para habilitar a rede avançada em uma distribuição do Linux diferente da Amazon Linux AMI ou do Ubuntu, como o SUSE Linux Enterprise Server (SLES).

Red Hat Enterprise Linux ou o CentOS. Antes de começar, consulte [Como testar se a rede avançada está habilitada \(p. 769\)](#) para verificar se sua instância já está habilitada para rede avançada. 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. Clone o código-fonte do módulo ena na instância a partir do GitHub em <https://github.com/amzn/amzn-drivers>. (Como o SUSE SLES 12 SP2 ou posterior incluem ENA 2.02 por padrão, não é necessário fazer download e compilar o driver ENA. Para o SLES 12 SP2 ou posterior, você deve enviar uma solicitação para adicionar a versão do driver desejada ao kernel padrão).

```
git clone https://github.com/amzn/amzn-drivers
```

3. Compile e instale o módulo ena na instância.
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 sua distribuição oferecer suporte a dracut, você poderá usar o seguinte comando:

```
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. Você pode verificar as versões do systemd ou udev em sistemas baseados em RPM com o seguinte comando:

```
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 para 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 Linux \(instâncias compatíveis com o –armazenamento de instâncias\) \(p. 775\)](#).

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 para Windows PowerShell)

```
Edit-EC2InstanceAttribute -InstanceId instance_id -EnaSupport $true
```

9. (Opcional) Crie uma AMI na instância, conforme descrito em [Criação de uma AMI do Linux com Amazon EBS \(p. 111\)](#). 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 para 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 \(ENA\) \(p. 786\)](#).

Para habilitar a rede avançada no Linux (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 [Criação de uma AMI em Linux com armazenamento de instâncias \(p. 115\)](#), habilitando o atributo de rede avançada ao registrar a AMI.

- [register-image](#) (AWS CLI)

```
aws ec2 register-image --ena-support ...
```

- [Register-EC2Image](#) (AWS Tools para Windows PowerShell)

```
Register-EC2Image -EnaSupport ...
```

Como habilitar a rede avançada com o Ubuntu com o 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 [Como habilitar a rede avançada no Ubuntu \(p. 772\)](#).

Important

O uso do DKMS anula o acordo de suporte da sua assinatura. Usar as configurações de kmod é uma alternativa aceitável para executar os últimos módulos do kernel disponíveis.

Para habilitar a rede avançada com o ENA no Ubuntu (instâncias com suporte do EBS)

1. Siga as etapas 1 e 2 em [Como habilitar a rede avançada no Ubuntu \(p. 772\)](#).
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 abaixo.

```
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 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 -c -k all
```

- Verifique se o módulo ena está instalado usando o comando modinfo ena em [???](#) (p. 769).

```
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:    9693C876C54CA64AE48F0CA
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)
```

- Passe para a etapa 3 em [Como habilitar a rede avançada no Ubuntu \(p. 772\)](#).

Solução de problemas

Para obter informações adicionais sobre como solucionar problemas do adaptador do ENA, consulte [Solução de problemas do Elastic Network Adapter \(ENA\) \(p. 786\)](#).

Otimizações do sistema operacional

Para obter o máximo desempenho da rede em instâncias com redes avançadas, pode ser necessário modificar a configuração do sistema operacional padrão. Recomendamos as seguintes alterações na configuração de aplicativos que exigem alto desempenho de rede.

Além dessas otimizações do sistema operacional, você também deve considerar a unidade de transmissão máxima (MTU - maximum transmission unit) de seu tráfego de rede e ajustá-la de acordo com sua carga de trabalho e arquitetura de rede. Para obter mais informações, consulte [Unidade de transmissão máxima \(MTU\) de rede para sua instância do EC2 \(p. 801\)](#).

Esses procedimentos foram escritos para o Amazon Linux 2 e a Amazon Linux AMI. No entanto, eles também podem funcionar para outras distribuições do Linux com kernel versão 3.9 ou mais recente. Para obter mais informações, consulte a documentação específica de seu sistema.

Para otimizar a instância do Amazon Linux para redes avançadas

- Verifique a origem do relógio de sua instância:

```
cat /sys/devices/system/clocksource/clocksource0/current_clocksource
```

- Se a origem do relógio for o xen, conclua as subetapas a seguir. Caso contrário, vá para a [Step 3 \(p. 778\)](#).

- a. Edite a configuração de GRUB e adicione `xen_nopvspin=1` e `clocksource=tsc` às opções de inicialização do kernel.

- No Amazon Linux 2, edite o arquivo `/etc/default/grub` e adicione essas opções à linha `GRUB_CMDLINE_LINUX_DEFAULT`, conforme mostrado a seguir:

```
GRUB_CMDLINE_LINUX_DEFAULT="console=tty0 console=ttyS0,115200n8 net.ifnames=0  
biosdevname=0 nvme_core.io_timeout=4294967295 xen_nopvspin=1 clocksource=tsc"  
GRUB_TIMEOUT=0
```

- No Amazon Linux AMI, edite o arquivo `/boot/grub/grub.conf` e adicione essas opções à linha `kernel`, conforme mostrado a seguir:

```
kernel /boot/vmlinuz-4.14.62-65.117.amzn1.x86_64 root=LABEL=/ console=tty1  
console=ttyS0 selinux=0 nvme_core.io_timeout=4294967295 xen_nopvspin=1  
clocksource=tsc
```

- b. (Somente no Amazon Linux 2) Reconstrua o arquivo de configuração de GRUB para incorporar estas alterações:

```
sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

3. Se seu tipo de instância estiver listado como compatível em [Controle do estado do processo para sua instância do EC2 \(p. 485\)](#), impeça o sistema de usar os estados C mais profundos para garantir desempenho de baixa latência do sistema. Para obter mais informações, consulte [Alto desempenho e baixa latência limitando os C-states mais profundos \(p. 487\)](#).

- a. Edite a configuração de GRUB e adicione `intel_idle.max_cstate=1` às opções de inicialização do kernel.

- No Amazon Linux 2, edite o arquivo `/etc/default/grub` e adicione essa opção à linha `GRUB_CMDLINE_LINUX_DEFAULT`, conforme mostrado a seguir:

```
GRUB_CMDLINE_LINUX_DEFAULT="console=tty0 console=ttyS0,115200n8  
net.ifnames=0 biosdevname=0 nvme_core.io_timeout=4294967295 xen_nopvspin=1  
clocksource=tsc intel_idle.max_cstate=1"  
GRUB_TIMEOUT=0
```

- No Amazon Linux AMI, edite o arquivo `/boot/grub/grub.conf` e adicione essa opção à linha `kernel`, conforme mostrado a seguir:

```
kernel /boot/vmlinuz-4.14.62-65.117.amzn1.x86_64 root=LABEL=/ console=tty1  
console=ttyS0 selinux=0 nvme_core.io_timeout=4294967295 xen_nopvspin=1  
clocksource=tsc intel_idle.max_cstate=1
```

- b. (Somente no Amazon Linux 2) Reconstrua o arquivo de configuração de GRUB para incorporar estas alterações:

```
sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

4. Verifique se a memória reservada do kernel é suficiente para sustentar uma alta taxa de alocações de buffer de pacote (o valor padrão pode ser muito pequeno).

- Abra (como `root` ou com `sudo`) o arquivo `/etc/sysctl.conf` com o editor de sua escolha.
- Adicione a linha `vm.min_free_kbytes` ao arquivo com o valor de memória reservada do kernel (em kilobytes) para seu tipo de instância. Como prática básica, você deve definir esse valor como 1 a 3% da memória disponível do sistema e ajustá-lo para cima ou para baixo para atender às necessidades de seu aplicativo.

```
vm.min_free_kbytes = 1048576
```

- c. Aplique essa configuração com o seguinte comando:

```
sudo sysctl -p
```

- d. Verifique se a configuração foi aplicada com o seguinte comando:

```
sudo sysctl -a 2>&1 | grep min_free_kbytes
```

5. Reinicialize a instância para carregar a nova configuração:

```
sudo reboot
```

6. (Opcional) Distribua manualmente interrupções de recebimento de pacotes para que elas sejam associadas a diferentes CPUs que pertençam ao mesmo nó NUMA. No entanto, use isso cuidadosamente, porque irqlimiter está desabilitado globalmente.

Note

A alteração da configuração nesta etapa não sobrevive a uma reinicialização.

- a. Crie um arquivo chamado `smp_affinity.sh` e cole o bloco de código a seguir nesse arquivo:

```
#!/bin/sh
service irqbalance stop
affinity_values=(00000001 00000002 00000004 00000008 00000010 00000020 00000040
 00000080)
irqs=($(grep eth /proc/interrupts|awk '{print $1}'|cut -d : -f 1))
irqLen=${#irqs[@]}
for (( i=0; i<${irqLen}; i++ )); do
    echo $(printf "0000,00000000,00000000,00000000,%s" ${affinity_values[$i]}) > /proc/
irq/${irqs[$i]}/smp_affinity;
    echo "IRQ ${irqs[$i]} =" $(cat /proc/irq/${irqs[$i]}/smp_affinity);
done
```

- b. Execute o script com o comando a seguir:

```
sudo bash ./smp_affinity.sh
```

7. (Opcional) Se as vCPUs que lidam com IRQs de recebimento estiverem sobrecarregadas, ou se o processamento de rede do aplicativo estiver exigindo CPU, você poderá descarregar parte do processamento de rede para outros núcleos com condução de recebimento de pacotes (RPS - receive packet steering). Verifique se os núcleos usados para RPS pertencem ao mesmo nó NUMA para evitar bloqueios de nós inter-NUMA. Por exemplo, para usar os núcleos 8 a 15 para processamento de pacotes, use o comando a seguir.

Note

A alteração da configuração nesta etapa não sobrevive a uma reinicialização.

```
for i in `seq 0 7`; do echo $(printf "0000,00000000,00000000,00000000,0000ff00") | sudo
tee /sys/class/net/eth0/queues/rx-$i/rps_cpus; done
```

8. (Opcional) Se possível, mantenha todo o processamento no mesmo nó NUMA.

- a. Instale o numactl:

```
sudo yum install -y numactl
```

- b. Ao executar o programa de processamento de rede, associe-o a um único nó NUMA. Por exemplo, o comando a seguir vincula o script de shell, run.sh, ao nó NUMA 0:

```
numactl --cpunodebind=0 --membind=0 run.sh
```

- c. Se tiver hyperthreading habilitado, você poderá configurar seu aplicativo para usar apenas um único thread de hardware por núcleo de CPU.
 - Você pode visualizar quais núcleos de CPU mapeiam para um nó NUMA com o comando lscpu:

```
lscpu | grep NUMA
```

Resultado:

```
NUMA node(s):      2
NUMA node0 CPU(s): 0-15,32-47
NUMA node1 CPU(s): 16-31,48-63
```

- Você pode visualizar threads de hardware que pertencem a uma CPU física com o seguinte comando:

```
cat /sys/devices/system/cpu/cpu0/topology/thread_siblings_list
```

Resultado:

```
0,32
```

Neste exemplo, os threads 0 e 32 são mapeados para a CPU 0.

- Para evitar a execução nos threads 32 a 47 (que são realmente threads de hardware das mesmas CPUs, como 0 a 15, use o seguinte comando:

```
numactl --physcpubind=+0-15 --membind=0 ./run.sh
```

9. Use várias interfaces de rede elástica para diferentes classes de tráfego. Por exemplo, se estiver executando um servidor Web que usa um banco de dados de back-end, use interfaces de rede elástica para o servidor web de front-end e outro para a conexão do banco de dados.

Como habilitar a rede avançada 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

- [Requisitos \(p. 781\)](#)
- [Como testar se a rede avançada está habilitada \(p. 781\)](#)
- [Como habilitar a rede avançada no Amazon Linux \(p. 783\)](#)
- [Como habilitar a rede avançada no Ubuntu \(p. 784\)](#)
- [Como habilitar a rede avançada em outras distribuições do Linux \(p. 784\)](#)

- [Solução de problemas de conectividade \(p. 786\)](#)

Requisitos

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 (excluindo 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 Amazon EBSrede avançada com suporte do — 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.
- Instale e configure a [AWS CLI](#) ou o [AWS Tools para Windows PowerShell](#) em qualquer computador de sua escolha, preferivelmente, em seu desktop ou notebook local. Para obter mais informações, consulte [Acessando o Amazon EC2 \(p. 3\)](#). 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 se isso ocorrer.

Como 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 (`sriovNetSupport`)

Para verificar se uma instância tem o atributo `sriovNetSupport` de rede avançada definido, use um dos seguintes comandos:

- [describe-instance-attribute](#) (AWS CLI)

```
aws ec2 describe-instance-attribute --instance-id instance_id --attribute sriovNetSupport
```

- [Get-EC2InstanceAttribute](#) (AWS Tools para Windows PowerShell)

```
Get-EC2InstanceAttribute -InstanceId instance_id -Attribute sriovNetSupport
```

Se o atributo não estiver definido, `SriovNetSupport` estará vazio. Caso contrário, estará definido da seguinte forma:

```
"SriovNetSupport": {  
    "Value": "simple"
```

},

Atributo de imagem (srivNetSupport)

Para verificar se uma AMI já tem o atributo `sriovNetSupport` de rede avançada definido, use um dos seguintes comandos:

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

```
aws ec2 describe-image-attribute --image-id ami_id --attribute sriovNetSupport
```

Observe que o comando funciona apenas para imagens de sua propriedade. Você recebe um erro `AuthFailure` para imagens que não pertencem à sua conta.

- [Get-EC2ImageAttribute](#) (AWS Tools para Windows PowerShell)

```
Get-EC2ImageAttribute -ImageId ami-id -Attribute sriovNetSupport
```

Se o atributo não estiver definido, `SriovNetSupport` estará vazio. Caso contrário, estará definido da seguinte forma:

```
"SriovNetSupport": {  
    "Value": "simple"  
},
```

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`.

```
[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
```

No caso acima, o módulo `ixgbevf` não está carregado porque o driver listado é `vif`.

```
[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
```

Nesse caso, o módulo `ixgbevf` está carregado. Essa instância configurou a rede avançada corretamente.

Como 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 [Como testar se a rede avançada está habilitada \(p. 781\)](#).

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 para 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 [Como testar se a rede avançada está habilitada \(p. 781\)](#).
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 para 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 \(instâncias compatíveis com o armazenamento de instâncias\) \(p. 784\)](#).

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 --sriov-net-support simple
```

- [Edit-EC2InstanceAttribute](#) (AWS Tools para Windows PowerShell)

```
Edit-EC2InstanceAttribute -InstanceId instance_id -SriovNetSupport "simple"
```

7. (Opcional) Crie uma AMI na instância, conforme descrito em [Criação de uma AMI do Linux com Amazon EBS \(p. 111\)](#). 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 para 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 [Como testar se a rede avançada está habilitada \(p. 781\)](#).

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 [Criação de uma AMI em Linux com armazenamento de instâncias \(p. 115\)](#), habilitando o atributo de rede avançada ao registrar a AMI.

- [register-image \(AWS CLI\)](#)

```
aws ec2 register-image --srivnet-support simple ...
```

- [Register-EC2Image \(AWS Tools para Windows PowerShell\)](#)

```
Register-EC2Image -SriovNetSupport "simple" ...
```

Como habilitar a rede avançada no Ubuntu

Antes de começar, o [verifica se a rede avançada já está habilitada \(p. 781\)](#) 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`.

Como habilitar a rede avançada em outras distribuições do Linux

Antes de começar, o [verifica se a rede avançada já está habilitada \(p. 781\)](#) 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, em seguida, atualizar o kernel sem recompilar o driver para o novo kernel, o sistema poderá reverter o módulo `ixgbevf` específico à distribuição na próxima reinicialização, o que pode 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 `inotifyfs` 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), [Stop-EC2Instance](#) (AWS Tools para 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 \(instâncias compatíveis com o armazenamento de instâncias\) \(p. 786\)](#).

8. 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 --srivnet-support simple
```

- [Edit-EC2InstanceAttribute](#) (AWS Tools para Windows PowerShell)

```
Edit-EC2InstanceAttribute -InstanceId instance_id -SriovNetSupport "simple"
```

9. (Opcional) Crie uma AMI na instância, conforme descrito em [Criação de uma AMI do Linux com Amazon EBS \(p. 111\)](#). 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.

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 para 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.

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 [Criação de uma AMI em Linux com armazenamento de instâncias \(p. 115\)](#), habilitando o atributo de rede avançada ao registrar a AMI.

- [register-image](#) (AWS CLI)

```
aws ec2 register-image --srivnet-support simple ...
```

- [Register-EC2Image](#) (AWS Tools para Windows PowerShell)

```
Register-EC2Image -SriovNetSupport "simple" ...
```

Solução de 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?](#).

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 [Solução de problemas de conectividade \(p. 787\)](#).

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

- [Solução de problemas de conectividade \(p. 787\)](#)
- [Mecanismo de keep-alive \(p. 788\)](#)
- [Registre o tempo limite de leitura \(p. 789\)](#)
- [Estatísticas \(p. 789\)](#)
- [Logs de erro do driver no syslog \(p. 791\)](#)

Solução de 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 para 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 \(instâncias com suporte do armazenamento de instâncias\) \(p. 787\)](#).

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 para 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 [Como habilitar a rede avançada com o Elastic Network Adapter \(ENA\) em instâncias do Linux compatíveis \(p. 769\)](#).

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 [Criação de uma AMI em Linux com armazenamento de instâncias \(p. 115\)](#). 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 para 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
```

Estatísticas

Se você tiver problemas de latência ou de desempenho 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
  io_suspend: 0
  io_resume: 0
  wd_expired: 0
  interface_up: 1
  interface_down: 0
  admin_q_pause: 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.

io_suspend: *N*

Não há suporte. Esse valor deve ser sempre zero.

`io_resume: N`

O número de vezes que o driver não recebeu o evento de keep-alive nos 3 segundos anteriores.

`wd_expired: N`

O número de vezes a interface do ENA foi ativada.

`interface_up: N`

O número de vezes a interface do ENA foi desativada.

`admin_q_pause: N`

A fila do administrador está em um estado instável. Esse valor deve ser sempre zero.

`queue_N_tx_cnt: N`

O número de pacotes transmitidos para a fila `N`.

`queue_N_tx_bytes: N`

O número de bytes transmitidos para a fila `N`.

`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_napi_comp: N`

O número de vezes que o manipulador `napi` chamou `napi_complete` para a fila `N`.

`queue_N_tx_poll: N`

O número de vezes que o manipulador `napi` foi programado para a fila `N`.

`queue_N_tx_doorbells: N`

O número de campainhas de transmissão para a fila `N`.

`queue_N_tx_linearize: N`

O número de vezes que a linearização de SKB foi tentada para a fila `N`.

`queue_N_tx_linearize_failed: N`

O número de vezes que a linearização de SKB falhou para a fila `N`.

`queue_N_tx_prepare_ctx_err: N`

O número de vezes que `ena_com_prepare_tx` falhou para a fila `N`. Esse valor sempre deve ser zero; caso contrário, consulte os logs do driver.

`queue_N_tx_missing_tx_comp: codeN`

O número de pacotes deixados sem conclusão para a fila `N`. Esse valor deve ser sempre zero.

`queue_N_tx_bad_req_id: N`

`req_id` inválido para a fila `N`. O `req_id` válido é zero, menos `queue_size`, menos 1.

`queue_N_rx_cnt: N`

O número de pacotes recebidos para a fila `N`.

`queue_N_rx_bytes: N`

O número de bytes recebidos para a fila `N`.

`queue_N_rx_refill_partial: N`

O número de vezes que o driver não teve sucesso ao reabastecer a parte vazia da fila `rx` com buffers para a fila `N`. 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 `N` (somente se o descarregamento da soma de verificação `rx` for compatível).

`queue_N_rx_page_alloc_fail: N`

O número de vezes que a alocação de página falhou para a fila `N`. 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 falhou para a fila `N`. 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 uso de buffers muito pequenos.

`queue_N_rx_small_copy_len_pkt: N`

Otimização: Para pacotes menores que esse limite, que é definido por `sysfs`, o pacote é copiado diretamente para a pilha para evitar alocação de uma página nova.

`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:1e:13:b5 Queues 8
Jun  3 22:37:46 ip-172-31-2-186 kernel: [ 480.805037] EXT4-fs (xvda1): 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.

fallha 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.

Placement groups

Você pode executar ou iniciar instâncias em um placement group, que determina como elas são colocadas no hardware subjacente. Ao criar um placement group, você especifica uma das seguintes estratégias para o grupo:

- Agrupar – agrupa instâncias em um grupo de baixa latência dentro de uma única zona de disponibilidade
- Partição – distribui instâncias entre partições lógicas, garantindo que instâncias em uma partição não compartilhem hardware subjacente com instâncias em outras partições.
- Distribuir – distribui instâncias em todo o hardware subjacente

Não há cobrança para criar um placement group.

Tópicos

- [Placement groups de cluster \(p. 793\)](#)
- [Placement groups de partição \(p. 794\)](#)
- [Placement groups de distribuição \(p. 795\)](#)
- [Regras e limitações do placement group \(p. 795\)](#)
- [Criação de um placement group \(p. 797\)](#)
- [Execução de instâncias em um placement group \(p. 797\)](#)
- [Descrever instâncias em um placement group \(p. 798\)](#)
- [Como alterar o placement group de uma instância \(p. 799\)](#)
- [Exclusão de um placement group \(p. 800\)](#)

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 pode abranger VPCs emparelhadas na mesma região. O principal benefício de um placement group de cluster, além de um limite de fluxo de 10 Gbps, é a característica de não bloquear, não sobrecarregar e de ser totalmente bidirecional da conectividade. Em outras palavras, todos os nós do placement group podem falar com todos os outros nós do placement group na taxa completa de 10 Gbps e 25 agregados sem qualquer lentidão devido à assinatura excessiva.

A imagem a seguir mostra instâncias colocadas em um placement group de cluster.



Os placement groups de cluster são recomendados para aplicativos que se beneficiam de uma baixa latência de rede, de uma alta taxa de transferência de rede ou de ambas, e se a maior parte do tráfego de rede for entre instâncias no grupo. Para fornecer a menor latência possível e o melhor desempenho 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 \(p. 768\)](#).

Recomendamos que você execute o número de instâncias necessário no placement group em uma única solicitação de execução e que use o mesmo tipo de instância para todas as instâncias do 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.

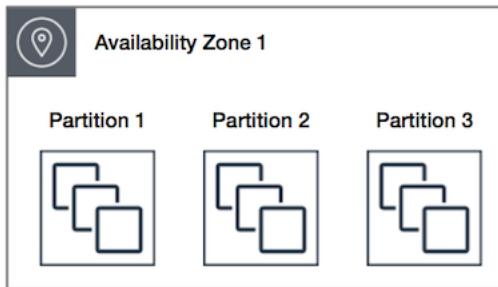
Se você interrompe uma instância em um placement group e depois a inicia novamente, ela ainda é executada no placement group. Contudo, ocorrerá uma falha na inicialização se não houver capacidade suficiente para a instância.

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. Reiniciar as instâncias pode migrá-las para o hardware que tenha capacidade para todas as instâncias solicitadas.

Placement groups de partição

Um placement group de partição é um grupo de instâncias distribuídas entre partições. Partições são agrupamentos lógicos de instâncias, nos quais as instâncias contidas não compartilham o mesmo hardware subjacente entre diferentes partições.

A imagem a seguir mostra sete instâncias em uma única zona de disponibilidade 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 o hardware subjacente com as instâncias nas outras partições, limitando o impacto da falha de hardware em apenas uma partição.



Placement groups de partição podem ser usados para distribuir a implantação de grandes cargas de trabalho distribuídas e replicadas, como HDFS, HBase e Cassandra, em hardware distinto para reduzir a probabilidade de falhas correlacionadas. 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.

Além disso, placement groups de partição oferecem visibilidade nas partições — você pode ver quais instâncias estão em quais partições. Você pode compartilhar essas informações com aplicativos atentos à topologia, como HDFS, HBase e Cassandra, que usam essas informações para tomar decisões inteligentes de replicação de dados para aumentar a durabilidade e a disponibilidade de dados.

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. Placement groups de partição também podem abranger várias zonas de disponibilidade na mesma região.

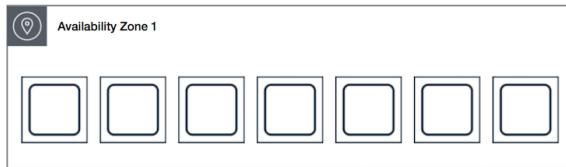
Se você iniciar ou executar uma instância em um placement group de partição e não houver uma quantidade suficiente de hardware exclusivo para atender à solicitação, ocorrerá uma falha. O Amazon EC2 disponibiliza mais hardware distinto ao longo do tempo, portanto, tente reenviar sua solicitação mais tarde.

No momento, placement groups de partição estão disponíveis somente pela API ou AWS CLI.

Placement groups de distribuição

Um placement group de distribuição é um grupo de instâncias que são colocadas em um hardware subjacente distinto.

A imagem a seguir mostra sete instâncias em uma única zona de disponibilidade que são colocadas em um placement group de distribuição. As instâncias não compartilham hardware subjacente umas com as outras.



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 o mesmo hardware subjacente. Os placement groups de distribuição concedem acesso ao hardware distinto e, portanto, são adequados para combinar diferentes tipos de instâncias ou executar instâncias ao longo do tempo.

Um placement group de distribuição pode abranger várias zonas de disponibilidade, e você pode ter no máximo sete instâncias em execução por zona de disponibilidade e por grupo.

Se você iniciar ou executar uma instância em um placement group de distribuição 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 que você especificar para um placement group deve ser exclusivo dentro da sua 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.
- As Instâncias reservadas 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.
- As instâncias com uma locação de host não podem ser executadas em placement groups.
- Para instâncias ativadas para a rede avançada, o tráfego entre instâncias dentro da mesma região da endereçada usando-se endereços IPv4 ou IPv6 pode usar até 5 Gbps para o tráfego de fluxo único e até 25 Gbps para o tráfego multifluxo. Um fluxo representa uma única conexão de rede ponto a ponto.

Regras e limitações do placement group de cluster

As seguintes regras se aplicam aos placement groups de cluster:

- A seguir, temos os únicos tipos de instância que você pode usar quando executar uma instância em um placement group de cluster:
 - Uso geral: A1, M4, M5, M5a e M5d
 - Computação otimizada: C3, C4, C5, C5d, C5n e cc2.8xlarge
 - Memória otimizada: cr1.8xlarge, R3, R4, R5, R5a, R5d, X1, X1e e z1d
 - Armazenamento otimizado: D2, H1, hs1.8xlarge, I2 e I3
 - Computação acelerada: F1, G2, G3, P2 e P3
- 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 aplicativos 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.
 - 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 instâncias são executadas em um placement group de partição, o Amazon EC2 tenta distribuir uniformemente as instâncias 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.
- Não há suporte para placement groups de partição em Hosts dedicados.
- No momento, placement groups de partição estão disponíveis somente pela API ou AWS CLI.

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. Isso não fornece garantias sobre a distribuição das instâncias entre os grupos, mas assegura que a distribuição para cada grupo seja feita de forma a limitar o impacto de determinadas categorias de falha.
- Não há suporte para placement groups de distribuição em Instâncias dedicadas ou Hosts dedicados.

Criação de um placement group

Você pode criar um placement group usando o console do Amazon EC2 ou a linha de comando.

Para criar um placement group (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 ele e escolha uma estratégia.

Note

Use a AWS CLI para especificar um placement group de partição.

4. Escolha Criar.

Para criar um placement group (linha de comando)

- [create-placement-group](#) (AWS CLI)
- [New-EC2PlacementGroup](#) (AWS Tools para Windows PowerShell)

Para criar um placement group de partição (AWS CLI)

- Use o comando [create-placement-group](#) e especifique o parâmetro `--strategy` com o valor `partition` e o parâmetro `--partition-count`. 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
```

Execução de instâncias em um placement group

Você pode criar uma AMI especificamente para as instâncias a serem executadas em um placement group. Para fazer isso, execute uma instância e instale o software e os aplicativos necessários nela. Em seguida, crie uma AMI a partir da instância. Para obter mais informações, consulte [Criação de uma AMI do Linux com Amazon EBS \(p. 111\)](#).

Para executar instâncias em um placement group (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 Amazon Machine Image (AMI), selecione uma AMI. Para selecionar uma AMI que você criou, escolha My AMIs.
 - Na página Choose an Instance Type, selecione um tipo de instância que possa ser executado em um placement group.
 - Na página Configure Instance Details, insira o número total de instâncias que você precisará nesse placement group, pois talvez você não possa adicionar instâncias ao placement group mais tarde.
 - Na página Configure Instance Details, selecione o placement group que você criou em Placement group. Se você não vir a lista Placement group nessa página, verifique se selecionou um tipo de

instância que pode ser executado em um placement group, pois essa opção não estará disponível de outra forma.

Para executar instâncias em um placement group (linha de comando)

1. Crie uma AMI para suas instâncias usando um dos seguintes comandos:
 - [create-image](#) (AWS CLI)
 - [New-EC2Image](#) (AWS Tools para Windows PowerShell)
2. Execute instâncias em seu placement group usando uma das seguintes opções:
 - `--placement` com [run-instances](#) (AWS CLI)
 - `-PlacementGroup` com [New-EC2Instance](#) (AWS Tools para Windows PowerShell)

Para executar instâncias em uma partição específica de um placement group de partição (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"
```

Descrever instâncias em um placement group

Você pode visualizar informações de posicionamento de suas instâncias usando a linha de comando ou o console do Amazon EC2. O placement group pode ser visualizado usando o console. No momento, o número da partição para instâncias em um placement group de partição pode ser visualizado somente usando a API ou AWS CLI.

Para visualizar o placement group de uma instância (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 Placement group. Se a instância não estiver em um placement group, o campo estará vazio. Caso contrário, o nome do placement group será exibido.

Para visualizar o número da partição para uma instância em um placement group de partição (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"
    }
```

Para filtrar instâncias para um placement group de partição e número de partição específicos (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"
        }
    }
],
```

Como alterar o placement group de uma instância

Você pode mover uma instância existente para um placement group, mover uma instância de um placement group para outro ou remover uma instância de um placement group. Antes de começar, a instância deve estar no estado `stopped`.

Você pode alterar o placement group para uma instância usando a linha de comando ou o AWS SDK.

Para mover uma instância para um placement group (linha de comando)

1. Pare a instância usando um dos seguintes comandos:

- [stop-instances](#) (AWS CLI)
- [Stop-EC2Instance](#) (AWS Tools para Windows PowerShell)

2. Use o comando [modify-instance-placement](#) (AWS CLI) 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
```

Você também pode usar o comando [Edit-EC2InstancePlacement](#) (AWS Tools para Windows PowerShell).

3. Reinicie a instância usando um dos seguintes comandos:
 - [start-instances](#) (AWS CLI)
 - [Start-EC2Instance](#) (AWS Tools para Windows PowerShell)

Para remover uma instância de um placement group (linha de comando)

1. Pare a instância usando um dos seguintes comandos:
 - [stop-instances](#) (AWS CLI)
 - [Stop-EC2Instance](#) (AWS Tools para Windows PowerShell)
2. Use o comando [modify-instance-placement](#) (AWS CLI) e especifique uma string vazia para o nome do grupo.

```
aws ec2 modify-instance-placement --instance-id i-0123a456700123456 --group-name ""
```

Você também pode usar o comando [Edit-EC2InstancePlacement](#) (AWS Tools para Windows PowerShell).

3. Reinicie a instância usando um dos seguintes comandos:
 - [start-instances](#) (AWS CLI)
 - [Start-EC2Instance](#) (AWS Tools para Windows PowerShell)

Exclusão de um placement group

Se precisar substituir um placement group ou se não precisar mais dele, você poderá excluí-lo. Para excluir o placement group, você deve encerrar todas as instâncias executadas no placement group ou movê-las para outro placement group.

Para encerrar ou mover instâncias e excluir um placement group (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 e encerre todas as instâncias no placement group. Você pode ver se a instância está em um placement group antes de encerrá-la verificando o valor de Placement Group no painel Details.

Você também pode seguir as etapas em [Como alterar o placement group de uma instância \(p. 799\)](#) para mover as instâncias para outro placement group.

4. No painel de navegação, escolha Placement Groups.
5. Selecione o placement group e escolha Delete Placement Group.
6. Quando a confirmação for solicitada, escolha Excluir.

Para encerrar instâncias e excluir um placement group (linha de comando)

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

- `terminate-instances` e `delete-placement-group` (AWS CLI)
- `Remove-EC2Instance` e `Remove-EC2PlacementGroup` (AWS Tools para Windows PowerShell)

Unidade de transmissão máxima (MTU) de rede para sua instância do EC2

A unidade de transmissão máxima (MTU) de uma conexão de rede é o tamanho, em bytes, do maior pacote permitível que pode ser passado pela conexão. Quanto maior a MTU de uma conexão, mais dados podem ser passados em um único pacote. Os pacotes de ethernet consistem no quadro, ou nos dados em si que você envia, e nas informações de overhead de rede que o cercam.

Os quadros de ethernet podem vir em diferentes formatos, sendo o mais comum o Ethernet v2 padrão. Ele é compatível com 1500 MTU, que é o maior tamanho de pacote de Ethernet sobre a 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.

Tópicos

- [Frames jumbo \(9001 MTU\) \(p. 801\)](#)
- [Path MTU Discovery \(p. 802\)](#)
- [Verifique o MTU do caminho entre dois hosts \(p. 802\)](#)
- [Verificar e definir o MTU na instância do Linux \(p. 803\)](#)
- [Solução de problemas \(p. 803\)](#)

Frames jumbo (9001 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. Contudo, fora de uma determinada região da AWS (EC2-Classic), uma única VPC ou uma conexão de pares de VPC, você experimentará um caminho máximo de 1500 MTU. Conexões VPN e tráfego enviados por um gateway de internet estão limitados a 1500 MTU. 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 cuidadosamente para o tráfego voltado para internet ou qualquer tráfego que sai 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 [Placement groups \(p. 793\)](#).

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 [Configuração de MTU de rede](#) no Guia do usuário do AWS Direct Connect.

As instâncias a seguir oferecem suporte a frames jumbo:

- Uso geral: A1, M3, M4, M5, M5a, M5d, T2 e T3
- Computação otimizada: C3, C4, C5, C5d, C5n e CC2
- Memória otimizada: CR1, R3, R4, R5, R5a, R5d, X1 e z1d
- Armazenamento otimizado: D2, H1, HS1, I2 e I3
- Computação acelerada: F1, G2, G3, P2 e P3
- Bare metal: i3.metal, u-6tb1.metal, u-9tb1.metal, and u-12tb1.metal

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 recepção. Se um host enviar um pacote que seja maior que a MTU do host de recebimento ou que seja maior que a MTU de um dispositivo ao longo do caminho, o host ou dispositivo de recebimento retornará a seguinte mensagem ICMP: **Destination Unreachable: Fragmentation Needed and Don't Fragment was Set** (Tipo 3, Código 4). Isso quando o host original a ajustar o MTU até que o pacote possa ser transmitido.

Por padrão, os security groups não permitem nenhum tráfego ICMP de entrada. Para garantir que sua instância possa receber essa mensagem e o pacote não tenha sido derrubado, adicione uma Regra de ICMP personalizada com o protocolo Destino inacessível para as regras do security group de entrada para sua instância. Para obter mais informações, consulte [Regras do Path MTU Discovery \(p. 638\)](#).

Important

Alterar o security group da sua instância para permitir Path MTU Discovery não garante que os frames jumbo não serão derrubados por alguns roteadores. Um gateway de Internet na sua VPC encaminhará somente pacotes até 1500 bytes. São recomendados 1500 pacotes de MTU para o tráfego de Internet.

Verifique 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 `iputils` 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
```

Resumo: 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. Talvez você queira usar frames jumbo para tráfego de rede na sua VPC ou usar quadros padrão para o tráfego de 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
```

- Para Amazon Linux, adicione as linhas a seguir ao seu arquivo /etc/dhcp/dhclient-eth0.conf.

```
interface "eth0" {
    supersede interface-mtu 1500;
}
```

- Para Ubuntu, adicione a linha a seguir para /etc/network/interfaces.d/eth0.cfg.

```
post-up /sbin/ifconfig eth0 mtu 1500
```

- Para outras distribuições de Linux, consulte a documentação específica.

3. (Opcional) Reinicialize sua instância e verifique se a configuração de MTU está correta.

Solução de problemas

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

Virtual Private Clouds

Amazon Virtual Private Cloud (Amazon VPC) permite que definir uma rede virtual em sua própria área isolada logicamente dentro da nuvem da AWS, conhecida como uma virtual private cloud (VPC). Inicie os recursos da Amazon EC2, como as instâncias, nas sub-redes da VPC. Seu 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 tenha suporte para a plataforma EC2-Classic em algumas regiões. Se você criou sua conta da AWS depois de 04/12/2013, ela não será compatível com EC2-Classic e os recursos deverão ser iniciados em uma VPC. Para obter mais informações, consulte [EC2-Classic \(p. 804\)](#).

Documentação do Amazon VPC

Para obter mais informações sobre uma Amazon VPC, consulte a seguinte documentação.

Guia	Descrição
Guia do usuário da Amazon VPC	Descreve os principais conceitos e disponibiliza instruções para uso dos recursos do Amazon VPC.
Amazon VPC Peering Guide	Descreve as conexões pares da VPC e disponibiliza instruções para usá-las.
Guia de administrador de rede do Amazon VPC	Ajuda os administradores de rede a configurar gateways do cliente.

EC2-Classic

Com EC2-Classic, suas instâncias executadas em uma única rede simples que você compartilha com outros clientes. Com Amazon VPC, suas instâncias executadas em uma nuvem privada virtual (VPC) que é isolada logicamente para sua conta da AWS.

A plataforma EC2-Classic foi introduzida na versão original do Amazon EC2. Se você criou sua conta da AWS depois de 04/12/2013, ela não será compatível com 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.

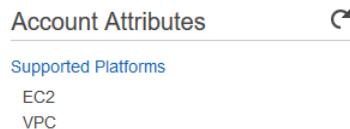
Detecção de plataformas com suporte

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 EC2-Classic

O painel exibe o seguinte em Account Attributes (Atribuições da conta) para indicar que a conta oferece suporte à plataforma EC2-Classic e a VPCs nessa região, mas a região não tem uma VPC padrão.



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"
                }
            ]
        }
    ]
}
```

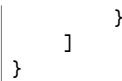
Contas que precisam de uma VPC

O painel exibe o seguinte em Account Attributes (Atribuições da conta) para indicar que a conta requer uma VPC para executar instâncias nessa região, não é compatível com a plataforma EC2-Classic nessa região, e a região tem uma VPC padrão com o identificador `vpc-1a2b3c4d`.



A saída do comando `describe-account-attributes` inclui somente o valor VPC do atributo `supported-platforms`.

```
aws ec2 describe-account-attributes --attribute-names supported-platforms
{
    "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 SDK da AWS para executar uma instância somente de VPC. Para obter mais informações, consulte [Criar uma Virtual Private Cloud \(VPC\) \(p. 26\)](#).
- 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 [Segurança em 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 [Migração de uma Instância do Linux no EC2-Classic para uma Instância do Linux em uma VPC \(p. 826\)](#).

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)	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	Por padrão, a instância não recebe um endereço IPv4 público, a menos que você especifique o contrário durante a execução ou

Característica	EC2-Classic	VPC padrão	VPC não padrão
públicos da Amazon)		especifique o contrário durante a execução ou modifique o atributo de endereço IPv4 público da sub-rede.	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.
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 security groups que pertencem a outras contas da AWS.	Um grupo de segurança só pode consultar security groups de sua VPC.	Um grupo de segurança só pode consultar security groups de sua VPC.

Característica	EC2-Classic	VPC padrão	VPC não padrão
Associação a grupos de segurança	<p>Você pode atribuir um número ilimitado de security groups a uma instância ao executá-la.</p> <p>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).</p>	<p>Você pode atribuir até 5 security groups a uma instância.</p> <p>Você pode atribuir security groups à sua instância ao executá-la e durante sua execução.</p>	<p>Você pode atribuir até 5 security groups a uma instância.</p> <p>Você pode atribuir security groups à sua instância ao executá-la e durante sua execução.</p>
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.

Security groups 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 security

group 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 security groups em cada região para cada conta. Você pode associar uma instância a até 500 security groups e adicionar até 100 regras a um security group.

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 Elastic IP

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.

Como 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 e reassociá-lo a outra instância \(p. 745\)](#).

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 [Límite de endereços IP elásticos \(p. 747\)](#).

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 [Acessando o Amazon EC2 \(p. 3\)](#).

- [move-address-to-vpc](#) (AWS CLI)
- [Move-EC2AddressToVpc](#) (AWS Tools para 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 [Acessando o Amazon EC2 \(p. 3\)](#).

- [restore-address-to-classic](#) (AWS CLI)
- [Restore-EC2AddressToClassic](#) (AWS Tools para 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 [Acessando o Amazon EC2 \(p. 3\)](#).

- [describe-moving-addresses](#) (AWS CLI)
- [Get-EC2Address](#) (AWS Tools para Windows PowerShell)

Compartilhamento e acesso a recursos entre o 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 \(p. 812\)](#).

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 [Migração de uma Instância do Linux no EC2-Classic para uma Instância do Linux em uma VPC \(p. 826\)](#).

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 Como migrar um endereço IP elástico do EC2-Classic (p. 810) .
Instância	Uma instância do EC2-Classic pode se comunicar com instâncias em uma VPC usando endereços

Recurso	Observações
	IPv4 públicos ou usar o ClassicLink para habilitar a comunicação por endereços IPv4 privados. Não é possível migrar uma instância do EC2-Classic para uma VPC. Contudo, é possível migrar seu aplicativo de uma instância na EC2-Classic para uma instância em uma VPC. Para obter mais informações, consulte Migração de uma Instância do Linux no EC2-Classic para uma Instância do Linux em uma VPC (p. 826) .
Par de chaves	
Load balancer	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. 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.
Grupo de posicionamento	
Instância reservada	Você pode alterar a plataforma de rede para Instâncias reservadas do EC2-Classic para uma VPC. Para obter mais informações, consulte Modificar Instâncias reservadas (p. 278) .
Grupo de segurança	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. 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 Criar um grupo de segurança (p. 630) .
Snapshot	

Os seguintes recursos não podem ser compartilhados nem movidos entre o EC2-Classic e uma VPC:

- Instâncias spot

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 a uma instância do EC2-Classic, permitirá a comunicação entre a instância do EC2-Classic e as instâncias na sua VPC usando endereços IPv4

privados. O ClassicLink remove a necessidade de usar endereços IPv4 públicos ou endereços IP elásticos para permitir a comunicação entre as instâncias nessas 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 [Migração de uma Instância do Linux no EC2-Classic para uma Instância do Linux em uma VPC \(p. 826\)](#).

Não há cobrança adicional pelo uso do ClassicLink. Aplicam-se as cobranças padrão pela transferência de dados e pelo uso de instâncias.

Tópicos

- [Noções básicas do ClassicLink \(p. 813\)](#)
- [Limitações do ClassicLink \(p. 816\)](#)
- [Trabalho com ClassicLink \(p. 816\)](#)
- [Exemplos de políticas do IAM para ClassicLink \(p. 820\)](#)
- [Visão geral sobre API e CLI \(p. 822\)](#)
- [Exemplo: Configuração do security group do ClassicLink para um aplicativo web de três níveis \(p. 824\)](#)

Noções básicas do 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. Após ter habilitado para a VPC para ClassicLink, você pode então vincular qualquer instância do EC2-Classic na mesma região da sua conta para 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.

Note

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 [Visualização das suas VPCs habilitadas para ClassicLink e instâncias do EC2-Classic vinculadas \(p. 818\)](#).

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 [Habilitação do suporte a DNS do ClassicLink \(p. 819\)](#).

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).

Controle do uso do 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 [IAM Políticas do Amazon EC2 \(p. 643\)](#).

Para obter mais informações sobre as políticas para trabalhar com ClassicLink, consulte o exemplo a seguir: [Exemplos de políticas do IAM para ClassicLink \(p. 820\)](#).

Security groups 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 security group do ClassicLink para um aplicativo web de três níveis \(p. 824\)](#).

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.

Habilitação de 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 está 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 mais informações, consulte o [Amazon VPC Peering Guide](#).
- 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 \(p. 815\)](#).
- As VPCs configuradas para locação de hardware dedicada não podem ser habilitadas para ClassicLink. Contate o suporte da AWS 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 AWS 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.

Trabalho 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

- [Habilitação de uma VPC para ClassicLink \(p. 817\)](#)
- [Vínculo de uma instância a VPC \(p. 817\)](#)
- [Criação de uma VPC com ClassicLink habilitado \(p. 818\)](#)
- [Vínculo de uma instância do EC2-Classic a uma VPC na execução \(p. 818\)](#)
- [Visualização das suas VPCs habilitadas para ClassicLink e instâncias do EC2-Classic vinculadas \(p. 818\)](#)
- [Habilitação do suporte a DNS do ClassicLink \(p. 819\)](#)
- [Desabilitar o suporte a DNS do ClassicLink \(p. 819\)](#)
- [Desvinculação de uma instância do EC2-Classic de uma VPC \(p. 819\)](#)
- [Desabilitação do ClassicLink de uma VPC \(p. 820\)](#)

Habilitação de uma 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 \(p. 815\)](#).

Para habilitar a VPC para ClassicLink

1. Abra o console de Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, escolha Your VPCs (Suas VPCs).
3. Escolha a VPC e, em seguida, escolha Actions (Ações), Enable (Habilitar) ClassicLink.
4. Na caixa de diálogo de confirmação, escolha Yes, Enable.

Vínculo de uma instância a VPC

Depois de habilitar uma VPC para ClassicLink, você pode vincular uma instância do EC2-Classic a ela.

Note

Você só pode vincular uma instância em execução do EC2-Classic a uma VPC. Você não pode vincular uma instância que está no estado stopped.

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 a instância em execução do EC2-Classic, escolha Actions (Ações), ClassicLink e Link to VPC (Vincular à VPC). Selecione mais de uma instância para vincular à mesma VPC.
4. Na caixa de diálogo exibida, selecione uma VPC na lista. São exibidas somente as VPCs que foram habilitadas para ClassicLink.
5. Selecione um ou mais dos security groups da VPC para associar à sua instância. Depois de concluir, escolha Link to VPC.

Criação de 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 de Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel do Amazon VPC, escolha Start VPC Wizard (Iniciar assistente de 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.

Vínculo de uma instância do EC2-Classic 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 escolha um tipo de instância. Na página Configure Instance Details (Configurar detalhes da instância), selecione Launch into EC2-Classic (Executar no EC2-Classic) na lista Network (Rede).

Note

Alguns tipos de instância, como tipos de instância T2, só podem ser executados em uma VPC. Selecione um tipo de instância que possa ser executado no EC2-Classic.

4. Na seção Link to VPC (ClassicLink) (Vincular à VPC (ClassicLink)), selecione uma VPC em Link to VPC (Vincular a uma VPC). Serão exibidas somente VPCs habilitadas para ClassicLink. Selecione os security groups da VPC a ser associada à instância. Preencha as outras opções de configuração na página e conclua o restante das etapas do assistente para executar sua instância. Para obter mais informações sobre o uso do assistente de execução, consulte [Execução da sua instância a partir de uma AMI \(p. 391\)](#).

Visualização das suas VPCs habilitadas para ClassicLink e instâncias do EC2-Classic 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 de Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, escolha Your VPCs (Suas VPCs).
3. Selecione uma VPC, e na guia Summary (Resumo), procure o campo ClassicLink. O valor Enabled (Habilitado) indica que a VPC está habilitada para o ClassicLink.
4. Você também pode procurar pela coluna ClassicLink e exibir o valor exibido para cada VPC (Enabled (Habilitado) ou Disabled (Desabilitado)). Se a coluna não estiver visível, escolha Edit Table Columns (Editar colunas da tabela) (o ícone de engrenagem), selecione o atributo ClassicLink e escolha Close (Fechar).

Para exibir as instâncias do EC2-Classic vinculadas

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 do EC2-Classic e, na guia Description (Descrição), procure pelo campo ClassicLink. Se a instância estiver vinculada à VPC, o campo exibirá o ID da VPC à qual a instância está vinculada. Se a instância não estiver vinculada a nenhuma VPC, o campo exibirá Unlinked (Não vinculada).
4. Como alternativa, você pode filtrar suas instâncias exibir somente as instâncias do EC2-Classic vinculadas para uma VPC ou security group específicos. Na barra de pesquisa, comece a digitar ClassicLink, selecione o atributo de recurso ClassicLink relevante e selecione um ID do grupo de segurança ou da VPC.

Habilitação do 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 de Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, escolha Your VPCs (Suas VPCs).
3. Selecione sua VPC e escolha Actions (Ações), Edit ClassicLink DNS Support (Editar suporte a DNS do ClassicLink).
4. Escolha Yes (Sim) para habilitar o suporte a DNS do ClassicLink e escolha Save (Salvar).

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 de Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, escolha Your VPCs (Suas VPCs).
3. Selecione sua VPC e escolha Actions (Ações), Edit ClassicLink DNS Support (Editar suporte a DNS do ClassicLink).
4. Escolha No (Não) para desabilitar o suporte a DNS do ClassicLink e escolha Save (Salvar).

Desvinculação de uma instância do EC2-Classic 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.

Note

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, selecione Instâncias e selecione sua instância.
3. Na lista Ações, selecione ClassicLink, Desvincular instância. Selecione mais de uma instância para desvincular da mesma VPC.
4. Selecione Yes (Sim) na caixa de diálogo de confirmação.

Desabilitação do ClassicLink de 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 de Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, escolha Your VPCs (Suas VPCs).
3. Selecione sua VPC, escolha Actions (Ações), Disable (Desabilitar) ClassicLink.
4. Na caixa de diálogo de confirmação, escolha Yes, Disable (Sim, desabilitar).

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 \(p. 820\)](#)
- [Habilitar e desabilitar uma VPC para o ClassicLink \(p. 821\)](#)
- [Vincular instâncias \(p. 821\)](#)
- [Desvincular instâncias \(p. 822\)](#)

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"  
        ]  
    }]  
}
```

```
        "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 'purpose=classiclink' específica. Os usuários não podem habilitar ou desabilitar nenhuma outra VPC para o ClassicLink.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:*VpcClassicLink",
            "Resource": "arn:aws:ec2:region:account:vpc/*",
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/purpose": "classiclink"
                }
            }
        }
    ]
}
```

Vincular instâncias

A política a seguir concede aos usuários permissões para vincular instâncias a uma VPC somente se a instância for um tipo de instância m3.large. A segunda declaração permite que os usuários usem a VPC e os recursos do security group que são necessários para vincular uma instância a uma VPC.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:AttachClassicLinkVpc",
            "Resource": "arn:aws:ec2:region:account:instance/*",
            "Condition": {
                "StringEquals": {
                    "ec2:InstanceType": "m3.large"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "ec2:AttachClassicLinkVpc",
            "Resource": [
                "arn:aws:ec2:region:account:vpc/*",
                "arn:aws:ec2:region:account:security-group/*"
            ]
        }
    ]
}
```

A política a seguir concede aos usuários permissões para vincular instâncias somente a uma VPC específica (vpc-1a2b3c4d) e associar somente security groups específicos da VPC à instância (sg-1122aabb e sg-aabb2233). Os usuários não podem vincular uma instância a nenhuma outra

VPC e não podem especificar nenhum outro security group da VPC para associação com a instância na solicitação.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": "ec2:AttachClassicLinkVpc",  
            "Resource": [  
                "arn:aws:ec2:region:account:vpc/vpc-1a2b3c4d",  
                "arn:aws:ec2:region:account:instance/*",  
                "arn:aws:ec2:region:account:security-group/sg-1122aabb",  
                "arn:aws:ec2:region:account:security-group/sg-aabb2233"  
            ]  
        }  
    ]  
}
```

Desvincular instâncias

O seguinte concede permissão aos usuários para desvincular qualquer instância do EC2-Classic vinculada de uma VPC, mas somente se a instância tiver a tag "unlink=true". A segunda instrução concede aos usuários permissões para usar o recurso da VPC, que é necessário para desvincular uma instância de uma VPC.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": "ec2:DetachClassicLinkVpc",  
            "Resource": [  
                "arn:aws:ec2:region:account:instance/*"  
            ],  
            "Condition": {  
                "StringEquals": {  
                    "ec2:ResourceTag/unlink": "true"  
                }  
            }  
        },  
        {  
            "Effect": "Allow",  
            "Action": "ec2:DetachClassicLinkVpc",  
            "Resource": [  
                "arn:aws:ec2:region:account:vpc/*"  
            ]  
        }  
    ]  
}
```

Visão geral sobre API e CLI

Você pode executar as tarefas descritas nesta página usando a linha de comando ou uma API de consulta. Para obter mais informações sobre as interfaces de linha de comando e sobre a lista de ações de API disponíveis, consulte [Acessando o Amazon EC2 \(p. 3\)](#).

Habilitar VPC para ClassicLink

- [enable-vpc-classic-link](#) (AWS CLI)
- [Enable-EC2VpcClassicLink](#) (AWS Tools para Windows PowerShell)
- [EnableVpcClassicLink](#) (API de consulta do Amazon EC2)

Vincular (associar) uma instância do EC2-Classic a uma VPC

- [attach-classic-link-vpc](#) (AWS CLI)
- [Add-EC2ClassicLinkVpc](#) (AWS Tools para Windows PowerShell)
- [AttachClassicLinkVpc](#) (API de consulta do Amazon EC2)

Desvincular (separar) uma instância do EC2-Classic de uma VPC

- [detach-classic-link-vpc](#) (AWS CLI)
- [Dismount-EC2ClassicLinkVpc](#) (AWS Tools para Windows PowerShell)
- [DetachClassicLinkVpc](#) (API de consulta do Amazon EC2)

Desabilitar ClassicLink para uma VPC

- [disable-vpc-classic-link](#) (AWS CLI)
- [Disable-EC2VpcClassicLink](#) (AWS Tools para Windows PowerShell)
- [DisableVpcClassicLink](#) (API de consulta do Amazon EC2)

Descrever o status do ClassicLink das VPCs

- [describe-vpc-classic-link](#) (AWS CLI)
- [Get-EC2VpcClassicLink](#) (AWS Tools para Windows PowerShell)
- [DescribeVpcClassicLink](#) (API de consulta do Amazon EC2)

Descrever as instâncias do EC2-Classic vinculadas

- [describe-classic-link-instances](#) (AWS CLI)
- [Get-EC2ClassicLinkInstance](#) (AWS Tools para Windows PowerShell)
- [DescribeClassicLinkInstances](#) (API de consulta do Amazon EC2)

Habilitar uma conexão de emparelhamento de VPC para ClassicLink

- [modify-vpc-peering-connection-options](#) (AWS CLI)
- [Edit-EC2VpcPeeringConnectionOption](#) (AWS Tools para Windows PowerShell)
- [ModifyVpcPeeringConnectionOptions](#) (API de consulta do Amazon EC2)

Habilitar uma VPC para suporte a DNS do ClassicLink

- [enable-vpc-classic-link-dns-support](#) (AWS CLI)
- [Enable-EC2VpcClassicLinkDnsSupport](#) (AWS Tools para Windows PowerShell)
- [EnableVpcClassicLinkDnsSupport](#) (API de consulta do Amazon EC2)

Desabilitar uma VPC para suporte a DNS do ClassicLink

- [disable-vpc-classic-link-dns-support](#) (AWS CLI)
- [Disable-EC2VpcClassicLinkDnsSupport](#) (AWS Tools para Windows PowerShell)
- [DisableVpcClassicLinkDnsSupport](#) (API de consulta do Amazon EC2)

Descrever suporte a DNS do ClassicLink para VPCs

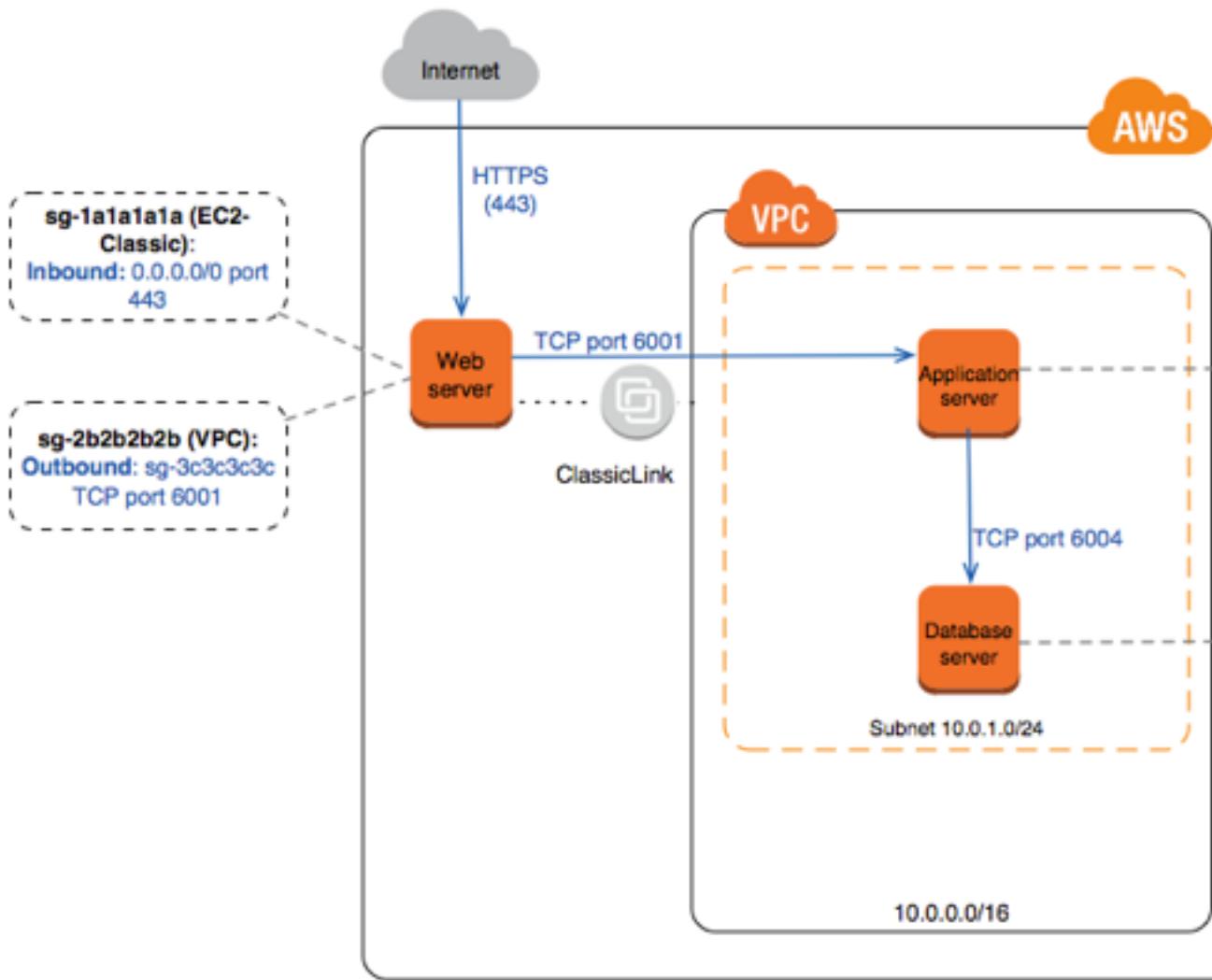
- [describe-vpc-classic-link-dns-support](#) (AWS CLI)
- [Get-EC2VpcClassicLinkDnsSupport](#) (AWS Tools para Windows PowerShell)
- [DescribeVpcClassicLinkDnsSupport](#) (API de consulta do Amazon EC2)

Exemplo: Configuração do security group do ClassicLink para um aplicativo web de três níveis

Neste exemplo, tiver um aplicativo com três instâncias: um servidor web voltado ao público, um servidor de aplicativos e um servidor de banco de dados. Seu servidor web aceita o tráfego HTTPS da Internet e se comunica com seu servidor de aplicativos pela porta TCP 6001. Seu servidor de aplicativos então se comunica com seu servidor de banco de dados pela porta TCP 6004. Você está no processo de migrar seu aplicativo inteiro para uma VPC na sua conta. Você tem migrado seu servidor de aplicativos 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 aplicativos (`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.



Security groups do seu 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 aplicativos.

A seguir estão as regras para grupos de segurança da EC2-Classic (**sg-1a1a1a1a**).

Inbound			
Source	Type	Port Range	Comments
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

Destination	Type	Port Range	Comments
sg-3c3c3c3c	TCP	6001	Permite tráfego de saída do seu servidor web para seu servidor de aplicativos na sua VPC (ou a alguma outra instância associada com sg-3c3c3c3c).

Security group para seu servidor de aplicativos (**sg-3c3c3c3c**)

A seguir estão as regras do security group para o security group da VPC associada com seu servidor de aplicativos.

Inbound			
Source	Type	Port Range	Comments
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 aplicativos.
Outbound			
Destination	Type	Port Range	Comments
sg-4d4d4d4d	TCP	6004	Permite tráfego de saída do seu servidor de aplicativos para o servidor do banco de dados (ou para qualquer outra instância associada com sg-4d4d4d4d).

Security group para seu 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			
Source	Type	Port Range	Comments
sg-3c3c3c3c	TCP	6004	Permite o tipo de tráfego especificado do seu servidor de aplicativos (ou qualquer outra instância associada com sg-3c3c3c3c) alcance seu servidor de banco de dados.

Migração de uma Instância do Linux no EC2-Classic para uma Instância do Linux em uma VPC

Caso você tenha criado sua conta da AWS antes de 4/12/2013, talvez tenha suporte para EC2-Classic em algumas regiões. 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 [Compartilhamento e acesso a recursos entre o EC2-Classic e uma VPC \(p. 811\)](#).

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.

Há duas formas de migrar para uma VPC. Você pode fazer uma migração completa ou uma migração incremental ao longo do tempo. O método escolhido depende do tamanho e da complexidade de seu aplicativo no EC2-Classic. Por exemplo, se seu aplicativo consistir em uma ou duas instâncias que executam um site estático e você puder arcar com um curto período de inatividade, poderá fazer a migração completa. Se você tiver um aplicativo de várias camadas com processos que não podem ser interrompidos, poderá fazer uma migração incremental usando ClassicLink. Isso permite que você transfira a funcionalidade de um componente de cada vez até que os aplicativos estejam sendo executados totalmente na VPC.

Se for necessário migrar uma instância Windows, consulte [Migração de uma instância Windows do EC2-Classic para uma VPC](#) no Guia do usuário do Amazon EC2 para instâncias do Windows.

Tópicos

- [Migração completa para uma VPC \(p. 827\)](#)
- [Migração incremental para uma VPC usando o ClassicLink \(p. 833\)](#)

Migração completa para uma VPC

Conclua as tarefas a seguir para migrar totalmente seu aplicativo do EC2-Classic para uma VPC.

Tarefas

- [Etapa 1: Criar uma VPC \(p. 827\)](#)
- [Etapa 2: Configurar o security group \(p. 828\)](#)
- [Etapa 3: Criar uma AMI da instância do EC2-Classic \(p. 828\)](#)
- [Etapa 4: Executar uma instância em sua VPC \(p. 829\)](#)
- [Exemplo: migração de um aplicativo web simples \(p. 831\)](#)

Etapa 1: Criar uma VPC

Para começar a usar uma VPC, verifique se há uma em sua conta. Você pode criar uma usando um destes métodos:

- Sua conta da AWS é fornecida com uma VPC padrão em cada região e está pronta para uso. As instâncias executadas são executados nessa VPC, por padrão, salvo especificação em contrário. Para obter mais informações sobre sua VPC padrão, consulte [VPC padrão e sub-redes](#). Use essa opção se preferir não configurar uma VPC por conta própria ou se não houver requisitos específicos para a configuração da VPC.
- Em sua conta da AWS existente, abra o console da Amazon VPC e use o assistente da VPC para criar uma nova VPC. Para obter mais informações, consulte [Cenários da Amazon VPC](#). Use essa opção se quiser configurar uma VPC rapidamente em sua conta existente do EC2-Classic usando um dos conjuntos de configurações disponíveis no assistente. Você especificará essa VPC sempre que executar uma instância.
- Em sua conta da AWS, abra o console da Amazon VPC e configure os componentes de uma VPC de acordo com seus requisitos. Para obter mais informações, consulte [VPC e sub-redes](#). Use essa opção se houver requisitos específicos para sua VPC, como um número específico de sub-redes. Você especificará essa VPC sempre que executar uma instância.

Etapa 2: Configurar o security group

Não é possível usar os mesmos security groups entre o EC2-Classic e uma VPC. 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 do EC2-Classic para um novo grupo de segurança da VPC.

Important

Somente é possível copiar as regras do security group para um novo security group na conta da AWS na mesma região. Se você tiver criado uma nova conta da AWS, não poderá usar esse método para copiar suas regras de security group existentes para a nova conta. Você precisará criar um novo security group e adicionar as regras por conta própria. Para obter mais informações sobre como criar um novo security group, consulte [Grupos de segurança do Amazon EC2 para instâncias do Linux \(p. 626\)](#).

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 sua instância do EC2-Classic e, em seguida, escolha Actions (Ações) e selecione Copy to new (Copiar para novo).
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 \(p. 626\)](#).

Note

Se tiver definido uma regra no security group do EC2-Classic que faça referência a outro security group, você não poderá usar a mesma regra em um security group da VPC. Modifique a regra para fazer referência a um security group na mesma VPC.

6. Escolha Criar.

Etapa 3: Criar uma AMI da instância do EC2-Classic

Uma AMI é um modelo para executar a instância. 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.

O método usado para criar a AMI depende do tipo de dispositivo raiz da instância e da plataforma de 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 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 oferece suporte ao tipo de virtualização que a AMI oferece. Se a AMI oferecer suporte à virtualização de

PV e você quiser usar um tipo de instância que ofereça suporte à virtualização de HVM, talvez seja necessário reinstalar o software em uma base da AMI de HVM. Para obter mais informações sobre virtualização de HVM e PV, consulte [Tipos de virtualização da AMI em Linux \(p. 94\)](#).

Tipo de dispositivo raiz da instância	Ação
EBS	Crie uma AMI baseada em EBS da instância. Para obter mais informações, consulte Criação de uma AMI do Linux com Amazon EBS (p. 111) .
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 Criação de uma AMI em Linux com armazenamento de instâncias (p. 115) .
Armazenamento de instâncias	Converta sua instância com armazenamento de instâncias em instâncias baseadas em EBS. Para obter mais informações, consulte Conversão de uma AMI com armazenamento de instâncias em uma AMI com Amazon EBS (p. 127) .

(Opcional) Armazene seus dados em volumes de 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 desconectadas 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 \(p. 841\)](#)
- [Criação de um volume do Amazon EBS \(p. 860\)](#)
- [Associação de um volume do Amazon EBS a uma instância \(p. 863\)](#)

Para fazer backup dos dados no volume de Amazon EBS, você pode gerar snapshots periódicos do volume. Se você precisar, poderá restaurar um volume de Amazon EBS do snapshot. Para obter mais informações sobre snapshots do Amazon EBS, consulte os seguintes tópicos:

- [Snapshots do Amazon EBS \(p. 896\)](#)
- [Criação de um snapshot do Amazon EBS \(p. 898\)](#)
- [Restauração de um volume do Amazon EBS a partir de um snapshot \(p. 861\)](#)

Etapa 4: Executar uma instância em sua VPC

Depois de criar AMIs, você pode executar uma instância em sua VPC. A instância terá os mesmos dados e configurações da instância do EC2-Classic existente.

Você pode iniciar sua instância em uma VPC que criou em sua conta existente ou em uma nova conta da AWS somente para VPC.

Usar a conta do EC2-Classic existente

Use o assistente de execução do Amazon EC2 para executar uma instância na VPC.

Para executar uma instância na VPC

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.

2. No painel, escolha Launch Instance.
3. Na página Choose an Amazon Machine Image, selecione a categoria My AMIs e selecione a AMI que você criou.
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 Configure Security Group.
6. Selecione Select an existing group e escolha o security group que você criou anteriormente. 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 [Execução de uma instância usando o assistente de execução de instância \(p. 391\)](#).

Usar sua nova conta somente para VPC

Para executar uma instância em sua nova conta da AWS, você terá primeiro que compartilhar a AMI que criou com sua nova conta. Depois, você pode usar o assistente de execução do Amazon EC2 para executar uma instância na VPC padrão.

Para compartilhar uma AMI com sua nova conta da AWS

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. Mude para a conta em que você criou a AMI.
3. No painel de navegação, selecione AMIs.
4. Na lista Filter, confirme se a opção Owned by me está selecionada e escolha sua AMI.
5. Na guia Permissions, escolha Edit. Insira o número de conta da sua nova conta da AWS, escolha Add Permission e selecione Save.

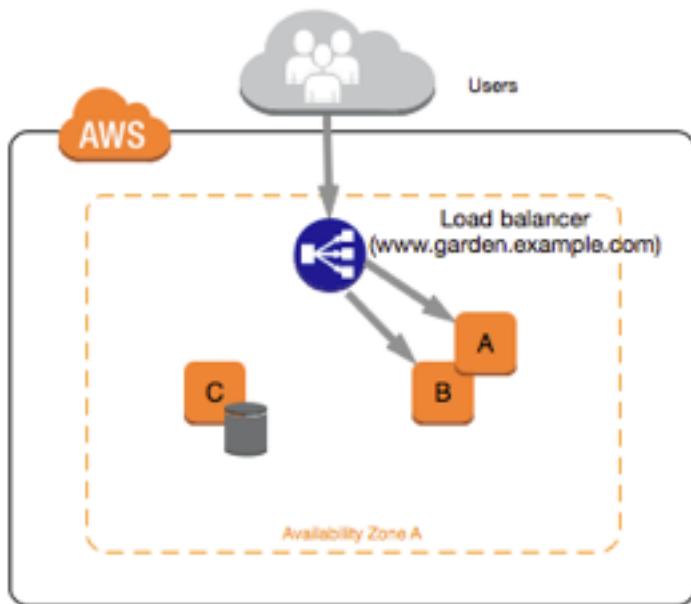
Para executar uma instância na VPC padrão

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. Mude para sua nova conta da AWS.
3. No painel de navegação, selecione AMIs.
4. Na lista Filter, selecione Private images. Selecione a AMI que você compartilhou de sua conta do EC2-Classic e escolha Launch (Iniciar).
5. Na página Choose an Instance Type, selecione o tipo de instância e escolha Next: Configure Instance Details.
6. Na página Configure Instance Details, a VPC padrão deve ser selecionada na lista Network. Configure todos os outros detalhes necessários e passe para as próximas páginas do assistente até chegar à página Configure Security Group.
7. Selecione Select an existing group e escolha o security group que você criou anteriormente. Escolha Review and Launch.
8. Reveja os detalhes da instância e selecione Launch para especificar um par de chaves e executar a instância.

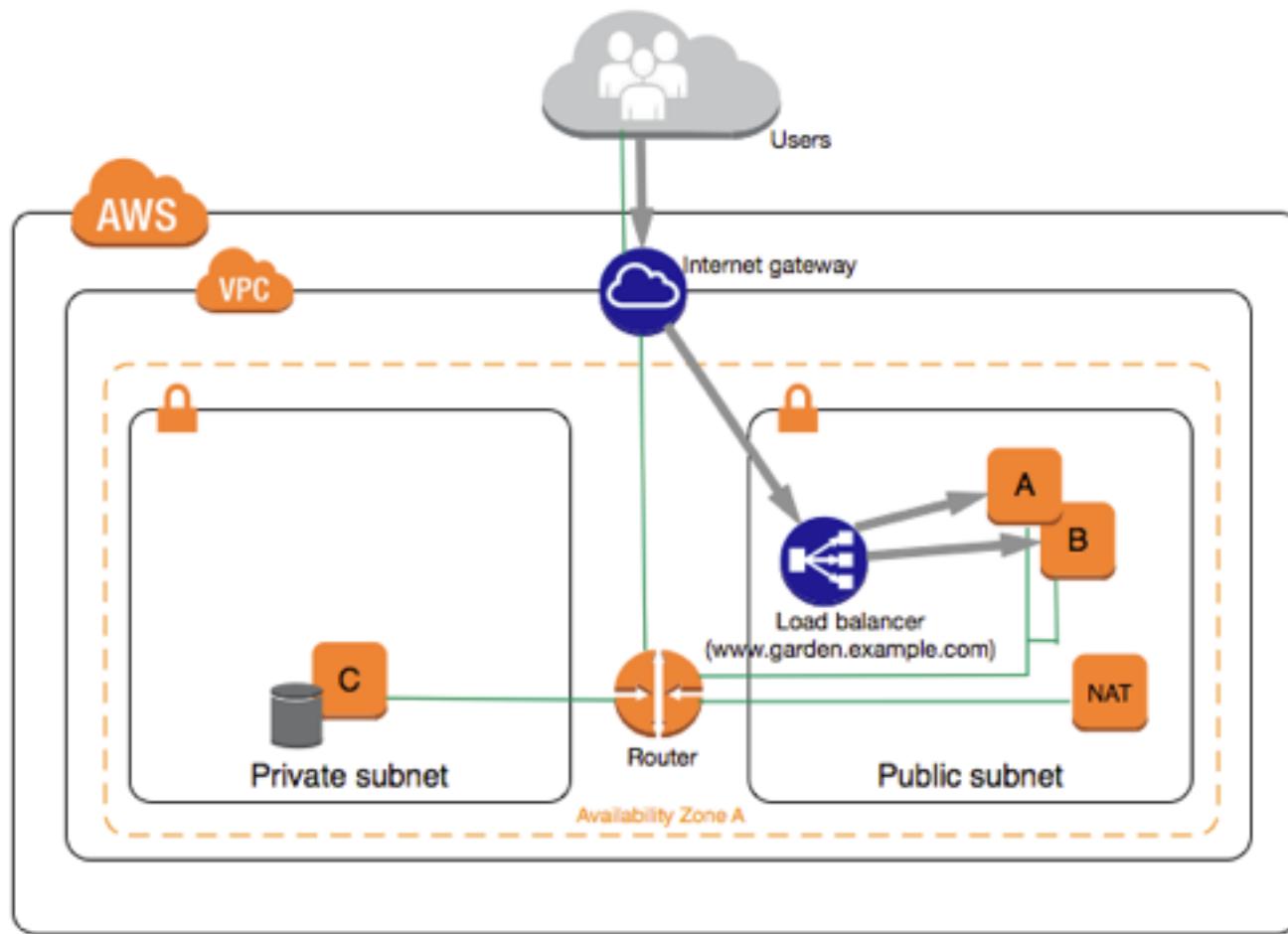
Para obter mais informações sobre os parâmetros que você pode configurar em cada etapa do assistente, consulte [Execução de uma instância usando o assistente de execução de instância \(p. 391\)](#).

Exemplo: migração de um aplicativo 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 seu aplicativo web voltado 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 load balancer.



A primeira parte da migração para uma VPC é decidir qual tipo de arquitetura da VPC será adequado a 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 através de um dispositivo de conversão de endereços de rede (NAT) na sub-rede pública. Talvez você queira configurar um dispositivo de 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 seu aplicativo 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 [Cenário 2: VPC com sub-redes públicas e privadas](#) no Guia do usuário da Amazon VPC.
- Criar AMIs de suas instâncias: crie AMIs de um dos servidores web e uma segunda AMI do servidor de banco de dados. Para obter mais informações, consulte [Etapa 3: Criar uma AMI da instância do EC2-Classic \(p. 828\)](#).
- 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 [Etapa 2: Configurar o security group \(p. 828\)](#).

Tip

Crie os security groups que são referenciados por outros security groups primeiro.

- Executar uma instância em sua VPC nova: execute servidores web de substituição em sua sub-rede pública e execute seu servidor de banco de dados de substituição em sua sub-rede privada. Para obter mais informações, consulte [Etapa 4: Executar uma instância em sua VPC \(p. 829\)](#).
- Configurar seu dispositivo de NAT: se você estiver usando uma instância NAT, deverá criar o security group para ela que permita o tráfego HTTP e HTTPS de sua sub-rede privada. Para mais informações,

consulte [Instâncias NAT](#). Se você estiver usando um gateway de NAT, o tráfego de sua sub-rede privada será permitido automaticamente.

- Configurar seu 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 para a AMI. Você pode ter de se conectar a seu novo servidor de banco de dados e atualizar os detalhes de configuração. Por exemplo, se você tiver configurado o banco de dados para conceder permissões completas de leitura, gravação e modificação aos servidores web no EC2-Classic, terá que 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 não pode 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 [Como migrar um endereço IP elástico do EC2-Classic \(p. 810\)](#).
- Criar um novo load balancer: para continuar usando o Elastic Load Balancing para balancear a carga do tráfego para suas instâncias, você deve compreender as diferentes maneiras de configurar seu load balancer na VPC. Para obter mais informações, consulte [Elastic Load Balancing na Amazon VPC](#).
- Atualizar seus registros DNS: após configurar seu load balancer em sua sub-rede pública, assegure-se de que seu `www.garden.example.com` domínio aponte para o novo load balancer. Para isso, você precisará atualizar os registros DNS e atualizar seu conjunto de registros de alias no Route 53. Para obter mais informações sobre como usar o Route 53, consulte [Conceitos básicos do Route 53](#).
- Desligar os recursos do EC2-Classic: após verificar se seu aplicativo 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. Encerre suas instâncias do EC2-Classic e libere seus endereços IP elásticos no EC2-Classic.

Migração incremental para uma VPC usando o ClassicLink

O recurso ClassicLink facilita o gerenciamento de uma migração incremental para uma VPC. ClassicLink permite vincular uma instância do EC2-Classic a uma VPC em sua conta na mesma região, permitindo que seus novos recursos da VPC se comuniquem com a instância do EC2-Classic usando endereços IPv4 privados. Então, você pode migrar a funcionalidade para a VPC dando um passo de cada vez. Este tópico fornece algumas etapas básicas para gerenciar uma migração incremental do EC2-Classic para uma VPC.

Para obter mais informações sobre ClassicLink, consulte [ClassicLink \(p. 812\)](#).

Tópicos

- [Etapa 1: Preparar a sequência de migração \(p. 834\)](#)
- [Etapa 2: Criar uma VPC \(p. 834\)](#)
- [Etapa 3: Habilitar sua VPC para o ClassicLink \(p. 834\)](#)
- [Etapa 4: Criar uma AMI de sua instância do EC2-Classic \(p. 834\)](#)
- [Etapa 5: Executar uma instância em sua VPC \(p. 835\)](#)

- [Etapa 6: Vincular as instâncias do EC2-Classic à VPC \(p. 836\)](#)
- [Etapa 7: Concluir a migração da VPC \(p. 836\)](#)

Etapa 1: Preparar a sequência de migração

Para usar o ClassicLink com eficácia, primeiro você deve identificar os componentes de seu aplicativo que devem ser migrados para a VPC e confirmar a ordem na qual essa funcionalidade será migrada.

Por exemplo, você tem um aplicativo que conta com um servidor web de apresentação, um servidor de banco de dados de back-end 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.

Etapa 2: Criar uma VPC

Para começar a usar uma VPC, verifique se há uma em sua conta. Você pode criar uma usando um destes métodos:

- Em sua conta da AWS existente, abra o console da Amazon VPC e use o assistente da VPC para criar uma nova VPC. Para obter mais informações, consulte [Cenários da Amazon VPC](#). Use essa opção se quiser configurar uma VPC rapidamente em sua conta existente do EC2-Classic usando um dos conjuntos de configurações disponíveis no assistente. Você especificará essa VPC sempre que executar uma instância.
- Em sua conta da AWS, abra o console da Amazon VPC e configure os componentes de uma VPC de acordo com seus requisitos. Para obter mais informações, consulte [VPC e sub-redes](#). Use essa opção se houver requisitos específicos para sua VPC, como um número específico de sub-redes. Você especificará essa VPC sempre que executar uma instância.

Etapa 3: Habilitar sua VPC para o ClassicLink

Depois de criar a VPC, você pode habilitá-la para o ClassicLink. Para obter mais informações sobre ClassicLink, consulte [ClassicLink \(p. 812\)](#).

Para habilitar a VPC para ClassicLink

1. Abra o console de Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, escolha Your VPCs (Suas VPCs).
3. Selecione sua VPC e escolha Enable ClassicLink na lista Actions.
4. Na caixa de diálogo de confirmação, escolha Yes, Enable.

Etapa 4: Criar uma AMI de sua instância do EC2-Classic

Uma AMI é um modelo para executar a instância. 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.

O método usado para criar a AMI depende do tipo de dispositivo raiz da instância e da plataforma de 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 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 oferece suporte ao tipo de virtualização que a AMI oferece. Se a AMI oferecer suporte à virtualização de PV e você quiser usar um tipo de instância que ofereça suporte à virtualização de HVM, talvez seja necessário reinstalar o software em uma base da AMI de HVM. Para obter mais informações sobre virtualização de HVM e PV, consulte [Tipos de virtualização da AMI em Linux \(p. 94\)](#).

Tipo de dispositivo raiz da instância	Ação
EBS	Crie uma AMI baseada em EBS da instância. Para obter mais informações, consulte Criação de uma AMI do Linux com Amazon EBS (p. 111) .
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 Criação de uma AMI em Linux com armazenamento de instâncias (p. 115) .
Armazenamento de instâncias	Converta sua instância com armazenamento de instâncias em uma instância baseada em EBS. Para obter mais informações, consulte Conversão de uma AMI com armazenamento de instâncias em uma AMI com Amazon EBS (p. 127) .

(Opcional) Armazene seus dados em volumes de 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 desconectadas 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 \(p. 841\)](#)
- [Criação de um volume do Amazon EBS \(p. 860\)](#)
- [Associação de um volume do Amazon EBS a uma instância \(p. 863\)](#)

Para fazer backup dos dados no volume de Amazon EBS, você pode gerar snapshots periódicos do volume. Se você precisar, poderá restaurar um volume de Amazon EBS do snapshot. Para obter mais informações sobre snapshots do Amazon EBS, consulte os seguintes tópicos:

- [Snapshots do Amazon EBS \(p. 896\)](#)
- [Criação de um snapshot do Amazon EBS \(p. 898\)](#)
- [Restauração de um volume do Amazon EBS a partir de um snapshot \(p. 861\)](#)

Etapa 5: Executar uma instância em sua VPC

A próxima etapa do processo de migração é executar instâncias em sua VPC para que você possa começar a transferir funcionalidades para elas. Você pode usar as AMIs que criou na etapa anterior para executar instâncias em sua VPC. As instâncias terão os mesmos dados e configurações das instâncias do EC2-Classic existentes.

Para executar uma instância em sua VPC usando a AMI personalizada

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel, escolha Launch Instance.
3. Na página Choose an Amazon Machine Image, selecione a categoria My AMIs e selecione a AMI que você criou.
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 Configure Security Group.
6. Selecione Select an existing group e escolha o security group que você criou anteriormente. 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 [Execução de uma instância usando o assistente de execução de instância \(p. 391\)](#).

Depois que você executar a instância e ela estiver no estado `running`, você poderá se conectar com ela e configurá-la conforme o necessário.

Etapa 6: Vincular as instâncias do EC2-Classic à VPC

Após você ter configurado suas instâncias e tornado a funcionalidade de seu aplicativo disponível na VPC, poderá usar o ClassicLink para permitir a comunicação privada de IP entre as novas instâncias da VPC e as instâncias do EC2-Classic.

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 a instância do EC2-Classic e escolha Actions (Ações), ClassicLink e Link to VPC (Vincular à VPC).

Note

Verifique se a instância está no estado `running`.

4. Na caixa de diálogo, selecione a VPC habilitada para o ClassicLink (somente VPCs habilitadas para o ClassicLink são exibidas).
5. Selecione um ou mais dos security groups da VPC para associar à sua instância. Depois de concluir, escolha Link to VPC.

Etapa 7: Concluir a migração da VPC

Dependendo do tamanho de seu aplicativo e da funcionalidade que deve ser migrada, repita as etapas 4 a 6 até transferir todos os componentes de seu aplicativo do EC2-Classic para a VPC.

Após habilitar a comunicação interna entre o EC2-Classic e as instâncias de VPC, você deverá atualizar seu aplicativo 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 seu aplicativo. 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. Você pode migrar seus endereços IP elásticos que estão em uso no momento na plataforma do EC2-Classic para a VPC. Para obter mais informações, consulte [Como migrar um endereço IP elástico do EC2-Classic \(p. 810\)](#).

Após concluir esta etapa e testar se o aplicativo está funcionando de sua VPC, você poderá encerrar as instâncias do EC2-Classic e desativar o ClassicLink para sua VPC. Você também pode limpar qualquer recurso do EC2-Classic que não seja mais necessário para evitar ser cobrado por eles. Por exemplo, você pode liberar endereços IP elásticos e excluir os volumes que estiverem associados às instâncias do EC2-Classic.

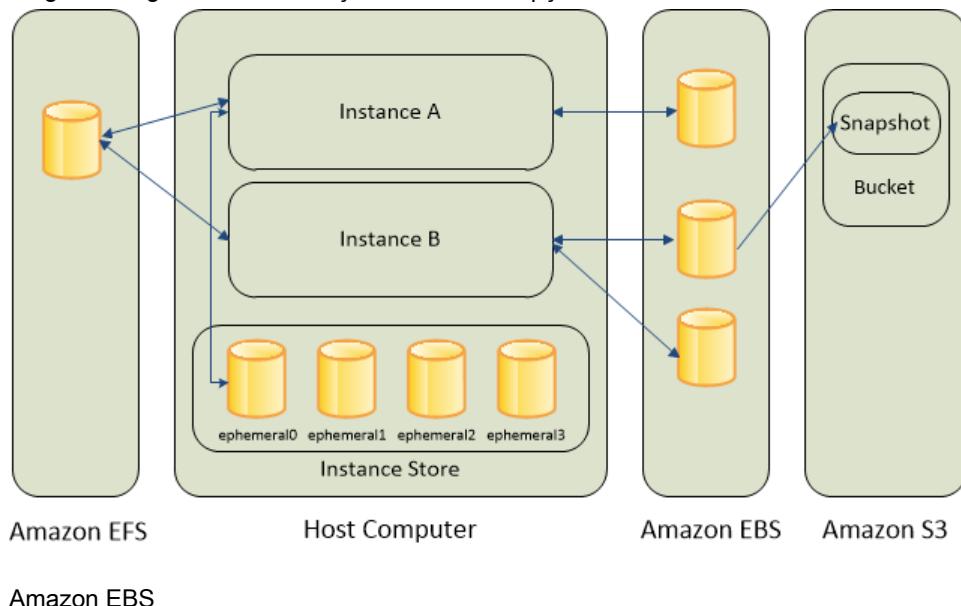
Armazenamento

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 desempenho 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 \(p. 839\)](#)
- [Armazenamento de instâncias do Amazon EC2 \(p. 958\)](#)
- [Amazon Elastic File System \(Amazon EFS\) \(p. 970\)](#)
- [Amazon Simple Storage Service \(Amazon S3\) \(p. 974\)](#)

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 [Amazon EBS Encryption \(p. 926\)](#).

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 \(p. 839\)](#).

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 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 \(p. 958\)](#).

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 cargas de trabalho e aplicativos em execução em várias instâncias. Para obter mais informações, consulte [Amazon Elastic File System \(Amazon EFS\) \(p. 970\)](#).

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 Amazon S3 para armazenar cópias de backup de seus dados e aplicativos. Amazon EC2 usa Amazon S3 para armazenar snapshots do EBS e AMIs com armazenamento de instâncias. Para obter mais informações, consulte [Amazon Simple Storage Service \(Amazon S3\) \(p. 974\)](#).

Como 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 [Mapeamento de dispositivos de blocos \(p. 979\)](#).

Você também pode anexar volumes do EBS a uma instância em execução. Para obter mais informações, consulte [Associação de um volume do Amazon EBS a uma instância \(p. 863\)](#).

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 são volumes de armazenamento altamente disponíveis e confiáveis que podem ser anexados a qualquer instância em execução na mesma zona de disponibilidade. Os volumes do EBS que estão anexados a uma instância do EC2 são expostos como volumes de armazenamento que persistem independentemente da vida útil da instância. 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 Projeção de custos da [página do Amazon Elastic Block Store](#).

O Amazon EBS é recomendado quando os dados devem ser rapidamente acessíveis e requer persistência no longo prazo. Os volumes do EBS são particularmente adequados ao uso como armazenamento principal para sistemas de arquivos, bancos de dados ou para todos os aplicativos que necessitem de atualizações granulares finas e acesso ao armazenamento em nível de bloco bruto e não formatado. O Amazon EBS é ideal para aplicativos no estilo de banco de dados que realizam leituras e gravações aleatórias, bem como para aplicativos com alta taxa de transferência que executam leituras e gravações longas e contínuas.

Para simplificar a criptografia de dados, você pode executar seus volumes do EBS como volumes criptografados. O Criptografia de Amazon EBS oferece uma solução de criptografia simples para os volumes do EBS sem a necessidade de criar, gerenciar e proteger sua própria infraestrutura de gerenciamento de chaves. 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, fornecendo criptografia de dados em trânsito entre as instâncias do EC2 e o armazenamento no EBS. Para obter mais informações, consulte [Amazon EBS Encryption \(p. 926\)](#).

O Criptografia de Amazon EBS usa chaves mestras do AWS Key Management Service (AWS KMS) para 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 mestre de cliente (CMK) criada separadamente usando o AWS Key Management Service. Criar sua própria CMK oferece maior flexibilidade ao definir controles de acesso, incluindo a capacidade de criar, ativar e desabilitar chaves para definir controles de acesso, além de auditar as chaves de criptografia que são específicas a aplicações individuais e usuários. Para obter mais informações, consulte o [AWS Key Management Service Developer Guide](#).

Você pode anexar vários volumes à mesma instância dentro dos limites especificados por sua conta da AWS. 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 o aumento deles, consulte [Solicitação para aumentar o limite de volumes do Amazon EBS](#).

Tópicos

- [Recursos do Amazon EBS \(p. 840\)](#)
- [Volumes do Amazon EBS \(p. 841\)](#)
- [Snapshots do Amazon EBS \(p. 896\)](#)
- [Amazon EBS – instâncias otimizadas \(p. 916\)](#)
- [Amazon EBS Encryption \(p. 926\)](#)
- [Amazon EBS e NVMe \(p. 929\)](#)
- [Desempenho do volume do Amazon EBS em instâncias do Linux \(p. 932\)](#)
- [Eventos do Amazon CloudWatch para Amazon EBS \(p. 950\)](#)

Recursos do Amazon EBS

- Você pode criar volumes do EBS Finalidade geral (SSD) (gp2), Provisioned IOPS SSD (io1), Disco rígido com throughput otimizado (st1) e Cold HDD (sc1) com até 16 TiB de tamanho. Você pode montar esses volumes como dispositivos em suas instâncias do Amazon EC2. É possível montar vários volumes a mesma instância, mas cada volume pode ser anexado a apenas uma instância por vez. Você pode alterar dinamicamente a configuração de um volume anexado a uma instância. Para obter mais informações, consulte [Criação de um volume do Amazon EBS \(p. 860\)](#).
- Com volumes Finalidade geral (SSD) (gp2), você pode esperar desempenho básico de 3 IOPS/GiB, com a capacidade de intermitência de 3.000 IOPS por longos períodos de tempo. Os volumes Gp2 são ideais para uma ampla gama de casos de uso, como volumes de inicialização, bancos de dados pequenos e médios e ambientes de desenvolvimento e teste. Os volumes Gp2 oferecem suporte a até 16,000 IOPS

e 250 MiB/s de taxa de transferência. Para obter mais informações, consulte [Volumes do Finalidade geral \(SSD\) \(gp2\) \(p. 847\)](#).

- Com volumes Provisioned IOPS SSD (io1), você pode provisionar um nível específico de desempenho de E/S. Os volumes io1 oferecem suporte a até 64,000 IOPS e 1,000 MB/s de taxa de transferência. Isso permite que você escala de forma previsível para dezenas de milhares de IOPS por instância do EC2. Para obter mais informações, consulte [Volumes do Provisioned IOPS SSD \(io1\) \(p. 850\)](#).
- Os volumes de Disco rígido com throughput otimizado (st1) fornecem armazenamento magnético de baixo custo que define o desempenho em termos de throughput, não IOPS. Com uma taxa de transferência de até 500 MiB/s, esse tipo de volume é ideal para cargas de trabalho grandes e sequenciais, como Amazon EMR, ETL, data warehouses e processamento de logs. Para obter mais informações, consulte [Volumes do Disco rígido com throughput otimizado \(st1\) \(p. 850\)](#).
- Os volumes de Cold HDD (sc1) fornecem armazenamento magnético de baixo custo que define o desempenho em termos de throughput, não IOPS. Com uma taxa de transferência de até 250 MiB/s, o sc1 é ideal para cargas de trabalho 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 armazenamento econômico. Para obter mais informações, consulte [Volumes do Cold HDD \(sc1\) \(p. 853\)](#).
- Os volumes do EBS se comportam como dispositivos de bloco brutos e não formatados. Você pode criar um sistema de arquivos sobre esses volumes ou utilizá-los de qualquer outra maneira que utilizaria um dispositivo de bloco (como um disco rígido). Para obter mais informações sobre como criar sistemas de arquivos e montar volumes, consulte [Disponibilização de um volume do Amazon EBS para uso no Linux \(p. 864\)](#).
- Você pode usar volumes do EBS criptografados para atender a uma ampla variedade de necessidades de criptografia dados em repouso para dados e aplicativos regulamentados/auditados. Para obter mais informações, consulte [Amazon EBS Encryption \(p. 926\)](#).
- 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 \(p. 896\)](#).
- Os volumes do EBS são criados em uma zona de disponibilidade específica e podem ser anexados a qualquer instância da 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 em outras regiões e então restaurá-los em novos volumes, facilitando o uso de várias regiões da AWS para expansão geográfica, a migração de datacenter e a recuperação de desastres. Para obter mais informações, consulte [Criação de um snapshot do Amazon EBS \(p. 898\)](#), [Restauração de um volume do Amazon EBS a partir de um snapshot \(p. 861\)](#) e [Cópia de um snapshot do Amazon EBS \(p. 902\)](#).
- Um grande repositório de snapshots de banco de dados públicos pode ser restaurado em volumes do EBS e facilmente integrado a aplicativos baseados na nuvem da AWS. Para obter mais informações, consulte [Como usar bancos de dados públicos \(p. 989\)](#).
- As métricas de desempenho, como a largura de banda, a taxa de transferência, a latência e o tamanho da fila média, estão disponíveis por meio do Console de gerenciamento da AWS. Essas métricas, fornecidas pelo Amazon CloudWatch, permitem que você monitore o desempenho de seus volumes para garantir que você forneça desempenho suficiente para seus aplicativos sem pagar por recursos de que não precisa. Para obter mais informações, consulte [Desempenho do volume do Amazon EBS em instâncias do Linux \(p. 932\)](#).

Volumes do Amazon EBS

Um volume do Amazon EBS é um dispositivo de armazenamento em blocos durável que você pode associar a uma única instância do EC2. 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 um aplicativo de banco de dados. Você também pode usá-los para aplicativos com muito throughput que executam verificações de disco contínuas. Os volumes do EBS persistem independentemente da vida útil de uma instância do EC2.

Depois de conectar um volume a uma instância, você poderá usá-lo como qualquer outra unidade rígida física. 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.

O Amazon EBS fornece os seguintes tipos de volume: Finalidade geral (SSD) (gp2), Provisioned IOPS SSD (io1), Disco rígido com throughput otimizado (st1), Cold HDD (sc1) e Magnético (standard, um tipo de geração anterior). Eles diferem em características de desempenho e preço, permitindo que você adapte o custo e o desempenho de armazenamento às necessidades dos aplicativos. Para obter mais informações, consulte [Tipos de volume do Amazon EBS \(p. 844\)](#).

Tópicos

- [Benefícios de usar volumes do EBS \(p. 842\)](#)
- [Tipos de volume do Amazon EBS \(p. 844\)](#)
- [Limites de tamanho e configuração de um volume do EBS \(p. 857\)](#)
- [Criação de um volume do Amazon EBS \(p. 860\)](#)
- [Restauração de um volume do Amazon EBS a partir de um snapshot \(p. 861\)](#)
- [Associação de um volume do Amazon EBS a uma instância \(p. 863\)](#)
- [Disponibilização de um volume do Amazon EBS para uso no Linux \(p. 864\)](#)
- [Como visualizar informações sobre um volume do Amazon EBS \(p. 867\)](#)
- [Como monitorar o status de seus volumes \(p. 868\)](#)
- [Como modificar o tamanho, o desempenho ou o tipo de um volume do EBS \(p. 882\)](#)
- [Separação de um volume do Amazon EBS de uma instância \(p. 893\)](#)
- [Exclusão de um volume do Amazon EBS \(p. 895\)](#)

Benefícios de usar volumes do EBS

Os volumes do EBS oferecem vários benefícios que não são compatíveis com volumes de armazenamento de instâncias.

- Disponibilidade de dados

Ao criar um volume do EBS em uma zona de disponibilidade, ele será automaticamente replicado dentro dessa zona para evitar perda de dados devido à falha de qualquer componente de hardware único. Depois de criar um volume, você pode associá-lo 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. A instância pode formatar o volume do EBS com um sistema de arquivos, como ext3 e, em seguida, instalar aplicativos.

Um volume do EBS só pode ser anexado a uma instância de cada vez, mas vários volumes podem ser conectados a uma única instância. Se você associar vários volumes a um dispositivo ao qual deu o nome, pode distribuir os dados pelos volumes para maior desempenho de E/S e throughput.

Um volume do EBS e a instância à qual ele é anexado devem estar na mesma zona de disponibilidade.

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 [Como monitorar volumes com o CloudWatch \(p. 868\)](#). Para obter informações sobre como acompanhar o status de seus volumes, consulte [Eventos do Amazon CloudWatch para Amazon EBS](#).

- 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.

Por padrão, os volumes do EBS associados a uma instância em execução separam-se automaticamente da instância com seus dados intactos quando essa instância é encerrada. O volume pode então ser reassociado a uma nova instância, permitindo a rápida recuperação. 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 [Amazon EBS Encryption \(p. 926\)](#).

Por padrão, os volumes do EBS criados e associados a uma instância ao ser executada são excluídos quando essa instância é encerrada. Você pode modificar esse comportamento alterando o valor do marcador `DeleteOnTermination` para `false` ao executar a instância. Esse valor modificado faz com que o volume persista mesmo após a instância ser encerrada e permite associar o volume a outra instância.

- 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 os volumes criptografados do EBS para atender a uma grande variedade de requisitos de criptografia de dados em repouso para dados e aplicativos regulamentadas/auditados. O Criptografia de Amazon EBS usa algoritmos Advanced Encryption Standard de 256 bits (AES-256) e uma infraestrutura de chave 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 [Amazon EBS Encryption \(p. 926\)](#).

O Criptografia de Amazon EBS usa chaves mestras do AWS Key Management Service (AWS KMS) para 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 [AWS Key Management Service Developer Guide](#).

- 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 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 restaurados a partir 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 incrementalmente, o processo de exclusão de snapshots foi projetado de forma que você precise reter somente o snapshot mais recente, a fim de restaurar o volume inteiro.

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 [Marcação dos seus recursos do Amazon EC2 \(p. 1003\)](#).

- Flexibilidade

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.

Tipos de volume do Amazon EBS

O Amazon EBS fornece os tipos de volume a seguir, que diferem em características de desempenho e preço, de forma que você adapte o custo e o desempenho de armazenamento às necessidades dos aplicativos. Os tipos de volumes se encaixam em duas categorias:

- Volumes baseados em SSD otimizados para workloads de transação envolvendo operações de leitura/gravação frequentes com o tamanho pequeno de E/S, onde o atributo dominante de desempenho é IOPS
- Volumes baseados em HDD otimizados para grandes workloads de streaming nas quais o throughput (medido em MiB/s) é uma medida de desempenho melhor que IOPS

A tabela a seguir descreve os casos de uso e as características de desempenho para cada tipo de volume.

Note

Atualizações da AWS para desempenho de tipos de volume do EBS podem não ter efeito imediato em seus volumes existentes. Para ver o desempenho completo 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](#).

	Unidades de estado sólido (SSD)		Unidades de disco rígido (HDD)	
Tipo de volume	Finalidade geral (SSD) (<code>gp2</code>)*	Provisioned IOPS SSD (<code>io1</code>)	Disco rígido com throughput otimizado (<code>st1</code>)	Cold HDD (<code>sc1</code>)
Descrição	Volume SSD de uso geral que equilibra preço e desempenho para uma ampla variedade de cargas de trabalho	O volume de SSD de mais de alto desempenho para cargas de trabalho de missão crítica de baixa latência ou de alto rendimento	Volume HDD de baixo custo projetado para cargas de trabalho acessadas com	O volume do HDD com o menor custo projetado para workloads acessados com menos frequência

	Unidades de estado sólido (SSD)		Unidades de disco rígido (HDD)	
			frequência e com altas taxas de transferência	
Casos de uso	<ul style="list-style-type: none"> Recomendado para a maioria dos workloads Volumes de inicialização do sistema Áreas de trabalho virtuais Aplicativos interativos de baixa latência Ambientes de teste e desenvolvimento 	<ul style="list-style-type: none"> Aplicativos críticos de negócios que exigem desempenho de IOPS sustentado ou mais de 16,000 IOPS ou 250 MiB/s de taxa de transferência por volume Workloads de grandes bancos de dados, como: <ul style="list-style-type: none"> MongoDB Cassandra Microsoft SQL Server MySQL PostgreSQL Oracle 	<ul style="list-style-type: none"> Workloads de streaming que exigem throughput consistente e rápido a um baixo preço Big data Data warehouses Processamento de logs Não pode ser um volume de inicialização 	<ul style="list-style-type: none"> Armazenamento orientado para throughput para grandes volumes de dados acessados raramente Cenários nos quais o menor custo de armazenamento é importante Não pode ser um volume de inicialização
Nome da API	gp2	io1	st1	sc1
Tamanho do volume	1 GiB – 16 TiB	4 GiB – 16 TiB	500 GiB – 16 TiB	500 GiB – 16 TiB
Max. IOPS**/Volume	16,000***	64,000****	500	250
Max. Taxa de transferência/volume	250 MiB/s***	1,000 MiB/s†	500 MiB/s	250 MiB/s
Max. IOPS/Instância††	80.000	80.000	80.000	80.000
Max. Taxa de transferência/instância††	1,750 MiB/s	1,750 MiB/s	1,750 MiB/s	1,750 MiB/s
Atributo de desempenho dominante	IOPS	IOPS	MiB/s	MiB/s

* O tipo de volume padrão para volumes do EBS criados no console é gp2. Os volumes criados usando a API `CreateVolume` sem um argumento do tipo de volume são padronizados como gp2 ou standard, de acordo com a região:

- standard: us-east-1, eu-west-1, eu-central-1, us-west-2, us-west-1, sa-east-1, ap-northeast-1, ap-northeast-2, ap-southeast-1, ap-southeast-2, ap-south-1, us-gov-west-1, cn-north-1
- gp2: todas as demais regiões

** gp2/io1 com base no tamanho de E/S 16KiB, st1/sc1 com base no tamanho de E/S de 1 MiB

*** Volumes SSD (gp2) de uso geral têm um limite de taxa de transferência entre 128 MiB/s e 250 MiB/s, dependendo do tamanho do volume. Os volumes maiores que 170 GiB e abaixo de 334 GiB fornecem uma taxa de transferência máxima de 250 MiB/s se houver créditos de intermitência disponíveis. Volumes com 334 GiB e acima entregam 250 MiB/s independentemente dos créditos de intermitência. Um volume gp2 mais antigo pode não apresentar desempenho completo a menos que uma ação `ModifyVolume` seja executada nele. Para obter mais informações, consulte [Modificação de tamanho, IOPS ou tipo de um volume do EBS no Linux](#).

IOPS máxima de 64,000 é garantida apenas em [Instâncias baseadas em Nitro](#). Outras famílias de instâncias garantem desempenho de até 32,000 IOPS.

†A taxa de transferência máxima de 1,000 MiB/s é garantida apenas em [Instâncias baseadas em Nitro](#). Outras famílias de instâncias garantem desempenho de até 500 MiB/s. Um volume io1 mais antigo pode não apresentar desempenho completo a menos que uma ação `ModifyVolume` seja executada nele. Para obter mais informações, consulte [Modificação de tamanho, IOPS ou tipo de um volume do EBS no Linux](#).

†† Para alcançar esse throughput, você deve ter uma instância compatível com ele. Para obter mais informações, consulte [Instâncias otimizadas para Amazon EBS](#).

A tabela a seguir descreve tipos de volumes do EBS de geração anterior. Se você precisar de desempenho superior ou de uma consistência de desempenho superior à dos volumes da geração anterior, recomendamos que use Finalidade geral (SSD) (gp2) ou outros tipos atuais de volume. Para obter mais informações, consulte [Volumes da geração anterior](#).

Volumes de geração anterior	
Tipo de volume	EBS Magnético
Descrição	HDD de geração anterior
Casos de uso	Workloads nos quais os dados são acessados raramente
Nome da API	<code>standard</code>
Tamanho do volume	1 GiB-1 TiB
Max. IOPS/Volume	40–200
Max. Taxa de transferência/volume	40–90 MiB/s
Max. IOPS/Instância	80.000
Max. taxa de transferência/instância	1,750 MiB/s
Atributo de desempenho dominante	IOPS

Note

As AMIs do Linux requerem tabelas de partição GPT e GRUB 2 para volumes de inicialização de 2 TiB (2048 GiB) ou mais. Muitas AMIs do Linux usam hoje o esquema de particionamento MBR, que é compatível somente com volumes de inicialização de 2047 GiB. Se sua instância não for inicializada com um volume de inicialização de 2 TiB ou mais, a AMI que você está usando pode ser limitada a um tamanho de volume de inicialização de 2047 GiB. Volumes de não inicialização não têm essas limitações nas instâncias do Linux.

Há vários fatores que podem afetar o desempenho dos volumes do EBS, como a configuração da instância, as características de E/S e a demanda do workload. Para obter mais informações sobre como aproveitar ao máximo seus volumes do EBS, consulte [Desempenho do volume do Amazon EBS em instâncias do Linux \(p. 932\)](#).

Para obter mais informações sobre o preço desses tipos de volume, consulte [Definição de preço do Amazon EBS](#).

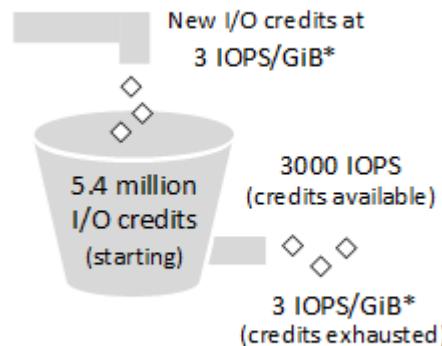
Volumes do Finalidade geral (SSD) (gp2)

Os volumes Finalidade geral (SSD) (gp2) oferecem armazenamento econômico ideal para uma ampla variedade de cargas de trabalho. 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 IOPS 100 (a 33,33 GiB ou menos) e um máximo de IOPS 16,000 (a 5.334 GiB ou mais), o desempenho basal faz uma escala linear a IOPS 3 por GiB de tamanho do volume. A AWS projeta volumes de gp2 para entregar 90% do desempenho provisionado em 99% do tempo. O volume do gp2 pode variar de tamanho entre 1 GiB e 16 TiB.

Créditos de E/S e desempenho de intermitência

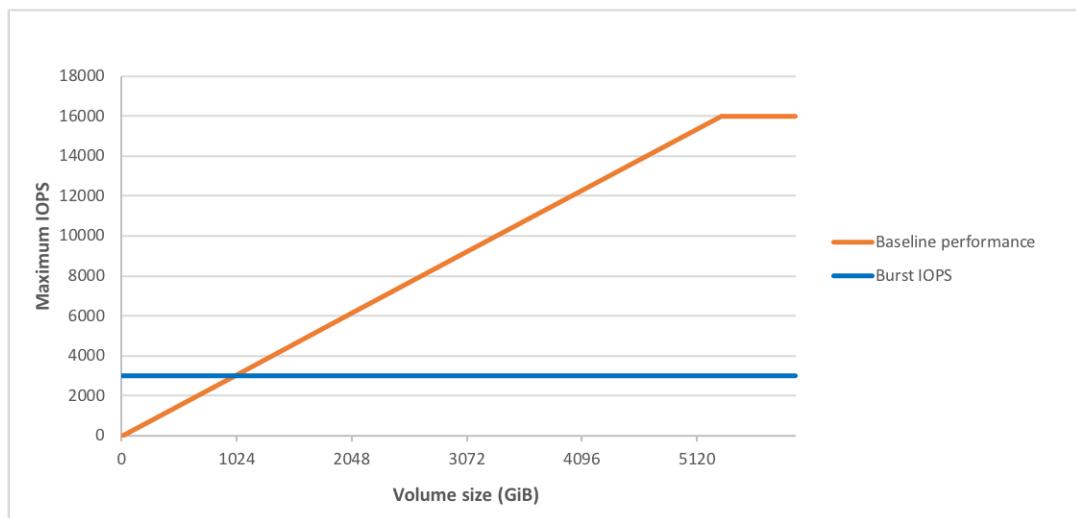
O desempenho dos volumes de gp2 é vinculado ao tamanho do volume, que determina o nível de desempenho basal do volume e a rapidez com que acumula créditos de E/S; volumes maiores têm níveis de desempenho basais mais altos e acumulam créditos de E/S com maior rapidez. Os créditos de E/S representam a largura de banda disponível que seu volume de gp2 pode usar para usar a intermitência de grandes quantidades de E/S quando mais desempenho basal for necessário. Quanto mais créditos seu volume tiver para E/S, mais tempo ele poderá ter intermitência além do nível de desempenho basal e melhor será o desempenho quando mais desempenho for necessário. 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 o desempenho máximo de intermitência de 3.000 IOPS por 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 outros aplicativos. Os volumes ganham créditos de E/S na taxa de desempenho de linha de base de 3 IOPS por GiB de tamanho do volume. Por exemplo, um volume de gp2 de 100 GiB tem um desempenho basal de 300 IOPS.



Quando seu volume exigir mais que o nível de E/S de desempenho basal, ele recorrerá a créditos de E/S no saldo de crédito para fazer a intermitência no nível de desempenho desejado, até o máximo de 3.000 IOPS. Volumes maiores que 1.000 GiB têm desempenho basal igual ou superior ao desempenho de intermitência máximo, e seu saldo de crédito de E/S nunca se esgota. 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).

Note

A tabela a seguir apresenta vários tamanhos de volume e o desempenho basal associado 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)	Desempenho basal (IOPS)	Duração mínima de intermitência a 3.000 IOPS (segundos)	Segundos para encher saldo de crédito vazio
1	100	1862	54,000
100	300	2.000	18,000
250	750	2.400	7.200
334 (tamanho mín. para taxa de transferência máx.)	1002	2703	5389
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*

* Os créditos de intermitência e E/S só são relevantes para volumes abaixo de 1.000 GiB, quando o desempenho de intermitência excede o desempenho da linha de base.

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:

$$\text{Burst duration} = \frac{(\text{Credit balance})}{(\text{Burst IOPS}) - 3(\text{Volume size in GiB})}$$

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, o desempenho máximo de IOPS do volume permanecerá no nível de desempenho basal de IOPS (a taxa em que seu volume ganha créditos) e o throughput máximo do volume será reduzido 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, o desempenho máximo 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 um desempenho basal de 300 IOPS e um limite de throughput 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 o desempenho basal e mais rapidamente o saldo de crédito é reabastecido. Para obter mais informações sobre como a IOPS é medida, consulte [Características de E/S](#).

Caso você perceba que o desempenho do volume é limitado frequentemente ao nível de linha de base (em função de um saldo de crédito de E/S vazio), considere usar um volume de gp2 maior (com um nível de desempenho de linha de base mais alto) ou trocar para um volume de io1 para cargas de trabalho que exigem desempenho de IOPS sustentado maior que 16,000 IOPS.

Para obter informações sobre como usar as métricas e os alarmes do CloudWatch para monitorar seu saldo do bucket de intermitência, consulte [Monitoramento do balanço do bucket de intermitência para volumes gp2, st1 e sc1 \(p. 857\)](#).

Desempenho de throughput

A taxa de transferência de um volume de gp2 pode ser calculada usando a seguinte fórmula, até o limite de 250 MiB/s:

$$\text{Throughput in MiB/s} = ((\text{Volume size in GiB}) \times (\text{IOPS per GiB}) \times (\text{I/O size in KiB}))$$

Supondo que V = tamanho do volume, I = tamanho de entrada/saída e R = taxa de entrada/saída T= taxa de transferência, isso pode ser simplificado em:

$$T = VIR$$

O menor tamanho de volume que atinge a taxa de transferência máxima é determinado por:

$$\begin{aligned} V &= \frac{T}{IR} \\ &= \frac{250 \text{ MiB/s}}{(256 \text{ KiB})(3 \text{ IOPS/GiB})} \\ &= \frac{[(250)(2^{20})(\text{Bytes})]/s}{(256)(2^{10})(\text{Bytes})([3 \text{ IOP/s}]/[(2^{30})(\text{Bytes})])} \end{aligned}$$

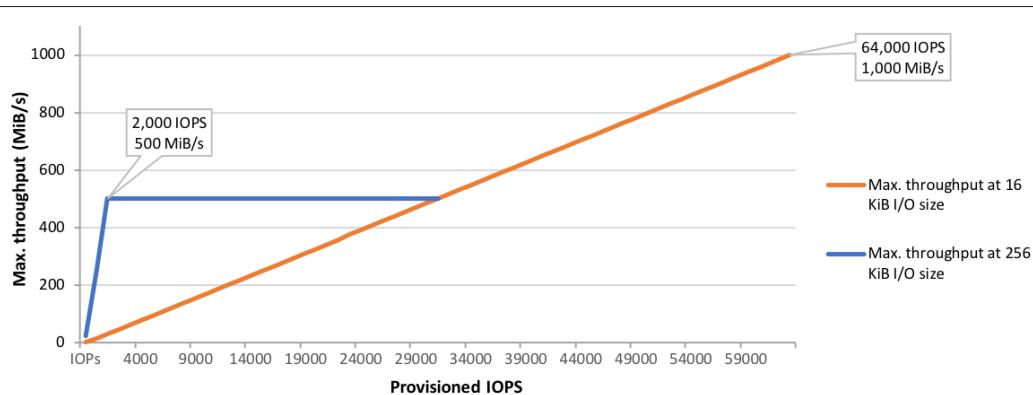
$$\begin{aligned}
 &= \frac{(250)(2^{20})(2^{30})(\text{Bytes})}{(256)(2^{10})(3)} \\
 &= 357,913,941,333 \text{ Bytes} \\
 &= 333\# \text{ GiB (334 GiB in practice because volumes are provisioned in whole gibibytes)}
 \end{aligned}$$

Volumes do Provisioned IOPS SSD (io1)

Os volumes de Provisioned IOPS SSD (io1) são projetados para atender às necessidades de workloads com E/S intensiva, especialmente workloads de bancos de dados, que são sensíveis a desempenho e consistência de armazenamento. Ao contrário de gp2, que usa um bucket e um modelo de crédito para calcular o desempenho, um volume de io1 permite que você especifique uma taxa de IOPS ao criar o volume, e o Amazon EBS entrega até 10% de desempenho de IOPS provisionadas 99,9% do tempo em um determinado ano.

Um volume de io1 pode variar de 4 GiB a 16 TiB. Você pode provisionar de 100 IOPS até 64,000 IOPS por volume em famílias de instâncias do [Sistema Nitro](#) e até 32,000 em outras famílias de instâncias. A razão máxima de IOPS provisionadas para o tamanho do volume solicitado (em GiB) é 50:1. Por exemplo, um volume de 100 GiB pode ser provisionado com até 5.000 IOPS. Em um tipo de instância compatível, qualquer volume de 1.280 GiB de tamanho ou maior permite provisionamento de até 64,000 IOPS no máximo ($50 \times 1.280 \text{ GiB} = 64.000$).

O limite da taxa de transferência de volumes de io1 é 256 KiB/s para cada IOPS provisionadas, até um máximo de 1.000 MiB/s (a 64,000 IOPS). Até 32.000 IOPS, o tamanho da E/S pode ser de até 256 KiB, enquanto que acima disso um tamanho de 16 KiB é usado.



Sua experiência de latência por E/S depende de IOPS provisionadas e do seu padrão de workload. Para obter a melhor experiência de latência de por E/S, recomendamos que você provisione uma razão de IOPS para GiB maior que 2:1. Por exemplo, um volume de IOPS de 2.000 devem ser menor que 1.000 GiB.

Note

Algumas contas da AWS criadas antes de 2012 podem ter acesso às Zonas de disponibilidade nas regiões us-west-1 ou ap-northeast-1 que não são compatíveis com volumes Provisioned IOPS SSD (io1). Caso não seja de criar um volume io1 (ou executar uma instância com um volume io1 no mapeamento de dispositivos do bloco) em uma dessas regiões, experimente uma zona de disponibilidade diferente na região. Você pode verificar se a zona de disponibilidade oferece suporte para volumes io1 ao criar um volume de io1 de 4 GiB naquela zona.

Volumes do Disco rígido com throughput otimizado (st1)

Os volumes de Disco rígido com throughput otimizado (st1) fornecem armazenamento magnético de baixo custo que define o desempenho em termos de throughput, não IOPS. Esse tipo de volume é ideal

para workloads grandes e sequenciais, como Amazon EMR, ETL, data warehouses e processamento de logs. Não há compatibilidade com volumes de `st1` inicializáveis.

Os volumes de Disco rígido com throughput otimizado (`st1`), embora semelhantes aos volumes de Cold HDD (`sc1`), são projetados para serem compatíveis com dados acessados com frequência.

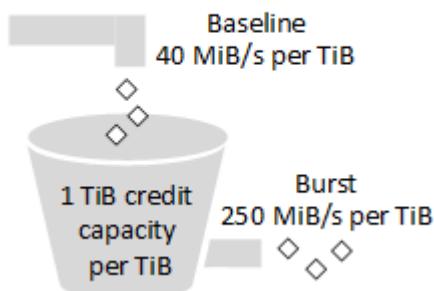
Esse tipo de volume é otimizado para workloads que envolvem E/S sequencial e grande, e recomendamos que clientes com workloads executando E/S pequena e aleatória usem `gp2`. Para obter mais informações, consulte [Ineficiência de pequenas leituras/escritas no HDD \(p. 857\)](#).

Créditos de throughput e desempenho de intermitência

Como o `gp2`, o `st1` usa um modelo de bucket de intermitência para desempenho. O tamanho do volume determina o throughput da linha de base do seu volume, que é a taxa na qual o volume acumula créditos de throughput. O tamanho do volume também determina o throughput de intermitência do seu volume, que é a taxa em que você pode gastar créditos quando estiverem disponíveis. Os volumes maiores têm throughput 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 throughput e limites de crédito de throughput, o throughput disponível de um volume `st1` é expressado pela seguinte fórmula:

$$(\text{Volume size}) \times (\text{Credit accumulation rate per TiB}) = \text{Throughput}$$

Para um volume de `st1` de 1-TiB, o throughput de intermitência está limitado 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 0,5 a 16 TiB, o throughput de linha de base varia de 20 até um limite de 500 MiB/s, que é acessado a 12,5 TiB, da seguinte forma:

$$12.5 \text{ TiB} \times \frac{40 \text{ MiB/s}}{1 \text{ TiB}} = 500 \text{ MiB/s}$$

O throughput varia de 125 MiB/s a um limite de 500 MiB/s, que é alcançado em 2 TiB, da seguinte forma:

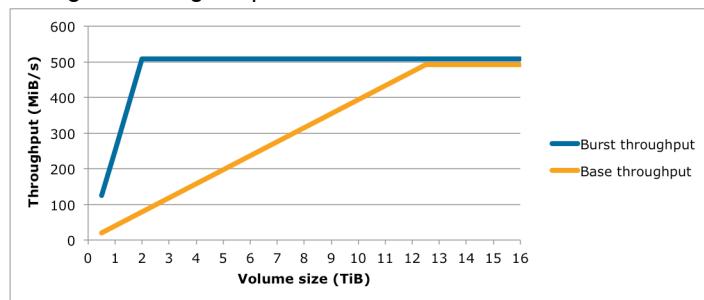
$$2 \text{ TiB} \times \frac{250 \text{ MiB/s}}{2 \text{ TiB}} = 500 \text{ MiB/s}$$

1 TiB

A tabela a seguir apresenta a gama completa de valores de throughput e intermitência para st1:

Tamanho do volume (TiB)	Throughput de base ST1 (MiB/s)	Throughput de intermitência do ST1 (MiB/s)
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 de Disco rígido com throughput otimizado (st1), o desempenho pode cair até o valor basal 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 [Monitoramento do balanço do bucket de intermitência para volumes gp2, st1 e sc1 \(p. 857\)](#).

Volumes do Cold HDD (sc1)

Os volumes de Cold HDD (sc1) fornecem armazenamento magnético de baixo custo que define o desempenho em termos de throughput, não IOPS. Com um limite menor de throughput que st1, sc1 é ideal de ajuste para workloads de cold data sequenciais grandes. 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 sc1 inicializáveis.

Os volumes de Cold HDD (sc1), embora semelhantes aos volumes de Disco rígido com throughput otimizado (st1), são projetados para serem compatíveis com dados acessados com pouca frequência.

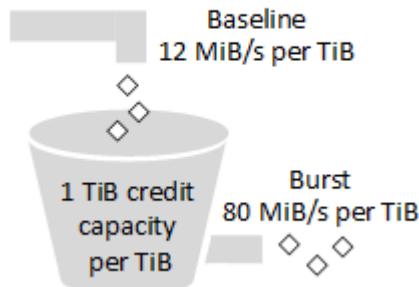
Note

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 \(p. 857\)](#).

Créditos de throughput e desempenho de intermitência

Como o gp2, o sc1 usa um modelo de bucket de intermitência para desempenho. O tamanho do volume determina o throughput da linha de base do seu volume, que é a taxa na qual o volume acumula créditos de throughput. O tamanho do volume também determina o throughput de intermitência do seu volume, que é a taxa em que você pode gastar créditos quando estiverem disponíveis. Os volumes maiores têm throughput basal e de intermitência mais altos. Quanto mais créditos seu volume tiver, ele será capaz de acionar E/S da unidade em nível de intermitência por mais tempo.

SC1 burst bucket



Sujeito a throughput e limites de crédito de throughput, o throughput disponível de um volume sc1 é expressado pela seguinte fórmula:

$$(\text{Volume size}) \times (\text{Credit accumulation rate per TiB}) = \text{Throughput}$$

Para um volume de sc1 de 1-TiB, o throughput de intermitência está limitado 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 volumes variando de 0,5 a 16 TiB, o throughput basal varia de 6 MiB/s até um máximo de 192 MiB/s, que é acessado a 16 TiB, da seguinte forma:

$$12 \text{ MiB/s} \\ 16 \text{ TiB} \times \frac{12 \text{ MiB/s}}{1 \text{ TiB}} = 192 \text{ MiB/s}$$

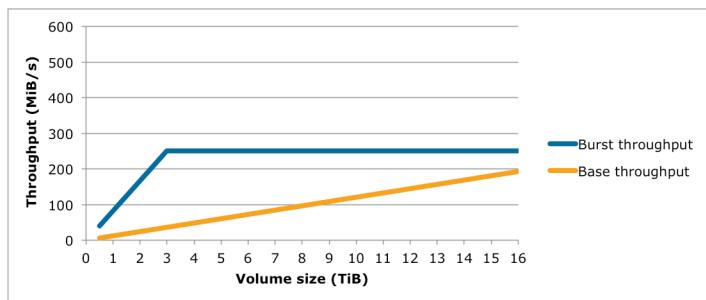
O throughput varia de 40 MiB/s a um limite de 250 MiB/s, que é alcançado em 3.125 TiB, da seguinte forma:

$$80 \text{ MiB/s} \\ 3.125 \text{ TiB} \times \frac{80 \text{ MiB/s}}{1 \text{ TiB}} = 250 \text{ MiB/s}$$

A tabela a seguir apresenta a gama completa de valores de throughput e intermitência para sc1:

Tamanho do volume (TiB)	Throughput de base SC1 (MiB/s)	Throughput de intermitência do SC1 (MiB/s)
0,5	6	40
1	12	80
2	24	160
3	36	240
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 de Cold HDD (sc1), o desempenho pode cair até o valor basal 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 [Monitoramento do balanço do bucket de intermitência para volumes gp2, st1 e sc1 \(p. 857\)](#).

Magnético (standard)

Os volumes Magnético são baseados em unidades magnéticas e adequadas para workloads nos quais os dados são acessados com pouca frequência, e cenários nos quais 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

Magnético é um volume de geração anterior. Para novos aplicativos, 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 [Monitoramento do balanço do bucket de intermitência para volumes gp2, st1 e sc1 \(p. 857\)](#).

Considerações sobre o desempenho ao usar volumes de HDD

Para resultados ideais de throughput usando volumes de HDD, planeje suas workloads com as seguintes considerações em mente.

Disco rígido com throughput otimizado x Cold HDD

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 throughput por instância e por volume. Os volumes associados a instâncias menores são limitados ao throughput por instância em vez de aos limites de throughput de st1 ou sc1.

Tanto st1 quanto sc1 são projetados para consistência de desempenho de 90% de throughput de intermitência em 99% do tempo. Períodos não compatíveis são distribuídos com uniformidade aproximada, destinando 99% do throughput total esperado a cada hora.

A tabela a seguir mostra o tempo de varredura ideal de volumes de vários tamanhos, pressupondo buckets cheios e throughput de instância suficiente.

Geralmente, os tempos de varredura são expressados por esta fórmula:

Volume size

$\frac{5 \text{ TiB}}{500 \text{ MiB/s}} = \frac{5 \text{ TiB}}{0.00047684 \text{ TiB/s}} = 10,486 \text{ s} = 2.91 \text{ hours (optimal)}$ $2.91 \text{ hours} + \frac{2.91}{(0.90)(0.99)} = 3.27 \text{ hours (minimum expected)}$ <small>--> From expected performance of 90% of burst 99% of the time</small>
--

Por exemplo, levando em conta as garantias de consistência do desempenho 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.

$\frac{5 \text{ TiB}}{0.000238418 \text{ TiB/s}} = 20972 \text{ s} = 5.83 \text{ hours (optimal)}$ $5.83 \text{ hours} + \frac{5.83}{(0.90)(0.99)} = 6.54 \text{ hours (minimum expected)}$
--

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.

$\frac{5 \text{ TiB}}{0.000238418 \text{ TiB/s}} = 20972 \text{ s} = 5.83 \text{ hours (optimal)}$ $5.83 \text{ hours} + \frac{5.83}{(0.90)(0.99)} = 6.54 \text{ hours (minimum expected)}$
--

Tamanho do volume (TiB)	Tempo de varredura de ST1 com intermitência (horas) *	Tempo de varredura de SC1 com intermitência (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

Tamanho do volume (TiB)	Tempo de varredura de ST1 com intermitência (horas) *	Tempo de varredura de SC1 com intermitência (horas) *
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 um workload orientado para throughput 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 desempenho da digitalização, use o sc1.

Ineficiência de pequenas leituras/escritas no HDD

O módulo de desempenho para os volumes st1 e sc1 é otimizado para E/Ss sequenciais, favorecendo workloads de alto throughput, oferecendo desempenho aceitável em workloads com IOPS e throughput 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 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 no throughput por instância

O throughput dos volumes st1 e sc1 sempre é determinado pela menor das seguintes opções:

- Limites de throughput do volume
- Limites de throughput da instância

Quanto a todos os volumes da Amazon EBS, recomendamos que você selecione uma instância do EC2 otimizada por EBS apropriada para evitar gargalos de rede. Para obter mais informações, consulte [Instâncias otimizadas para Amazon EBS](#).

Monitoramento do balanço do bucket de intermitência para volumes gp2, st1 e sc1

Você pode monitorar o nível do bucket de intermitência para os volumes gp2, st1 e sc1 usando a métrica `BurstBalance` do EBS disponível no Amazon CloudWatch. Essa métrica mostra a porcentagem de créditos de E/S (para gp2) ou créditos de throughput (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 de E/S e monitoramento](#). O CloudWatch também permite que você defina um alarme que envia uma notificação quando o valor de `BurstBalance` cai para um determinado nível. Para obter mais informações, consulte [Criação de alarmes do Amazon CloudWatch](#).

Limites 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 físico 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.

A tabela a seguir resume as capacidades de armazenamento teóricas e implementadas para a maioria dos sistemas de arquivos usados comumente no Amazon EBS, assumindo 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	Máx. suportado pelo EBS
MBR	2^{32}	2 TiB	2 TiB	2 TiB	2 TiB	2 TiB
GPT	2^{64}	$8 \text{ ZiB} = 8 \times 1024^3 \text{ TiB}$ (50 TiB certificados em RHEL7)	$1 \text{ EiB} = 1024^2 \text{ TiB}$ (50 TiB certificados em RHEL7)	500 TiB (Certificado na RHEL7)	256 TiB	16 TiB

* https://ext4.wiki.kernel.org/index.php/Ext4_Howto e <https://access.redhat.com/solutions/1532>

** <https://access.redhat.com/solutions/1532>

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.

Conteúdo

- [Limitações de serviços \(p. 858\)](#)
- [Esquemas de particionamento \(p. 858\)](#)
- [Tamanhos de blocos de dados \(p. 859\)](#)

Limitações de serviços

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 16 TiB. Isso significa que você pode criar um volume do EBS de até 16 TiB, mas se o sistema operacional reconhecerá toda essa capacidade dependerá de suas próprias características de projeto e de como o volume está dividido.
- O Amazon EC2 requer volumes de inicialização do Windows para usar o particionamento de MBR. Como discutido em [Esquemas de particionamento \(p. 858\)](#), isso significa que os volumes de inicialização não podem ser maiores que 2 TiB. Os volumes de dados do Windows não estão sujeitos a esse limite e podem ser particionados pela GPT.
- Os volumes de inicialização do Linux podem ser MBR ou GPT, e os volumes de inicialização GPT não estão sujeitos ao limite de 2 TiB.

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 \(p. 859\)](#). 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 por:

$$(2^{32} - 1) \times \text{Block size} = \text{Number of addressable blocks}$$

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 por:

$$(2^{64} - 1) \times \text{Block size} = \text{Number of addressable blocks}$$

O tamanho de bloco para volumes GPT normalmente é de 4.096 bytes. Portanto:

$$(2^{64} - 1) \times 4,096 \text{ bytes} = 8 \text{ ZiB} - 4,096 \text{ bytes} = 8 \text{ billion TiB} - 4,096 \text{ bytes}$$

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 cargas de trabalho 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 têm 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

Tamanho de bloco	Tamanho máx. do volume
8 KiB	32 TiB
16 KiB	64 TiB
32 KiB	128 TiB
64 KiB (máximo)	256 TiB

O limite imposto pelo EBS no tamanho do volume (16 TiB) atualmente é igual ao tamanho máximo permitido pelos blocos de dados de 4 KiB.

Criação de um volume do Amazon EBS

Você pode criar um volume do Amazon EBS, que então poderá associar a qualquer instância do EC2 dentro da mesma zona de disponibilidade. Você pode optar por criar um volume do EBS criptografado, mas os volumes criptografados só podem ser associados a tipos de instância selecionados. Para obter mais informações, consulte [Tipos de instâncias compatíveis \(p. 927\)](#). Você pode usar as políticas do IAM para forçar a criptografia nos novos volumes. Para obter mais informações, consulte as políticas de exemplo do IAM em [Como trabalhar com volumes \(p. 683\)](#) e [Executar instâncias \(RunInstances\) \(p. 689\)](#).

Você também pode criar e associar volumes do EBS ao executar instâncias, especificando um mapeamento de dispositivos de blocos. Para obter mais informações, consulte [Execução de uma instância usando o assistente de execução de instância \(p. 391\)](#) e [Mapeamento de dispositivos de blocos \(p. 979\)](#). Você pode restaurar volumes de snapshots previamente criados. Para obter mais informações, consulte [Restauração de um volume do Amazon EBS a partir de um snapshot \(p. 861\)](#).

Você pode aplicar tags nos volumes do EBS no momento da criação. Com o uso de tags, você pode simplificar o rastreamento do seu inventário de recursos do Amazon EC2. Usar tags na criação pode ser combinado com a política da IAM de forçar o uso de tags nos novos volumes. Para obter mais informações, consulte [Como marcar seus recursos](#).

Se você estiver criando um volume para um cenário de armazenamento de alto desempenho, use um volume Provisioned IOPS SSD (io1) e associe-o a uma instância com o largura de banda suficiente para ser compatível com seu aplicativo, como instância otimizada para EBS ou instância com conectividade de rede de 10 Gigabits. O mesmo conselho vale para os volumes de Disco rígido com throughput otimizado (st1) e Cold HDD (sc1). Para obter mais informações, consulte [Configuração de instância do Amazon EC2 \(p. 935\)](#).

Os novos volumes do EBS recebem seu desempenho máximo no momento em que são disponibilizados e não requerem inicialização (antes conhecido como pré-aquecimento). Contudo, blocos de armazenamento em volumes que foram restaurados a partir de snapshots devem ser inicializados (puxados do Amazon S3 e gravados no volume) antes de 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. Para a maioria dos aplicativos, é aceitável amortizar esse custo ao longo da vida útil do volume. O desempenho é restaurado depois de os dados serem acessados uma vez. Para obter mais informações, consulte [Inicialização de volumes do Amazon EBS \(p. 939\)](#).

Para criar um volume do EBS usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. Da 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 [Locais de recursos \(p. 992\)](#).
3. No painel de navegação, escolha ELASTIC BLOCK STORE, Volumes.

4. Escolha Criar volume.
5. Em Tipo de volume, escolha um tipo de volume. Para obter mais informações, consulte [Tipos de volume do Amazon EBS \(p. 844\)](#).

Note

Algumas contas da AWS criadas antes de 2012 podem ter acesso às Zonas de disponibilidade nas regiões us-west-1 ou ap-northeast-1 que não são compatíveis com volumes Provisioned IOPS SSD (io1). Caso não seja de criar um volume io1 (ou executar uma instância com um volume io1 no mapeamento de dispositivos do bloco) em uma dessas regiões, experimente uma zona de disponibilidade diferente na região. Você pode verificar se a zona de disponibilidade oferece suporte para volumes io1 ao criar um volume de io1 de 4 GiB naquela zona.

6. Para Tamanho (GiB), insira o tamanho do volume.
7. Com um volume Provisioned IOPS SSD, para IOPS, insira o número máximo de operações de entrada/saída por segundo (IOPS) com que o volume deveria ser compatível.
8. Para Zona de disponibilidade, escolha a zona de disponibilidade na qual criar o volume. Os volumes do EBS só podem ser associados a instâncias do EC2 dentro da mesma zona de disponibilidade.
9. (Opcional) Para criar um volume criptografado, selecione a caixa Criptografado e escolha a chave mestra que deseja usar para criptografar o volume. Você pode escolher a chave mestra padrão da sua conta ou qualquer chave mestra do cliente (CMK) que tiver criado anteriormente usando o AWS Key Management Service. As chaves disponíveis podem ser vistas no menu Chave mestra; você também pode colar o ARN completo de qualquer chave à qual tenha acesso. Para obter mais informações, consulte o [AWS Key Management Service Developer Guide](#).

Note

Os volumes criptografados só podem ser associados aos tipos de instâncias selecionados. Para obter mais informações, consulte [Tipos de instâncias compatíveis \(p. 927\)](#).

10. (Opcional) Escolha Criar tags adicionais para adicionar tags ao volume. Forneça uma chave e um valor para cada tag.
11. Escolha Criar volume.

Para criar 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 [Acessando o Amazon EC2 \(p. 3\)](#).

- `create-volume`AWS CLI
- `New-EC2Volume`AWS Tools para Windows PowerShell

Restauração de um volume do Amazon EBS a partir de um snapshot

Você pode restaurar um volume do Amazon EBS com dados de um snapshot armazenado no Amazon S3. Você precisa saber o ID do snapshot do qual deseja restaurar seu volume e ter permissões de acesso para o snapshot. Para obter mais informações sobre snapshots, consulte [Snapshots do Amazon EBS \(p. 896\)](#).

Snapshots do EBS são a ferramenta de backup preferida do Amazon EC2 devido à sua velocidade, conveniência e custo. Ao restaurar um volume de um snapshot, você recria o estado dele para um ponto específico no passado com todos os dados intactos. Ao associar um volume restaurado 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 associado. Para obter mais informações, consulte [Snapshots do Amazon EBS](#).

Os novos volumes criados com base em snapshots existentes do EBS são carregados como processo de fundo. Isso significa que, após a criação de um volume a partir de um snapshot, não há necessidade de esperar que todos os dados sejam transferidos do Amazon S3 para o seu volume do EBS antes que a instância conectada possa começar a acessar o volume 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 em segundo plano.

Os volumes do EBS restaurados a partir de snapshots criptografados são criptografados automaticamente. Os volumes criptografados só podem ser associados aos tipos de instâncias selecionados. Para obter mais informações, consulte [Tipos de instâncias compatíveis \(p. 927\)](#).

Devido a restrições de segurança, você não pode restaurar diretamente um volume do EBS a partir de um snapshot criptografado compartilhado que você não possui. Você deve primeiro criar uma cópia do snapshot que você possui. Então, poderá restaurar um volume a partir dessa cópia. Para obter mais informações, consulte [Criptografia do Amazon EBS](#)

Os novos volumes do EBS recebem seu desempenho máximo no momento em que são disponibilizados e não requerem inicialização (antes conhecido como pré-aquecimento). Contudo, blocos de armazenamento em volumes que foram restaurados a partir de snapshots devem ser inicializados (puxados do Amazon S3 e gravados no volume) antes de 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. O desempenho é restaurado depois de os dados serem acessados uma vez.

Para a maioria dos aplicativos, é aceitável a amortização do custo de inicialização ao longo da vida útil do volume. Para garantir que seu volume restaurado sempre funcione na capacidade máxima de produção, você pode forçar a inicialização imediata do volume inteiro usando dd ou fio. Para obter mais informações, consulte [Inicialização de volumes do Amazon EBS \(p. 939\)](#).

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 restaurar o snapshot para um volume em outra região, você pode copiar seu snapshot para a nova região e restaurá-lo para um volume nessa região. Para obter mais informações, consulte [Cópia de um snapshot do Amazon EBS \(p. 902\)](#).

3. No painel de navegação, escolha ELASTIC BLOCK STORE, Volumes.
4. Escolha Criar volume.
5. Em Tipo de volume, escolha um tipo de volume. Para obter mais informações, consulte [Tipos de volume do Amazon EBS \(p. 844\)](#).

Note

Algumas contas da AWS criadas antes de 2012 podem ter acesso às Zonas de disponibilidade nas regiões us-west-1 ou ap-northeast-1 que não são compatíveis com volumes Provisioned IOPS SSD (io1). Caso não seja de criar um volume io1 (ou executar uma instância com um volume io1 no mapeamento de dispositivos do bloco) em uma dessas regiões, experimente uma zona de disponibilidade diferente na região. Você pode verificar se a zona de disponibilidade oferece suporte para volumes io1 ao criar um volume de io1 de 4 GiB naquela zona.

6. Para 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.

Os volumes restaurados de snapshots criptografados só podem ser associados a instâncias compatíveis com Criptografia de Amazon EBS. Para obter mais informações, consulte [Tipos de instâncias compatíveis \(p. 927\)](#).

7. Para Tamanho (GiB), digite o tamanho do volume ou verifique se o tamanho padrão do snapshot é adequado.

Note

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 Tamanho. Todos os códigos de produto de AWS Marketplace do snapshot são propagados para o volume.

8. Com um volume Provisioned IOPS SSD, para IOPS, insira o número máximo de operações de entrada/saída por segundo (IOPS) com que o volume deveria ser compatível.
9. Para Zona de disponibilidade, escolha a zona de disponibilidade na qual criar o volume. Os volumes do EBS só podem ser anexados a instâncias do EC2 na mesma zona de disponibilidade.
10. (Opcional) Escolha Criar tags adicionais para adicionar tags ao volume. Forneça uma chave e um valor para cada tag.
11. Escolha Criar volume.
12. Depois de restaurar um novo volume a partir de um snapshot, você poderá associá-lo a uma instância para começar a utilizá-lo. Para obter mais informações, consulte [Associação de um volume do Amazon EBS a uma instância \(p. 863\)](#).
13. Se você tiver restaurado um snapshot para um volume maior que o padrão para esse snapshot, deverá ampliar o sistema de arquivos no volume para usufruir do espaço extra. Para obter mais informações, consulte [Como modificar o tamanho, o desempenho ou o tipo de um volume do EBS \(p. 882\)](#).

Para restaurar 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 [Acessando o Amazon EC2 \(p. 3\)](#).

- [create-volume](#) AWS CLI
- [New-EC2Volume](#) AWS Tools para Windows PowerShell

Associação de um volume do Amazon EBS a uma instância

Você pode associar um volume do EBS disponível a uma de suas instâncias que está na mesma zona de disponibilidade que o volume.

Pré-requisitos

- Determine quantos volumes você pode associar à sua instância. Para obter mais informações, consulte [Limites de volume de instância \(p. 976\)](#).
- 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 \(p. 927\)](#).
- Se um volume tiver o código de produto do AWS Marketplace:
 - O volume só poderá ser associado a uma instância interrompida.
 - Você deve ser inscrito no código do AWS Marketplace que está no volume.
 - A configuração (tipo de instância, sistema operacional) da instância deve oferecer suporte a esse código específico AWS Marketplace. Por exemplo, você não pode obter um volume de uma instância do Windows e associá-la a uma instância do Linux.
 - Os códigos de produto do AWS Marketplace são copiados do volume para a instância.

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 [Nomenclatura de dispositivos nas instâncias do Linux \(p. 978\)](#).
6. Escolha Associar.
7. Conecte-se à sua instância e monte o volume. Para obter mais informações, consulte [Disponibilização de um volume do Amazon EBS para uso no Linux \(p. 864\)](#).

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 [Acessando o Amazon EC2 \(p. 3\)](#).

- [attach-volume](#) (AWS CLI)
- [Add-EC2Volume](#) (AWS Tools para Windows PowerShell)

Disponibilização de um volume do Amazon EBS para uso no Linux

Depois de anexar um volume do Amazon EBS à instância, ele é 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 aplicativos 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 \(p. 896\)](#).

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 \(p. 439\)](#).
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 [Nomenclatura de dispositivos nas instâncias do Linux \(p. 978\)](#). 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.

O exemplo a seguir mostra a saída de uma [instância baseada em Nitro \(p. 179\)](#), que expõe os volumes do EBS como dispositivos de blocos NVMe. O dispositivo raiz é /dev/nvme0n1. O volume anexado é /dev/nvme1n1, que ainda 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. O volume anexado é /dev/xvdf, que ainda 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 restaurados a partir dos snapshots provavelmente já têm um sistema de arquivos neles; se você criar um novo sistema de arquivos no sistema de arquivos existente, a operação sobrescreverá seus dados.

Use o comando file -s para obter informações sobre o dispositivo, 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 e você deverá criar um.

```
[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)
```

4. (Condisional) 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 tenha dados (por exemplo, um volume que foi restaurado de um snapshot). Caso contrário, você formatará o volume e excluirá os dados existentes.

```
[ec2-user ~]$ sudo mkfs -t xfs /dev/xvdf
```

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 aplicativos 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. 866).

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. 930).

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.

```
[ec2-user ~]$ sudo blkid
/dev/xvda1: LABEL="/" UUID="ca774df7-756d-4261-a3f1-76038323e572" TYPE="xfs"
PARTLABEL="Linux" PARTUUID="02dcd367-e87c-4f2e-9a72-a3cf8f299c10"
/dev/xvdf: UUID="aebf131c-6957-451e-8d34-ec978d9581ae" TYPE="xfs"
```

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: valor de UUID retornado pelo `blkid`, ponto de montagem, sistema de arquivos e opções recomendadas de montagem do sistema de arquivos. Para obter mais informações, consulte a página do manual para o `fstab` (execute o `man fstab`).

```
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
```

Como 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 descritivas

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. Para ver mais informações sobre um volume, selecione-o. No painel de detalhes, você pode inspecionar as informações fornecidas sobre o volume.
4. No painel de detalhes, você pode inspecionar as informações fornecidas sobre o volume.

Para visualizar os volumes do EBS que são associados 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. Para ver mais informações sobre uma instância, selecione-a.
4. No painel de detalhes, você pode inspecionar as informações fornecidas sobre dispositivos de blocos e raiz.

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 [Acessando o Amazon EC2 \(p. 3\)](#).

- [describe-volumes](#) (AWS CLI)
- [Get-EC2Volume](#) (AWS Tools para Windows PowerShell)

Visualizar espaço em disco disponível

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% /
```

Como monitorar o status de seus volumes

A Amazon Web Services (AWS) fornece automaticamente dados, como as métricas do Amazon CloudWatch e as verificações de status de volume, que você pode usar para monitorar seus volumes do Amazon Elastic Block Store (Amazon EBS).

Tópicos

- [Como monitorar volumes com o CloudWatch \(p. 868\)](#)
- [Como monitorar volumes com verificações de status \(p. 873\)](#)
- [Como monitorar os eventos de volumes \(p. 876\)](#)
- [Como trabalhar com um volume danificado \(p. 877\)](#)
- [Como trabalhar com o atributo de volume AutoEnableIO \(p. 880\)](#)

Como monitorar volumes com o CloudWatch

As métricas do CloudWatch são dados estatísticos que você pode usar para visualizar, analisar e definir alarmes sobre o comportamento operacional de seus volumes.

A tabela a seguir descreve os tipos de dados de monitoramento disponíveis para seus volumes do Amazon EBS.

Tipo	Descrição
Basic	Os dados são disponibilizados automaticamente em períodos de cinco minutos, sem custo adicional. Isso inclui dados dos volumes de dispositivos raiz de instâncias com suporte do EBS.
Detalhado	Os volumes do Provisioned IOPS SSD (io1) enviam automaticamente métricas de um minuto ao CloudWatch.

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 cinco minutos -). Recomendamos especificar um período em sua solicitação que seja igual ou superior ao 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.

Métricas do Amazon EBS

O Amazon Elastic Block Store (Amazon EBS) envia pontos de dados para o CloudWatch para várias métricas. Volumes de SSD de propósito geral do Amazon EBS (gp2), HDD otimizado para throughput (st1), Cold HDD (sc1) e Magnetic (padrão) enviam automaticamente métricas de cinco minutos para o

CloudWatch. Volumes de SSD de IOPS provisionadas (io1) enviam automaticamente métricas de um minuto para o CloudWatch. Os dados são reportados para o CloudWatch somente quando o volume está vinculado a uma instância.

Algumas dessas métricas têm diferenças em instâncias baseadas em Nitro. Para obter uma lista dos tipos de instância baseadas no sistema Nitro, consulte [Instâncias baseadas em Nitro \(p. 179\)](#).

O namespace AWS/EBS inclui as métricas a seguir.

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>Unidade: 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>Unidade: bytes</p>
VolumeReadOps	<p>O número total de operações de leitura em um período especificado.</p> <p>Para calcular a média de operações de leitura por segundo (IOPS de leitura) para o período, divida o total das operações de leitura pelo número de segundos no período em questão.</p> <p>As estatísticas Minimum e Maximum nessa métrica são compatíveis somente com volumes anexados às instâncias baseada em Nitro.</p>

Métrica	Descrição
	Unidade: contagem
<code>VolumeWriteOps</code>	<p>O número total de operações de gravação em um período especificado.</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 <code>Minimum</code> e <code>Maximum</code> nessa métrica são compatíveis somente com volumes anexados às instâncias baseada em Nitro.</p> <p>Unidade: contagem</p>
<code>VolumeTotalReadTime</code>	<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 5 minutos (300 segundos): se 700 operações foram concluídas durante esse período, e cada operação levou 1 segundo, o valor seria 700 segundos. Para instâncias de Xen, os dados são informados apenas quando há atividades de leitura no volume.</p> <p>A estatística <code>Average</code> nessa métrica não é relevante para volumes anexados a instâncias baseadas em Nitro.</p> <p>As estatísticas <code>Minimum</code> e <code>Maximum</code> nessa métrica são compatíveis somente com volumes anexados às instâncias baseada em Nitro.</p> <p>Unidade: segundos</p>
<code>VolumeTotalWriteTime</code>	<p>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 5 minutos (300 segundos): se 700 operações foram concluídas durante esse período, e cada operação levou 1 segundo, o valor seria 700 segundos. Para instâncias de Xen, os dados são informados apenas quando há atividades de gravação no volume.</p> <p>A estatística <code>Average</code> nessa métrica não é relevante para volumes anexados a instâncias baseadas em Nitro.</p> <p>As estatísticas <code>Minimum</code> e <code>Maximum</code> nessa métrica são compatíveis somente com volumes anexados às instâncias baseada em Nitro.</p> <p>Unidade: segundos</p>

Métrica	Descrição
<code>VolumeIdleTime</code>	<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>Unidade: contagem</p>
<code>VolumeThroughputPercentage</code>	<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 do Provisioned IOPS SSD fornecem cerca de 10% do desempenho de IOPS provisionadas em 99,9% do tempo em um determinado ano.</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, o desempenho 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>Unidade: percentual</p>
<code>VolumeConsumedReadWriteOps</code>	<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>Unidade: contagem</p>

Métrica	Descrição
BurstBalance	<p>Usado somente com volumes do Finalidade geral (SSD) (gp2), Disco rígido com throughput otimizado (st1) e Cold HDD (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 Sum nessa métrica não é relevante para volumes anexados a instâncias baseadas em Nitro.</p> <p>Unidade: percentual</p>

Dimensões para métricas do Amazon EBS

A única dimensão que o Amazon EBS envia para o CloudWatch é o ID do volume. Isso significa que todas as estatísticas disponíveis são filtradas por ID de volume.

Gráficos no console do Amazon EC2

Depois de criar um volume, você visualizará os gráficos de monitoramento de volumes no console do Amazon EC2. Selecione um volume na página Volumes no console e escolha Monitoring. A tabela a seguir lista os gráficos exibidos. A coluna à direita descreve como as métricas de dados brutos da API do CloudWatch são usadas para produzir cada gráfico. O período de todos os gráficos é de cinco minutos.

Gráfico	Descrição usando métricas brutas
Largura de banda de leitura (KiB/s)	<code>Sum(VolumeReadBytes) / Period / 1024</code>
Largura de banda de gravação (KiB/s)	<code>Sum(VolumeWriteBytes) / Period / 1024</code>
Taxa de transferência de leitura (IOPS)	<code>Sum(VolumeReadOps) / Period</code>
Taxa de transferência de gravação (IOPS)	<code>Sum(VolumeWriteOps) / Period</code>
Comprimento médio da fila (operações)	<code>Avg(VolumeQueueLength)</code>
% de tempo ocioso gasto	<code>Sum(VolumeIdleTime) / Period × 100</code>
Tamanho médio de leitura (KiB/operação)	<p><code>Avg(VolumeReadBytes) / 1024</code></p> <p>Para as instâncias baseadas em Nitro, a fórmula a seguir gera o tamanho médio de leitura usando a Matemática de métricas do CloudWatch:</p> $(\text{Sum}(\text{VolumeReadBytes}) / \text{Sum}(\text{VolumeReadOps})) / 1024$ <p>As métricas <code>VolumeReadBytes</code> e <code>VolumeReadOps</code> estão disponíveis no console do EBS CloudWatch.</p>
Tamanho médio de gravação (KiB/operação)	<code>Avg(VolumeWriteBytes) / 1024</code>

Gráfico	Descrição usando métricas brutas
	<p>Para as instâncias baseadas em Nitro, a fórmula a seguir gera o tamanho médio de gravação usando a Matemática de métricas do CloudWatch:</p> $(\text{Sum}(\text{VolumeWriteBytes}) / \text{Sum}(\text{VolumeWriteOps})) / 1024$ <p>As métricas <code>VolumeWriteBytes</code> e <code>VolumeWriteOps</code> estão disponíveis no console do EBS CloudWatch.</p>
Latência média de leitura (ms/operação)	$\text{Avg}(\text{VolumeTotalReadTime}) \times 1000$ <p>Para as instâncias baseadas em Nitro, a fórmula a seguir gera a latência média de leitura usando a Matemática de métricas do CloudWatch:</p> $(\text{Sum}(\text{VolumeTotalReadTime}) / \text{Sum}(\text{VolumeReadOps})) \times 1000$ <p>As métricas <code>VolumeTotalReadTime</code> e <code>VolumeReadOps</code> estão disponíveis no console do EBS CloudWatch.</p>
Latência média de gravação (ms/operação)	$\text{Avg}(\text{VolumeTotalWriteTime}) \times 1000$ <p>Para as instâncias baseadas em Nitro, a fórmula a seguir gera a latência média de gravação usando a Matemática de métricas do CloudWatch:</p> $(\text{Sum}(\text{VolumeTotalWriteTime}) / \text{Sum}(\text{VolumeWriteOps})) * 1000$ <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.

Como monitorar volumes com verificações de status

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).

Se a consistência de um volume específico não for uma preocupação para você, e você preferir que o volume seja disponibilizado imediatamente se estiver danificado, você poderá substituir o comportamento padrão configurando o volume para permitir E/S automaticamente. Se você ativar o atributo de volume `AutoEnableIO`, a verificação de status de volume continuará sendo aprovada. Além disso, você verá um evento que permite que você saiba 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 do desempenho de E/S compara o desempenho do volume real com o desempenho esperado de um volume, e alerta você se o volume estiver executando abaixo das expectativas. Esta verificação de status está disponível somente para volumes de `io1` que são anexados a uma instância e não são válidos para volumes de Finalidade geral (SSD) (`gp2`), Disco rígido com throughput otimizado (`st1`), Cold HDD (`sc1`) ou Magnético (`standard`). A verificação do status do desempenho de E/S é executada após cada minuto, e o CloudWatch coleta esses dados a cada cinco minutos, portanto, pode demorar até cinco minutos depois da anexação do volume de `io1` a uma instância para que essa verificação relate o status do desempenho de E/S.

Important

Durante a inicialização dos volumes de `io1` que foram restaurados de snapshots, o desempenho do volume pode ser reduzido 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. Isso é esperado, e você pode ignorar o estado de `warning` em volumes `io1` enquanto estiver inicializando esses volumes. Para obter mais informações, consulte [Inicialização de volumes do Amazon EBS \(p. 939\)](#).

A tabela a seguir lista os status dos volumes do Amazon EBS.

Status dos volumes	Status de E/S habilitado	Status do desempenho de E/S (disponível somente para volumes de IOPS provisionados)
<code>ok</code>	Habilitado (E/S habilitada ou E/S habilitada automaticamente)	Normal (o desempenho do volume é o esperado)
<code>warning</code>	Habilitado (E/S habilitada ou E/S habilitada automaticamente)	Degrado (o desempenho do volume está abaixo das expectativas) Seramente degradado (o desempenho do volume está muito abaixo das expectativas)
<code>impaired</code>	Habilitado (E/S habilitada ou E/S habilitada automaticamente) Desabilitado (o volume está offline e com recuperação pendente ou está aguardando o usuário habilitar a E/S)	Paralisado (o desempenho do volume está severamente impactado) Não disponível (incapaz de determinar o desempenho da E/S porque a E/S é desabilitada)

Status dos volumes	Status de E/S habilitado	Status do desempenho de E/S (disponível somente para volumes de IOPS provisionados)
insufficient-data	Habilitado (E/S habilitada ou E/S habilitada automaticamente) Dados insuficientes	Dados insuficientes

Para visualizar e trabalhar com verificações de status, você pode usar o console, a API ou a interface da linha de comando do Amazon EC2.

Para visualizar as verificações de status no console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Volumes.
3. Na página EBS Volumes, a coluna Volume Status lista os status operacional de cada volume.
4. Para visualizar o status de um volume individual, selecione o volume e escolha Status Checks.

Volumes: vol-d882c69b

⚠️ IO operations have been disabled since 16 hours and 58 minutes ago ago. Data inconsistencies may occur.

Description Status Checks Monitoring Tags

Volume Status impaired

IO Status Disabled

Since December 23, 2013 7:06:41 PM UTC+2

Description Awaiting Action: Enable IO

Auto-Enabled IO Disabled [Edit](#)

[Find out more](#) about working with volume status checks and events.
If you need technical assistance with your volume, post your issue to the [Developer Forums](#) or visit our [Support forums](#).

5. Se você tiver um volume com uma verificação de status com falha (o status for impaired), consulte [Como trabalhar com um volume danificado \(p. 877\)](#).

Como alternativa, você pode usar o painel Events para visualizar todos os eventos de suas instâncias e volumes em um único painel. Para obter mais informações, consulte [Como monitorar os eventos de volumes \(p. 876\)](#).

Para visualizar informações de status de volumes com a linha de comando

Você pode usar um dos seguintes comandos para visualizar o status de seus volumes do Amazon EBS. Para obter mais informações sobre essas interfaces de linha de comando, consulte [Acessando o Amazon EC2 \(p. 3\)](#).

- [describe-volume-status](#) (AWS CLI)

- [Get-EC2VolumeStatus](#) (AWS Tools para Windows PowerShell)

Como monitorar os eventos de volumes

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 `AutoEnableIO`. Para obter mais informações sobre como alterar esse atributo, consulte [Como trabalhar com um volume danificado \(p. 877\)](#).

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:

Esperando a ação: habilitar E/S

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.

E/S habilitada

As operações de E/S foram habilitadas explicitamente para esse volume.

E/S habilitada automaticamente

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

Para volumes de `io1` somente. O desempenho do volume é o esperado.

Reduzido

Para volumes de `io1` somente. O desempenho do volume está abaixo das expectativas.

Severamente degradado

Para volumes de `io1` somente. O desempenho do volume está muito abaixo das expectativas.

Paralisado

Para volumes de `io1` somente. O desempenho do volume está severamente impactado.

Você pode visualizar eventos de seus volumes usando o console do Amazon EC2 a API ou a interface da linha de comando.

Para visualizar os eventos de seus volumes no console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Events.
3. Todas as instâncias e volumes que têm eventos são listados. 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.

Actions ▾

Filter: Volume resources ▾ All event types ▾ Ongoing and scheduled ▾ Search Events

	Resource Name	Resource Type	Resource Id	Availability Zone	Event Type	Event Status
<input type="checkbox"/>	volume	vol-0381c540	us-east-1d	potential-data-i...	Awa...	Waiting Action: Enable IO
<input checked="" type="checkbox"/>	volume	vol-3682c675	us-east-1d	potential-data-i...	Awa...	Waiting Action: Enable IO

Event: vol-3682c675

A IO operations have been disabled since 30 days, 15 hours and 22 minutes ago. Data inconsistency detected.

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](#).

Se você tiver um volume com a E/S desabilitada, consulte [Como trabalhar com um volume danificado \(p. 877\)](#). Se você tiver um volume em que o desempenho 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.).

Para visualizar eventos de volumes 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 [Acessando o Amazon EC2 \(p. 3\)](#).

- [describe-volume-status](#) (AWS CLI)
- [Get-EC2VolumeStatus](#) (AWS Tools para Windows PowerShell)

Como trabalhar com um volume danificado

Esta seção aborda opções para quando um volume está danificado devido aos dados do volume estarem potencialmente inconsistentes.

Opções

- [Opção 1: Executar uma verificação de consistência no volume anexado a sua instância \(p. 878\)](#)
- [Opção 2: Executar uma verificação de consistência no volume usando outra instância \(p. 879\)](#)
- [Opção 3. Excluir o volume se não precisar mais dele \(p. 880\)](#)

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.
 - a. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
 - b. No painel de navegação, escolha Volumes.
 - c. Selecione o volume no qual habilitar as operações de E/S.
 - d. No painel de detalhes, escolha Enable Volume IO.

Volumes: vol-d882c69b

Description	Status Checks	Monitoring	Tags
<p>! IO operations have been disabled since 16 hours and 58 minutes ago ago. Data inconsistency may occur.</p>			
Volume ID	vol-d882c69b		
Capacity	100 GiB		
Created	November 21, 2013 3:42:01 PM UTC+2		
State	available		
Volume type	io1		
Product codes	-		

- e. Em Enable Volume IO, escolha Yes, Enable.
3. Verifique os dados no volume.
 - a. Execute o comando fsck.
 - b. (Opcional) Analise todos os logs disponíveis do aplicativo ou do sistema para verificar se há mensagens de erro relevantes.
 - c. Se o volume estiver danificado por mais de 20 minutos você poderá entrar em contato com o suporte. Escolha Troubleshoot e, em seguida, na caixa de diálogo Troubleshoot Status Checks, escolha Contact Support para enviar um caso de suporte.

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 [Acessando o Amazon EC2 \(p. 3\)](#).

- [enable-volume-io \(AWS CLI\)](#)

- [Enable-EC2VolumeIO](#) (AWS Tools para Windows PowerShell)

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 todos os aplicativos.
2. Desanexe o volume da instância.
 - a. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
 - b. No painel de navegação, escolha Volumes.
 - c. Selecione volume a ser desanexado.
 - d. Escolha Actions, Force Detach Volume. Será solicitada uma confirmação.
3. Habilite a E/S no volume.
 - a. No painel de navegação, escolha Volumes.
 - b. Selecione o volume que você desanexou na etapa anterior.
 - c. No painel de detalhes, escolha Enable Volume IO.

Volumes: vol-d882c69b

Description	Status Checks	Monitoring	Tags
<p>⚠ IO operations have been disabled since 16 hours and 58 minutes ago ago. Data inconsistency may occur.</p>			
Volume ID	vol-d882c69b		
Capacity	100 GiB		
Created	November 21, 2013 3:42:01 PM UTC+2		
State	available		
Volume type	io1		
Product codes	-		

- d. Na caixa de diálogo Enable Volume IO, escolha Yes, Enable.
4. Anexe o volume a outra instância. Para obter informações, consulte [Executar sua instância \(p. 390\)](#) e [Associação de um volume do Amazon EBS a uma instância \(p. 863\)](#).
5. Verifique os dados no volume.
 - a. Execute o comando fsck.
 - b. (Opcional) Analise todos os logs disponíveis do aplicativo ou do sistema para verificar se há mensagens de erro relevantes.
 - c. Se o volume estiver danificado por mais de 20 minutos, você poderá entrar em contato com o suporte. Escolha Troubleshoot e, em seguida, na caixa de diálogo de solução de problemas, escolha Contact Support para enviar um caso de suporte.

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 [Acessando o Amazon EC2 \(p. 3\)](#).

- [enable-volume-io](#) (AWS CLI)
- [Enable-EC2VolumeIO](#) (AWS Tools para Windows PowerShell)

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 [Exclusão de um volume do Amazon EBS \(p. 895\)](#).

Se você tiver um snapshot recente que faça o backup dos dados no volume, você poderá criar um novo volume do snapshot. Para obter informações sobre como criar um novo volume de um snapshot, consulte [Restauração de um volume do Amazon EBS a partir de um snapshot \(p. 861\)](#).

Como trabalhar com o atributo de volume AutoEnableIO

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 para você, e você preferir que o volume seja disponibilizado imediatamente se estiver `impaired`, você poderá substituir o comportamento padrão configurando o volume para permitir E/S automaticamente. Se você ativar o atributo de volume `AutoEnableIO`, E/S entre o volume e a instância serão reativados automaticamente 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 [Como monitorar os eventos de volumes \(p. 876\)](#).

Esta seção explica como exibir e modificar o atributo `AutoEnableIO` de um volume usando o console do Amazon EC2, a interface da linha de comando ou a API.

Para visualizar o atributo AutoEnableIO de um volume no 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.
4. No painel inferior, escolha Status Checks.
5. Na guia Status Checks, Auto-Enable IO exibe a configuração atual do volume, `Enabled` ou `Disabled`.

Volumes: vol-d882c69b

A IO operations have been disabled since 16 hours and 58 minutes ago ago. Data inconsistencies may occur.

Description Status Checks Monitoring Tags

Volume Status Impaired

IO Status Disabled

Since December 23, 2013 7:06:41 PM UTC+2

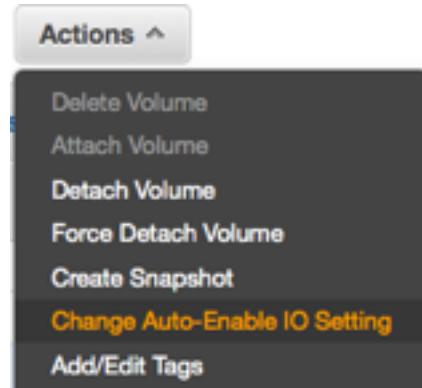
Description Awaiting Action: Enable IO

Auto-Enabled IO Disabled [Edit](#)

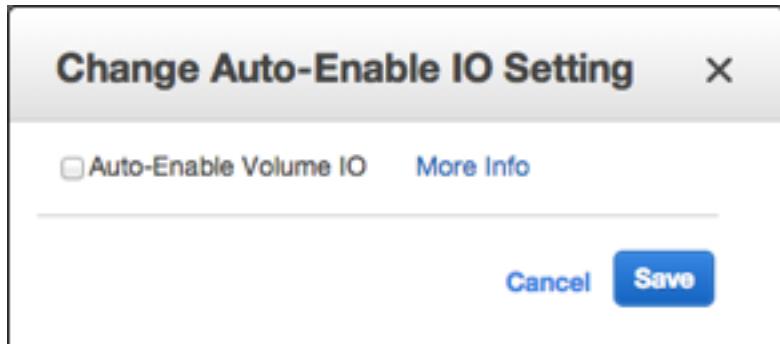
[Find out more](#) about working with volume status checks and events.
If you need technical assistance with your volume, post your issue to the [Developer Forums](#) or visit our [Support forums](#).

Para modificar o atributo AutoEnableIO de um volume no 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.
4. Na parte superior da página Volumes, escolha Actions.
5. Escolha Change Auto-Enable IO Setting.



6. Na caixa de diálogo Change Auto-Enable IO Setting, selecione a opção Auto-Enable Volume IO para habilitar a E/S automaticamente para um volume danificado. Para desabilitar o recurso, limpe a opção.



7. Escolha Salvar.

Como alternativa, em vez de concluir as etapas 4 a 6 no procedimento anterior, escolha Status Checks, Edit.

Para visualizar ou modificar o atributo AutoEnableIO de um volume com a linha de comando

Você pode usar um dos seguintes comandos para visualizar o atributo AutoEnableIO dos volumes do Amazon EBS. Para obter mais informações sobre essas interfaces de linha de comando, consulte [Acessando o Amazon EC2 \(p. 3\)](#).

- [describe-volume-attribute](#) (AWS CLI)
- [Get-EC2VolumeAttribute](#) (AWS Tools para Windows PowerShell)

Para modificar o atributo AutoEnableIO de um volume, você pode usar um dos comandos a seguir.

- [modify-volume-attribute](#) (AWS CLI)
- [Edit-EC2VolumeAttribute](#) (AWS Tools para Windows PowerShell)

Como modificar o tamanho, o desempenho ou o tipo de um volume do EBS

É possível aumentar o tamanho do volume, alterar o tipo de volume ou ajustar o desempenho 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 seu aplicativo 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 [Definição de preço do Amazon EBS](#).

Tópicos

- [Requisitos ao modificar volumes \(p. 882\)](#)
- [Como solicitar modificações em seus volumes do EBS \(p. 884\)](#)
- [Monitoramento do progresso das modificações de volume \(p. 887\)](#)
- [Como estender um sistema de arquivos Linux após um redimensionamento de volume \(p. 890\)](#)

Requisitos ao modificar volumes

Os seguintes requisitos e limitações se aplicam quando você modifica um volume do Amazon EBS. Este tópico da seção descreve os requisitos gerais aplicáveis a todos os volumes do EBS, bem como

os requisitos associados ao seu sistema operacional. Para obter mais informações, consulte [Limites de tamanho e configuração de um volume do EBS](#).

Supporte de instância do Amazon EC2

Elastic Volumes são compatíveis com as seguintes instâncias:

- Todas as [instâncias da geração atual \(p. 177\)](#)
- Famílias de instâncias da geração anterior C1, C3, CC2, CR1, G2, I2, M1, M3 e R3

Se o tipo de instância não oferecer suporte a Elastic Volumes, consulte [Como modificar um volume do EBS se não houver suporte para Elastic Volumes \(p. 887\)](#).

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 AMI 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
```

Limitações

- O novo tamanho do volume não pode exceder a capacidade de volume suportada. Para obter mais informações, consulte [Limites de tamanho e configuração de um volume do EBS \(p. 857\)](#).
- Se o volume foi anexado antes de 2 de novembro de 2016, você deve inicializar o suporte aos Elastic Volumes. Para obter mais informações, consulte [Como inicializar o suporte aos Elastic Volumes \(p. 885\)](#).

- Se você estiver usando um tipo de instância da geração anterior incompatível, ou se encontrar um erro ao tentar uma modificação de volume, consulte [Como modificar um volume do EBS se não houver suporte para Elastic Volumes \(p. 887\)](#).
- Um volume do gp2 anexado a uma instância como um volume raiz não pode ser modificado para um volume do st1 ou sc1. Se desanexado e modificado para st1 ou sc1, não poderá ser anexado a uma instância como o volume raiz.
- Um volume do gp2 não poderá ser modificado para um volume st1 ou sc1 se o tamanho do volume solicitado estiver abaixo do tamanho mínimo dos volumes st1 e sc1.
- Em alguns casos, você deve desanexar o volume ou interromper a instância para a modificação ter continuidade. 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 (inicialização), pare a instância, aplique as modificações e reinicie a instância.
- Após provisionar mais de 32,000 IOPSs em um volume io1 existente, pode ser necessário proceder de uma das seguintes formas para ver as melhorias completas no desempenho:
 - Desanexar e anexar o volume.
 - Reinicie a instância.
- Não há compatibilidade para 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 aplicativo, como rsync.
- Depois de modificar um volume, aguarde pelo menos seis horas e garanta que o volume esteja no estado `in-use` ou `available` antes de realizar mais modificações ao mesmo volume.
- Embora as instâncias do m3.medium ofereçam total suporte à modificação de volumes, algumas instâncias do m3.large, do m3.xlarge e do m3.2xlarge podem não oferecer suporte a todos os recursos de modificação de volume. Se você detectar um erro, consulte ???.

Como solicitar modificações em seus volumes do EBS

Com os Elastic Volumes, é possível modificar dinamicamente o tamanho, o desempenho e o tipo de volume dos seus volumes do Amazon EBS sem desanexá-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 [Como criar um snapshot do Amazon EBS](#).
2. Solicite a modificação do volume.
3. Monitore o progresso da modificação do volume. Para obter mais informações, consulte [Monitoramento do progresso das modificações de volume \(p. 887\)](#).
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 [Como estender um sistema de arquivos Linux após um redimensionamento de volume \(p. 890\)](#).

Tópicos

- [Como modificar um volume do EBS usando Elastic Volumes \(console\) \(p. 885\)](#)
- [Como modificar um volume do EBS usando Elastic Volumes \(AWS CLI\) \(p. 885\)](#)
- [Como inicializar o suporte aos Elastic Volumes \(se necessário\) \(p. 885\)](#)
- [Como modificar um volume do EBS se não houver suporte para Elastic Volumes \(p. 887\)](#)

Como modificar um volume do EBS usando Elastic Volumes (console)

Use o procedimento a seguir para modificar um volume do EBS.

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 Modificar volume exibe o ID de volume e a configuração atual do volume, incluindo tipo, tamanho e IOPS. Você pode alterar qualquer uma dessas configurações, ou todas elas, em uma única ação. 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 valor inteiro permitido para Tamanho.
 - Se você escolher Provisioned IOPS SSD (io1) (IOPS provisionadas [io1]) como o tipo de volume, insira um valor inteiro permitido para IOPS.
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 [Como estender um sistema de arquivos Linux após um redimensionamento de volume \(p. 890\)](#).

Como modificar um volume do EBS usando Elastic Volumes (AWS CLI)

Use o comando `modify-volume` para modificar uma ou mais definições de configuração de um volume. Por exemplo, se você tiver um volume do tipo gp2 com um tamanho de 100 GiB, o comando a seguir alterará a configuração para um volume do tipo io1 com 10.000 IOPS e um tamanho de 200 GiB.

```
aws ec2 modify-volume --volume-type io1 --iops 10000 --size 200 --volume-id vol-1111111111111111
```

A seguir está um exemplo de saída:

```
{  
    "VolumeModification": {  
        "TargetSize": 200,  
        "TargetVolumeType": "io1",  
        "ModificationState": "modifying",  
        "VolumeId": "vol-1111111111111111",  
        "TargetIops": 10000,  
        "StartTime": "2017-01-19T22:21:02.959Z",  
        "Progress": 0,  
        "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 [Como estender um sistema de arquivos Linux após um redimensionamento de volume \(p. 890\)](#).

Como inicializar o suporte aos Elastic Volumes (se necessário)

Antes que você possa modificar um volume que foi anexado a uma instância antes de 1º de novembro de 2016, é necessário inicializar o suporte à modificação de volumes usando uma das ações a seguir:

- Desanexar e anexar o volume
- Reinicie a instância

Use um dos procedimentos a seguir para determinar se suas instâncias estão prontas para modificação de volume.

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:2
i-719f99a8	December 8, 2016 at 2:21:51 PM UTC-8	/dev/xvda=vol-bad60e7a:attached:2
i-006b02c1b78381e57	May 17, 2017 at 1:52:52 PM UTC-7	/dev/sda1=vol-0de9250441c73024c
i-e3d172ed	May 17, 2017 at 2:48:54 PM UTC-7	/dev/sda1=vol-04c34d0b:attached:2

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 1º de novembro de 2016.

```
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
```

Como 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, o desempenho 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 [Como estender um sistema de arquivos Linux após um redimensionamento de volume \(p. 890\)](#).

Monitoramento do 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. É raro uma falha transitória na AWS resultar no estado `failed`. Se isso ocorrer, tente novamente a modificação do volume.

Quando o volume está no estado `optimizing`, seu desempenho de volume está entre as especificações de configuração de origem e de destino. O desempenho de volume transitório não será menor que o desempenho de volume de origem. Se você está fazendo downgrade do IOPS, o desempenho do volume transitório não é inferior ao desempenho 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 de o volume entrar no estado `Optimizing`.
- As alterações de desempenho (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 surtir efeito 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 desempenho.

Use um dos métodos a seguir para monitorar o progresso de uma modificação de volume.

Tópicos

- [Como monitorar o progresso de uma modificação de volume \(console\) \(p. 887\)](#)
- [Como monitorar o progresso de uma modificação de volume \(AWS CLI\) \(p. 888\)](#)
- [Como monitorar o progresso de uma modificação de volume \(Eventos do CloudWatch\) \(p. 889\)](#)

[Como monitorar o progresso de uma modificação de volume \(console\)](#)

Use o procedimento a seguir para visualizar o progresso de uma ou mais modificações de volume.

Para monitorar o progresso de uma modificação 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 o volume. O status do volume é exibido na coluna State (Estado) e no campo State (Estado) do painel de detalhes. Neste exemplo, o estado da modificação é completed (concluído).
4. Abra o ícone de informações ao lado do campo State (Estado) para exibir antes e depois de as informações sobre a ação de modificação mais recente, conforme mostrado neste exemplo.

The screenshot shows the AWS EC2 Volume Details page for a volume with ID vol-065fc28c... The volume is 1000 GiB, gp2 type, and has 3000 IOPS. It was created on January 25, 2017. The 'Description' tab is selected, showing the following details:

Volume ID	vol-065fc28c...
Size	1000 GiB
Created	January 25, 2017 at 4:26:36 PM UTC-8
State	available - completed (100%)

Attachment information:

Volume type	gp2
Product codes	-
IOPS	3000

A modal window titled "Volume modification detail" is open, showing the original and target configurations for the volume:

Original Volume Type	gp2
Original Size	1000 GiB
Original IOPS	3000
Target Volume Type	gp2
Target Size	1000 GiB
Target IOPS	3000
Status message	-

Como monitorar o progresso de uma modificação de volume (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-id vol-1111111111111111 vol-2222222222222222
```

Na saída de exemplo a seguir, as modificações de volume ainda estão no estado `modifying`.

```
{  
    "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"  
    }  
]
```

Como monitorar o progresso de uma modificação de volume (Eventos do CloudWatch)

Com o Eventos do CloudWatch, 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.

Para monitorar o progresso de uma modificação usando Eventos do CloudWatch

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"  
        ]  
    }  
}
```

A seguir, um exemplo de um evento típico:

```
Body:  
{  
    "version": "0",  
    "id": "1ea2ace2-7790-46ed-99ab-d07a8bd68685",  
    "detail-type": "EBS Volume Notification",  
    "source": "aws.ec2",  
    "account": "065441870323",  
    "time": "2017-01-12T21:09:07Z",  
    "region": "us-east-1",  
    "resources": [  
        "arn:aws:ec2:us-east-1:065441870323:volume/vol-03a55cf56513fa1b6"  
    ],  
    "detail": {  
        "result": "optimizing",  
        "cause": "",  
        "event": "modifyVolume",  
        "request-id": "auto-58c08bad-d90b-11e6-a309-b51ed35473f8"  
    }  
}
```

Como estender um sistema de arquivos Linux após um redimensionamento de volume

Depois de aumentar o tamanho de um volume do EBS, você deve 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 voltar suas alterações. Para obter mais informações, consulte [Criação de um snapshot do Amazon EBS \(p. 898\)](#).

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.

Para as tarefas a seguir, suponha que você tenha redimensionado o volume de inicialização de uma instância de 8 GB para 16 GB e um volume adicional de 8 GB para 30 GB.

Tarefas

- [Como identificar o sistema de arquivos de um volume \(p. 891\)](#)
- [Como estender uma partição \(se necessário\) \(p. 891\)](#)
- [Como estender o sistema de arquivo \(p. 892\)](#)

Como identificar o sistema de arquivos de um volume

Para verificar o sistema de arquivos em uso para cada volume em sua instância, [conecte-se à sua instância \(p. 439\)](#) e execute o comando file -s.

Example Exemplo: sistemas de arquivos em uma instância baseada em Nitro

O exemplo a seguir mostra uma [instância baseada em Nitro \(p. 179\)](#) que tem um volume de inicialização com um sistema de arquivos XFS e um volume adicional com um sistema de arquivos XFS.

```
[ec2-user ~]$ sudo file -s /dev/nvme?n*
/dev/nvme0n1:      x86 boot sector ...
/dev/nvme0n1p1:    SGI XFS filesystem data ...
/dev/nvme0n1p128:  data
/dev/nvme1n1:      SGI XFS filesystem data ...
```

Example Exemplo: sistemas de arquivos em uma instância T2

O exemplo a seguir mostra uma instância T2 que tem um volume de inicialização com um sistema de arquivos ext4 e um volume adicional com um sistema de arquivos XFS.

```
[ec2-user ~]$ sudo file -s /dev/xvd*
/dev/xvda:  DOS/MBR boot sector ..
/dev/xvda1: Linux rev 1.0 ext4 filesystem data ...
/dev/xvdf:  SGI XFS filesystem data ...
```

Como estender uma partição (se necessário)

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.

Use o comando lsblk para exibir informações sobre os dispositivos de blocos anexados à sua instância. Se um volume redimensionado tiver uma partição e a partição não refletir o novo tamanho do volume, use o comando growpart para estender a partição. Para obter informações sobre como estender uma partição do LVM, consulte [Estender um volume lógico](#).

Example Exemplo: partições em uma instância baseada em Nitro

O exemplo a seguir mostra os volumes em uma instância baseada em Nitro:

```
[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
```

- 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.

Para estender a partição no volume raiz, use o seguinte comando growpart. Observe que há um espaço entre o nome do dispositivo e o número da partição.

```
[ec2-user ~]$ sudo growpart /dev/nvme0n1 1
```

Você pode verificar se a partição reflete o aumento do tamanho do volume usando o comando lsblk novamente.

```
[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
```

Example Exemplo: partições em uma instância T2

O exemplo a seguir mostra os volumes em uma instância T2:

```
[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
```

- 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.

Para estender a partição em cada volume, use os seguintes comandos growpart. 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
```

Você pode verificar se as partições refletem o aumento do tamanho do volume usando o comando lsblk novamente.

```
[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
```

Como estender o sistema de arquivo

Use o comando específico do sistema de arquivos para redimensionar cada sistema de arquivos de acordo com a capacidade do novo volume. Para um sistema de arquivos diferente dos exemplos mostrados aqui, consulte a documentação do sistema de arquivos para obter instruções.

Example Exemplo: estenda um sistema de arquivos ext2, ext3 ou ext4

Use o comando df -h para verificar o tamanho do sistema de arquivos de cada volume. Neste exemplo, /dev/xvda1 e /dev/xvdf refletem o tamanho original dos volumes, 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
...
```

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
```

Você pode verificar se cada sistema de arquivos reflete o aumento do tamanho do volume usando o comando `df -h` novamente.

```
[ec2-user ~]$ df -h
Filesystem      Size  Used Avail Use% Mounted on
/dev/xvda1       16G  1.9G  6.2G  12% /
/dev/xvdf1       30G   45M  8.0G   1% /data
...
```

Example Exemplo: estender um sistema de arquivos XFS

Use o comando `df -h` para verificar o tamanho do sistema de arquivos de cada volume. Neste exemplo, cada sistema de arquivos reflete 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    30G   33M  8.0G   1% /data
...
```

Para estender o sistema de arquivos XFS, instale as ferramentas XFS da seguinte maneira, se elas ainda não estiverem instaladas.

```
[ec2-user ~]$ sudo yum install xfsprogs
```

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
```

Você pode verificar se cada sistema de arquivos reflete o aumento do tamanho do volume usando o comando `df -h` novamente.

```
[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
...
```

Separação de um volume do Amazon EBS de uma instância

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.

Quando um volume com o código de produto AWS Marketplace é destacado de uma instância, ele não estará mais associado à instância.

Important

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 [Exclusão de um volume do Amazon EBS \(p. 895\)](#).

Este exemplo desmonta o volume e o separa explicitamente da instância. Isso é útil quando você deseja encerrar uma instância ou associar um volume a uma instância diferente. Para verificar se o volume não está mais associado à instância, consulte [Como visualizar informações sobre um volume do Amazon EBS \(p. 867\)](#).

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.

Para separar um volume do EBS usando o console

1. Use o comando a seguir para desmontar o dispositivo /dev/sdh.

```
[ec2-user ~]$ umount -d /dev/sdh
```

2. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
3. No painel de navegação, escolha Volumes.
4. Selecione um volume e escolha Ações, Separar volume.
5. Na caixa de diálogo de confirmação, escolha Sim, separar.

Para separar um volume do EBS 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 [Acessando o Amazon EC2 \(p. 3\)](#).

- [detach-volume](#) (AWS CLI)
- [Dismount-EC2Volume](#) (AWS Tools para Windows PowerShell)

Solução de problemas

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 separar 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 tiver tentado forçar o volume a separar várias vezes durante vários minutos e ele ficar no estado `detaching`, pode publicar uma solicitação de ajuda no [Amazon EC2 forum](#). 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:

```
aws ec2 describe-volumes --region us-west-2 --volume-ids vol-1234abcd
{
    "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.

Exclusão de um volume do 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.

Para excluir um volume, ele deve estar no estado `available` (não associado a uma instância). Para obter mais informações, consulte [Separação de um volume do Amazon EBS de uma instância \(p. 893\)](#).

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.
4. Na caixa de diálogo de confirmação, escolha Yes, Delete.

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 [Acessando o Amazon EC2 \(p. 3\)](#).

- `delete-volume` (AWS CLI)
- `Remove-EC2Volume` (AWS Tools para Windows PowerShell)

Solutions 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. Ao excluir um snapshot, somente os dados exclusivos desse snapshot serão removidos. 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 de forma lenta 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 [Criação de um snapshot do Amazon EBS \(p. 898\)](#).

É possível acompanhar o status de seus snapshots do EBS pelo Eventos do CloudWatch. Para obter mais informações, consulte [Eventos do Amazon CloudWatch para Amazon EBS](#).

Tópicos

- [Como funcionam os snapshots incrementais \(p. 896\)](#)
- [Cópia e compartilhamento de snapshots \(p. 898\)](#)
- [Suporte a criptografia para snapshots \(p. 898\)](#)
- [Criação de um snapshot do Amazon EBS \(p. 898\)](#)
- [Exclusão de um snapshot do Amazon EBS \(p. 900\)](#)
- [Cópia de um snapshot do Amazon EBS \(p. 902\)](#)
- [Exibição de informações do snapshot da Amazon EBS \(p. 904\)](#)
- [Compartilhamento de um snapshot do Amazon EBS \(p. 905\)](#)
- [Automação do ciclo de vida de snapshot do Amazon EBS \(p. 907\)](#)

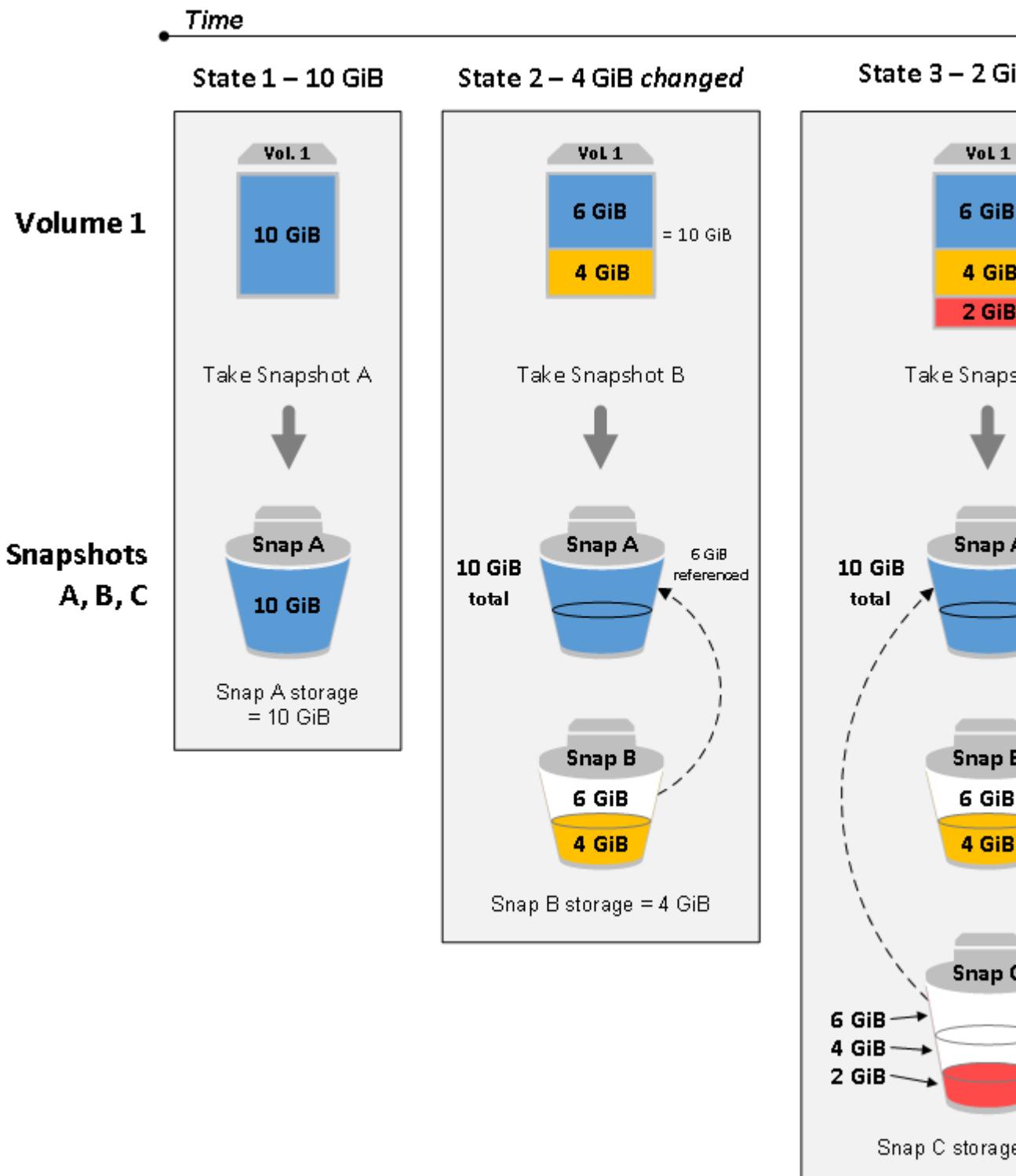
Como funcionam os snapshots incrementais

Esta seção traz ilustrações de como um snapshot do EBS captura o estado de um volume em um ponto no tempo, e também como snapshots sucessivos de um volume em constante mudança criam um histórico dessas alterações.

No diagrama abaixo, Volume 1 é mostrado em três pontos no tempo. Um snapshot é retirado de cada um desses três estados de volumes.

- 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, para um total de 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 múltiplos snapshots de um volume



Para obter mais informações sobre como os dados são gerenciados ao excluir um snapshot, consulte [Exclusão de um snapshot do Amazon EBS \(p. 900\)](#).

Cópia e compartilhamento de 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 [Compartilhamento de um snapshot do Amazon EBS \(p. 905\)](#).

Um snapshot é restrito à região onde 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 [Restauração de um volume do Amazon EBS a partir de um snapshot \(p. 861\)](#). 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 [Cópia de um snapshot do Amazon EBS \(p. 902\)](#).

Suporte a criptografia para snapshots

Os snapshots do EBS oferecem amplo suporte à criptografia do EBS.

- Snapshots de volumes criptografados são criptografados automaticamente.
- Os volumes criados a partir de snapshots criptografados são criptografados automaticamente.
- 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, pode recriptografá-lo com uma chave diferente durante o processo de cópia.

Para obter mais informações, consulte [Criptografia do Amazon EBS](#).

Criação de um snapshot do Amazon EBS

Um snapshot de ponto no tempo de um volume do EBS pode ser usado como uma linha de base para novos volumes ou para backup de dados. Se você fizer snapshots periódicos de um volume, eles serão incrementais: somente os blocos no dispositivo que tiverem mudado depois do último snapshot serão salvos no novo snapshot. Mesmo que os snapshots sejam salvos incrementalmente, o processo de exclusão de snapshots foi projetado de forma que você precise reter somente o snapshot mais recente para restaurar o volume inteiro.

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.

Important

Embora você possa fazer um snapshot de um volume enquanto um snapshot anterior desse está no status `pending`, ter múltiplos snapshots `pending` de um volume pode resultar em desempenho reduzido do volume até o snapshot ser concluído.

Há um limite de cinco snapshots `pending` para um único volume `gp2`, `io1` ou Magnético, e um snapshot `pending` para um único volume `st1` ou `sc1`. Se você receber um erro `ConcurrentSnapshotLimitExceeded` ao tentar criar múltiplos snapshots simultâneos do mesmo volume, espere por um ou mais snapshots `pending` serem concluídos antes de criar outro snapshot desse volume.

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 do Amazon EBS](#).

Por padrão, só você pode criar volumes a partir dos snapshots que possui. Contudo, 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 [Compartilhamento de um snapshot do Amazon EBS \(p. 905\)](#).

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 então usar essa cópia para restaurar o volume. Sua cópia de um snapshot compartilhado e criptografado também pode ser recriptografada com uma chave diferente. Para obter mais informações, consulte [Compartilhamento de um snapshot do Amazon EBS \(p. 905\)](#).

Quando um snapshot for criado a partir de um volume com um código de produto AWS Marketplace, o código do produto será propagado para o snapshot.

Você pode tirar um snapshot de um volume associado 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 aplicativos 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. Você pode remontar e usar o volume enquanto o status do snapshot for pending.

Para criar um snapshot para volume do Amazon EBS que serve como dispositivo raiz, pare a instância antes de tirar o snapshot.

Para desmontar o volume no Linux, use o comando a seguir, onde `device_name` é o nome do dispositivo (por exemplo, `/dev/sdh`):

```
umount -d device_name
```

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 [Marcação dos seus recursos do Amazon EC2 \(p. 1003\)](#).

Para criar 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 Criar snapshot.
4. Na página Create Snapshot (Criar snapshot), selecione o volume para o qual criar um snapshot.
5. (Opcional) Selecione Add tags to your snapshot (Adicionar tags ao snapshot). Forneça uma chave e um valor para cada tag.
6. Selecione Criar snapshot.

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 [Acessando o Amazon EC2 \(p. 3\)](#).

- [create-snapshot](#) (AWS CLI)
- [New-EC2Snapshot](#) (AWS Tools para Windows PowerShell)

Exclusão de um snapshot do Amazon EBS

Ao excluir um snapshot, somente os dados mencionados exclusivamente por esse snapshot são removidos. A exclusão de snapshots anteriores de um volume não afeta sua capacidade para restaurar volumes de snapshots posteriores desse volume.

A exclusão de um snapshot de um volume não tem efeito sobre o volume. A exclusão de um volume não tem efeito sobre os snapshots feitos deles.

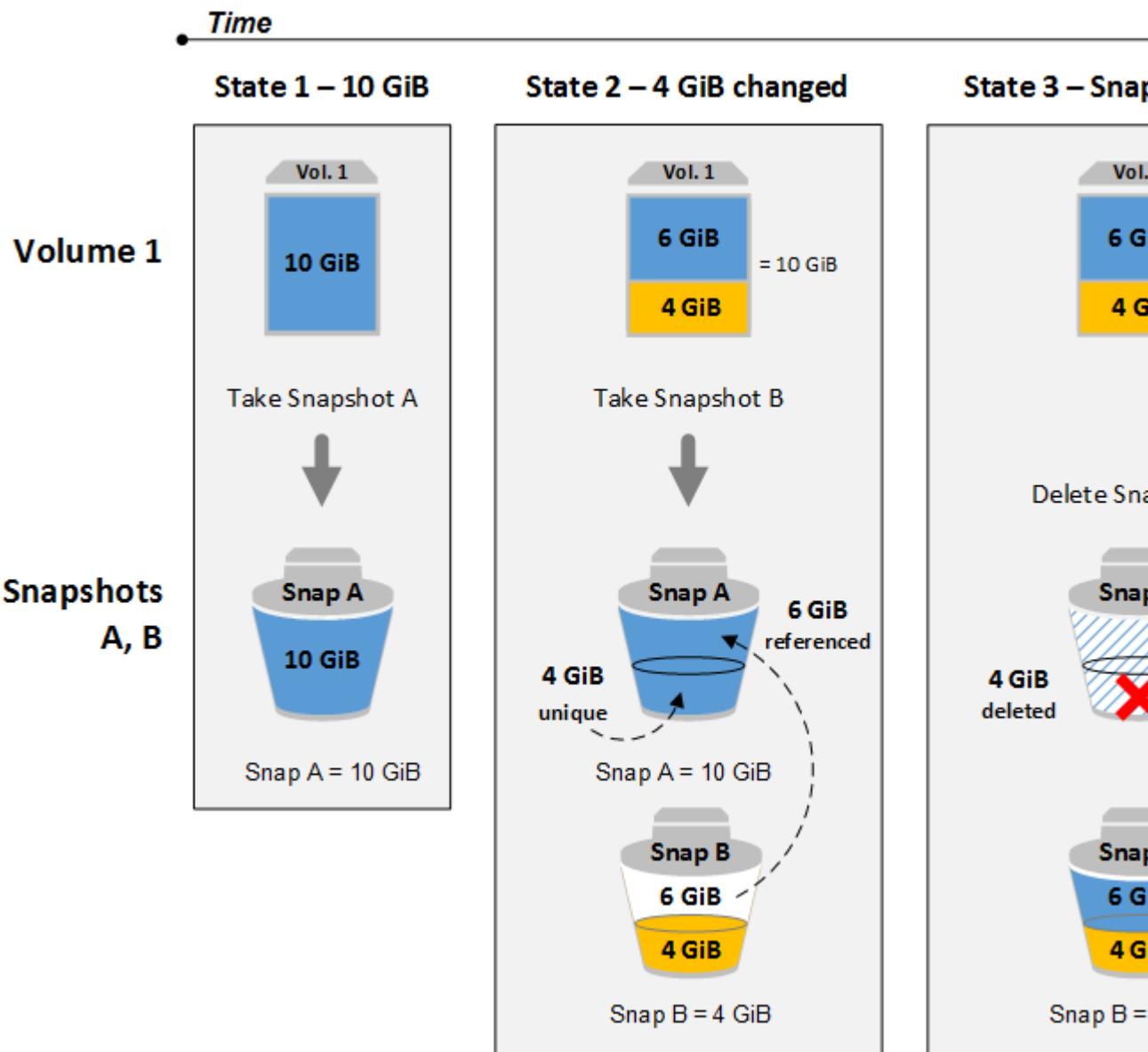
Se você fizer snapshots periódicos de um volume, eles serão incrementais, o que significa que somente os blocos no dispositivo que tiverem mudado depois do último snapshot serão salvos no novo snapshot. Mesmo que os snapshots sejam salvos incrementalmente, o processo de exclusão de snapshots foi projetado de forma que você precise reter somente o snapshot mais recente, a fim de restaurar o volume inteiro.

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. 896) e o exemplo abaixo.

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.

Exemplo 1: Exclusão de um snapshot com alguns de seus dados mencionados por outro snapshot



Observe que você não pode excluir um snapshot do dispositivo raiz de um volume do EBS suado por um AMI registrado. Você deve primeiro cancelar a AMI antes de excluir o snapshot. Para obter mais informações, consulte [Cancelar o registro da AMI do Linux \(p. 156\)](#).

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.

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 [Acessando o Amazon EC2 \(p. 3\)](#).

- [delete-snapshot](#) (AWS CLI)
- [Remove-EC2Snapshot](#) (AWS Tools para Windows PowerShell)

Note

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 demorar bastante tempo. Se você também estiver no limite simultâneo do snapshot (cinco snapshots em andamento) e tentar tirar um snapshot adicional, poderá obter o erro `ConcurrentSnapshotLimitExceeded`.

Cópia de 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 de criar um snapshot e finalizar a cópia no 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 no lado do servidor do Amazon S3 (AES de 256 bits) protege os dados em trânsito de um snapshot durante uma operação de cópia. A cópia do snapshot recebe um ID diferente do ID do snapshot original.

Para obter informações sobre como copiar um snapshot do Amazon RDS, consulte [Cópia de um DB Snapshot](#) no Guia do usuário da Amazon RDS.

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 [Compartilhamento de um snapshot do Amazon EBS \(p. 905\)](#).

Para obter informações de preços para cópias de snapshots entre regiões e contas, 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. A cópia de um snapshot para uma nova região gera novos custos de armazenamento.

Casos de uso

- **Expansão geográfica:** execute seus aplicativos em uma nova região.
- **Migração:** move um aplicativo 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 seus aplicativos 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 previamente não criptografado, altere a chave com a qual o snapshot foi criptografado ou, para snapshots criptografados compartilhados com você, crie uma cópia de sua propriedade para restaurar um volume a partir deles.
- **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.

Pré-requisitos

- 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.

Limites

- Cada conta pode ter até 5 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. Depois de a operação de cópia ser concluída, você poderá aplicar tags definidas pelo usuário para o novo snapshot. Para obter mais informações, consulte [Marcação dos seus recursos do Amazon EC2 \(p. 1003\)](#).
- Os snapshots criados pela ação `CopySnapshot` têm um ID arbitrário de volume que não deve ser usado para nenhuma outra finalidade.

Fazer cópias incrementais entre regiões

A primeira cópia do snapshot para outra região é sempre uma cópia completa. Para snapshots não criptografados, cada cópia subsequente do snapshot de mesmo volume é incremental, o que significa que a AWS copia somente os dados que foram alterados desde a última cópia do snapshot na mesma região de destino. Isso permite cópias mais rápidas e custos mais baixos de armazenamento.

No caso de snapshots criptografados, você deve criptografar a mesma CMK que foi usada, para que as cópias obtenham cópias incrementais. Os exemplos a seguir ilustram como isso funciona:

- Se você copiar um snapshot não criptografado da Leste dos EUA (Norte da Virgínia) para a Oeste dos EUA (Oregon), a primeira cópia do snapshot será uma cópia completa, e as cópias subsequentes dos snapshots de mesmo volume transferidas entre as mesmas regiões serão incrementais.
- Se você copiar um snapshot criptografado da região Leste dos EUA (Norte da Virgínia) para a Oeste dos EUA (Oregon), a primeira cópia do snapshot do volume será completa.
 - Se você criptografar o mesmo CMK em uma cópia subsequente do snapshot para o mesmo volume entre as mesmas regiões, a cópia será incremental.
 - Se você criptografar uma CMK diferente em uma cópia subsequente do snapshot de mesmo volume entre as mesmas regiões, a cópia será uma nova cópia completa do snapshot.

Para obter mais informações, consulte [Criptografar um snapshot para uma nova CMK](#).

Screenshots criptografados

Quando você copiar um snapshot, poderá optar por criptografar uma cópia (se o snapshot original não tiver sido criptografado) ou especificar um CMK diferente do original, e o snapshot copiado resultante usará o novo CMK. Contudo, a alteração do status de criptografia de um snapshot durante uma operação de cópia resulta em uma cópia (não adicional) 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 CMK própria. Isso o protegerá se a CMK original estiver comprometida ou se o proprietário revogá-la por algum motivo, o que pode fazer com que você perca o acesso aos volumes criptografados criados usando o snapshot. Para obter mais informações, consulte [Compartilhamento de um snapshot do Amazon EBS \(p. 905\)](#).

Cópia de um snapshot

Use o procedimento a seguir para copiar um snapshot usando o console do Amazon EC2.

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. Você não pode remover a criptografia de um snapshot criptografado.
 - Chave mestra: A chave mestra (CMK) do cliente que deve ser usada para criptografar esse snapshot. Você pode selecionar entre as chaves mestras da conta ou digitar/colar o ARN de uma chave de uma conta diferente. Você pode criar uma nova chave mestra de criptografia no console do IAM.
 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.

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. Por exemplo:

```
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 apresentado 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](#).

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 [Acessando o Amazon EC2 \(p. 3\)](#).

- [copy-snapshot](#) (AWS CLI)
- [Copy-EC2Snapshot](#) (AWS Tools para Windows PowerShell)

Exibição de informações do snapshot da Amazon EBS

Você pode visualizar informações detalhadas sobre seus snapshots.

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 pode filtrar os snapshots ainda mais usando as opções avançadas de pesquisa. Escolha a barra de pesquisa para ver os filtros disponíveis.
4. Para ver mais informações sobre um snapshot, selecione-o.

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 [Acessando o Amazon EC2 \(p. 3\)](#).

- [describe-snapshots \(AWS CLI\)](#)
- [Get-EC2Snapshot \(AWS Tools para Windows PowerShell\)](#)

Compartilhamento de um snapshot do Amazon EBS

Ao modificar as permissões de um snapshot, você poderá compartilhá-lo com as contas AWS que você especificar. Os usuários autorizados por você poderão usar os snapshots que você compartilhar como base para criar seus próprios volumes do EBS, ao passo que seu snapshot original não será afetado. Se você desejar, poderá disponibilizar os snapshots não criptografados publicamente para todos os usuários da AWS. Você não pode disponibilizar publicamente seus snapshots criptografados.

Quando compartilha um snapshot criptografado, você precisa compartilhar também a CMK personalizada usada para criptografar o snapshot. Você pode aplicar permissões entre contas a uma CMK personalizada quando ela é criada ou posteriormente.

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 com quem você deseja compartilhar todos os dados do snapshot.

Considerações

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. Para obter mais informações, consulte [Cópia de um snapshot do Amazon EBS \(p. 902\)](#).
- Se seu snapshot usar o formato de ID de recurso mais longo, você só poderá compartilhá-lo com outra conta que também oferecer suporte a IDs mais longos. Para obter mais informações, consulte [IDs de recursos](#).
- A AWS impede que você compartilhe snapshots criptografados com o CMK padrão. Os snapshots que você pretende compartilhar devem ser criptografados com um CMK personalizado. Para obter mais informações, consulte [Como criar chaves](#) no AWS Key Management Service Developer Guide.
- Os usuários com quem você compartilha sua CMK que estão acessando snapshots criptografados devem ter permissões para executar as seguintes ações na chave: `kms:DescribeKey`, `kms>CreateGrant`, `GenerateDataKey` e `kms:ReEncrypt`. Para obter mais informações, consulte [Controle de acesso às chaves mestras do cliente](#) no AWS Key Management Service Developer Guide.
- Se você tiver acesso a um snapshot criptografado compartilhado e quiser restaurar um volume a partir dele, deverá criar uma cópia pessoal do snapshot e usar essa cópia para restaurar o volume. Recomendamos que você recriptografe o snapshot durante o processo de cópia com uma chave diferente que você controle. Isso protegerá seu acesso ao volume se a chave original estiver comprometida ou se o proprietário revogar a chave por algum motivo.

Compartilhamento de um snapshot não criptografado usando o console

Para compartilhar 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 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.

Essa não é uma opção válida para snapshots criptografados ou snapshots com um código de produto do AWS Marketplace.

 - Para compartilhar o snapshot com uma ou mais contas da AWS, escolha Private (Privado), digite o ID da conta da AWS (sem hifen) em AWS Account Number (Número da conta da AWS) e escolha Add Permission (Adicionar permissão). Repita a ação para as contas adicionais da AWS.
5. Escolha Salvar.

Para usar um snapshot não criptografado que foi compartilhado comigo de forma privada

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. Selecione Snapshots no painel de navegação.
3. Escolha o filtro Private Snapshots (Snapshots privados).
4. Localize o snapshot pelo ID ou pela descrição. Você pode usar esse snapshot como usa qualquer outro; por exemplo, você pode criar um volume a partir do snapshot ou copiá-lo em outra região.

Compartilhamento de um snapshot criptografado usando o console

Para compartilhar um snapshot criptografado usando o console

1. Abra o console do IAM em <https://console.aws.amazon.com/iam/>.
2. Escolha Encryption keys (Chaves de criptografia) no painel de navegação.
3. Escolha o alias da chave personalizada usada para criptografar o snapshot.
4. Para cada conta da AWS, escolha Add External Accounts (Adicionar contas externas) e digite o ID de conta da AWS quando solicitado. Quando você adicionar todas as contas da AWS, escolha Save Changes (Salvar alterações).
5. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
6. Selecione Snapshots no painel de navegação.
7. Selecione o snapshot e, em seguida, escolha Actions (Ações), Modify Permissions (Modificar permissões).
8. Para cada conta da AWS, digite o ID da conta em AWS Account Number (Número da conta da AWS) e escolha Add Permission (Adicionar permissão). Quando você adicionar todas as contas da AWS, escolha Save (Salvar).

Para usar um snapshot criptografado que foi compartilhado comigo

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. Selecione Snapshots no painel de navegação.
3. Escolha o filtro Private Snapshots (Snapshots privados). Como alternativa, adicione o filtro Encrypted (Criptografado).
4. Localize o snapshot pelo ID ou pela descrição.
5. Recomendamos que você criptografe novamente o snapshot com uma chave diferente que seja sua. Isso o protegerá se a chave original estiver comprometida ou se o proprietário revogá-la por algum motivo, o que pode fazer com que você perca o acesso aos volumes criptografados criados a partir do snapshot.
 - a. Selecione o snapshot e escolha Actions (Ações), Copy (Copiar).

- b. (Opcional) Selecione uma região de destino.
- c. Selecione uma CMK personalizada que seja sua.
- d. Escolha Copiar.

Compartilhar um snapshot usando a linha de comando

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 modificar as permissões de snapshots usando a linha de comando

Use um dos seguintes comandos:

- [modify-snapshot-attribute](#) (AWS CLI)
- [Edit-EC2SnapshotAttribute](#) (AWS Tools para Windows PowerShell)

Para visualizar permissões de snapshots usando a linha de comando

Use um dos seguintes comandos:

- [describe-snapshot-attribute](#) (AWS CLI)
- [Get-EC2SnapshotAttribute](#) (AWS Tools para Windows PowerShell)

Para obter mais informações sobre essas interfaces de linha de comando, consulte [Acessando o Amazon EC2 \(p. 3\)](#).

Automação do ciclo de vida de snapshot do Amazon EBS

Você pode usar o Gerenciador de ciclo de vida de dados da Amazon (Amazon DLM) para automatizar a criação, retenção e exclusão de snapshots obtidos para fazer backup de seus volumes do Amazon EBS. A automação do gerenciamento de snapshots ajuda você a:

- Proteger dados valiosos impondo uma programação regular de backup.
- Reter os backups conforme exigido por auditores ou pelas regras de conformidade interna.
- Reduzir os custos de armazenamento ao excluir backup obsoletos.

Combinado com os recursos de monitoramento do Eventos do Amazon CloudWatch e do AWS CloudTrail, o Amazon DLM oferece uma solução completa de backup para volumes do EBS sem custo adicional.

Noções básicas do Amazon DLM

Veja a seguir os elementos principais que você deve compreender antes de começar a usar o Amazon DLM.

Screenshots

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 [Screenshots do Amazon EBS](#).

Tags de volume

O Amazon DLM usa tags de recursos para identificar os volumes do EBS para fazer backup. As tags são metadados personalizáveis que você pode atribuir aos recursos da AWS (inclusive a volumes do EBS e snapshots). Uma política do Amazon DLM (descrita abaixo) segmenta um volume para backup usando uma tag exclusiva. Várias tags podem ser atribuídas a um volume se você quiser executar várias políticas nele.

Não é possível usar o caractere “\” ou “=” em uma chave de tag.

Para mais informações sobre marcação de objetos do Amazon EC2, consulte [Como marcar seus recursos do Amazon EC2](#).

Tags de snapshot

O Amazon DLM aplica as seguintes tags a todos os snapshots criados por uma política a fim de distinguir os snapshots criados por outros meios:

- `aws:dlm:lifecycle-policy-id`
- `aws:dlm:lifecycle-schedule-name`

Você também pode especificar tags personalizadas para aplicar durante a criação de um snapshot.

Não é possível usar o caractere “\” ou “=” em uma chave de tag.

Todas as tags definidas pelo usuário em um volume de origem podem opcionalmente serem copiadas em snapshots criados por uma política.

Políticas de ciclo de vida

Uma política de ciclo de vida consiste nessas configurações principais:

- Tipo de recurso — o recurso da AWS gerenciado pela política; nesse caso, os volumes do EBS.
- Tag de destino — a tag que deve ser associada com o volume do EBS a ser gerenciado pela política.
- Programação — define a frequência de criação de snapshots e o número máximo de snapshots a serem mantidos. A criação de um snapshot é iniciada dentro de uma hora a partir do horário de início especificado. Se a criação de um novo snapshot ultrapassar o número máximo de snapshots a serem mantidos para o volume, o snapshot mais antigo será excluído.

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.
- Os snapshots começam a ser criados por uma política dentro de uma hora, a partir do horário de início especificado.
- Se você modificar uma política removendo ou alterando sua tag de destino, os volumes do EBS que possuem essa tag 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.
- Você pode criar várias políticas para fazer backup de um volume do EBS, desde que cada política segmente uma tag exclusiva no volume. As tags de destino não podem ser reutilizadas nas políticas, mesmo em políticas desabilitadas. 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 DLM cria snapshots de acordo com as programações de ambas as políticas.

- Quando você copia um snapshot criado por uma política, a programação de retenção não é transferida para a cópia. Dessa forma, o Amazon DLM evita a exclusão de snapshots que devem ser retidos por um período mais longo.

Por exemplo, você pode criar uma política para gerenciar todos os volumes do EBS com a tag `account=Finance`, criar snapshots a cada 24 horas a partir de 0900 e manter os cinco snapshots mais recentes. A criação do snapshot pode iniciar até 0959.

Permissões para Amazon DLM

O Amazon DLM usa uma função do IAM para obter as permissões necessárias para gerenciar snapshots em seu nome. O Amazon DLM cria a função `AWSDataLifecycleManagerDefaultRole` na primeira vez que você cria uma política de ciclo de vida usando o Console de gerenciamento da AWS. Você também pode criar esta função usando o comando [create-default-role](#) da seguinte forma:

```
aws dlm create-default-role
```

Como alternativa, você pode criar uma função do IAM personalizada com as permissões necessárias e selecioná-la ao criar uma política de ciclo de vida.

Para criar uma função do IAM personalizada

1. Crie uma função com as seguintes permissões:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateSnapshot",
                "ec2:DeleteSnapshot",
                "ec2:DescribeVolumes",
                "ec2:DescribeSnapshots"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:*::snapshot/*"
        }
    ]
}
```

Para obter mais informações, consulte [Criar uma função](#) no Guia do usuário do IAM.

2. Adicione uma relação de confiança à função.
 - a. No console do IAM, selecione Roles (Funções).
 - b. Selecione a função que você criou e, em seguida, escolha Trust relationships (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 DLM:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "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.

Limites

Sua conta da AWS tem os limites a seguir, relativos ao Amazon DLM:

- Você pode criar até 100 políticas de ciclo de vida por região.
- Você pode adicionar até 50 tags por recurso.
- Você pode criar uma programação por política de ciclo de vida.

Trabalho com Amazon DLM usando o console

Os exemplos a seguir mostram como usar o Amazon DLM para executar procedimentos típicos de gerenciamento de backup de volumes do EBS.

Como criar 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, Lifecycle Manager (Gerenciador de ciclo de vida), 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.
 - Target volumes with tags (Volumes de destino com tags) – As tags de recurso que identificam os volumes para fazer backup.

- Schedule Name (Nome da programação) – Um nome para a programação de backup.
 - Create snapshots every (Criar snapshots a cada) n (x) Hours (horas) – O número de horas entre cada execução de política. Os valores com suporte são 12 e 24.
 - Snapshot creation start time (Hora de início da criação do snapshot) hh:mm UTC – O horário do dia em que as execuções de políticas estão agendadas para começar. A execução da política inicia uma hora após o horário agendado.
 - Retention rule (Regra de retenção) – O número máximo de snapshots a serem retidos para cada volume. O intervalo com suporte é de 1 a 1000. Quando o limite for atingido, o snapshot o mais antigo será excluído quando um novo for criado.
 - Copy tags (Copiar tags) – Copia todas as tags definidas pelo usuário em um volume de origem para snapshots do volume criado por essa política.
 - Tag created snapshots (Snapshots criados com tags) – As tags de recursos a serem aplicadas aos snapshots que forem criados. Essas tags são aplicadas além das tags aplicadas pelo Amazon DLM.
 - IAM role (Função do IAM) – Uma função do IAM que tem permissões para criar, excluir e descrever de snapshots e para descrever volumes. A AWS fornece uma função padrão, AWSDataLifecycleManagerDefaultRole ou você pode criar uma função do IAM personalizada.
 - 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.
4. Selecione Create Policy (Criar política).

Para 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:
 - Policy ID (ID da política)
 - Date created (Data da criação)
 - Date modified (Data de modificação)
 - Target volumes with these tags (Volumes de destino com essas tags)
 - Rule summary (Resumo da regra)
 - Description (Descrição)
 - Policy state (Estado da política)
 - Tags added to snapshots (Tags adicionadas aos snapshots)

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 policy (Modificar política).
5. Na política de ciclo de vida atual, você pode modificar os seguintes valores:
 - Description (Descrição) – Uma descrição da política.
 - Target volumes with tags (Volumes de destino com tags) – As tags de recurso que identificam os volumes para fazer backup.

- Schedule Name (Nome da programação) – Um nome para a programação de backup.
- Create snapshots every (Criar snapshots a cada) n (x) Hours (horas) – O número de horas entre cada execução de política. Os valores com suporte são 12 e 24.
- Snapshot creation start time (Hora de início da criação do snapshot) hh:mm UTC – O horário do dia em que as execuções de políticas estão agendadas para começar. A execução da política inicia uma hora após o horário agendado.
- Retention rule (Regra de retenção) – O número máximo de snapshots a serem retidos para cada volume. O intervalo com suporte é de 1 a 1000. Quando o limite for atingido, o snapshot o mais antigo será excluído quando um novo for criado.
- Copy tags (Copiar tags) – Copia todas as tags definidas pelo usuário em um volume de origem para snapshots do volume criado por essa política.
- Tag created snapshots (Snapshots criados com tags) – As tags de recursos a serem aplicadas aos snapshots que forem criados. Essas tags são aplicadas além das tags aplicadas pelo Amazon DLM.
- IAM role (Função do IAM) – Uma função do IAM que tem permissões para criar, excluir e descrever de snapshots e para descrever volumes. A AWS fornece uma função padrão, AWSDataLifecycleManagerDefaultRole ou você pode criar uma função do IAM personalizada.
- 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.

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) e, depois, Delete policy (Excluir política).

Trabalho com Amazon DLM usando a linha de comando

Os exemplos a seguir mostram como usar o Amazon DLM para executar procedimentos típicos de gerenciamento de backup de volumes do EBS.

Example Exemplo: como criar uma política de ciclo de vida

Use o comando `create-lifecycle-policy` para criar uma política de ciclo de vida. Para simplificar a sintaxe, este exemplo faz referência ao arquivo JSON `policyDetails.json` que inclui os detalhes da política.

```
aws dlm create-lifecycle-policy --description "My first policy" --state ENABLED --  
execution-role-arn arn:aws:iam::12345678910:role/AWSDataLifecycleManagerDefaultRole --  
policy-details file://policyDetails.json
```

Veja a seguir um exemplo do arquivo `policyDetails.json`:

```
{  
    "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  
}  
]  
}
```

Se for bem-sucedido, o comando retornará o ID da política criada recentemente. A seguir está um exemplo de saída:

```
{  
    "PolicyId": "policy-0123456789abcdef0"  
}
```

Example Exemplo: como exibir uma política de ciclo de vida

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": {  
            "ResourceTypes": [  
                "VOLUME"  
            ],  
            "TargetTags": [  
                {  
                    "Value": "115",  
                    "Key": "costcenter"  
                }  
            ],  
            "Schedules": [  
                {  
                    "TagsToAdd": [  
                        {  
                            "Key": "costcenter",  
                            "Value": "115"  
                        }  
                    ]  
                }  
            ]  
        }  
    }  
}
```

```
        "Value": "myDailySnapshot",
        "Key": "type"
    }
],
"RetainRule": {
    "Count": 5
},
"CopyTags": false,
"CreateRule": {
    "Interval": 24,
    "IntervalUnit": "HOURS",
    "Times": [
        "03:00"
    ]
},
"Name": "DailySnapshots"
}
]
}
}
```

Example Para modificar uma política de ciclo de vida

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
```

Veja a seguir um exemplo do arquivo `policyDetailsUpdated.json`:

```
{
    "ResourceTypes": [
        "VOLUME"
    ],
    "TargetTags": [
        {
            "Key": "costcenter",
            "Value": "120"
        }
    ],
    "Schedules": [
        {
            "Name": "DailySnapshots",
            "TagsToAdd": [
                {
                    "Key": "type",
                    "Value": "myDailySnapshot"
                }
            ],
            "CreateRule": {
                "Interval": 12,
                "IntervalUnit": "HOURS",
                "Times": [
                    "15:00"
                ]
            },
            "RetainRule": {
                "Count": 5
            },

```

```
        "CopyTags": false
    }
}
```

Para visualizar a política atualizada, use o comando `get-lifecycle-policy`. Você pode ver que o estado, o valor da tag, o intervalo de snapshots e o horário de início do snapshot foram alterados.

Example Exemplo: como excluir uma política de ciclo de vida

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.

```
aws dlm delete-lifecycle-policy --policy-id policy-0123456789abcdef0
```

Trabalho com o Amazon DLM usando a API

A [Referência de API do Gerenciador de ciclo de vida de dados da Amazon](#) fornece as descrições e a sintaxe de cada uma das ações e tipos de dados para a API de consulta do Amazon DLM.

Como alternativa, você pode usar um dos AWS SDKs para acessar uma API que seja personalizada para a linguagem de programação ou a plataforma que você está usando. Para obter mais informações, consulte [SDKs da AWS](#).

Monitoramento do ciclo de vida de snapshot

Você pode usar os seguintes recursos para monitorar o ciclo de vida de seus snapshots.

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 criado por uma política possui um time stamp e tags relacionadas à política. Você pode filtrar snapshots 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 [Para exibir uma política de ciclo de vida \(p. 911\)](#). Para obter informações sobre a exibição de informações sobre as políticas de ciclo de vida usando a CLI, consulte [Exemplo: como exibir uma política de ciclo de vida \(p. 913\)](#).

Eventos do CloudWatch

O Amazon EBS e o Amazon DLM geram eventos relacionados às ações das políticas de ciclo de vida. Você pode usar o AWS Lambda e o Eventos do Amazon CloudWatch para tratar as notificações de eventos de forma programática. Para obter mais informações, consulte [Guia do usuário do Eventos do Amazon CloudWatch](#).

Os seguintes eventos estão disponíveis:

- `createSnapshot` – um evento do Amazon EBS gerado quando uma ação `CreateSnapshot` é bem-sucedida ou falha. Para obter mais informações, consulte [Eventos do Amazon CloudWatch para Amazon EBS](#).
- `DLM Policy State Change` – um evento do Amazon DLM 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"
    }
}
```

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 mais informações, consulte o [AWS CloudTrail User Guide](#).

AWS CloudFormation

Ao implantar pilhas de recursos com o AWS CloudFormation, você pode incluir políticas do Amazon DLM em seus modelos do AWS CloudFormation. Para obter mais informações, consulte [Referência de tipos de recurso do Gerenciador de ciclo de vida de dados da Amazon](#).

Amazon EBS – instâncias otimizadas

Uma instância otimizada para Amazon EBS usa uma pilha de configuração otimizada e fornece capacidade dedicada adicional para E/S do Amazon EBS. Essa otimização proporciona o melhor desempenho para seus volumes do EBS ao minimizar a contenção entre a E/S do Amazon EBS e outros tráfegos da sua instância.

As instâncias otimizadas para EBS fornecem largura de banda dedicada ao Amazon EBS, com opções entre 425 Mbps e 14,000 Mbps, dependendo do tipo de instância que você usa. Quando anexados a uma instância otimizada para EBS, os volumes Finalidade geral (SSD) (gp2) foram desenvolvidos para proporcionar um desempenho dentro de 10% de sua linha de base e um desempenho intermitente durante 99% do tempo em um determinado ano, e os volumes Provisioned IOPS SSD (io1) foram desenvolvidos para proporcionar um desempenho dentro de 10% de seu desempenho provisionado durante 99,9% do tempo em um ano. A garantia da consistência de desempenho Disco rígido com throughput otimizado (st1) e Cold HDD (sc1) é de 90% da taxa de transferência intermitente durante 99% do tempo em um

determinado ano. Períodos não compatíveis são distribuídos com uniformidade aproximada, destinando 99% do throughput total esperado a cada hora. Para obter mais informações, consulte [Tipos de volume do Amazon EBS \(p. 844\)](#).

Tópicos

- [Tipos de instâncias que oferecem suporte à otimização de EBS \(p. 917\)](#)
- [Ativar a otimização para Amazon EBS na execução \(p. 924\)](#)
- [Modificar a otimização para Amazon EBS para uma instância em execução \(p. 925\)](#)

Tipos de instâncias que oferecem suporte à otimização de EBS

As tabelas a seguir mostram quais tipos de instância comportam otimização de EBS, a largura de banda dedicada para Amazon EBS, o número máximo de IOPS que a instância pode comportar se você estiver usando um tamanho de E/S de 16 KB e a taxa de transferência máxima agregada normal que pode ser atingida nessa conexão em MiB/s com uma carga de trabalho de leitura de streaming e tamanho de E/S de 128 KB. Escolha uma instância otimizada para EBS que forneça uma taxa de transferência do Amazon EBS mais dedicada do que o necessário para seu aplicativo; caso contrário, a conexão entre o Amazon EBS e o Amazon EC2 pode tornar-se um gargalo de desempenho.

Para os tipos de instância que são otimizadas para EBS por padrão, não há necessidade de habilitar a otimização de EBS e não haverá efeito se você desabilitar a otimização para EBS. Para instâncias que não são otimizadas para EBS por padrão, você poderá ativar a otimização para EBS ao executar as instâncias, ou ativar a otimização para EBS quando as instâncias estiverem em execução. As instâncias devem ter a otimização para EBS ativada para alcançar o nível de desempenho descrito na tabela abaixo.

Ao ativar a otimização para 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 de definição de preços do Amazon EC2 para instâncias sob demanda](#).

As instâncias `i2.8xlarge`, `c3.8xlarge` e `r3.8xlarge` não possuem largura de banda EBS dedicada e, portanto, não oferecem otimização para EBS. Nessas instâncias, o tráfego de rede e o tráfego de Amazon EBS compartilham a mesma interface de rede de 10 gigabits.

Tipos de instância da geração atual compatíveis

A tabela a seguir lista os tipos de instância da geração atual compatíveis com a otimização para EBS.

Tipo de instância	Otimizado por EBS por padrão	Largura de banda máxima (Mbps)	Total de transferência máxima (MB/s, E/S de 128 KB)	IOPS máximo (E/S de 16 KB)
<code>a1.medium</code>	Sim	3,500	437,5	20.000
<code>a1.large</code>	Sim	3,500	437,5	20.000
<code>a1.xlarge</code>	Sim	3,500	437,5	20.000
<code>a1.2xlarge</code>	Sim	3,500	437,5	20.000
<code>a1.4xlarge</code>	Sim	3,500	437,5	20.000
<code>c4.large</code>	Sim	500	62.5	4.000
<code>c4.xlarge</code>	Sim	750	93.75	6.000 USD
<code>c4.2xlarge</code>	Sim	1.000	125	8,000

Tipo de instância	Otimizado por EBS por padrão	Largura de banda máxima (Mbps)	Total de transferência máxima (MB/s, E/S de 128 KB)	IOPS máximo (E/S de 16 KB)
c4.4xlarge	Sim	2.000	250	16,000
c4.8xlarge	Sim	4.000	500	32,000
c5.large *	Sim	3,500	437,5	20.000
c5.xlarge *	Sim	3,500	437,5	20.000
c5.2xlarge *	Sim	3,500	437,5	20.000
c5.4xlarge	Sim	3,500	437,5	20.000
c5.9xlarge	Sim	7,000	875	40.000
c5.18xlarge	Sim	14,000	1,750	80.000
c5d.large *	Sim	3,500	437,5	20.000
c5d.xlarge *	Sim	3,500	437,5	20.000
c5d.2xlarge *	Sim	3,500	437,5	20.000
c5d.4xlarge	Sim	3,500	437,5	20.000
c5d.9xlarge	Sim	7,000	875	40.000
c5d.18xlarge	Sim	14,000	1,750	80.000
c5n.large *	Sim	3,500	437,5	20.000
c5n.xlarge *	Sim	3,500	437,5	20.000
c5n.2xlarge *	Sim	3,500	437,5	20.000
c5n.4xlarge	Sim	3,500	437,5	20.000
c5n.9xlarge	Sim	7,000	875	40.000
c5n.18xlarge	Sim	14,000	1,750	80.000
d2.xlarge	Sim	750	93.75	6.000 USD
d2.2xlarge	Sim	1.000	125	8,000
d2.4xlarge	Sim	2.000	250	16,000
d2.8xlarge	Sim	4.000	500	32,000
f1.2xlarge	Sim	1,700	212,5	12,000
f1.4xlarge	Sim	3,500	400	44,000
f1.16xlarge	Sim	14,000	1,750	75,000
g3s.xlarge	Sim	850	100	5,000
g3.4xlarge	Sim	3,500	437,5	20.000

Tipo de instância	Otimizado por EBS por padrão	Largura de banda máxima (Mbps)	Total de transferência máxima (MB/s, E/S de 128 KB)	IOPS máximo (E/S de 16 KB)
g3.8xlarge	Sim	7,000	875	40.000
g3.16xlarge	Sim	14,000	1,750	80.000
h1.2xlarge	Sim	1,750	218,75	12,000
h1.4xlarge	Sim	3,500	437,5	20.000
h1.8xlarge	Sim	7,000	875	40.000
h1.16xlarge	Sim	14,000	1,750	80.000
i3.large	Sim	425	53,13	3000
i3.xlarge	Sim	850	106,25	6000
i3.2xlarge	Sim	1,700	212,5	12,000
i3.4xlarge	Sim	3,500	437,5	16,000
i3.8xlarge	Sim	7,000	875	32,500
i3.16xlarge	Sim	14,000	1,750	65.000
i3.metal	Sim	14,000	1,750	65.000
m4.large	Sim	450	56.25	3,600
m4.xlarge	Sim	750	93.75	6.000 USD
m4.2xlarge	Sim	1.000	125	8,000
m4.4xlarge	Sim	2.000	250	16,000
m4.10xlarge	Sim	4.000	500	32,000
m4.16xlarge	Sim	10.000	1,250	65.000
m5.large *	Sim	3,500	437,5	18,750
m5.xlarge *	Sim	3,500	437,5	18,750
m5.2xlarge *	Sim	3,500	437,5	18,750
m5.4xlarge	Sim	3,500	437,5	18,750
m5.12xlarge	Sim	7,000	875	40.000
m5.24xlarge	Sim	14,000	1,750	80.000
m5a.large *	Sim	2.120	265	16,000
m5a.xlarge *	Sim	2.120	265	16,000
m5a.2xlarge *	Sim	2.120	265	16,000
m5a.4xlarge	Sim	2.120	265	16,000

Tipo de instância	Otimizado por EBS por padrão	Largura de banda máxima (Mbps)	Total de transferência máxima (MB/s, E/S de 128 KB)	IOPS máximo (E/S de 16 KB)
m5a.12xlarge	Sim	5,000	625	30.000
m5a.24xlarge	Sim	10.000	1.250	60.000
m5d.large *	Sim	3,500	437,5	18,750
m5d.xlarge *	Sim	3,500	437,5	18,750
m5d.2xlarge *	Sim	3,500	437,5	18,750
m5d.4xlarge	Sim	3,500	437,5	18,750
m5d.12xlarge	Sim	7,000	875	40.000
m5d.24xlarge	Sim	14,000	1.750	80.000
p2.xlarge	Sim	750	93.75	6.000 USD
p2.8xlarge	Sim	5,000	625	32,500
p2.16xlarge	Sim	10.000	1.250	65.000
p3.2xlarge	Sim	1,750	218	10.000
p3.8xlarge	Sim	7,000	875	40.000
p3.16xlarge	Sim	14,000	1.750	80.000
p3dn.24xlarge	Sim	14,000	1.750	80.000
r4.large	Sim	425	53,13	3,000
r4.xlarge	Sim	850	106,25	6.000 USD
r4.2xlarge	Sim	1,700	212,5	12,000
r4.4xlarge	Sim	3,500	437,5	18,750
r4.8xlarge	Sim	7,000	875	37,500
r4.16xlarge	Sim	14,000	1.750	75,000
r5.large *	Sim	3,500	437,5	18,750
r5.xlarge *	Sim	3,500	437,5	18,750
r5.2xlarge *	Sim	3,500	437,5	18,750
r5.4xlarge	Sim	3,500	437,5	18,750
r5.12xlarge	Sim	7,000	875	40.000
r5.24xlarge	Sim	14,000	1.750	80.000
r5a.large *	Sim	2.210	265	16,000
r5a.xlarge *	Sim	2.210	265	16,000

Tipo de instância	Otimizado por EBS por padrão	Largura de banda máxima (Mbps)	Total de transferência máxima (MB/s, E/S de 128 KB)	IOPS máximo (E/S de 16 KB)
r5a.2xlarge *	Sim	2.210	265	16,000
r5a.4xlarge	Sim	2.210	265	16,000
r5a.12xlarge	Sim	5,000	625	30.000
r5a.24xlarge	Sim	10.000	1,250	60.000
r5d.large *	Sim	3,500	437,5	18,750
r5d.xlarge *	Sim	3,500	437,5	18,750
r5d.2xlarge *	Sim	3,500	437,5	18,750
r5d.4xlarge	Sim	3,500	437,5	18,750
r5d.12xlarge	Sim	7,000	875	40.000
r5d.24xlarge	Sim	14,000	1,750	80.000
t3.nano *	Sim	1,536	192	11,800
t3.micro *	Sim	1,536	192	11,800
t3.small *	Sim	1,536	192	11,800
t3.medium *	Sim	1,536	192	11,800
t3.large *	Sim	2,048	256	15,700
t3.xlarge *	Sim	2,048	256	15,700
t3.2xlarge *	Sim	2,048	256	15,700
u-6tb1.metal	Sim	14,000	1,750	80.000
u-9tb1.metal	Sim	14,000	1,750	80.000
u-12tb1.metal	Sim	14,000	1,750	80.000
x1.16xlarge	Sim	7,000	875	40.000
x1.32xlarge	Sim	14,000	1,750	80.000
x1e.xlarge	Sim	500	62.5	3.700
x1e.2xlarge	Sim	1.000	125	7.400
x1e.4xlarge	Sim	1,750	218,75	10.000
x1e.8xlarge	Sim	3,500	437,5	20.000
x1e.16xlarge	Sim	7,000	875	40.000
x1e.32xlarge	Sim	14,000	1,750	80.000
z1d.large *	Sim	2,333	291	13,333

Tipo de instância	Otimizado por EBS por padrão	Largura de banda máxima (Mbps)	Total de transferência máxima (MB/s, E/S de 128 KB)	IOPS máximo (E/S de 16 KB)
<code>z1d.xlarge</code> *	Sim	2,333	291	13,333
<code>z1d.2xlarge</code>	Sim	2,333	292	13,333
<code>z1d.3xlarge</code>	Sim	3,500	438	20.000
<code>z1d.6xlarge</code>	Sim	7,000	875	40.000
<code>z1d.12xlarge</code>	Sim	14,000	1,750	80.000

* Esses tipos de instância podem dar suporte a um desempenho máximo por 30 minutos a cada 24 horas pelo menos. Por exemplo, as instâncias `c5.large` podem fornecer 437,5 MB/s por 30 minutos pelo menos a cada 24 horas. Se você tiver uma carga de trabalho que exija desempenho máximo sustentado por mais de 30 minutos, selecione um tipo de instância de acordo com o desempenho da linha de base conforme mostrado na tabela a seguir:

Tipo de instância	Largura de banda da linha de base (Mbps)	Taxa de transferência da linha de base (MB/s, E/S de 128 KB)	IOPS da linha de base (E/S de 16 KB)
<code>c5.large</code>	525	65.625	4.000
<code>c5.xlarge</code>	800	100	6.000 USD
<code>c5.2xlarge</code>	1,750	218,75	10.000
<code>c5d.large</code>	525	65.625	4.000
<code>c5d.xlarge</code>	800	100	6.000 USD
<code>c5d.2xlarge</code>	1,750	218,75	10.000
<code>c5n.large</code>	525	65.625	4.000
<code>c5n.xlarge</code>	800	100	6.000 USD
<code>c5n.2xlarge</code>	1,750	218,75	10.000
<code>m5.large</code>	480	60	3,600
<code>m5.xlarge</code>	850	106,25	6.000 USD
<code>m5.2xlarge</code>	1,700	212,5	12,000
<code>m5a.large</code>	480	60	3,600
<code>m5a.xlarge</code>	800	100	6.000 USD
<code>m5a.2xlarge</code>	1.166	146	8.333
<code>m5d.large</code>	480	60	3,600
<code>m5d.xlarge</code>	850	106,25	6.000 USD
<code>m5d.2xlarge</code>	1,700	212,5	12,000

Tipo de instância	Largura de banda da linha de base (Mbps)	Taxa de transferência da linha de base (MB/s, E/S de 128 KB)	IOPS da linha de base (E/S de 16 KB)
r5.large	480	60	3,600
r5.xlarge	850	106,25	6.000 USD
r5.2xlarge	1,700	212,5	12,000
r5a.large	480	60	3,600
r5a.xlarge	800	100	6.000 USD
r5a.2xlarge	1.166	146	8.333
r5d.large	480	60	3,600
r5d.xlarge	850	106,25	6.000 USD
r5d.2xlarge	1,700	212,5	12,000
t3.nano	32	4	250
t3.micro	64	8	500
t3.small	128	16	1.000
t3.medium	256	32	2.000
t3.large	512	64	4.000
t3.xlarge	512	64	4.000
t3.2xlarge	512	64	4.000
z1d.large	583	73	3,333
z1d.xlarge	1,167	146	6.667

As métricas `EBSIOBalance%` e `EBSByteBalance%` podem ajudar você 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 [Monitoramento das suas instâncias usando o CloudWatch \(p. 575\)](#).

Tipos de instância da geração anterior compatíveis

A tabela a seguir lista os tipos de instância da geração anterior compatíveis com a otimização para EBS.

Instâncias de gerações anteriores

Tipo de instância	Otimizado por EBS por padrão	Largura de banda máxima (Mbps)	Total de transferência máxima (MB/s, E/S de 128 KB)	IOPS máximo (E/S de 16 KB)
c1.xlarge	Não	1.000	125	8,000

Tipo de instância	Otimizado por EBS por padrão	Largura de banda máxima (Mbps)	Total de transferência máxima (MB/s, E/S de 128 KB)	IOPS máximo (E/S de 16 KB)
c3.xlarge	Não	500	62.5	4.000
c3.2xlarge	Não	1.000	125	8.000
c3.4xlarge	Não	2.000	250	16.000
g2.2xlarge	Não	1.000	125	8.000
i2.xlarge	Não	500	62.5	4.000
i2.2xlarge	Não	1.000	125	8.000
i2.4xlarge	Não	2.000	250	16.000
m1.large	Não	500	62.5	4.000
m1.xlarge	Não	1.000	125	8.000
m2.2xlarge	Não	500	62.5	4.000
m2.4xlarge	Não	1.000	125	8.000
m3.xlarge	Não	500	62.5	4.000
m3.2xlarge	Não	1.000	125	8.000
r3.xlarge	Não	500	62.5	4.000
r3.2xlarge	Não	1.000	125	8.000
r3.4xlarge	Não	2.000	250	16.000

Ativar a otimização para Amazon EBS na execução

Você pode habilitar a otimização para uma instância definindo o atributo otimizado para Amazon EBS.

Para ativar a otimização para 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, por padrão, o tipo de instância selecionado for otimizado para Amazon EBS, 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 uma das seguintes opções com o comando correspondente. Para obter mais informações sobre essas interfaces de linha de comando, consulte [Acessando o Amazon EC2 \(p. 3\)](#).

- `--ebs-optimized` com [run-instances](#) (AWS CLI)
- `-EbsOptimized` com [New-EC2Instance](#) (AWS Tools para Windows PowerShell)

Modificar a otimização para Amazon EBS para uma instância em execução

Você pode habilitar ou desabilitar a otimização para uma instância em execução modificando o atributo de instância otimizada para Amazon EBS.

Para habilitar a otimização para EBS para uma instância em execução usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, clique em Instances (Instâncias) e selecione a instância.
3. Clique em Actions (Ações), selecione Instance State (Estado da instância) e clique em Stop (Interromper).

Warning

Quando você interrompe uma instância, os dados em todos os volumes de armazenamento de instâncias são apagados. Para manter dados de volumes do armazenamento de instâncias, certifique-se de fazer backup deles em um armazenamento persistente.

4. Na caixa de diálogo de confirmação, clique em Yes, Stop (Sim, interromper). Pode demorar alguns minutos para que a instância pare.
5. Com a instância ainda selecionada, clique em Actions (Ações), selecione Instance Settings (Configurações da instância) e clique em Change Instance Type (Alterar tipo de instância).
6. Na caixa de diálogo Change Instance Type (Alterar tipo de instância), execute um dos seguintes procedimentos:
 - Se, por padrão, o tipo de sua instância for otimizado para Amazon EBS, 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 oferecer suporte à otimização para Amazon EBS, escolha EBS-optimized (Otimizada para EBS) e clique em Apply (Aplicar).
 - Se o tipo de instância não oferecer suporte à otimização para 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 ofereça suporte à otimização para Amazon EBS e, em seguida, selecionar EBS-optimized (Otimizada para EBS) e Apply (Aplicar).
7. Escolha Ações, Estado da instância, Iniciar.

Para habilitar a otimização para EBS para uma instância em execução usando a linha de comando

Você pode usar uma das seguintes opções com o comando correspondente. Para obter mais informações sobre essas interfaces de linha de comando, consulte [Acessando o Amazon EC2 \(p. 3\)](#).

- `--ebs-optimized` com [modify-instance-attribute](#) (AWS CLI)
- `-EbsOptimized` com [Edit-EC2InstanceAttribute](#) (AWS Tools para Windows PowerShell)

Amazon EBS Encryption

O Criptografia de Amazon EBS oferece uma solução de criptografia simples para os volumes do EBS sem a necessidade de criar, manter e proteger sua própria infraestrutura de gerenciamento de chaves. 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 snapshots criados a partir desses snapshots

As operações de criptografia ocorrem nos servidores que hospedam instâncias do EC2, assegurando a segurança dos dados em repouso e dos dados em trânsito entre uma instância e seu armazenamento do EBS anexado.

A criptografia é compatível com todos os tipos de volume do EBS (Finalidade geral (SSD) [gp2], Provisioned IOPS SSD [io1], Disco rígido com throughput otimizado [st1], Cold HDD [sc1] e Magnético [standard]). Você pode esperar o mesmo desempenho 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 seus aplicativos.

Não há suporte para snapshots públicos de volumes criptografado, mas você pode compartilhar um snapshot criptografado com contas específicas. Para obter mais informações sobre como compartilhar snapshots criptografados, consulte [Compartilhamento de um snapshot do Amazon EBS](#).

O Criptografia de Amazon EBS só está disponível em alguns tipos de instância. Você pode anexar volumes criptografados e não criptografados a um tipo de instância com suporte. Para obter mais informações, consulte [Tipos de instâncias compatíveis \(p. 927\)](#).

Tópicos

- [Gerenciamento de chave de criptografia \(p. 926\)](#)
- [Tipos de instâncias compatíveis \(p. 927\)](#)
- [Alteração do estado de criptografia de seus dados \(p. 927\)](#)
- [Criptografia do Amazon EBS e Eventos do CloudWatch \(p. 929\)](#)

Gerenciamento de chave de criptografia

O Criptografia de Amazon EBS usa chaves mestras do cliente (CMKs) do AWS Key Management Service (AWS KMS) para criar volumes criptografados e quaisquer snapshots criados a partir delas. Uma CMK exclusiva gerenciada pela AWS é criada automaticamente em cada região onde os ativos da AWS são armazenados. Essa chave é usada para o Criptografia de Amazon EBS, a menos que você especifique uma CMK gerenciada pelo cliente que você tenha criado separadamente por meio do AWS KMS.

Note

A criação de sua própria CMK oferece a você mais flexibilidade, inclusive a capacidade de criar, girar e desabilitar chaves para definir controles de acesso. Para obter mais informações, consulte o [AWS Key Management Service Developer Guide](#).

Você não pode alterar a CMK que está associada a um snapshot existente ou a um volume criptografado. No entanto, você pode associar um CMK diferente durante uma operação de cópia de snapshot para que o snapshot copiado resultante use a CMK do navegador.

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 os dados criptografados, mas não antes de o EBS criptografá-la com a CMK; ela nunca aparece em texto sem formatação. A mesma chave de dados é compartilhada pelos snapshots do volume e de quaisquer volumes subsequentes criados a partir desses snapshots.

Para mais informações sobre as permissões de gerenciamento e acesso de chaves, consulte [Como o Amazon Elastic Block Store \(Amazon EBS\) usa o AWS KMS e Autenticação e controle de acesso para o AWS KMS](#) no AWS Key Management Service Developer Guide.

Tipos de instâncias compatíveis

O Criptografia de Amazon EBS está disponível nos tipos de instância indicados a seguir. Você pode anexar volumes criptografados e não criptografados a esses tipos de instância de forma simultânea.

- Uso geral: A1, M3, M4, M5, M5d, T2 e T3
- Computação otimizada: C3, C4, C5, C5d e C5n
- Memória otimizada: `cr1.8xlarge`, R3, R4, R5, R5d, X1, X1e e z1d
- Armazenamento otimizado: D2, h1.2xlarge, h1.4xlarge, I2 e I3
- Computação acelerada: F1, G2, G3, P2 e P3
- Bare metal: `i3.metal`, `u-6tb1.metal`, `u-9tb1.metal`, and `u-12tb1.metal`

Para obter mais informações sobre esses tipos de instância, consulte [Tipos de instância do Amazon EC2](#).

Alteração do estado de criptografia de seus dados

Não há nenhuma maneira direta de criptografar um volume não criptografado existente nem de remover a criptografia de um volume criptografado. Contudo, é possível migrar dados entre volumes criptografados e não criptografados. Você também pode aplicar um novo status de criptografia para copiar um snapshot:

- Ao copiar um snapshot não criptografado de um volume não criptografado, você pode criptografar uma cópia. Os volumes restaurados dessa cópia criptografada também são criptografados.
- Ao copiar um snapshot criptografado de um volume criptografado, você pode associar a cópia a uma CMK diferente. Os volumes restaurados da cópia criptografada só são acessíveis usando a CMK recentemente aplicada.

Você não pode remover a criptografia de um snapshot criptografado.

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.

Para migrar dados entre volumes criptografados e não criptografados

1. Crie o volume de destino (criptografado ou não criptografado, dependendo de sua necessidade) seguindo os procedimentos em [Criação de um volume do Amazon EBS \(p. 860\)](#).
2. Anexe o volume de destino à instância que hospeda os dados a serem migrados. Para obter mais informações, consulte [Associação de um volume do Amazon EBS a uma instância \(p. 863\)](#).
3. Disponibilize o volume de destino disponível seguindo os procedimentos em [Disponibilização de um volume do Amazon EBS para uso no Linux \(p. 864\)](#). Para instâncias Linux, você pode criar um ponto de montagem em `/mnt/destination` e montar o volume de destino.
4. Copie os dados do seu diretório de origem no volume de destino. Pode ser muito mais conveniente usar um utilitário de volume em massa para isso.

Linux

Use o comando rsync da seguinte forma para copiar os dados de sua origem no volume de destino. Nesse exemplo, os dados de origem estão localizados em /mnt/source e o volume de destino é montado em /mnt/destination.

```
[ec2-user ~]$ sudo rsync -avh --progress /mnt/source/ /mnt/destination/
```

Windows

Em um prompt de comando, use o comando robocopy para copiar os dados de sua origem no volume de destino. Nesse exemplo, os dados de origem estão localizados em D:\ e o volume de destino é montado em E:\.

```
PS C:\> robocopy D:\<sourcefolder> E:\<destinationfolder> /e /copyall /eta
```

Note

Recomendamos nomear as pastas explicitamente, em vez de copiar o volume todo, para evitar problemas potenciais com pastas ocultas.

Aplicar a criptografia ao copiar um snapshot

Como você pode aplicar a criptografia a um snapshot durante a cópia, outro caminho para a criptografia de seus dados é o procedimento a seguir.

Para criptografar os dados de um volume por meio de cópia de snapshot

1. Crie um snapshot de seu volume não criptografado do EBS. Esse snapshot também não é criptografado.
2. Copie o snapshot para aplicar os parâmetros de criptografia. O snapshot de destino resultante é criptografado.
3. Restaure o snapshot criptografado em um novo volume, que também é criptografado.

Para obter mais informações, consulte [Cópia de um snapshot do Amazon EBS](#).

Criptografar um snapshot para uma nova CMK

A capacidade de criptografar um snapshot durante a cópia também permite a você aplicar uma nova CMK a um snapshot já criptografado. Os volumes restaurados da cópia resultante só são acessíveis usando a nova CMK.

Note

Se você copiar um snapshot para uma nova CMK, uma cópia (não incremental) completa será criada sempre, resultando em custos adicionais de armazenamento.

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. Para que você possa restaurar um volume de um snapshot criptografado compartilhado, você deve criar sua própria cópia dele. Por padrão, a cópia é criptografada com uma CMK compartilhada pelo proprietário do snapshot. No entanto, recomendamos que você crie uma cópia do snapshot compartilhado usando uma CMK diferente que esteja sob seu controle. Isso protegerá seu acesso ao volume se a CMK original estiver comprometida ou se o proprietário revogar a CMK por algum motivo.

O procedimento a seguir demonstra como criar uma cópia de um snapshot compartilhado para uma CMK de sua propriedade e gerenciada pelo cliente.

Para copiar um snapshot de sua propriedade para uma nova CMK personalizada usando o console

1. Criar uma CMK gerenciada pelo cliente. Para obter mais informações, consulte [AWS Key Management Service Developer Guide](#).
2. Crie um volume do EBS criptografado (para este exemplo) para a CMK gerenciada pela AWS.
3. Crie um snapshot de seu volume criptografado do EBS. Esse snapshot também é criptografado para a CMK gerenciada pela AWS.
4. Na página Snapshots, escolha Ações, Copiar.
5. Na janela Copy Snapshot, forneça o ARN completo da CMK gerenciada pelo cliente (no formato `arn:aws:kms:us-east-1:012345678910:key/abcd1234-a123-456a-a12b-a123b4cd56ef`) no campo Master Key ou escolha-a no menu. Escolha Copiar.

A cópia resultante do snapshot e todos os volumes restaurados dele são criptografados para a CMK gerenciada pelo cliente.

O procedimento a seguir demonstra como criar uma cópia de um snapshot criptografado e compartilhado para uma nova CMK de sua propriedade. Para que isso funcione, você também precisa de permissões de acesso ao snapshot criptografado e compartilhado e à CMK para a qual ele foi originalmente criptografado.

Para copiar um snapshot compartilhado para uma CMK de sua propriedade usando o console

1. Selecione o snapshot criptografado compartilhado na página Snapshots, escolha Ações e Copiar.
2. Na janela Copiar snapshot, forneça o nome de recurso da Amazon (ARN) completo de uma CMK que você possua (no formato `arn:aws:kms:us-east-1:012345678910:key/abcd1234-a123-456a-a12b-a123b4cd56ef`) no campo Chave mestra ou escolha-a no menu. Escolha Copiar.

A cópia resultante do snapshot e todos os volumes restaurados dele são criptografados para a CMK fornecida. As alterações feitas no snapshot compartilhado original, seu status de criptografia ou a CMK compartilhada não têm efeito em sua cópia.

Para obter mais informações, consulte [Cópia de um snapshot do Amazon EBS](#).

Criptografia do Amazon EBS e Eventos do CloudWatch

O Amazon EBS oferece suporte ao Eventos do Amazon CloudWatch para determinados cenários relacionados à criptografia. Para obter mais informações, consulte [Eventos do Amazon CloudWatch para Amazon EBS](#).

Amazon EBS e NVMe

Os volumes do EBS são expostos como dispositivos de blocos NVMe em [Instâncias baseadas em Nitro \(p. 179\)](#). Os nomes dos dispositivos são `/dev/nvme0n1`, `/dev/nvme1n1` etc. 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.

Note

As garantias de desempenho do EBS declaradas em [Detalhes do produto Amazon EBS](#) são válidas, independentemente da interface do dispositivo de blocos.

As seguintes instâncias baseadas em Nitro oferecem suporte a volumes de armazenamento de instâncias NVMe: C5d, I3, F1, M5d, p3dn.24xlarge, R5d e z1d. Para obter mais informações, consulte [Volumes SSD de NVMe \(p. 966\)](#).

Tópicos

- [Instalar ou atualizar o driver NVMe \(p. 930\)](#)
- [Identificar o dispositivo EBS \(p. 930\)](#)
- [Trabalhar com volumes de NVMe do EBS \(p. 932\)](#)
- [Tempo limite de operação de E/S \(p. 932\)](#)

Instalar ou atualizar o driver NVMe

As seguintes AMIs incluem os drivers NVMe necessários:

Se estiver usando uma AMI que não inclua o driver NVMe, você poderá instalar o driver em sua instância usando o procedimento a seguir.

Para instalar o driver NVMe

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 upgrade -y linux-aws
```

Para o Ubuntu 14.04, você pode instalar o pacote mais recente `linux-aws` da seguinte maneira:

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.

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.
 - Os volumes do EBS anexados pelo NVMe têm o ID do volume do EBS definido como o número de série na identificação do dispositivo.
 - 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 [Criação de um volume do Amazon EBS para uso no Linux](#) e [Inicialização do volume incorreto](#).

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:

```
[ec2-user ~]$ sudo /sbin/ebsnvme-id /dev/nvme1n1
Volume ID: vol-01324f611e2463981
/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.

Outras APIs 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.

O exemplo a seguir obtém o ID do volume e o nome do dispositivo. O nome do dispositivo está disponível por meio da extensão específica ao fornecedor do controlador NVMe (384:4095 bytes da identificação do controlador):

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	MOUNTPOINT
nvme0n1	/
loop0	

```
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 [Disponibilização de um volume do Amazon EBS para uso no Linux \(p. 864\)](#).

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
```

Antes de desanexar um volume de NVMe do EBS, você deverá sincronizá-lo e desmontá-lo. Quando você desanexa um volume de NVMe do EBS, a opção de forçar fica implicitamente ativada. Portanto, a instância não tem oportunidade de liberar caches ou metadados do sistema de arquivos antes de desanexar o volume.

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` (ou o parâmetro de inicialização `nvme.io_timeout` para kernels Linux anteriores à versão 4.6). Para fins de teste, você também pode atualizar dinamicamente o tempo limite gravando no `/sys/module/nvme_core/parameters/io_timeout` usando o editor de texto de sua preferência. Se a latência de E/S exceder o valor desse parâmetro, o driver NVMe do Linux falhará na E/S e retornará um erro ao sistema de arquivos ou ao aplicativo. Dependendo da operação de E/S, seu sistema de arquivos ou aplicativo 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 a instâncias do Xen, recomendamos configurar esse tempo limite com o maior valor possível. Para os kernels atuais, o máximo é 4294967295, enquanto para os kernels anteriores o máximo é 255. O parâmetro de inicialização `nvme.io_timeout` já está definido como o valor máximo para as seguintes distribuições do Linux:

- AMI do Amazon Linux 2017.09.01 ou posterior
- Canonical 4.4.0-1041 ou posterior
- SLES 12 SP2 (4.4 kernel) ou posterior
- RHEL 7.5 (3.10.0-862 kernel) ou posterior

Você pode 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 `Numerical result out of range` ao tentar salvar o arquivo.

Desempenho do volume do Amazon EBS em instâncias do Linux

Vários fatores, como as características de E/S e a configuração das instâncias e volumes, podem afetar o desempenho 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 um bom desempenho imediatamente. Contudo, há alguns casos em que talvez seja necessário fazer alguns ajustes para atingir o desempenho máximo na plataforma. Este tópico discute práticas recomendadas gerais, bem como o ajuste de desempenho específico de alguns casos de uso. Recomendamos que você ajuste o desempenho com informações de sua carga de trabalho 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 o desempenho de E/S necessário e as opções para melhorar o desempenho de Amazon EBS a fim de atender a esses requisitos.

Note

Atualizações da AWS para desempenho de tipos de volume do EBS podem não ter efeito imediato em seus volumes existentes. Para ver o desempenho completo 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 desempenho do Amazon EBS \(p. 933\)](#)
- [Configuração de instância do Amazon EC2 \(p. 935\)](#)
- [Características e monitoramento de E/S \(p. 937\)](#)
- [Inicialização de volumes do Amazon EBS \(p. 939\)](#)
- [Configuração RAID no Linux \(p. 940\)](#)
- [Comparar volumes do EBS \(p. 945\)](#)

Dicas de desempenho do Amazon EBS

Essas dicas representam as melhores práticas para obter o desempenho 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 [Configuração de instância do Amazon EC2 \(p. 935\)](#).

Noções de como o desempenho é calculado

Quando você mede o desempenho dos volumes do EBS, é importante compreender as unidades de medida envolvidas e como o desempenho é calculado. Para obter mais informações, consulte [Características e monitoramento de E/S \(p. 937\)](#).

Noções da carga de trabalho

Há uma relação entre o desempenho máximo 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 (desempenho, E/S e latência) afeta os outros, e aplicativos diferentes são mais sensíveis em relação a um fator do que outros. Para obter mais informações, consulte [Comparar volumes do EBS \(p. 945\)](#).

Esteja ciente da penalidade de desempenho 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 restaurado de um snapshot. Você pode evitar esse impacto de desempenho acessando cada bloco antes de colocar o volume em produção. Esse processo é chamado

inicialização (conhecido anteriormente como pré-aquecimento). Para obter mais informações, consulte [Inicialização de volumes do Amazon EBS \(p. 939\)](#).

Fatores que podem reduzir o desempenho do HDD

Quando você cria um snapshot de um volume de Disco rígido com throughput otimizado (`st1`) ou Cold HDD (`sc1`), o desempenho pode cair até o valor basal do volume enquanto o snapshot estiver em andamento. Esse comportamento é específico desses tipos de volumes. Outros fatores que podem limitar o desempenho incluem controlar uma taxa de transferência maior do que a instância pode suportar, a penalidade de desempenho encontrada ao inicializar volumes restaurados de um snapshot e 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 volumes do Amazon EBS](#).

O desempenho também pode ser afetado se seu aplicativo 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 seu aplicativo 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 um desempenho consistente dos volumes, consulte [Características e monitoramento de E/S \(p. 937\)](#).

Aumentar a leitura antecipada para alta taxa de transferência, cargas de trabalho com muita leitura em `st1` e `sc1`

Algumas cargas de trabalho 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 é retornada 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 carga de trabalho consistir em grandes E/S sequenciais. Se consistir principalmente em pequenas E/S aleatórias, essa configuração acabará reduzindo o desempenho. Em geral, se sua carga de trabalho consiste principalmente em operações de E/S pequenas ou aleatórias, você deve considerar usar um volume Finalidade geral (SSD) (`gp2`) em vez de `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 \(p. 937\)](#).

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
```

Reinicie sua instância para que essa configuração seja implementada.

Para obter mais informações, consulte [Configuração de GRUB](#). 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 o desempenho](#) referente a esse tópico.

Use 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. Você pode adicionar vários volumes `gp2`, `io1`, `st1` ou `sc1` juntos em uma configuração de RAID 0 para utilizar a largura de banda disponível para essas instâncias. Para obter mais informações, consulte [Configuração RAID no Linux \(p. 940\)](#).

Acompanhar o desempenho usando o Amazon CloudWatch

A Amazon Web Services fornece métricas de desempenho 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 [Como monitorar o status de seus volumes \(p. 868\)](#).

Configuração de instância do Amazon EC2

Quando você planeja e configura volumes do EBS para seu aplicativo, é importante considerar a configuração das instâncias às quais você anexará volumes. Para que os volumes do EBS tenham o melhor desempenho possível, você deve anexá-los a uma instância com largura de banda suficiente para comportar seus volumes, como uma instância otimizada para EBS ou uma instância com conectividade de rede de 10 gigabits. Isso é especialmente importante para o stripe de vários volumes juntos em uma configuração de RAID.

Usar instâncias otimizadas para EBS ou de rede de 10 gigabits

Todas as cargas de trabalho sensíveis ao desempenho que exijam uma variabilidade mínima e Amazon EC2 dedicado ao tráfego de Amazon EBS, como bancos de dados de produção ou aplicativos de negócios, devem usar volumes que sejam anexados a uma instância otimizada para EBS ou a uma

instância com conectividade de rede de 10 gigabits. As instâncias do EC2 que não atendem a esses critérios não oferecem nenhuma garantia de recursos de rede. A única forma de garantir uma largura de banda de rede constante e confiável entre sua instância do EC2 e seus volumes do EBS é executar a instância do EC2 como otimizada para EBS ou escolher um tipo de instância com conectividade de rede de 10 gigabits. Para ver quais tipos de instância incluem conectividade de rede de 10 gigabits, consulte [Tipos de instâncias do Amazon EC2](#). Para obter informações sobre a configuração de instâncias otimizadas para EBS, consulte [Instâncias otimizadas para Amazon EBS](#).

Escolher uma instância do EC2 com largura de banda suficiente

Ao executar uma instância otimizada para EBS, você obtém uma conexão dedicada entre a instância do EC2 e o volume do EBS. Contudo, ainda é possível provisionar volumes do EBS que ultrapassem a largura de banda disponível para determinados tipos de instância, especialmente quando é feito o stripe de vários volumes em uma configuração de RAID. Para obter informações sobre os tipos de instância disponíveis a serem executadas como instâncias otimizadas para EBS, a taxa de transferência dedicada a esses tipos de instância, a largura de banda dedicada ao Amazon EBS, a quantidade máxima de IOPS que a instância pode suportar se você estiver usando E/S de 16 KB tamanho e largura de banda de E/S aproximada disponível nessa conexão, consulte [Tipos de instâncias que oferecem suporte à otimização de EBS \(p. 917\)](#).

Escolha uma instância otimizada para EBS que forneça uma taxa de transferência de EBS mais dedicada do que as necessidades de sua aplicação. Caso contrário, a conexão de Amazon EBS para Amazon EC2 será um gargalo para o desempenho.

Observe que algumas instâncias com interfaces de rede de 10 gigabits não oferecem otimização para EBS e, portanto, não têm largura de banda de EBS dedicada disponível. No entanto, você poderá usar toda essa largura de banda para o tráfego de Amazon EBS se o aplicativo não estiver pressionando outros tráfegos de rede competindo com o Amazon EBS. Algumas instâncias de rede de 10 gigabits oferecem largura de banda de Amazon EBS dedicada além de uma interface de 10 gigabits que é usada exclusivamente para o tráfego de rede.

Se um tipo de instância tiver um valor máximo de IOPS de 16 KB igual a 4.000, esse valor será um melhor cenário absoluto e não será garantido, a menos que a instância seja executada como otimizada para EBS. Para obter consistentemente o melhor desempenho, você precisa executar instâncias como otimizadas para EBS. Contudo, se você anexar um volume de `io1` de 4.000 IOPS a uma instância otimizada para EBS com um valor de IOPS de 16 KB igual a 4.000, o limite da largura de banda da conexão entre o Amazon EC2 e o Amazon EBS impedirá que esse volume forneça a taxa de transferência agregada máxima de 500 MB/s disponível. Nesse caso, devemos usar uma instância do EC2 otimizada para EBS que ofereça suporte a uma taxa de transferência de 500 MB/s pelo menos.

Volumes do tipo Finalidade geral (SSD) (`gp2`) têm um limite de taxa de transferência entre 128 MiB/s e 250 MiB/s por volume (dependendo do tamanho do volume), que é ideal para uma conexão otimizada para EBS de 1.000 Mbps. Tipos de instância que oferecem mais de 1.000 Mbps de taxa de transferência para Amazon EBS podem usar mais de um volume do `gp2` para usufruir da taxa de transferência disponível. Volumes do tipo Provisioned IOPS SSD (`io1`) têm um limite de taxa de transferência de 256 KiB para cada IOPS provisionadas, até o máximo de 1.000 MiB/s (a 64.000 IOPS). Para obter mais informações, consulte [Tipos de volume do Amazon EBS \(p. 844\)](#).

Note

Esses valores de desempenho para `io1` são garantidos apenas para volumes anexados a instâncias baseadas em Nitro. Para outras instâncias, o AWS garante desempenho de até 500 MiB/s e 32.000 IOPS por volume. Para obter mais informações, consulte [Tipos de volumes do Amazon EBS](#).

Tipos de instância com conectividade de rede de 10 gigabits oferecem suporte a até 800 MB/s de taxa de transferência e 48.000 IOPS de 16 K para volumes do Amazon EBS descriptografados e a até 25.000 IOPS de 16 K para volumes do Amazon EBS criptografados. Como o valor máximo de `io1` para volumes do EBS é 64.000 para volumes de `io1` e 16.000 para volumes de `gp2`, você pode usar vários volumes do

EBS simultaneamente para atingir o nível de desempenho de E/S disponível para esses tipos de instância. Para obter informações sobre quais tipos de instância incluem conectividade de rede de 10 gigabits, consulte [Tipos de instâncias do Amazon EC2](#).

Você deve usar instâncias otimizadas para EBS quando disponível para obter todos os benefícios dos volumes de Amazon EBS e gp2 do io1. Para obter mais informações, consulte [Amazon EBS – instâncias otimizadas \(p. 916\)](#).

Características e monitoramento de E/S

Em uma determinada configuração de volume, certas características de E/S controlam o desempenho dos volumes do EBS. Volumes baseados em SSD (Finalidade geral (SSD) (gp2) e Provisioned IOPS SSD (io1)) apresentam desempenho consistente quando uma operação de E/S é aleatória ou sequencial. Volumes baseados em HDD (Disco rígido com throughput otimizado (st1) e Cold HDD (sc1)) apresentam desempenho ideal somente quando as operações de E/S são grandes e sequenciais. Para entender como os volumes de SSD e HDD serão executados em seu aplicativo, 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.

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 é contabilizado como uma única E/S. O tamanho de E/S é limitado a 256 KiB para os volumes SSD e 1.024 KiB para volumes HDD, pois os volumes SSD lidam com E/S pequena ou aleatória de maneira muito mais eficiente do que os volumes HDD.

Quando operações de E/S pequenas (maior ou igual a 32 KiB) são fisicamente contíguas, o Amazon EBS tenta fundi-las em uma única operação E/S até o tamanho máximo. Por exemplo, para volumes de SSD, uma única operação de E/S de 1.024 KiB é contada como 4 operações ($1.024 \div 256 = 4$), enquanto 8 operações contíguas de E/S a 32 KiB são contadas como 1 operação ($8 \times 32 = 256$). Contudo, 8 operações aleatórias de E/S em 32 KiB cada contam como 8 operações. Cada operação de E/S com menos de 32 KiB conta como 1 operação.

Da mesma forma, para volumes baseados em HDD, uma única operação de E/S de 1.024 KiB e 8 operações sequenciais de 128 KiB contam como uma operação. Contudo, 8 operações aleatórias de E/S em 128 KiB contam como 8 operações.

Portanto, quando você cria um volume baseado em SSD com suporte a 3.000 IOPS (provisionando um volume de io1 com 3.000 IOPS ou dimensionando um volume de gp2 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 carga de trabalho, dependendo da sensibilidade de seu aplicativo específico em relação à IOPS e à latência. Se sua carga de trabalho não estiver fornecendo solicitações de E/S suficientes para usar integralmente o desempenho disponível para seu volume do EBS, o volume pode não fornecer a IOPS ou a taxa de transferência que você provisionou.

Os aplicativos com transações intensivas são sensíveis ao aumento de latência de E/S e são bem adequados para volumes io1 e gp2 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.

Os aplicativos com taxa de transferência intensiva são menos sensíveis ao aumento da latência de E/S e são bem adequados para volumes de `st1` e de `sc1` 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 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 \(p. 844\)](#).

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 carga de trabalho 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 carga de trabalho 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 o desempenho ideal. Para obter mais informações, consulte [Configuração de instância do Amazon EC2 \(p. 935\)](#). Outra causa possível para a ausência da IOPS prevista é que você não está conduzindo E/S suficientes para volumes do EBS.

Monitorar características de E/S com o CloudWatch

Você pode monitorar essas características de E/S com as [métricas do CloudWatch de cada volume \(p. 868\)](#). Métricas importantes a serem consideradas:

- `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, créditos de E/S de volume (para volumes `gp2`) ou créditos de taxa de transferência de volume (para volumes `st1` e `sc1`) são limitados à linha de base. Verifique o valor `BurstBalance` para determinar se seu volume está sendo limitado por esse motivo.

Os volumes `st1` e `sc1` baseados em HDD são projetados para ter desempenho melhor com cargas de trabalho 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 o desempenho.

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 o aplicativo não está tentando gerar mais IOPS do que você provisionou. Se o aplicativo exigir um número maior de IOPS do que seu volume pode fornecer, você deve considerar usar um volume `gp2` maior com um nível de desempenho básico superior ou um volume `io1` com mais IOPS provisionada para atingir latências mais rapidamente.

Para obter mais informações sobre as características de E/S do Amazon EBS, consulte a apresentação re:Invent [Amazon EBS: como projetar visando o desempenho](#) referente a esse tópico.

Inicialização de volumes do Amazon EBS

Os novos volumes do EBS recebem seu desempenho máximo no momento em que são disponibilizados e não requerem inicialização (antes conhecido como pré-aquecimento). Contudo, blocos de armazenamento em volumes que foram restaurados a partir de snapshots devem ser inicializados (puxados do Amazon S3 e gravados no volume) antes de 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. Para a maioria dos aplicativos, é aceitável amortizar esse custo ao longo da vida útil do volume. O desempenho é restaurado depois de os dados serem acessados uma vez.

Você pode evitar esse impacto no desempenho em um ambiente de produção lendo todos os blocos em seu volume antes de usá-lo. Esse processo se chama inicialização. Para um novo volume criado de um snapshot, você deve ler todos os blocos que têm dados antes de usar o volume.

Important

Durante a inicialização dos volumes de `io1` que foram restaurados de snapshots, o desempenho do volume pode ser reduzido 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. Isso é esperado, e você pode ignorar o estado de `warning` em volumes `io1` enquanto estiver inicializando esses volumes. Para obter mais informações, consulte [Como monitorar volumes com verificações de status \(p. 873\)](#).

Inicialização de volumes de Amazon EBS no Linux

Os novos volumes do EBS recebem seu desempenho máximo no momento em que são disponibilizados e não requerem inicialização (antes conhecido como pré-aquecimento). Para volumes que foram restaurados 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 inicializar um volume restaurado 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 o desempenho 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` variará 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 [Disponibilização de um volume do Amazon EBS para uso no Linux \(p. 864\)](#).

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. Para obter um desempenho de E/S melhor do que o alcançável com um único volume, o RAID 0 pode distribuir vários volumes juntos; para redundância na instância, o RAID 1 pode espelhar dois volumes juntos.

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 Windows, consulte [Configuração de RAID no Windows](#) no Guia do usuário do Amazon EC2 para instâncias do Windows.

Tópicos

- [Opções de configuração de RAID \(p. 941\)](#)
- [Criação de uma matriz de RAID no Linux \(p. 942\)](#)
- [Criar snapshots de volumes em um array RAID \(p. 945\)](#)

Opções de configuração de RAID

A tabela a seguir compara as opções comuns de RAID 0 e de RAID 1.

Configuração	Use	Vantagens	Desvantagens
RAID 0	Quando o desempenho de E/S é mais importante do que a tolerância a falhas; por exemplo, como em um banco de dados muito usado (onde a replicação de dados já está configurada separadamente).	A E/S é distribuída entre os volumes em uma stripe. Se você adicionar um volume, obterá a adição direta de taxa de transferência.	O desempenho da stripe é limitado pelo volume de pior desempenho do conjunto. A perda de um único volume leva a uma perda completa dos dados da matriz.
RAID 1	Quando a tolerância a falhas é mais importante do que o desempenho de E/S; por exemplo, em um aplicativo crítico.	Mais seguro do ponto de vista da durabilidade de dados.	Não proporciona melhoria do desempenho da gravação; 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.

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.

Criar uma matriz de RAID 0 permite atingir um nível de desempenho para um sistema de arquivos maior do que você pode provisionar em um único volume Amazon EBS. Uma matriz de RAID 1 oferece um "espelho" de seus dados para redundância adicional. Antes de executar esse procedimento, você precisa decidir o tamanho que deve ter sua matriz de RAID e quantos IOPS você deseja provisionar.

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. O tamanho e a largura de banda resultantes de uma matriz de RAID 1 são iguais ao tamanho e à largura de banda dos volumes na matriz. Por exemplo, dois volumes de io1 do Amazon EBS de 500 GiB, com 4.000 IOPS provisionadas cada um, criarião uma matriz de RAID 0 de 1.000 GiB com uma largura de banda de 8.000 IOPS e 1.000 MB/s de taxa de transferência ou uma matriz RAID 1 de 500 GiB com uma largura de banda de 4.000 IOPS e 500 MB/s de taxa de transferência.

Esta documentação fornece exemplos básicos de configuração de RAID. Para obter mais informações sobre a configuração de RAID, desempenho e recuperação, consulte o Wiki de RAID do Linux em https://raid.wiki.kernel.org/index.php/Linux_Raid.

Criação de uma matriz de RAID no Linux

Use o procedimento a seguir para criar a matriz de RAID. Você pode obter instruções sobre instâncias Windows em [Criação de uma matriz RAID no Windows](#) no Guia do usuário do Amazon EC2 para instâncias do Windows.

Para criar uma matriz de RAID no Linux

1. Crie os volumes do Amazon EBS para sua matriz. Para obter mais informações, consulte [Criação de um volume do Amazon EBS \(p. 860\)](#).

Important

Crie volumes com tamanho e valores idênticos de IOPS 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 [Configuração de instância do Amazon EC2 \(p. 935\)](#).

2. Anexe os volumes do Amazon EBS à instância na qual você deseja hospedar a matriz. Para obter mais informações, consulte [Associação de um volume do Amazon EBS a uma instância \(p. 863\)](#).
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.

(Somente RAID 0) 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
```

(Somente RAID 1) Para criar uma matriz de RAID 1, execute o seguinte comando (observe a opção --level=1 para espelhar a matriz):

```
[ec2-user ~]$ sudo mdadm --create --verbose /dev/md0 --level=1 --name=MY_RAID --raid-devices=number_of_volumes device_name1 device_name2
```

4. 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 : [raid1]
md0 : active raid1 xvdf[1] xvdf[0]
      20955008 blocks super 1.2 [2/2] [UU]
      [======>.....]  resync = 46.8% (9826112/20955008) finish=2.9min
      speed=63016K/sec
```

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 : Mon Jun 27 11:31:28 2016
      Raid Level : raid1
      Array Size : 20955008 (19.98 GiB 21.46 GB)
      Used Dev Size : 20955008 (19.98 GiB 21.46 GB)
      Raid Devices : 2
      Total Devices : 2
      Persistence : Superblock is persistent

      Update Time : Mon Jun 27 11:37:02 2016
      State : clean
...
...
...

      Number  Major  Minor  RaidDevice State
          0      202      80          0    active sync   /dev/sdf
          1      202      96          1    active sync   /dev/sdg
```

- 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 do aplicativo 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).

- 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 colocar esse arquivo em outro local. Para obter mais informações, consulte man mdadm.conf no sistema 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 que valores deve inserir, use os valores no exemplo abaixo (`defaults,nofail 0 2`). Para obter mais informações sobre as entradas /etc/fstab, consulte a página manual fstab (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 um array 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, não como um todo. A restauração dos volumes do EBS em um array RAID de snapshots que não estão sincronizados prejudica a integridade do array.

Para criar um conjunto consistente de snapshots para o array RAID, impeça que os aplicativos gravem no array RAID e descarregue todos os caches no disco. Para impedir gravações no array RAID, você pode executar etapas, como interromper aplicativos, interromper a instância ou desmontar o array RAID. Após interromper todas as atividades de E/S, você pode criar os snapshots. Quando o snapshot foi iniciado ou a API do snapshot retorna com sucesso, é seguro retomar toda a atividade de E/S.

Ao restaurar os volumes do EBS em um array RAID de um conjunto de snapshots, interrompa todas as atividades de E/S, como você fez ao criar os snapshots, e, em seguida, restaure os volumes dos snapshots.

Comparar volumes do EBS

Você pode testar o desempenho dos volumes do Amazon EBS simulando cargas de trabalho 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 o desempenho de E/S.
6. Compare o desempenho 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 o desempenho 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 [Amazon EBS – instâncias otimizadas \(p. 916\)](#).

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 [Amazon EBS – instâncias otimizadas \(p. 916\)](#).

Definição de volumes Provisioned IOPS SSD (io1)

Para criar um volume de io1, escolha Provisioned IOPS SSD ao criar o volume usando o console do Amazon EC2 ou, na linha de comando, especifique --type io1 --iops n, em que n é um número inteiro entre 100 e 64,000. Para obter especificações mais detalhadas do volume do EBS, consulte [Tipos de volume do Amazon EBS \(p. 844\)](#). Para obter informações sobre como criar um volume do EBS, consulte [Criação de um volume do Amazon EBS \(p. 860\)](#). Para obter informações sobre como anexar um volume a uma instância, consulte [Associação de um volume do Amazon EBS a uma instância \(p. 863\)](#).

Para os testes de exemplo, recomendamos que você crie uma matriz de RAID com 6 volumes, que oferece um alto nível de desempenho. Como você será cobrado por gigabytes provisionados (e pelo número de IOPS provisionadas para volumes io1), não pelo número de volumes, não há nenhum custo adicional para criar vários volumes menores e utilizá-los para criar um conjunto de stripe. 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 criar com um conjunto de stripe de seis volumes no Amazon Linux, use um comando como este:

```
[ec2-user ~]$ sudo mdadm --create /dev/md0 --level=0 --chunk=64 --raid-devices=6 /dev/sdf /dev/sdg /dev/sdh /dev/sdi /dev/sdj /dev/sdk
```

Neste exemplo, o arquivo do sistema é XFS. Use o sistema de arquivos que atenda a seus requisitos. Use o comando a seguir para instalar o suporte do sistema de arquivos XFS:

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

Então, use esses comandos para criar, montar e atribuir propriedade ao sistema de arquivos XFS:

```
[ec2-user ~]$ sudo mkdir -p /mnt/p_iops_volo && sudo mkfs.xfs /dev/md0
[ec2-user ~]$ sudo mount -t xfs /dev/md0 /mnt/p_iops_volo
[ec2-user ~]$ sudo chown ec2-user:ec2-user /mnt/p_iops_volo/
```

Estabelecimento de volumes de Disco rígido com throughput otimizado (st1) ou Cold HDD (sc1)

Para criar um volume st1, escolha Disco rígido com throughput otimizado 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 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 [Criação de um volume do Amazon EBS \(p. 860\)](#). Para obter informações sobre como anexar esses volumes à sua instância, consulte [Associação de um volume do Amazon EBS a uma instância \(p. 863\)](#).

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 fácil de configurar um ambiente de testes de desempenho 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.

Para criar um volume de HDD com 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 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 \(p. 947\)](#).

Instalar ferramentas de comparação

A tabela a seguir lista algumas ferramentas possíveis que você pode usar para comparar o desempenho dos volumes do EBS.

Ferramenta	Descrição
fio	<p>Para comparar o desempenho 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> <div style="border: 1px solid black; padding: 5px;"><pre>[ec2-user ~]\$ sudo yum install -y fio</pre></div> <p>Para instalar fio no Ubuntu, execute o seguinte comando:</p> <div style="border: 1px solid black; padding: 5px;"><pre>sudo apt-get install -y fio</pre></div>
Ferramenta de calibração do Oracle Orion	Para calibrar o desempenho 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 cargas de trabalho às quais seus volumes oferecerão suporte. Os comandos fornecidos abaixo servem como exemplos para ajudá-lo a começar a usar.

Escolha do comprimento da fila de volume

Escolha do melhor comprimento da fila de volume com base em sua carga de trabalho e tipo de volume.

Tamanho da fila em volumes baseados em SSD

Para determinar o tamanho ideal da fila para sua carga de trabalho em volumes baseados em SSD, recomendamos que você foque em um comprimento da fila de 1 para cada 1000 IOPS disponíveis (linha de base para volumes gp2 e a quantidade provisionada para volumes io1). Depois, você pode monitorar o desempenho de seu aplicativo e ajustar esse valor com base nos requisitos do aplicativo.

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 seu aplicativo.

Tamanho da fila em volumes baseados em HDD

Para determinar o tamanho ideal da fila para sua carga de trabalho 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 o desempenho 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 seu aplicativo.

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](#).

Desativação de estados C em um sistema 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
```

Comparação de desempenho

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 restaurados de snapshots, certifique-se de inicializá-los antes de avaliar. Para obter mais informações, consulte [Inicialização de volumes do Amazon EBS \(p. 939\)](#).

Quando você terminar de testar seus volumes, consulte os seguintes tópicos para obter ajuda para limpar: [Exclusão de um volume do Amazon EBS \(p. 895\)](#) e [Encerre sua instância \(p. 470\)](#).

Comparação de volumes io1

Execute fio no conjunto de stripe que você criou.

O seguinte comando executa operações de gravação aleatórias de 16 KB.

```
[ec2-user ~]$ sudo fio --directory=/mnt/p_iops_volo --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 aleatória 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 desempenho de E/S de disco com fio](#).

Comparação dos volumes 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 alta taxa de transferência, cargas de trabalho com muita leitura em st1 e sc1 \(p. 934\)](#).

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 cargas de trabalho executam uma combinação de leituras e gravações sequenciais para diferentes partes de dispositivo de blocos. Para comparar essa carga de trabalho, 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 carga de trabalho é um pouco mais complicado do que uma carga de trabalho 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
offset_increment=100g

[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
```

Em seguida, execute o seguinte comando:

```
[ec2-user ~]$ sudo fio fio_rw_mix.cfg
```

Para obter mais informações sobre como interpretar os resultados, consulte o tutorial [Inspeção de desempenho 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.

Eventos do Amazon CloudWatch para Amazon EBS

O Amazon EBS emite notificações com base no Eventos do Amazon CloudWatch para uma variedade de alterações no status da criptografia, do snapshot e do volume. Com o Eventos do CloudWatch, 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.

Para obter mais informações, consulte [Como usar eventos](#) no Guia do usuário do Amazon CloudWatch. Para referência da API completa, consulte a [Referência de API do EC2](#).

Tópicos

- [Eventos de volume do EBS \(p. 950\)](#)
- [Eventos de snapshot do EBS \(p. 953\)](#)
- [Uso do Amazon Lambda para manipular o Eventos do CloudWatch \(p. 956\)](#)

Eventos de volume do EBS

Esta seção define os eventos de volume do Amazon EBS com suporte e fornece exemplos de saída de eventos para cenários específicos. Os eventos no CloudWatch são representados como objetos JSON. Para obter mais informações sobre o formato e o conteúdo de objetos de evento, consulte [Eventos e padrões de eventos](#) no Guia do usuário do Eventos do Amazon CloudWatch.

Note

Informações adicionais sobre volumes do EBS que não são capturadas pelo Cloudwatch são disponibilizadas através da API [DescribeVolumes](#) e do comando [describe-volumes](#) da CLI.

Os campos que são exclusivos a eventos de EBS estão contidos na seção "detalhes" dos objetos JSON mostrados abaixo. O campo "evento" contém o nome do evento. O campo "resultados" contém o status concluído da ação que acionou o evento.

Tópicos

- Criar volume (`createVolume`) (p. 951)
- Excluir volume (`deleteVolume`) (p. 952)
- Anexar ou reanexar volumes (`attachVolume`, `reattachVolume`) (p. 952)

Criar volume (`createVolume`)

O evento `createVolume` é enviado à sua conta da AWS quando uma ação para criar um volume é concluída. Esse evento pode ter um resultado de `available` ou `failed`. Ocorrerá uma falha se uma chave inválida do KMS 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 de 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 de 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 é concluída. 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. Se você usar uma chave do KMS para criptografar um volume do EBS e a chave se tornar inválida, o EBS emitirá um evento se a chave for usada posteriormente para anexar ou reanexar 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 de KMS.

Note

A AWS pode tentar reanexar a um volume seguindo a manutenção rotineira do servidor.

```
{  
    "version": "0",  
    "id": "01234567-0123-0123-0123-0123456789ab",  
    "detail-type": "EBS Volume Notification",  
    "source": "aws.ec2",  
    "account": "012345678901",  
    "time": "yyyy-mm-ddThh:mm:ssZ",  
    "region": "us-east-1",  
    "resources": [  
        "arn:aws:ec2:us-east-1:0123456789ab:volume/vol-01234567",  
        "arn:aws:kms:us-east-1:0123456789ab:key/01234567-0123-0123-0123-0123456789ab"  
    ],  
    "detail": {  
        "event": "attachVolume",  
        "result": "failed",  
        "cause": "arn:aws:kms:us-east-1:0123456789ab:key/01234567-0123-0123-0123-0123456789ab  
is pending deletion.",  
        "request-id": ""  
    }  
}
```

A lista abaixo é um exemplo de um objeto JSON emitido por EBS depois de um evento `reattachVolume` com falha. A causa da falha foi a exclusão pendente de uma chave de 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

Tópicos

- [Criar snapshot \(createSnapshot\) \(p. 953\)](#)
- [Copiar snapshot \(copySnapshot\) \(p. 954\)](#)
- [Compartilhar snapshot \(shareSnapshot\) \(p. 955\)](#)

Criar snapshot (createSnapshot)

O evento `createSnapshot` é enviado à sua conta da AWS quando uma ação para criar um snapshot 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 `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"    }  
}
```

Copiar snapshot (`copySnapshot`)

O evento `copySnapshot` é enviado à sua conta da AWS quando uma ação para copiar um snapshot 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 pelo EBS após um evento `copySnapshot` bem-sucedido. O valor de `snapshot_id` é o ARN do snapshot recém-criado. Na seção `detail`, o valor de `source` é o ARN do snapshot de origem. `StartTime` e `EndTime` representam o início e o fim da ação `copy-snapshot`.

```
{  
    "version": "0",  
    "id": "01234567-0123-0123-0123-012345678901",  
    "detail-type": "EBS Snapshot Notification",  
    "source": "aws.ec2",  
    "account": "123456789012",  
    "time": "yyyy-mm-ddThh:mm:ssZ",  
    "region": "us-east-1",  
    "resources": [  
        "arn:aws:ec2::us-west-2:snapshot/snap-01234567"  
    ],  
    "detail": {  
        "event": "copySnapshot",  
        "result": "succeeded",  
        "cause": "",  
        "request-id": "",  
        "snapshot_id": "arn:aws:ec2::us-west-2:snapshot/snap-01234567",  
        "source": "arn:aws:ec2::eu-west-1:snapshot/snap-76543210",  
        "StartTime": "yyyy-mm-ddThh:mm:ssZ",  
        "EndTime": "yyyy-mm-ddThh:mm:ssZ",  
        "Incremental": "True"  
    }  
}
```

}

A lista abaixo é um exemplo de um objeto JSON emitido por EBS depois de um evento `copySnapshot` com falha. A causa da falha era um ID de snapshot de origem inválido. O valor de `snapshot_id` é o nome de recurso da Amazon (ARN) do snapshot com falha. Na seção `detail`, o valor de `source` é o ARN do snapshot de origem. `StartTime` e `EndTime` representam o início e o fim da ação `copy-snapshot`.

```
{  
    "version": "0",  
    "id": "01234567-0123-0123-0123-012345678901",  
    "detail-type": "EBS Snapshot Notification",  
    "source": "aws.ec2",  
    "account": "123456789012",  
    "time": "yyyy-mm-ddThh:mm:ssZ",  
    "region": "us-east-1",  
    "resources": [  
        "arn:aws:ec2::us-west-2:snapshot/snap-01234567"  
    ],  
    "detail": {  
        "event": "copySnapshot",  
        "result": "failed",  
        "cause": "Source snapshot ID is not valid",  
        "request-id": "",  
        "snapshot_id": "arn:aws:ec2::us-west-2:snapshot/snap-01234567",  
        "source": "arn:aws:ec2::eu-west-1:snapshot/snap-76543210",  
        "StartTime": "yyyy-mm-ddThh:mm:ssZ",  
        "EndTime": "yyyy-mm-ddThh:mm:ssZ"  
    }  
}
```

Compartilhar snapshot (`shareSnapshot`)

O evento `shareSnapshot` é enviado à sua conta da AWS quando outra conta compartilha um snapshot com ela. O resultado é sempre `succeeded`.

Dados de eventos

A lista abaixo é um exemplo de um objeto JSON emitido por EBS depois de um evento `shareSnapshot` concluído. Na seção `detail`, o valor de `source` é o número da conta da AWS do usuário que compartilhou o snapshot com você. `StartTime` e `EndTime` representam o início e o fim da ação `shareSnapshot`. O evento `shareSnapshot` é emitido somente quando um snapshot privado é compartilhado com outro usuário. Compartilhar um snapshot público não aciona o evento.

```
{  
    "version": "0",  
    "id": "01234567-0123-0123-0123-012345678901",  
    "detail-type": "EBS Snapshot Notification",  
    "source": "aws.ec2",  
    "account": "012345678901",  
    "time": "yyyy-mm-ddThh:mm:ssZ",  
    "region": "us-east-1",  
    "resources": [  
        "arn:aws:ec2::us-west-2:snapshot/snap-01234567"  
    ],  
    "detail": {  
        "event": "shareSnapshot",  
        "result": "succeeded",  
        "cause": "",  
        "request-id": "",  
        "snapshot_id": "arn:aws:ec2::us-west-2:snapshot/snap-01234567",  
        "source": 012345678901,  
        "target": 123456789012  
    }  
}
```

```
        "StartTime": "yyyy-mm-ddThh:mm:ssZ",
        "EndTime": "yyyy-mm-ddThh:mm:ssZ"
    }
}
```

Uso do Amazon Lambda para manipular o Eventos do CloudWatch

Você pode usar o Amazon EBS e o Eventos do CloudWatch 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 Eventos do Amazon CloudWatch 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.

Para copiar um snapshot concluído em outra região

1. Crie uma política do IAM, como a mostrada no exemplo a seguir, para fornecer permissões para executar uma ação `CopySnapshot` e gravá-la no log do Eventos do CloudWatch. 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 (Snapshots do Amazon EBS).
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 Habilida).
10. Selecione Criar regra.

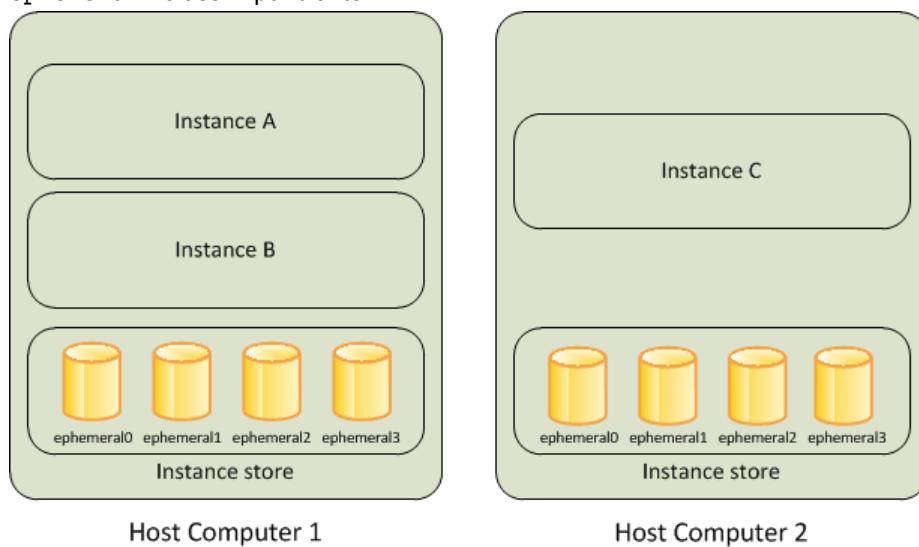
A regra agora deve aparecer na guia Rules (Regras). No exemplo mostrado, o evento que você configurou deve ser emitido pelo EBS na próxima vez você copiar um snapshot.

Armazenamento de instâncias do Amazon EC2

Um armazenamento de instâncias fornece armazenamento temporário em nível de bloco para a instância. Esse armazenamento está localizado em discos que estão anexados fisicamente ao computador host. O armazenamento de instâncias é ideal para o armazenamento temporário de informações que são alteradas frequentemente, como buffers, caches, dados de rascunho e outros conteúdos temporários ou para dados replicados em toda a frota de instâncias, como um grupo com平衡amento de carga de servidores Web.

Um armazenamento de instâncias consiste em um ou mais volumes de armazenamento de instâncias expostos como dispositivos de bloco. O tamanho de um armazenamento de instância e o número de dispositivos disponíveis varia por tipo de instância.

Os dispositivos virtuais para volumes de armazenamento de instâncias são `ephemeral[0-23]`. Tipos de instância que oferecem suporte a um volume de armazenamento de instâncias têm `ephemeral0`. Os tipos de instância que oferecem suporte a dois volumes de armazenamento de instâncias têm `ephemeral0` e `ephemeral1` e assim por diante.



Tópicos

- [Vida útil do armazenamento de instâncias \(p. 958\)](#)
- [Volumes de armazenamento de instâncias \(p. 959\)](#)
- [Adicionar volumes de armazenamento de instâncias à instância do EC2 \(p. 962\)](#)
- [Volumes de armazenamento de instâncias SSD \(p. 965\)](#)
- [Volumes de troca de armazenamento de instâncias \(p. 967\)](#)
- [Como otimizar o desempenho dos discos para volumes de armazenamento de instâncias \(p. 969\)](#)

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 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 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.

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 \(p. 962\)](#).

Alguns tipos de instância usam unidades de estado sólido (SSD) NVMe ou SATA para fornecer um alto desempenho 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 \(p. 965\)](#).

A tabela a seguir fornece a quantidade, o tamanho, o tipo e as otimizações de desempenho 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	✓	
c5d.large	1 x 50 GB	SSD de NVMe		✓

Amazon Elastic Compute Cloud
User Guide for Linux Instances
Volumes de armazenamento de instâncias

Tipo de instância	Volumes de armazenamento de instâncias	Tipo	Precisa de inicialização*	Suporte para TRIM**
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.18xlarge	2 x 900 GB (1.8 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		
d2.8xlarge	24 x 2.000 GB (48 TB)	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	✓	
h1.2xlarge	1 x 2000 GB (2 TB)	HDD		
h1.4xlarge	2 x 2000 GB (4 TB)	HDD		
h1.8xlarge	4 x 2000 GB (8 TB)	HDD		
h1.16xlarge	8 x 2000 GB (16 TB)	HDD		
hs1.8xlarge	24 x 2.000 GB (48 TB)	HDD	✓	
i2.xlarge	1 x 800 GB	SSD		✓
i2.2xlarge	2 x 800 GB (1.6 TB)	SSD		✓
i2.4xlarge	4 x 800 GB (3.2 TB)	SSD		✓
i2.8xlarge	8 x 800 GB (6.4 TB)	SSD		✓
i3.large	1 x 475 GB	SSD de NVMe		✓
i3.xlarge	1 x 950 GB	SSD de NVMe		✓
i3.2xlarge	1 x 1.900 GB	SSD de NVMe		✓
i3.4xlarge	2 x 1.900 GB (3,8 TB)	SSD de NVMe		✓
i3.8xlarge	4 x 1.900 GB (7,6 TB)	SSD de NVMe		✓

Tipo de instância	Volumes de armazenamento de instâncias	Tipo	Precisa de inicialização*	Suporte para TRIM**
i3.16xlarge	8 x 1.900 GB (15,2 TB)	SSD de NVMe		✓
i3.metal	8 x 1.900 GB (15,2 TB)	SSD de NVMe		✓
m1.small	1 x 160 GB†	HDD	✓	
m1.medium	1 x 410 GB	HDD	✓	
m1.large	2 x 420 GB (840 GB)	HDD	✓	
m1.xlarge	4 x 420 GB (1.6 TB)	HDD	✓	
m2.xlarge	1 x 420 GB	HDD	✓	
m2.2xlarge	1 x 850 GB	HDD	✓	
m2.4xlarge	2 x 840 GB (1.68 TB)	HDD	✓	
m3.medium	1 x 4 GB	SSD	✓	
m3.large	1 x 32 GB	SSD	✓	
m3.xlarge	2 x 40 GB (80 GB)	SSD	✓	
m3.2xlarge	2 x 80 GB (160 GB)	SSD	✓	
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.12xlarge	2 x 900 GB (1.8 TB)	SSD de NVMe		✓
m5d.24xlarge	4 x 900 GB (3.6 TB)	SSD de NVMe		✓
p3dn.24xlarge	2 x 900 GB (1.8 TB)	SSD de NVMe		✓
r3.large	1 x 32 GB	SSD		✓
r3.xlarge	1 x 80 GB	SSD		✓
r3.2xlarge	1 x 160 GB	SSD		✓
r3.4xlarge	1 x 320 GB	SSD		✓
r3.8xlarge	2 x 320 GB (640 GB)	SSD		✓
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.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.24xlarge	4 x 900 GB (3.6 TB)	SSD de NVMe		✓
x1.16xlarge	1 x 1.920 GB	SSD		
x1.32xlarge	2 x 1.920 GB (3,84 TB)	SSD		
x1e.xlarge	1 x 120 GB	SSD		
x1e.2xlarge	1 x 240 GB	SSD		
x1e.4xlarge	1 x 480 GB	SSD		
x1e.8xlarge	1 x 960 GB	SSD		
x1e.16xlarge	1 x 1.920 GB	SSD		
x1e.32xlarge	2 x 1.920 GB (3,84 TB)	SSD		
z1d.large	1 x 75 GB	SSD de NVMe		✓
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		✓

* Volumes anexados a determinadas instâncias sofrem uma penalidade de primeira gravação a menos que inicializados. Para obter mais informações, consulte [Como otimizar o desempenho dos discos para volumes de armazenamento de instâncias \(p. 969\)](#).

** Para obter mais informações, consulte [Suporte a TRIM do volume de armazenamento de instâncias \(p. 966\)](#).

† Os tipos de instância `c1.medium` e `m1.small` também incluem um volume de troca de armazenamento de instâncias 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 \(p. 967\)](#).

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 [Mapeamento de dispositivos de blocos \(p. 979\)](#).

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 \(p. 91\)](#). 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 \(p. 841\)](#).

Você pode especificar os volumes de armazenamento de instâncias para uma instância somente ao executar uma instância. Você não pode anexar volumes de armazenamento de instâncias depois de executar a instância.

O número e o tamanho de volumes de armazenamento de instâncias disponíveis varia por tipo de instância. Alguns tipos de instância não oferecem suporte a volumes de armazenamento de instâncias. 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 \(p. 959\)](#). Se o tipo de instância escolhido para a instância oferecer suporte aos volumes de armazenamento de instâncias, adicione-os ao mapeamento de dispositivos de blocos da instância ao executá-la. Depois de executar a instância, verifique se os volumes de armazenamento de instâncias de sua 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

- [Como adicionar volumes de armazenamento de instâncias a uma AMI \(p. 963\)](#)
- [Como adicionar volumes de armazenamento de instâncias a uma instância \(p. 964\)](#)
- [Como disponibilizar volumes de armazenamento de instâncias na instância \(p. 965\)](#)

Como 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. Depois de adicionar volumes de armazenamento de instâncias a uma AMI, qualquer instância que você execute na AMI incluirá esses volumes de armazenamento de instâncias. Quando você executa uma instância, você pode omitir volumes especificados no mapeamento de dispositivos de blocos da AMI e adicionar novos volumes.

Important

Para instâncias M3, especifique volumes de armazenamento de instâncias no mapeamento de dispositivos de blocos da instância, e não a AMI. Amazon EC2 pode ignorar volumes de armazenamento de instâncias que são especificados apenas no mapeamento de dispositivos de blocos da AMI.

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 [Nomenclatura de dispositivos nas instâncias](#))

do Linux (p. 978).) 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 [Acessando o Amazon EC2 \(p. 3\)](#).

- `create-image` ou `register-image` (AWS CLI)
- `New-EC2Image` e `Register-EC2Image` (AWS Tools para Windows PowerShell)

Como 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.

Important

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.

Important

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 Launch Instance (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.

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 [Acessando o Amazon EC2 \(p. 3\)](#).

- `--block-device-mappings` com [run-instances](#) (AWS CLI)
- `-BlockDeviceMapping` com [New-EC2Instance](#) (AWS Tools para Windows PowerShell)

Como 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 \(p. 966\)](#). 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 [Visualização do mapeamento de dispositivos de blocos da instância para volumes do armazenamento de instâncias \(p. 988\)](#).

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 [Como listar os 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.
2. Use o comando `df -h` para visualizar os volumes formatados e montados. Use o `lsblk` para visualizar todos os volumes que foram mapeados na inicialização, mas não formatados e montados.
3. 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`.
 - b. Crie um diretório no qual montar o dispositivo usando o comando `mkdir`.
 - c. Monte o dispositivo no diretório recém-criado usando o comando `mount`.

Volumes de armazenamento de instâncias SSD

A seguintes instâncias oferecem suporte a volumes de armazenamento de instâncias que usam SSD para fornecer alto desempenho de E/S aleatória: C, G2, 2, I3, 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 \(p. 959\)](#).

Para garantir o melhor desempenho 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 o desempenho máximo 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 \(p. 962\)](#).

Volumes SSD de NVMe

As instâncias a seguir oferecem volumes de armazenamento de instâncias SSD de memória expressa não volátil (NVMe): C5d, I3, F1, M5d, p3dn.24xlarge, R5d e z1d. Para acessar os volumes de NVMe, os [drivers de NVMe \(p. 930\)](#) devem ser instalados. As AMIs a seguir atendem a este requisito:

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 estiver usando um sistema operacional compatível mas não vir os dispositivos de NVMe, verifique se o módulo de NVMe está carregado usando o seguinte comando `lsmod`.

```
[ec2-user ~]$ lsmod | grep nvme
nvme               48813   0
```

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.

Supporte a TRIM do volume de armazenamento de instâncias

As seguintes instâncias oferecem suporte a volumes SSD com TRIM: C5d, F1, I2, I3, M5d, p3dn.24xlarge, R3, R5d e z1d.

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 o desempenho. No Linux, você pode usar 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 carga de trabalho 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 \(p. 247\)](#).

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 \(p. 959\)](#).

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 swap space 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. Isso inclui a formatação do espaço de troca do armazenamento de instâncias criadas em [Step 3 \(p. 968\)](#). 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 \(p. 968\)](#) até a [Step 5 \(p. 969\)](#) no novo volume de armazenamento de instâncias.

Como otimizar o desempenho 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 na maioria dos volumes de armazenamento de instâncias ocorre mais lentamente que as gravações subsequentes. Para a maioria dos aplicativos, a amortização desse custo ao longo da vida útil da instância é aceitável. Entretanto, se você precisar de alto desempenho 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 desempenho máximo 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 \(p. 959\)](#).

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 aplicativos acessem os dados por meio de sistemas de arquivos compartilhados. Essa compatibilidade faz do armazenamento de arquivos na nuvem uma opção ideal para cargas de trabalho 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 arquivo de nó único em uma instância de computação usando armazenamento em bloco como base sem escalabilidade ou poucas redundâncias para proteger os dados, a uma solução clusterizada do tipo "faça você mesmo", a uma solução totalmente gerenciada, como [Amazon Elastic File System \(Amazon EFS\) \(p. 970\)](#) ou [Amazon FSx para servidor de arquivos do Windows \(p. 974\)](#).

Amazon Elastic File System (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 cargas de trabalho e aplicativos em execução em várias instâncias. Para obter mais informações, consulte a [página do produto Amazon Elastic File System](#).

Neste tutorial, você cria um sistema de arquivos de EFS e duas instâncias Linux que podem compartilhar dados usando o sistema de arquivos.

Important

O Amazon EFS não tem suporte em instâncias Windows.

Tarefas

- [Pré-requisitos \(p. 971\)](#)
- [Etapa 1: Criar um sistema de arquivos do EFS \(p. 971\)](#)
- [Etapa 2: Montar o sistema de arquivos \(p. 971\)](#)

- [Etapa 3: Testar o sistema de arquivos \(p. 973\)](#)
- [Etapa 4: Limpeza \(p. 973\)](#)

Pré-requisitos

- 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 Amazon EFS \(p. 639\)](#) e [Grupos de segurança para instâncias do Amazon EC2 e destinos de montagem](#) 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 \(p. 23\)](#).

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. Na página Configure file system access (Configurar acesso ao sistema de arquivos), faça o seguinte:
 - a. Em VPC, selecione a VPC a ser usada para suas instâncias.
 - b. Para Create mount targets (Criar destinos de montagem), selecione todas as zonas de disponibilidade.
 - c. Para cada zona de disponibilidade, certifique-se de que o valor de Security group (Grupo de segurança) seja o grupo de segurança criado em [Pré-requisitos \(p. 971\)](#).
 - d. Escolha Next Step (Próxima etapa).
4. Na página Configure optional settings (Definir configurações opcionais), faça o seguinte:
 - a. Para adicionar uma tag com Key=Name, digite o nome do sistema de arquivos em Value (Valor).
 - b. Para Choose performance mode (Escolher modo de desempenho), mantenha a opção padrão, General Purpose (Uso geral).
 - c. Escolha Next Step (Próxima etapa).
5. Na página Review and create (Revisar e criar), escolha Create File System (Criar sistema de arquivos).
6. Depois que o sistema de arquivos for criado, anote o ID do sistema de arquivos, pois você o usará mais adiante neste tutorial.

Etapa 2: Montar o sistema de arquivos

Use o procedimento a seguir para executar duas instâncias `t2.micro`. O script de dados de usuário monta o sistema de arquivos nas duas instâncias durante a execução e as atualizações /etc/fstab para garantir que o sistema de arquivos seja remontado após uma reinicialização de instância. 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. Na página Choose an Amazon Machine Image (Escolher uma imagem de máquina da Amazon), selecione uma AMI do Amazon Linux com o tipo de virtualização de HVM.
4. Na página Choose an Instance Type (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 página Configure Instance Details (Configurar detalhes da instância), faça o seguinte:
 - a. Em Number of instances (Número de instâncias), digite 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 Advanced Details (Detalhes avançados), selecione As text (Como texto) e cole o script a seguir em User data (Dados do usuário). Atualize FILE_SYSTEM_ID com o ID do sistema de arquivos. Você pode atualizar MOUNT_POINT com um diretório para o sistema de arquivos montado.

```
#!/bin/bash
yum update -y
yum install -y nfs-utils
FILE_SYSTEM_ID=fs-xxxxxxxx
AVAILABILITY_ZONE=$(curl -s http://169.254.169.254/latest/meta-data/placement/
availability-zone )
REGION=${AVAILABILITY_ZONE:0:-1}
MOUNT_POINT=/mnt/efs
mkdir -p ${MOUNT_POINT}
chown ec2-user:ec2-user ${MOUNT_POINT}
echo ${FILE_SYSTEM_ID}.efs.${REGION}.amazonaws.com:/ ${MOUNT_POINT} nfs4
    nfsvers=4.1,rsize=1048576,wszie=1048576,hard,timeo=600,retrans=2,_netdev 0 0 >> /
etc/fstab
mount -a -t nfs4
```

- e. Avance para a etapa 6 do assistente.
6. Na página Configure Security Group (Configurar grupo de segurança), escolha Select an existing security group (Selecionar um grupo de segurança existente) e selecione o grupo de segurança criado por você em [Pré-requisitos \(p. 971\)](#) e escolha Review and Launch (Revisar e executar).
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.

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 \(p. 439\)](#).
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 Actions (Ações), Instance State (Estado da instância), Terminate (Encerrar).
5. Quando a confirmação for solicitada, escolha Sim, 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, digite o ID do sistema de arquivos e escolha Delete File System (Excluir sistema de arquivos).

Amazon FSx para servidor de arquivos do Windows

O Amazon FSx para servidor de arquivos do Windows fornece servidores de arquivos do Windows totalmente gerenciados, baseadas em um sistema totalmente nativo de arquivos do Windows com os recursos, o desempenho e a compatibilidade para mudar com facilidade aplicativos empresariais para a AWS.

O Amazon FSx oferece suporte a um amplo conjunto de cargas de trabalho empresariais do Windows com armazenamento de arquivos totalmente gerenciado criado no Microsoft Windows Server. O Amazon FSx tem suporte nativo para recursos do sistema de arquivos do Windows e para o protocolo de Server Message Block (SMB) padrão do setor para acessar o armazenamento de arquivos por uma rede. O Amazon FSx é otimizado para aplicativos empresariais na Nuvem AWS com compatibilidade, desempenho empresarial e recursos nativos do Windows, além de latências consistentes abaixo de milissegundos.

Com o armazenamento de arquivos no Amazon FSx, o código, os aplicativos e as ferramentas que os desenvolvedores e administradores do Windows usam hoje em dia podem continuar a funcionar sem alterações. As cargas de trabalho e os aplicativos do Windows que são ideais para o Amazon FSx incluem cargas de trabalho de aplicativos empresariais, diretórios iniciais, serviço web, gerenciamento de conteúdo, análise de dados, configurações de criação de software e processamento de mídia.

Como um serviço totalmente gerenciado, o Amazon FSx para servidor de arquivos do Windows elimina os custos administrativos indiretos de configurar e provisionar servidores de arquivos e volumes de armazenamento. Além disso, ele mantém o software do Windows atualizado, detecta e resolve falhas de hardware e realiza backups. Ele também fornece integração avançada com outros serviços da AWS, incluindo o AWS Directory Service para Microsoft Active Directory, Amazon WorkSpaces, AWS Key Management Service e AWS CloudTrail.

Para mais informações, consulte o [Amazon FSx para servidor de arquivos do Windows User Guide](#).

Important

O Amazon FSx para servidor de arquivos do Windows não tem suporte em instâncias Linux.

Amazon Simple Storage Service (Amazon S3)

O Amazon S3 é um repositório para dados de Internet que fornece acesso a uma infraestrutura de armazenamento de dados confiável, rápida e econômica. Ele foi projetado para facilitar a computação dimensionável na web, permitindo o armazenamento e a recuperação de qualquer quantidade de dados do Amazon EC2, ou de qualquer lugar na web, em qualquer momento. O Amazon S3 armazena objetos de dados de forma redundante em vários dispositivos e em várias instalações, e permite o acesso simultâneo de leitura ou gravação a esses objetos de dados por muitos clientes ou threads de aplicativos separados. Você pode usar os dados redundantes armazenados no Amazon S3 para recuperação rápida e confiável em caso de falhas da instância ou do aplicativo.

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 do aplicativo 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 \(p. 839\)](#).

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 endereço de URL HTTP. Por exemplo, se um objeto com um valor de chave /photos/mygarden.jpg estiver armazenado no bucket myawsbucket, ele será endereçável usando a URL `http://myawsbucket.s3.amazonaws.com/photos/mygarden.jpg`.

Para obter mais informações sobre os recursos do Amazon S3, consulte a [página do produto Amazon S3](#).

Amazon S3 e Amazon EC2

Considerando os benefícios do Amazon S3 para armazenamento, você pode decidir usar esse serviço para armazenar arquivos e bancos 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 mais informações, consulte o [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 mais informações, consulte o [Guia do desenvolvedor do Amazon Simple Storage Service](#). Você pode usar essa API e os respectivos exemplos para ajudar a desenvolver seu aplicativo e a integrá-lo com outras APIs e SDKs, como a interface boto do Python.

Limites de volume 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 volume específicos do Linux \(p. 976\)](#)
- [Limites de volume específicos do Windows \(p. 977\)](#)
- [Limites de tipo de instância \(p. 977\)](#)
- [Largura de banda x capacidade \(p. 977\)](#)

Limites de volume específicos do Linux

Anexar mais de 40 volumes pode causar falhas de inicialização. Observe que 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.

Limites de volume específicos do Windows

A tabela a seguir mostra os limites de volumes para instâncias Windows com base no driver usado. Observe que esses números incluem o volume raiz, mais os volumes do EBS e os volumes de armazenamento de instâncias anexados.

Important

Anexar mais do que os volumes a seguir a uma instância Windows tem suporte somente em uma base de melhor esforço e não é garantido.

Driver	Solicitação de volume
AWS PV	26
Citrix PV	26
Red Hat PV	17

Não recomendamos a anexação de mais de 26 volumes a uma instância Windows com drivers AWS PV ou Citrix PV, pois é provável que isso cause problemas de desempenho.

Para determinar quais drivers PV sua instância está usando ou atualizar sua instância Windows do Red Hat para drivers Citrix PV, consulte [Atualização de drivers PV em sua instância Windows](#).

Para obter mais informações sobre como nomes de dispositivos se relacionaram a volumes, consulte [Mapeamento de discos para volumes em sua instância Windows do EC2](#) no Guia do usuário do Amazon EC2 para instâncias do Windows.

Limites de tipo de instância

As instâncias do A1, C5, C5d, C5n, M5, M5a, M5d, p3dn.24xlarge, R5, R5a, R5d, T3 e z1d oferecem suporte a um máximo de 28 anexos, incluindo interfaces de rede, volumes do EBS e volumes de armazenamento de instâncias de NVMe. Cada instância tem pelo menos um anexo de interface de rede. Os volumes de armazenamento de instâncias de NVMe são anexados automaticamente. 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 obter mais informações, consulte [Interfaces de rede elástica \(p. 747\)](#) e [Volumes de armazenamento de instâncias \(p. 959\)](#).

As instâncias i3.metal oferecem suporte a um máximo de 31 volumes do EBS.

As instâncias u-6tb1.metal, u-9tb1.metal, and u-12tb1.metal oferecem suporte a um máximo de 13 volumes do EBS.

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 [Configuração de instância do Amazon EC2 \(p. 935\)](#) para fazer a correspondência entre a IOPS provisionada para seus volumes e a largura de banda disponível para suas instâncias a fim de obter o desempenho máximo. Para configurações de RAID, muitos administradores acham que matrizes com mais de 8 volumes prejudicam o desempenho devido à maior sobrecarga de E/S. Teste o desempenho de aplicativos individuais e ajuste, se necessário.

Nomenclatura de dispositivos nas 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 volume de instância \(p. 976\)](#).

Tópicos

- [Nomes de dispositivos disponíveis \(p. 978\)](#)
- [Considerações sobre nomes de dispositivos \(p. 979\)](#)

Para obter informações sobre os nomes de dispositivos em instâncias Windows, consulte [Nomenclatura de dispositivos em instâncias 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. Alguns tipos de instância são compatíveis com PV e HVM, alguns oferecem suporte apenas a HVM e outros oferecem suporte apenas a 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 \(p. 94\)](#).

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] /dev/sd[b-y] (hs1.8xlarge)
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[b-e] /dev/sd[] BH (h1.16xlarge) /dev/sd[b-y] (d2.8xlarge) /dev/sd[b-y] (hs1.8xlarge) /dev/sd[b-i] (i2.8xlarge)

Tipo de virtualização	Disponível	Reservado para raiz	Recomendado para volumes do EBS	Volumes de armazenamento de instâncias
				**

* 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 \(p. 958\)](#). Para obter mais informações sobre volumes NVMe do EBS, consulte [Amazon EBS e NVMe \(p. 929\)](#).

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 CentOS), mesmo a letra à direita pode ser alterada (em que `/dev/sda` pode ser `/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` for renomeado como `/dev/xvdf`, `/dev/sdc` será renomeado como `/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]`.

Mapeamento de dispositivos de blocos

Cada instância em execução tem um volume do 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 [Associação de um volume do Amazon EBS a uma instância \(p. 863\)](#). Contudo, a única forma de associar volumes de armazenamento de instâncias a uma instância é usar o mapeamento de dispositivos de blocos para associá-los à medida que a instância é executada.

Para obter mais informações sobre volumes de dispositivos raiz, consulte [Alteração do volume do dispositivo raiz para persistência \(p. 18\)](#).

Tópicos

- [Conceitos de mapeamento de dispositivos de blocos \(p. 980\)](#)
- [Mapeamento de dispositivos de blocos da AMI \(p. 983\)](#)
- [Mapeamento de dispositivos de blocos da instância \(p. 985\)](#)

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 unidades flash. Um dispositivo de blocos pode ser fisicamente anexado a um computador ou acessado remotamente, como se estivesse ligado fisicamente ao computador. O Amazon EC2 oferece suporte a dois tipos de dispositivos 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 \(p. 980\)](#)
- [Advertências do armazenamento de instâncias do mapeamento de dispositivos de blocos \(p. 981\)](#)
- [Exemplo de mapeamento de dispositivos de blocos \(p. 982\)](#)
- [Como os dispositivos são disponibilizados no sistema operacional \(p. 982\)](#)

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 [Nomenclatura de dispositivos nas instâncias do Linux \(p. 978\)](#).
- [Volumes do armazenamento de instâncias] O dispositivo virtual: `ephemeral[0-23]`. Observe que o número e o tamanho de volumes de armazenamento de instâncias disponíveis varia por tipo de instância.

- [Volumes de armazenamento de instâncias de NVMe] Esse volumes são automaticamente enumerados e atribuídos a um nome de dispositivo; incluí-los no seu mapeamento de dispositivos de blocos não surtirá nenhum efeito.
- [Volumes do EBS] 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.
- [Volumes do EBS] O tamanho do volume, em GiB. O tamanho especificado deve ser maior que ou igual ao tamanho do snapshot especificado.
- [Volumes do EBS] Determina se o volume no encerramento da instância deve ser excluído (`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.
- [Volumes do EBS] O tipo de volume, que pode ser `gp2` para Finalidade geral (SSD), `io1` para Provisioned IOPS SSD, `st1` para Disco rígido com throughput otimizado, `sc1` para Cold HDD ou `standard` para Magnético. O valor padrão é `gp2` no console do Amazon EC2 e `standard` nos SDKs da AWS e na AWS CLI.
- [Volumes do EBS] O número de operações de entrada/saída por segundo (IOPS) que o volume é capaz de suportar. (Não é usado com volumes `gp2`, `st1`, `sc1` ou `standard`.)

Advertências do armazenamento de instâncias do 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.

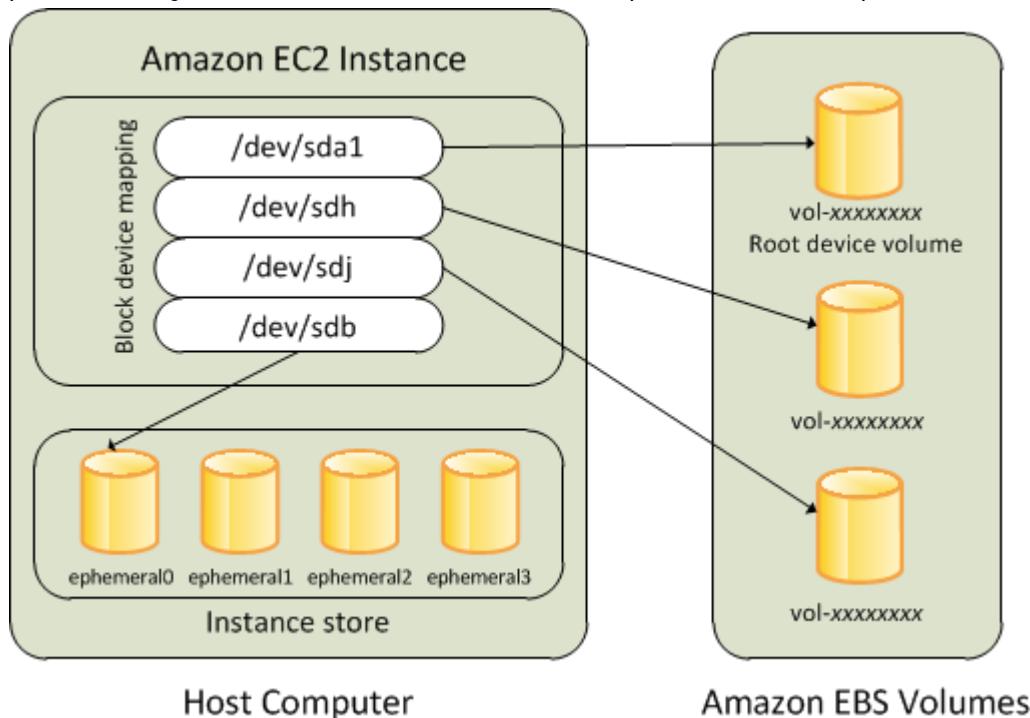
Note

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 [Especificação de um mapeamento de dispositivos de blocos para uma AMI \(p. 983\)](#) e [Atualização do mapeamento de dispositivos de blocos ao executar uma instância \(p. 985\)](#).

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 \(p. 958\)](#). 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 [Associação de um volume do Amazon EBS a uma instância \(p. 863\)](#).

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

- [Especificação de um mapeamento de dispositivos de blocos para uma AMI \(p. 983\)](#)
- [Visualização dos volumes do EBS em um mapeamento de dispositivo de blocos da AMI \(p. 984\)](#)

Especificação de 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 (Imagem), Create Image (Criar imagem).
4. Na caixa de diálogo Create Image (Criar imagem), escolha Add New Volume (Adicionar novo volume).
5. Selecione um tipo de volume na lista Type (Tipo) e um nome de dispositivo na lista Device (Dispositivo). Para um volume do EBS, é possível especificar um snapshot, o tamanho do volume e o tipo de volume.
6. Escolha Create Image.

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 a seguir:

```
--block-device-mappings [mapping, ...]
```

Para adicionar um volume de armazenamento de instâncias, use o mapeamento a seguir:

```
{  
    "DeviceName": "/dev/sdf",  
    "VirtualName": "ephemeral0"  
}
```

Para adicionar um volume Magnético 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 para 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 para Windows PowerShell):

- [New-EC2Image](#)
- [Register-EC2Image](#)

Visualização dos 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. (Lembre-se de que 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 para Windows PowerShell) para enumerar os volumes do EBS no mapeamento de dispositivos de blocos para uma AMI.

Mapeamento de dispositivos de blocos da 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.

Limites

- 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

- [Atualização do mapeamento de dispositivos de blocos ao executar uma instância \(p. 985\)](#)
- [Atualização do mapeamento de dispositivos de blocos de uma instância em execução \(p. 987\)](#)
- [Visualização dos volumes do EBS em um mapeamento de dispositivo de blocos da instância \(p. 987\)](#)
- [Visualização do mapeamento de dispositivos de blocos da instância para volumes do armazenamento de instâncias \(p. 988\)](#)

Atualização do 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 inicia-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).

To add volumes to an instance using the command line (Para adicionar volumes a uma instância usando a linha de comando)

Use o comando [run-instances](#) da AWS CLI para especificar um mapeamento de dispositivos de blocos para uma instância.

Especifique o mapeamento de dispositivos de blocos usando o parâmetro a seguir:

```
--block-device-mappings [mapping, ...]
```

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 se ligue a uma instância em execução por esta 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 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.

```
{  
    "DeviceName": "/dev/sdc",  
    "VirtualName": "ephemeral1"  
}
```

Como alternativa, você pode usar o parâmetro `-BlockDeviceMapping` com o comando [New-EC2Instance](#) (AWS Tools para Windows PowerShell).

Atualização do 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. Observe que você não precisa parar a instância antes de alterar esse atributo.

```
aws ec2 modify-instance-attribute --instance-id i-1a2b3c4d --block-device-mappings file://mapping.json
```

Por exemplo: para preservar o volume do dispositivo raiz no encerramento da instância, especifique o seguinte em `mapping.json`:

```
[  
    {  
        "DeviceName": "/dev/sda1",  
        "Ebs": {  
            "DeleteOnTermination": false  
        }  
    }  
]
```

Como alternativa, você pode usar o parâmetro `-BlockDeviceMapping` com o comando [Edit-EC2InstanceAttribute](#) (AWS Tools para Windows PowerShell).

Visualização dos volumes do EBS em um mapeamento de dispositivo de blocos da instância

Você pode facilmente enumerar volumes do EBS para a instância.

Note

Para instâncias executadas antes do lançamento da API de 2009-10-31, 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 barra de pesquisa, digite 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 Description (Descrição). No mínimo, estarão disponíveis as informações a seguir para o dispositivo raiz:

- Root device type (Tipo de dispositivo raiz) (ebs)
- Root device (Dispositivo raiz) (por exemplo, /dev/sda1)
- Block devices (Dispositivos de blocos) (por exemplo /dev/sda1, /dev/sdh e /dev/sdj)

Se a instância tiver sido executada com volumes do EBS adicionais usando um mapeamento de dispositivos de blocos, o campo Block devices (Dispositivos de blocos) exibirá esses volumes adicionais e também o dispositivo raiz. (Lembre-se de que essa caixa de diálogo não exibe volumes de armazenamento de instâncias.)

Root device type	ebs
Root device	/dev/sda1
Block devices	/dev/sda1 /dev/sdf

5. Para exibir informações adicionais sobre um dispositivo de blocos, selecione a entrada ao lado de Block devices (Dispositivos de blocos). Isso exibe as informações a seguir para o dispositivo de blocos:
 - EBS ID (ID do EBS) (vol-xxxxxxxx)
 - Root device type (Tipo de dispositivo raiz) (ebs)
 - Attachment time (Hora de anexação) (yyyy-mmThh:mm:ss.ssTZD)
 - Block device status (Status do dispositivo de blocos) (attaching, attached, detaching, detached)
 - Delete on termination (Excluir no encerramento) (Yes, No)

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 para Windows PowerShell) para enumerar os volumes do EBS no mapeamento de dispositivos de blocos para uma instância.

Visualização do mapeamento de dispositivos de blocos da instância para volumes do armazenamento de instâncias

Quando você ver o mapeamento de dispositivos de blocos para sua instância, verá somente os volumes do EBS, não os volumes de armazenamento de instâncias. Você pode usar os metadados da instância para consultar o mapeamento de dispositivos de blocos inteiro. O URI de base de todas as solicitações de metadados da instância é <http://169.254.169.254/latest/>.

Important

Os volumes de armazenamento de instâncias de NVMe não são incluídos no mapeamento de dispositivos de blocos

Primeiro, conecte-se à instância em execução. Com base na instância, use esta consulta para obter o mapeamento de dispositivos de blocos.

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/block-device-mapping/
```

A resposta inclui o nome dos dispositivos de blocos para a instância. Por exemplo, a saída de uma instância m1.small com armazenamento de instâncias 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.

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/block-device-mapping/ephemeral0
```

Para obter mais informações, consulte [Metadados da instância e dados do usuário \(p. 516\)](#).

Como usar bancos de dados públicos

O Amazon Web Services fornece um repositório de bancos de dados públicos que pode ser integrado perfeitamente em aplicativos baseados na nuvem da AWS. A Amazon armazena bancos de dados públicos gratuitamente para a comunidade e, como todos os serviços da AWS, você paga somente pela computação e pelo armazenamento que utiliza para seus próprios aplicativos.

Tópicos

- [Conceitos de bancos de dados públicos \(p. 989\)](#)
- [Como localizar bancos de dados públicos \(p. 990\)](#)
- [Como criar um volume de banco de dados público em um snapshot \(p. 990\)](#)
- [Como anexar e montar o volume de banco de dados público \(p. 991\)](#)

Conceitos de bancos de dados públicos

Anteriormente, os grandes conjuntos de dados, como o mapeamento do Genôma Humano e os dados do Censo norte-americano, necessitaram de horas ou dias para localização, download, personalização e análise. Agora, qualquer pessoa pode acessar esses bancos de dados em uma instância do EC2 e começar a computar os dados em minutos. Você também pode utilizar todo o ecossistema da AWS e colaborar facilmente com outros usuários da AWS. Por exemplo, você pode produzir ou utilizar imagens de servidores pré-criadas com ferramentas e aplicativos para análise dos bancos de dados. Com a hospedagem desses dados úteis e importantes com serviços econômicos, como o Amazon Amazon EC2, a AWS espera oferecer aos pesquisadores de várias disciplinas e setores as ferramentas que permitem mais inovação de modo mais rápido.

Para obter mais informações, acesse a página [Bancos de dados públicos da AWS](#).

Bancos de dados públicos disponíveis

Atualmente, os bancos de dados públicos estão disponíveis nas seguintes categorias:

- Biologia — inclui o Projeto de genoma humano, o GenBank e outros conteúdos.
- Química — inclui várias versões do PubChem e outros conteúdos.
- Economia — inclui dados de recenseamento, estatísticas de trabalho, estatísticas de transporte e outros conteúdos.

- Enciclopédico — inclui o conteúdo da Wikipédia de várias origens e outros conteúdos.

Como localizar bancos de dados públicos

Para poder usar um banco de dados público, você deve localizar o banco de dados e determinar o formato no qual o banco de dados está hospedado. Os bancos de dados estão disponíveis em dois formatos possíveis: snapshots do Amazon EBS ou buckets do Amazon S3.

Para localizar um banco de dados público e determinar seu formato

1. Acesse a página [Bancos de dados públicos da AWS](#) para ver uma lista de todos os bancos de dados públicos disponíveis. Você também pode digitar uma frase de pesquisa nessa página para consultar as listagens de bancos de dados públicos disponíveis.
2. Clique no nome de um banco de dados para ver a página de detalhes.
3. Na página de detalhes do banco de dados, procure uma listagem de IDs de snapshots para identificar um banco de dados formatado pelo Amazon EBS ou uma URL do Amazon S3.

Os bancos de dados que estão em formato de snapshot são usados para criar novos volumes do EBS que você anexa a uma instância do EC2. Para obter mais informações, consulte [Como criar um volume de banco de dados público em um snapshot \(p. 990\)](#).

Para bancos de dados no formato do Amazon S3, você pode usar os SDKs da AWS ou a API de consulta HTTP para acessar as informações, ou usar a AWS CLI para copiar ou sincronizar os dados para/da instância. Para obter mais informações, consulte [Amazon S3 e Amazon EC2 \(p. 975\)](#).

Você também pode usar o Amazon EMR para analisar e trabalhar com bancos de dados públicos. Para obter mais informações, consulte [O que é o Amazon EMR?](#).

Como criar um volume de banco de dados público em um snapshot

Para usar um banco de dados público que está no formato de snapshot, crie um novo volume especificando o ID do snapshot do banco de dados público. Você pode criar o novo volume usando o Console de gerenciamento da AWS da seguinte forma. Se preferir, você poderá usar o comando `create-volume` da AWS CLI.

Para criar um volume de banco de dados público em um snapshot

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 de banco de dados está localizado.

Se precisar criar esse volume em outra região, você poderá copiar o snapshot naquela região e usá-lo para criar um volume nessa região. Para obter mais informações, consulte [Cópia de um snapshot do Amazon EBS \(p. 902\)](#).

3. No painel de navegação, escolha ELASTIC BLOCK STORE, Volumes.
4. Escolha Criar volume.
5. Em Tipo de volume, escolha um tipo de volume. Para obter mais informações, consulte [Tipos de volume do Amazon EBS \(p. 844\)](#).
6. Para Snapshot, comece a digite o ID ou a descrição do snapshot que tem o banco de dados e escolha-o na lista.

Se o snapshot que você espera ver não aparecer, você pode ter selecionado uma região em que ele não está. Se o banco de dados que você identificou em [Como localizar bancos de dados](#)

públicos (p. 990) não especificar uma região na página de detalhes, ele provavelmente estará contido na região us-east-1 Leste dos EUA (Norte da Virgínia).

7. Para Size (GiB) (Tamanho (GiB)), digite o tamanho do volume ou verifique se o tamanho padrão do snapshot é adequado.

Note

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).

8. Com um volume Provisioned IOPS SSD, para IOPS, insira o número máximo de operações de entrada/saída por segundo (IOPS) com que o volume deveria ser compatível.
9. Para Zona de disponibilidade, escolha a zona de disponibilidade na qual criar o volume. Os volumes do EBS só podem ser anexados a instâncias na mesma Zona de disponibilidade.
10. (Opcional) Escolha Criar tags adicionais para adicionar tags ao volume. Forneça uma chave e um valor para cada tag.
11. Escolha Criar volume.

Como anexar e montar o volume de banco de dados público

Depois de criar seu novo volume de banco de dados, você precisará anexá-lo a uma instância do EC2 para acessar os dados (essa instância também deve estar na mesma Zona de disponibilidade que o volume novo). Para obter mais informações, consulte [Associação de um volume do Amazon EBS a uma instância \(p. 863\)](#).

Depois de anexar o volume a uma instância, você precisará montar o volume na instância. Para obter mais informações, consulte [Disponibilização de um volume do Amazon EBS para uso no Linux \(p. 864\)](#).

Se você tiver restaurado um snapshot para um volume maior que o padrão para esse snapshot, deverá ampliar o sistema de arquivos no volume para usufruir do espaço extra. Para obter mais informações, consulte [Como modificar o tamanho, o desempenho ou o tipo de um volume do EBS \(p. 882\)](#).

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

- [Locais de recursos \(p. 992\)](#)
- [IDs de recursos \(p. 993\)](#)
- [Listagem e filtragem dos seus recursos \(p. 999\)](#)
- [Marcação dos seus recursos do Amazon EC2 \(p. 1003\)](#)
- [Limites de serviço do Amazon EC2 \(p. 1013\)](#)
- [Relatórios de uso do Amazon EC2 \(p. 1015\)](#)

Locais de recursos

Alguns recursos podem ser usados em todas as regiões (globais) e alguns recursos são específicos da região ou da zona de disponibilidade na qual eles residem.

Recurso	Tipo	Descrição
Conta da AWS	Global	Você pode usar a mesma conta da AWS em todas as regiões.
Pares de chaves	Global ou regional	Os pares de chaves criados com o Amazon EC2 são vinculados à região onde você os criou. Você pode criar seu próprio par de chaves de RSA e fazer upload dele na região em que deseja usá-lo; portanto, você pode tornar seu par de chaves globalmente disponível fazendo upload dele em cada região. Para obter mais informações, consulte Pares de chaves do Amazon EC2 (p. 616) .
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 onde você criou o recurso.
Nomes de recursos fornecidos pelo usuário	Regional	Cada nome de recurso, como um nome de security group ou de par de chaves, é vinculado à sua região e só pode ser usado na região onde você criou o recurso. Embora você possa criar recursos com o mesmo nome em várias regiões, eles não são relacionados.

Recurso	Tipo	Descrição
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 Cópia de uma AMI (p. 150) .
Endereços IP elásticos	Regional	Um endereço IP elástico está vinculado a uma região e pode ser associado apenas a uma instância na mesma região.
Grupos de segurança	Regional	Um security group 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 security group. O tráfego de uma instância em outra região é considerado como a largura de banda de WAN.
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. Para obter mais informações, consulte Cópia de um snapshot do Amazon EBS (p. 902) .
Volumes do EC2	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.
Instâncias	Availability Zone	Uma instância é vinculada às zonas de disponibilidade na qual você a executou. Contudo, observe que o ID da instância está ligado à região.

IDs de recursos

Ao criarmos recursos, atribuímos a cada um deles um ID de recurso exclusivo. 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

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. A partir de janeiro de 2016, gradualmente, estamos adotando IDs de comprimento mais longo para os tipos de recursos do Amazon EC2 e do Amazon EBS. O tamanho da combinação de caracteres alfanuméricos estava em um formato de 8 caracteres; os novos IDs estão em um formato de 17 caracteres, por exemplo, `i-1234567890abcdef0`, para um ID de instância.

Os tipos de recursos compatíveis têm um período de inclusão, durante o qual você pode escolher um formato de ID de recursos e uma data de prazo, após a qual o recurso voltará a usar o formato padrão de ID mais longo. Após o prazo para um tipo de recurso específico, você não poderá mais desabilitar o formato de ID mais longo para aquele tipo de recurso.

Os diferentes tipos de recursos têm diferentes períodos de inclusão e datas de prazo. A tabela a seguir lista os tipos de recursos compatíveis, junto com os períodos de inclusão e as datas de prazo.

Tipo de recurso	Período de inclusão	Data de prazo
instance snapshot reservation volume	Não está mais disponível	15 de dezembro de 2016
bundle conversion-task customer-gateway dhcp-options elastic-ip-allocation elastic-ip-association export-task flow-log image import-task internet-gateway network-acl network-acl-association network-interface network-interface-attachment prefix-list route-table route-table-association security-group subnet subnet-cidr-block-association vpc vpc-cidr-block-association vpc-endpoint vpc-peering-connection vpn-connection vpn-gateway	9 de fevereiro de 2018 - 30 de junho de 2018	30 de junho de 2018

Durante o período de inclusão

Você pode habilitar ou desabilitar os IDs mais longos para um recurso em qualquer momento durante o período de inclusão. Depois que você habilita os IDs mais longos para um tipo de recurso, todos os novos recursos são criados com um ID mais longo.

Note

Os IDs de recursos não mudam depois que são criados. Portanto, a habilitação ou desabilitação de IDs mais longos durante o período de inclusão não afeta os IDs de recursos já existentes.

Dependendo de quando você criou sua conta da AWS, os tipos de recursos com suporte podem ter como padrão IDs mais longos. No entanto, você pode optar por não usar IDs mais longos até a data de prazo para esse tipo de recurso. Para obter mais informações, consulte [IDs mais longos de recursos do EC2 e do EBS](#) nas Perguntas frequentes sobre o Amazon EC2.

Após a data de prazo

Não é possível desabilitar os IDs mais longos para um tipo de recurso após a sua data de prazo. Todos os novos recursos que você criar serão criados com um ID mais longo.

Como trabalhar com IDs mais longos

Você pode habilitar ou desabilitar IDs mais longos por usuário e função do IAM. Por padrão, um usuário ou função do IAM assume como padrão as mesmas configurações que o usuário raiz.

Tópicos

- [Visualizar configurações de ID mais longo \(p. 995\)](#)
- [Modificar configurações de ID mais longo \(p. 996\)](#)

Visualizar configurações de ID mais longo

Você pode usar o console e as ferramentas da linha de comando para visualizar os tipos de recursos que são compatíveis com IDs mais longos.

Para visualizar as configurações de ID mais longo usando o 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 região para a qual deseja visualizar as configurações de ID mais longo.
3. No painel, em Account Attributes (Atributos da conta), escolha Resource ID length management (Gerenciamento do tamanho do ID dos recursos).
4. Expanda Advanced Resource ID Management (Gerenciamento avançado de ID de recurso) para visualizar os tipos de recursos que são compatíveis com IDs mais longos e suas datas de prazo.

Para visualizar as configurações de ID mais longo usando a linha de comando

Use um dos seguintes comandos:

- [describe-id-format](#) (AWS CLI)

```
aws ec2 describe-id-format --region region
```

- [Get-EC2IdFormat](#) (AWS Tools para Windows PowerShell)

```
Get-EC2IdFormat -Region region
```

Para visualizar as configurações de ID mais longo para um usuário ou função específico do IAM utilizando a linha de comando

Use um dos seguintes comandos e especifique o nome de recurso da Amazon (ARN) de um usuário ou função do IAM ou uma conta de usuário raiz na solicitação.

- [describe-identity-id-format](#) (AWS CLI)

```
aws ec2 describe-identity-id-format --principal-arn arn-of-iam-principal --region region
```

- [Get-EC2IdentityIdFormat](#) (AWS Tools para Windows PowerShell)

```
Get-EC2IdentityIdFormat -PrincipalArn arn-of-iam-principal -Region region
```

Para visualizar as configurações de ID mais longo agregadas para uma região específica utilizando a linha de comando

Use o comando [describe-aggregate-id-format](#) da AWS CLI para visualizar as configurações de ID mais longo agregadas para a região inteira, bem como as configurações de ID mais longo agregadas de todos os ARNs para cada tipo de recurso. Este comando é útil para executar uma auditoria rápida para determinar se uma região específica está inteiramente incluída para obter IDs mais longos.

```
aws ec2 describe-aggregate-id-format --region region
```

Para identificar os usuários que definiram explicitamente as configurações personalizadas de ID mais longo

Use o comando `describe-principal-id-format` da AWS CLI para visualizar as configurações de formato de ID mais longo para o usuário raiz e todas as funções e usuários do IAM que tenham especificado explicitamente uma preferência por IDs mais longos. Este comando é útil para identificar usuários e funções do IAM que substituíram as configurações padrão de ID mais longo.

```
aws ec2 describe-principal-id-format --region region
```

Modificar configurações de ID mais longo

Você pode usar o console e as ferramentas de linha de comando para modificar as configurações de ID mais longo para os tipos de recursos que ainda estejam no período de inclusão.

Note

Os comandos da AWS CLI e do AWS Tools para Windows PowerShell nesta seção são apresentados somente por região. Eles se aplicam à região padrão a menos que seja especificado de outra forma. Para modificar as configurações para outras regiões, inclua o parâmetro `region` no comando.

Para modificar as configurações de ID mais longo usando o 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 região para a qual deseja modificar as configurações de ID mais longo.
3. No painel, em Account Attributes (Atributos da conta), escolha Resource ID length management (Gerenciamento do tamanho do ID dos recursos).
4. Faça uma das coisas a seguir:
 - Para habilitar os IDs mais longos para todos os tipos de recursos compatíveis com todos os usuários do IAM em todas as regiões, escolha Switch to longer IDs (Mudar para IDs mais longos) e Yes, switch to longer IDs (Sim, mude para IDs mais longos).

Important

Os usuários e as funções do IAM precisam da permissão `ec2:ModifyIdentityIdFormat` para executar essa ação.

- Para modificar as configurações de ID mais longo para um tipo de recurso específico para sua conta de usuário do IAM, expanda Advanced Resource ID Management (Gerenciamento avançado de ID de recurso) e, em seguida, marque a caixa de seleção correspondente na coluna My IAM Role/User (Meu usuário/função do IAM) para habilitar os IDs mais longos, ou desmarque a caixa para desabilitar os IDs mais longos.
- Para modificar as configurações de ID mais longo para um tipo de recurso específico para todos os usuários do IAM, expanda Advanced Resource ID Management (Gerenciamento avançado de ID de recurso) e, em seguida, marque a caixa de seleção correspondente na coluna All IAM Roles/Users (Todos os usuários/funções do IAM) para habilitar os IDs mais longos, ou desmarque a caixa para desabilitar os IDs mais longos.

Para modificar configurações de ID mais longo para sua conta de usuário do IAM usando a linha de comando

Use um dos seguintes comandos:

Note

Se você estiver usando esses comandos como o usuário raiz, essas configurações se aplicarão a toda a conta da AWS, a menos que um usuário ou uma função do IAM cancele explicitamente essas configurações por conta própria.

- [modify-id-format \(AWS CLI\)](#)

```
aws ec2 modify-id-format --resource resource_type --use-long-ids
```

Você também pode usar o comando para modificar as configurações de ID mais longo para todos os tipos de recursos compatíveis. Para fazer isso, substitua o parâmetro *resource_type* pelo *all-current*.

```
aws ec2 modify-id-format --resource all-current --use-long-ids
```

Note

Para desabilitar IDs mais longos, substitua o parâmetro *use-long-ids* pelo *no-use-long-ids*.

- [Edit-EC2IdFormat \(AWS Tools para Windows PowerShell\)](#)

```
Edit-EC2IdFormat -Resource resource_type -UseLongId boolean
```

Você também pode usar o comando para modificar as configurações de ID mais longo para todos os tipos de recursos compatíveis. Para fazer isso, substitua o parâmetro *resource_type* pelo *all-current*.

```
Edit-EC2IdFormat -Resource all-current -UseLongId boolean
```

Para modificar as configurações de ID mais longo para um usuário ou função específica do IAM utilizando a linha de comando

Use um dos seguintes comandos e especifique o nome de recurso da Amazon (ARN) de um usuário ou função do IAM ou um usuário raiz na solicitação.

- [modify-identity-id-format \(AWS CLI\)](#)

```
aws ec2 modify-identity-id-format --principal-arn arn-of-iam-principal --  
resource resource_type --use-long-ids
```

Você também pode usar o comando para modificar as configurações de ID mais longo para todos os tipos de recursos compatíveis. Para fazer isso, especifique *all-current* para o parâmetro *--resource*.

```
aws ec2 modify-identity-id-format --principal-arn arn-of-iam-principal --resource all-  
current --use-long-ids
```

Note

Para desabilitar IDs mais longos, substitua o parâmetro *use-long-ids* pelo *no-use-long-ids*.

- [Edit-EC2IdentityIdFormat \(AWS Tools para Windows PowerShell\)](#)

```
Edit-EC2IdentityIdFormat -PrincipalArn arn-of-iam-principal -Resource resource_type -  
UseLongId boolean
```

Você também pode usar o comando para modificar as configurações de ID mais longo para todos os tipos de recursos compatíveis. Para fazer isso, especifique `all-current` para o parâmetro `-Resource`.

```
Edit-EC2IdentityIdFormat -PrincipalArn arn-of-iam-principal -Resource all-current -  
UseLongId boolean
```

Controle do acesso a configurações de ID mais longo

Por padrão, os usuários e as funções do IAM não têm permissão para usar as seguintes ações, a menos que seja concedida permissão explicitamente a elas por meio de suas políticas associadas ao IAM:

- `ec2:DescribeIdFormat`
- `ec2:DescribeIdentityIdFormat`
- `ec2:DescribeAggregateIdFormat`
- `ec2:DescribePrincipalIdFormat`
- `ec2:ModifyIdFormat`
- `ec2:ModifyIdentityIdFormat`

Por exemplo, uma função do IAM pode ter permissão para usar todas as ações do Amazon EC2 por meio do elemento "Action": "ec2:*" na instrução da política.

Para impedir que os usuários e as funções do IAM visualizem ou alterem as configurações de ID de recurso mais longo para eles ou outros usuários e funções em sua conta, garanta que a política do IAM contenha o seguinte comando:

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Deny",  
            "Action": [  
                "ec2:ModifyIdFormat",  
                "ec2:DescribeIdFormat",  
                "ec2:ModifyIdentityIdFormat",  
                "ec2:DescribeIdentityIdFormat",  
                "ec2:DescribeAggregateIdFormat",  
                "ec2:DescribePrincipalIdFormat"  
            ],  
            "Resource": "*"  
        }  
    ]  
}
```

Não oferecemos suporte a permissões no nível do recurso para as seguintes ações:

- `ec2:DescribeIdFormat`
- `ec2:DescribeIdentityIdFormat`
- `ec2:DescribeAggregateIdFormat`
- `ec2:DescribePrincipalIdFormat`
- `ec2:ModifyIdFormat`
- `ec2:ModifyIdentityIdFormat`

Listagem e filtragem dos 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, pode filtrar os resultados para incluir somente aqueles que correspondem a determinados critérios.

Tópicos

- [Pesquisa avançada \(p. 999\)](#)
- [Listagem dos recursos usando o console \(p. 1000\)](#)
- [Filtro dos recursos usando o console \(p. 1001\)](#)
- [Listagem e filtragem com o uso de CLI e API \(p. 1002\)](#)

Pesquisa avançada

A pesquisa avançada permite que você faça uma pesquisa usando uma combinação de filtros para obter resultados precisos. Você pode filtrar por palavras-chave, chaves de tag definidas pelo usuário e atributos de recursos predefinidos.

Os tipos específicos de pesquisa disponíveis são:

- Pesquisa por palavra-chave

Para pesquisar por palavra-chave, digite ou cole o que você procura na caixa de pesquisa e escolha Enter. Por exemplo, para pesquisar uma instância específica, você pode digitar o ID da instância.

- Pesquisa por campos

Você também pode pesquisar por campos, tags e atributos associados a um recurso. Por exemplo, para encontrar todas as instâncias no estado interrompido:

1. Na caixa de pesquisa, comece a digitar **Instance State**. À medida que digita, você verá uma lista de campos sugeridos.
 2. Selecione Instance State (Estado da instância) na lista.
 3. Selecione Stopped (Interrompido) na lista de valores sugeridos.
 4. Para refinar ainda mais sua lista, selecione a caixa de pesquisa para obter mais opções de pesquisa.
- Pesquisa avançada

Você pode criar consultas avançadas ao adicionar vários filtros. Por exemplo, você pode pesquisar por tags e ver instâncias do projeto Flying Mountain em execução no stack Produção e, em seguida, pesquisar por atributos para ver todas as instâncias de t2.micro, ou todas as instâncias em us-west-2a, ou ambos.

- Pesquisa inversa

Você pode pesquisar pelos recursos que não correspondem a um valor especificado. Por exemplo, para listar todas as instâncias que não estão encerradas, pesquise pelo campo Instance State (Estado da instância) e use como prefixo no valor de Terminated (Encerrado) um ponto de exclamação (!).

- Pesquisa parcial

Para procurar por campo, você também pode inserir uma string parcial para encontrar todos os recursos que contêm a string nesse campo. Por exemplo, pesquise por Instance Type (Tipo de instância) e, depois, digite **t2** para encontrar todas as instâncias t2.micro, t2.small ou t2.medium.

- Expressão regular

As expressões regulares são úteis quando você precisa corresponder os valores de um campo com um padrão específico. Por exemplo, pesquise pela tag Nome e, depois, digite `^s.*` para ver todas as instâncias com uma tag Nome que comece com um 's'. A pesquisa de expressão regular não diferencia maiúsculas e minúsculas.

Depois de pegar os resultados precisos da sua pesquisa, você pode marcar o URL como favorito para facilitar a consulta. Nas situações em que você tem milhares de instâncias, filtros e favoritos podem economizar muito tempo; você não tem de realizar pesquisas repetidamente.

Combinação de filtros de pesquisa

No geral, vários filtros com o mesmo campo-chave (por exemplo, tag:Name, pesquisar, estado de instância) são automaticamente unidos com OR. Isso é intencional, pois a vasta maioria dos filtros não seria lógica se fosse juntada com AND. Por exemplo, você obteria zero resultados para a pesquisa Instance State=running E Instance State=stopped. Em muitos casos, você pode granularizar os resultados usando termos de pesquisa complementares em campos-chave diferentes, onde a regra AND é automaticamente aplicada. Se você pesquisar por tag: Name:=All values e tag:Instance State=running, obterá os resultados de pesquisa que contêm ambos os critérios. Para fazer o ajuste fino dos resultados, basta remover um filtro da string até que os resultados se encaixem nos seus requisitos.

Listagem dos 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, selecione a opção correspondente ao recurso, como AMIs ou Instances (Instâncias).

EC2 Dashboard

Events

Tags

Reports

Limits

INSTANCES

Instances

Launch Templates

Spot Requests

Reserved Instances

Dedicated Hosts

Scheduled Instances

IMAGES

AMIs

Bundle Tasks

ELASTIC BLOCK STORE

Volumes

Snapshots

NETWORK & SECURITY

3. A página exibe todos os recursos disponíveis.

Filtro dos recursos usando o console

Você pode executar a filtragem e classificação dos tipos de recurso mais comuns usando o console do Amazon EC2. Por exemplo, você pode usar a barra de pesquisa na página de instâncias para classificar instâncias por tags, atributos ou palavras-chave.

Você também pode usar o campo de pesquisa em cada página para encontrar os recursos com atributos ou valores específicos. Você pode usar expressões regulares para pesquisar strings parciais ou múltiplas. Por exemplo, para encontrar todas as instâncias que estão usando o security group MySG, digite `MySG` no campo de pesquisa. Os resultados incluirão todos os valores que contêm `MySG` como parte da string, como `MySG2` e `MySG3`. Para limitar os resultados somente ao MySG, digite `\bMySG\b` no campo de pesquisa. Para listar todas as instâncias cujo tipo é `m1.small` ou `m1.large`, digite `m1.small|m1.large` no campo de pesquisa.

Para listar volumes na zona de disponibilidade **us-east-1b** com status de **available**

1. No painel de navegação, escolha Volumes.
2. Clique na caixa de pesquisa, selecione Attachment Status (Status da associação) no menu e selecione Detached (Separado). (O volume separado está disponível para ser associado a uma instância na mesma zona de disponibilidade.)
3. Clique na caixa de pesquisa novamente, selecione State (Estado) e, em seguida, selecione Available (Disponível).

4. Clique na caixa de pesquisa novamente, selecione Availability Zone (Zona de disponibilidade) e selecione us-east-1b.
5. Todos os volumes que atenderem a esses critérios serão exibidos.

Para listar as AMIs do Linux públicas de 64 bits com Amazon EBS

1. No painel de navegação, selecione AMIs.
2. No painel Filter (Filtro), selecione Public images (Imagens públicas), EBS images (Imagens do EBS) e, então, sua distribuição Linux nas listas Filter (Filtro).
3. Digite x86_64 no campo de pesquisa.
4. Todas as AMIs que atenderem a esses critérios serão exibidas.

Listagem e filtragem com o uso de CLI e API

Cada tipo de recurso tem um comando CLI correspondente ou solicitação de API que você usa para listar os recursos desse tipo. Por exemplo, você pode listar imagens de máquina da Amazon (AMI) usando `ec2-describe-images` ou `DescribeImages`. A resposta contém informações para todos os recursos.

As listas de recursos resultantes podem ser longas, por isso melhor filtrar os resultados para incluir somente os recursos que correspondem a determinados critérios. Você pode especificar múltiplos valores de filtro e também especificar múltiplos filtros. Por exemplo, você pode listar todas as instâncias cujo tipo é `m1.small` ou `m1.large` e que tenham um volume do EBS associado definido para exclusão quando a instância for encerrada. A instância deve corresponder a todos os seus filtros para ser incluída nos resultados.

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.

Por exemplo, você pode usar `database` como o valor do filtro para obter apenas os snapshots do EBS cuja descrição é igual a `database` na descrição. Se você especificar `*database*`, então todos os snapshots cuja descrição inclui `database` serão retornados. Se você especificar `database?`, somente os snapshots cuja descrição corresponde a um dos padrões a seguir são retornados: igual a `database` ou `database` seguido por um caractere.

O número de pontos de interrogação determina o número máximo de caracteres a serem incluídos nos resultados. Por exemplo, se você especificar `database????`, somente os snapshots cujas descrições sejam iguais a `database` seguidas por até quatro caracteres são retornados. Descrições com cinco ou mais caracteres após `database` são excluídas dos resultados da pesquisa.

Os valores do filtro diferenciam maiúsculas de minúsculas. Nós oferecemos suporte somente à correspondência exata de strings ou de substrings (com caracteres curingas). Se uma lista de recursos resultante for longa, usar um filtro exato de strings pode apresentar a resposta mais rápido.

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\?\\\` pesquisa pela string literal, `*amazon?\\`.

Para uma lista de filtros suportados pelo recurso Amazon EC2, consulte a documentação relevante:

- Para a AWS CLI, consulte o comando `describe` relevante em [AWS CLI Command Reference](#).
- Para o Windows PowerShell, consulte o comando `Get` relevante em [AWS Tools para PowerShell Cmdlet Reference](#).
- Para a API de consulta, consulte a ação da API `Describe` relevante no [Amazon EC2 API Reference](#).

Marcação dos seus 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. Este tópico descreve tags e mostra a você como criá-los.

Tópicos

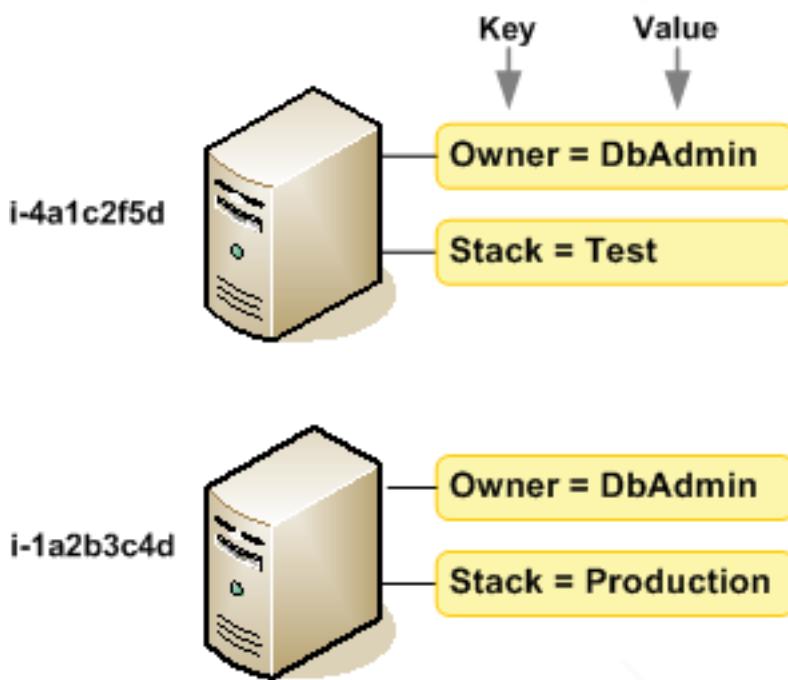
- [Conceitos básicos de tags \(p. 1003\)](#)
- [Marcação dos seus recursos \(p. 1004\)](#)
- [Restrições de tag \(p. 1007\)](#)
- [Marcação dos seus recursos para faturamento \(p. 1007\)](#)
- [Trabalho com tags usando o console \(p. 1008\)](#)
- [Trabalho com tags usando a CLI ou a API \(p. 1011\)](#)

Conceitos básicos de tags

Tag é um rótulo que você atribui a um recurso da AWS. Cada tag consiste de 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). 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. 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.

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.

Você pode trabalhar com tags usando o Console de gerenciamento da AWS, a AWS CLI e a API do Amazon EC2.

Se você estiver usando 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 [Como controlar o acesso aos recursos do Amazon EC2 \(p. 641\)](#).

Marcação dos seus recursos

Você pode usar tags na maioria dos recursos do Amazon EC2 que já existem na sua conta. A [tabela \(p. 1005\)](#) 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.

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 SDK da AWS.

Uso de tags para suporte aos recursos do Amazon EC2

Recurso	Compatível com tags	Oferece suporte à marcação na criação
AFI	Sim	Não
AMI	Sim	Não
Tarefa de pacote	Não	Não
Reserva de capacidade	Sim	Sim
Gateway do cliente	Sim	Não
Host dedicado	Sim	Sim
Opção de DHCP	Sim	Não
Snapshot do EBS	Sim	Sim
Volume do EBS	Sim	Sim
Frota do EC2	Sim	Sim
Gateway da Internet somente de saída	Não	Não
Endereços elastic IP (EIPs)	Sim	Não
Instância	Sim	Sim
Volumes de armazenamento de instâncias	N/D	N/D
Gateway da Internet	Sim	Não
Par de chaves	Não	Não
Modelo de execução	Sim	Não
Versão do modelo de execução	Não	Não
gateway NAT	Sim	Não
Conexão ACL	Sim	Não
Interface de rede	Sim	Não
Placement group	Não	Não
Instância reservada	Sim	Não

Recurso	Compatível com tags	Oferece suporte à marcação na criação
Listagem do Instância reservada	Não	Não
Tabela de rotas	Sim	Não
Solicitação do Instância spot	Sim	Não
Grupo de segurança	Sim	Não
Sub-rede	Sim	Não
Transit gateway	Sim	Sim
Tabela de rotas do Transit Gateway	Sim	Sim
Anexo da VPC do Transit Gateway	Sim	Sim
Gateway privado virtual	Sim	Não
VPC	Sim	Não
VPC endpoint	Não	Não
Serviço de VPC endpoint	Não	Não
Log do fluxo da VPC	Não	Não
Conexão de emparelhamento de VPC	Sim	Não
Conexão VPN	Sim	Não

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 estiverem devidamente protegidos contra tags de criação aplicadas imediatamente aos seus 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 [Permissões em nível do recurso compatíveis para ações da API do Amazon EC2 \(p. 653\)](#) e [Políticas de exemplo para trabalhar com a AWS CLI ou um AWS SDK \(p. 680\)](#).

Para obter mais informações sobre como marcar seus recursos com tags para faturamento, consulte [Uso de tags de alocação de custos](#) no Guia do usuário do AWS Billing and Cost Management.

Restrições de tag

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
- Valor máximo da chave: 256 caracteres Unicode em UTF-8
- Embora o EC2 permita qualquer caractere em suas tags, outros serviços podem ser mais restritivos. Em geral, os caracteres permitidos são: letras, números e espaços representáveis em UTF-8 e os seguintes caracteres: + - = . _ : / @. Estes caracteres podem não ser permitidos por serviços mais restritivos.
- As chaves e os valores de tags diferenciam maiúsculas de minúsculas.
- Não use o prefixo `aws`: para chaves nem valores, pois ele é reservado para uso da AWS. Você não pode editar nem excluir chaves nem valores de tag com esse prefixo. As tags com esse prefixo 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`.

Você pode marcar com tag recursos públicos ou compartilhados, mas as tags que você atribuir só estarão disponíveis para sua conta AWS e não para outras contas com as quais o recurso é compartilhado.

Você não pode marcar com tag todos os recursos. Para obter mais informações, consulte [Uso de tags para suporte aos recursos do Amazon EC2 \(p. 1005\)](#).

Marcação dos seus recursos para faturamento

Você pode usar tags para organizar sua conta AWS e refletir sua própria estrutura de custos. Para isso, inscreva-se para obter sua conta da AWS com os valores de chave de tags incluídos. Para obter mais informações sobre como configurar um relatório de alocação de custos com tags, consulte [Relatório de alocação de custos mensal](#) no Guia 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 [Uso de tags de alocação de custos](#) no Guia 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 [Volumes e snapshots do Amazon Elastic Block Store](#) no Guia do usuário do AWS Billing and Cost Management.

Note

Os endereços IP elásticos marcados não são exibidos no seu relatório de alocação de custos.

Trabalho 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 específica. 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 [Listagem e filtragem dos seus recursos \(p. 999\)](#).

Para facilidade de uso e melhores resultados, use o Tag Editor no Console de gerenciamento da AWS, que fornece uma forma unificada e central para criar e gerenciar suas tags. Para obter mais informações, consulte [Como trabalhar com o Tag Editor](#) no Conceitos básicos do Console de Gerenciamento da AWS.

Tópicos

- [Exibição de tags \(p. 1008\)](#)
- [Adição e exclusão de tags em um recurso individual \(p. 1009\)](#)
- [Adição e exclusão de tags a um grupo de recursos \(p. 1009\)](#)
- [Adição de uma tag ao executar uma instância \(p. 1010\)](#)
- [Filtragem de uma lista de recursos por tags \(p. 1011\)](#)

Exibição de 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 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, você verá as tags na guia Tags do painel de detalhes.

Você pode adicionar uma coluna à lista de recursos que mostra todos os valores das tags com a mesma chave. Essa coluna permite que você classifique e filtre a lista de recursos pela tag. 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.

Manage Tags						
Filter: <input type="text"/> Search Keys		Search Values				
	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

Adição e exclusão de 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 [Locais de recursos \(p. 992\)](#).
3. No painel de navegação, selecione um tipo de recurso (por exemplo, Instâncias).
4. Selecione o recurso da lista de recursos e selecione Tags, Add/Edit Tags.
5. Na caixa de diálogo Adicionar/editar tags, especifique a chave e o valor de cada tag e selecione 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 [Locais de recursos \(p. 992\)](#).
3. No painel de navegação, selecione um tipo de recurso (por exemplo, Instâncias).
4. Selecione o recurso da lista de recursos e selecione Tags.
5. Escolha Adicionar/editar tags, selecione o ícone Excluir para a tag e escolha Salvar.

Adição e exclusão de 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 [Locais de recursos \(p. 992\)](#).
3. No painel de navegação, selecione Tags.

4. Na parte superior do painel de conteúdo, escolha Gerenciar tags.
5. Para Filtro, selecione o tipo de recurso (por exemplo, instâncias) aos quais adicionar tags.
6. Na lista de recursos, selecione a caixa ao lado de cada recurso ao qual adicionar tags.
7. Em Adicionar tag, para Chave e Valor, digite a chave e os valores da tag e selecione 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 [Locais de recursos \(p. 992\)](#).
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. Para Filtro, selecione o tipo de recurso (por exemplo, instâncias) dos quais as tags devem ser removidas.
6. Na lista de recursos, selecione a caixa ao lado de cada recurso do qual as tags devem ser removidas.
7. Em Remover tag, para Chave, digite o nome da tag e selecione Remover tag.

Adição de uma tag ao executar uma instância

Para adicionar uma tag usando o assistente de execução

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 satisfaz suas necessidades. Para obter mais informações, consulte [Locais de recursos \(p. 992\)](#).
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 sobre a seleção de uma AMI, consulte [Localizar uma AMI do Linux \(p. 95\)](#).
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.

Filtragem de uma lista de recursos por tags

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. Exiba uma coluna para o tag da seguinte forma:
 - a. Selecione um recurso.
 - b. No painel de detalhes, escolha tags.
 - c. Encontre a tag na lista e escolha Mostrar coluna.
2. Escolha o ícone de filtro no canto superior direito da coluna para a tag exibir a lista de filtros.
3. Selecione os valores das tags e escolha Aplicar filtro para filtrar a lista dos resultados.

Note

Para obter mais informações sobre os filtros, consulte [Listagem e filtragem dos seus recursos \(p. 999\)](#).

Trabalho com tags usando a CLI ou a API

Use o seguinte para adicionar, atualizar, listar e excluir as tags para seus recursos. A documentação correspondente traz exemplos.

Tarefa	AWS CLI	AWS Tools para Windows PowerShell	Ação API
Adicione ou sobrescreva uma ou mais tags.	create-tags	New-EC2Tag	CreateTags
Exclua uma ou mais tags.	delete-tags	Remove-EC2Tag	DeleteTags
Descreva uma ou mais tags.	describe-tags	Get-EC2Tag	DescribeTags

Você também pode filtrar uma lista de recursos de acordo com as tags deles. Os exemplos a seguir demonstram como filtrar suas instâncias usando tags com o comando [describe-instances](#).

Note

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 estabelecer 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 [Especificar valores de parâmetro para a interface da linha de comando da AWS](#).

Exemplo 1: 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-key,Values=Stack
```

Exemplo 2: 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
```

Exemplo 3: Descreva as instâncias com o valor de tag especificado

O comando a seguir descreve as instâncias com uma tag com produção de valor, independentemente da chave da tag.

```
aws ec2 describe-instances --filters Name=tag-value,Values=production
```

Algumas ações de criação de recursos permitem especificar as tags ao criar o recurso. As ações a seguir são compatíveis com o uso de tags na criação.

Tarefa	AWS CLI	AWS Tools para Windows PowerShell	Ação API
Execute uma ou mais instâncias.	run-instances	New-EC2Instance	RunInstances
Crie um volume do EBS.	create-volume	New-EC2Volume	CreateVolume

Os exemplos a seguir demonstram como aplicar tags ao criar recursos.

Exemplo 4: Execute uma instância e aplique tags à instância e ao volume

O comando a seguir executa uma instância e aplica uma tag com uma chave de `webserver` e um valor de `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}]'
```

Exemplo 5: Crie um o volume e aplique uma tag

O comando a seguir 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}]'
```

Exemplo 6: adicionar uma tag a um recurso

Este exemplo 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
```

Exemplo 7: 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
```

Exemplo 8: adicionar tags com caracteres especiais

Este exemplo adiciona a tag `[Group]=test` a uma instância. Os colchetes (`[e]`) são caracteres especiais e devem ser recuados com uma barra invertida (`\`).

```
aws ec2 create-tags --resources i-1234567890abcdef0 --tags Key=\[Group\],Value=test
```

Se você estiver usando o Windows PowerShell, divida os caracteres com uma barra invertida (`\`), coloque-os entre aspas duplas (`"`) e depois coloque a estrutura de chave e valor inteira entre aspas simples (`'`).

```
aws ec2 create-tags --resources i-1234567890abcdef0 --tags 'Key=\\"[Group]\\",Value=test'
```

Se você estiver usando Linux ou OS X, coloque toda a estrutura de chave e valor entre aspas simples (`'`) e coloque o elemento com o caractere especial entre aspas duplas (`"`).

```
aws ec2 create-tags --resources i-1234567890abcdef0 --tags 'Key=\"[Group]\",Value=test'
```

Limites 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 limites padrão nesses recursos de acordo com a região. Por exemplo, há um limite no número total de instâncias que você pode iniciar em uma região. Portanto, quando você executar uma instância em Oeste dos EUA (Oregon) region, a solicitação não deverá fazer com que seu uso exceda o limite de instâncias atual 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 sobre os limites de outros serviços, consulte [Limites de serviços da AWS](#) no Referência geral do Amazon Web Services.

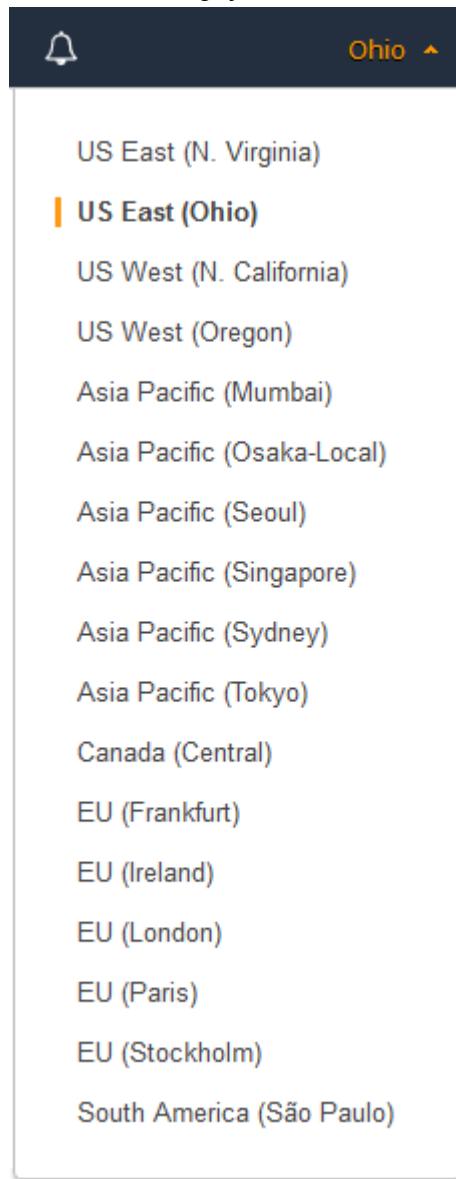
Visualizando seus limites atuais.

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.

Para visualizar seus 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. A coluna Limite atual exibe o máximo atual desse recurso para sua conta.

Como solicitar um aumento de limite

Use a página Limites no console do Amazon EC2 para solicitar um aumento nos limites dos recursos fornecidos pelo Amazon EC2 ou pela Amazon VPC por região.

Para solicitar um aumento de limite

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. Escolha Solicitar aumento de limite.
5. Preencha os campos necessários no formulário de aumento de limite. Responderemos usando o método de contato que você especificou.

Limites de e-mails enviados usando a porta 25

O Amazon EC2 regula o tráfego pela porta 25 de todas as instâncias por padrão. Você pode solicitar que essa limitação seja removida. Para obter mais informações, consulte [Como faço para remover a limitação da porta 25 na minha instância do EC2?](#) no Centro de conhecimento da AWS.

Relatórios de uso do Amazon EC2

A AWS fornece uma ferramenta de geração de relatório gratuita, chamada Custo Explorer, que permite analisar o custo e o uso das instâncias do EC2 e uso das instâncias reservadas.

O Cost Explorer é uma ferramenta gratuita que você pode usar para exibir gráficos de uso e custos. 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 por contas da AWS?
- Até que ponto estou aproveitando bem minhas Instâncias reservadas?
- Minhas Instâncias reservadas estão me ajudando a economizar?

Para exibir o relatório do Amazon EC2 no Cost Explorer

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Reports (Relatórios) e selecione um relatório a ser exibido.

O relatório é aberto no Cost Explorer. Ele fornece uma exibição pré-configurada, com base em configurações de filtro fixas, que mostra informações sobre suas tendências de uso e custo.

Para obter mais informações sobre como trabalhar com relatórios no Cost Explorer, incluindo relatórios de economia, consulte [Como analisar seus custos com o Cost Explorer](#).

Como 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.

Note

Se você estiver usando uma instância Windows, consulte [EC2Rescue para Windows Server](#).

Tópicos

- [Instalação do EC2Rescue para Linux \(p. 1016\)](#)
- [Como trabalhar com EC2Rescue para Linux \(p. 1019\)](#)
- [Desenvolvimento de módulos do EC2Rescue \(p. 1021\)](#)

Instalação do EC2Rescue para Linux

A ferramenta EC2Rescue para Linux pode ser instalada em uma instância Linux do Amazon EC2 que atenda aos seguintes pré-requisitos.

Pré-requisitos

- Sistemas operacionais com suporte:
 - Amazon Linux 2
 - Amazon Linux 2016.09+
 - SLES 12+
 - RHEL 7+
 - Ubuntu 16.04+
- Requisitos de software:
 - Python 2.7.9+ ou 3.2+

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 do EC2Rescue para Linux \(p. 1017\)](#).
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
```

- Desembale o tarball:

```
tar -xvf ec2rl.tgz
```

- 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 \(p. 1017\)](#)
- [Autenticar e importar a chave pública \(p. 1018\)](#)
- [Verificar a assinatura do pacote \(p. 1018\)](#)

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
```

- 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>.

Como trabalhar com EC2Rescue para Linux

Veja a seguir as tarefas comuns que você pode realizar para começar a usar essa ferramenta.

Tarefas

- [Executar o EC2Rescue para Linux \(p. 1019\)](#)
- [Como fazer upload dos resultados \(p. 1020\)](#)
- [Criação de backups \(p. 1020\)](#)
- [Receber ajuda \(p. 1021\)](#)

Executar o 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/temp/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
```

Como 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 os resultados no 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](#).

Criação de 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 com 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
```

Receber 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
```

Desenvolvimento de 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.

Como 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.

Atributo	Descrição
title	Um título curto e descritivo para o módulo. Esse valor precisa ter 50 caracteres ou menos.
helptext	<p>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.</p> <p>Por exemplo:</p> <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	<p>O estágio no qual o módulo deve ser executado. Valores com suporte:</p> <ul style="list-style-type: none"> pré-diagnóstico executar pós-diagnóstico
linguagem	<p>A linguagem em que o código do módulo está escrito. Valores com suporte:</p> <ul style="list-style-type: none"> bash python <p>Note</p> <p>O código Python deve ser compatível com o Python 2.7.9+ e o Python 3.2+.</p>
correção	<p>Indica se o módulo dá suporte a correção. Os valores compatíveis são <code>True</code> ou <code>False</code>.</p> <p>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.</p>
conteúdo	A totalidade do código do script.
restrição	O nome do objeto que contém os valores de limite.
domínio	<p>Um descritor de como o módulo é agrupado ou classificado. O conjunto de módulos incluídos usa os seguintes domínios:</p> <ul style="list-style-type: none"> aplicativo net os desempenho

Atributo	Descrição
classe	<p>Um descritor do tipo da tarefa executada pelo módulo. O conjunto de módulos incluídos usa as seguintes classes:</p> <ul style="list-style-type: none"> • coletar (coleta a saída dos programas) • diagnosticar (é aprovado/falha com base em um conjunto de critérios) • recolher (copia os arquivos e grava em um arquivo específico)
distro	<p>A lista de distribuições Linux às quais esse módulo oferece suporte. O conjunto de módulos usa as seguintes distribuições:</p> <ul style="list-style-type: none"> • alami (Amazon Linux) • rhel • ubuntu • suse
obrigatório	Os argumentos necessários que o módulo está consumindo das opções de CLI.
opcional	Os argumentos opcionais que o módulo pode usar.
software	<p>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.</p>
pacote	<p>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.</p>
sudo	<p>Indica se o acesso raiz é necessário para executar o módulo.</p> <p>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.</p>
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 <code>--perfimpact=true</code> 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.

Como adicionar variáveis de ambiente

A tabela a seguir lista as variáveis de ambiente disponíveis.

Variável de ambiente	Descrição
EC2RL_CALLPATH	O caminho para <code>ec2rl.py</code> . Esse caminho pode ser usado para encontrar o diretório lib e utilizar os módulos Python do fornecedor.
EC2RL_WORKDIR	O diretório tmp principal para a ferramenta de diagnóstico. Valor padrão: <code>/var/tmp/ec2rl</code> .
EC2RL_RUNDIR	O diretório no qual a saída é armazenada. Valor padrão: <code>/var/tmp/ec2rl/<date&timestamp></code> .
EC2RL_GATHEREDDIR	O diretório raiz para colocar os dados de módulo reunidos. Valor padrão: <code>/var/tmp/ec2rl/<date&timestamp>/mod_out/gathered/</code> .
EC2RL_NET_DRIVER	O driver em uso na primeira interface de rede não virtual, ordenada alfabeticamente, na instância. Exemplos: <ul style="list-style-type: none">• <code>xen_netfront</code>• <code>ixgbefv</code>• <code>ena</code>
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">• <code>default-hvm</code>• <code>default-paravirtual</code>
EC2RL_INTERFACES	Uma lista enumerada de interfaces no sistema. O valor é uma string que contém nomes, como <code>eth0eth1</code> , etc. É gerada pelo <code>functions.bash</code> e está disponível somente para os módulos que a originaram.

Uso da 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 módulo

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
```

Solução de problemas das instâncias

A documentação a seguir podem ajudar a solucionar problemas que você venha a ter com sua instância.

Tópicos

- [Solução de problemas de execução de instâncias \(p. 1026\)](#)
- [Resolução de problemas para se conectar à sua instância \(p. 1028\)](#)
- [Solução de problemas da parada da sua instância \(p. 1035\)](#)
- [Solução de problemas de encerramento \(desativação\) da sua instância \(p. 1037\)](#)
- [Solução de problemas em instâncias com falha nas verificações de status \(p. 1038\)](#)
- [Solucione problemas de falhas de recuperação da instância \(p. 1061\)](#)
- [Como obter a saída do console \(p. 1061\)](#)
- [Inicialização a partir do volume errado \(p. 1064\)](#)

Para obter mais ajuda com instâncias Windows, consulte [Solução de problemas das instâncias Windows](#) no Guia do usuário do Amazon EC2 para instâncias do Windows.

Você também pode pesquisar respostas e postar perguntas no [Amazon EC2 forum](#).

Solução de problemas de execução de instâncias

Os problemas a seguir impedem que você execute uma instância.

Problemas de execução

- [Limite de instâncias excedido \(p. 1026\)](#)
- [Capacidade insuficiente da instância \(p. 1027\)](#)
- [A instância é encerrada imediatamente \(p. 1027\)](#)

Limite de instâncias excedido

Descrição

Você obtém o erro `InstanceLimitExceeded` ao tentar executar uma nova instância ou reiniciar uma instância interrompida.

Causa

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.

Solução

Você pode solicitar um aumento de limite de instâncias por região. Para obter mais informações, consulte [Limites de serviço do Amazon EC2 \(p. 1013\)](#).

Capacidade insuficiente da instância

Descrição

Você obtém o erro `InsufficientInstanceCapacity` ao tentar executar uma nova instância ou reiniciar uma instância interrompida.

Causa

Se você receber um erro `InsufficientInstanceCapacity` 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.

Solução

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 \(p. 247\)](#).
- 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 \(p. 795\)](#).
- Tente criar um Reserva de capacidade sob demanda, o que permite reservar capacidade do Amazon EC2 por qualquer duração. Para obter mais informações, consulte [Reservas de capacidade sob demanda \(p. 376\)](#).
- Tente comprar instâncias reservadas, que são uma reserva de capacidade de longo prazo. Para obter mais informações, consulte [Instâncias reservadas do Amazon EC2](#).

A instância é encerrada imediatamente

Descrição

Sua instância passa do estado `pending` para o estado `terminated` assim que é reiniciada.

Causa

A seguir estão alguns motivos pelos quais a instância pode ser imediatamente encerrada:

- Você alcançou o limite do volume do EBS.
- Um snapshots do EBS está corrompido.
- O volume EBS raiz é criptografado e você não tem permissões para acessar a chave do KMS para descriptografia.
- A AMI com armazenamento de instâncias que você usou para executar a instância não tem um item necessário (um arquivo `image.part.xx`).

Solução

Você pode usar o console do Amazon EC2 ou a AWS Command Line Interface para obter o motivo do encerramento.

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 guia Description (Descrição), anote o motivo ao lado da etiqueta State transition reason (Motivo da 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"  
},
```

Para resolver o problema

Execute uma das ações a seguir dependendo do motivo do encerramento observado:

- Se o motivo for `Client.VolumeLimitExceeded: Volume limit exceeded`, isso significa que você atingiu o limite do volume do EBS. Para obter mais informações, consulte [Limites de volume de instância \(p. 976\)](#). Para enviar uma solicitação para aumentar o limite de volume do Amazon EBS, preencha o formulário [Criar caso](#) do AWS Support Center. Para obter mais informações, consulte [Limites de serviço do Amazon EC2 \(p. 1013\)](#).
- Se o motivo for `Client.InternalError: Client error on launch`, isso em geral indica que o volume raiz está criptografado e que você não tem permissões para acessar a chave do KMS para a descriptografia. Para obter permissões acessar a chave necessária do KMS, adicione as permissões apropriadas do KMS ao usuário do IAM. Para obter mais informações, consulte [Como usar políticas de chave no AWS KMS](#) no AWS Key Management Service Developer Guide.

Resolução de problemas para se conectar à sua instância

A seguir estão os possíveis problemas que possíveis você pode ter e mensagens de erro que você poderá ver ao tentar se conectar à sua instância.

Tópicos

- [Erro ao se conectar à sua instância: limite de tempo da conexão atingido \(p. 1029\)](#)
- [Erro: Chave do usuário não reconhecida pelo servidor \(p. 1031\)](#)

- Erro: Chave do host não encontrada, permissão negada (publickey) ou Falha na autenticação, permissão negada (p. 1032)
- Erro: Arquivo de chave privada desprotegido (p. 1033)
- Erro: a chave privada deve começar com "----BEGIN RSA PRIVATE KEY----" e terminar com "----END RSA PRIVATE KEY----" (p. 1034)
- Erro: O servidor recursou nossa chave ou Não há métodos de autenticação compatíveis (p. 1034)
- Erro ao usar o MindTerm no navegador Safari (p. 1035)
- Não é possível fazer o ping da instância (p. 1035)

Para obter mais ajuda com instâncias Windows, consulte [Solução de problemas das instâncias Windows](#) no Guia do usuário do Amazon EC2 para instâncias do Windows.

Você também pode pesquisar respostas e postar perguntas no [Amazon EC2 forum](#).

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.
 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 mais informações, consulte [Autorização de acesso de rede para suas instâncias](#) (p. 720).

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.
 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 de 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-xxxxxxx) 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 Network ACLs devem permitir tráfego de entrada e de saída do seu endereço IP local na porta apropriada. A Network ACL padrão permite todo o tráfego de entrada e saída.
 1. Abra o console de Amazon VPC em <https://console.aws.amazon.com/vpc/>.
 2. No painel de navegação, selecione Sub-redes e selecione sua sub-rede.
 3. Na guia Description (Descrição), localize Network ACL (Conexão ACL) e escolha o seu ID (acl-xxxxxxx).
 4. Selecione a Network ACL. Na guia Regras de entrada, verifique se as regras permitem tráfego a partir do seu computador. Caso contrário, exclua ou modifique a regra que está bloqueando tráfego do seu computador.
 5. Na guia Regras de saída, verifique se as regras permitem tráfego para o seu computador. Caso contrário, exclua ou modifique a regra que está bloqueando tráfego para seu computador.
 - Se seu computador estiver em uma rede corporativa, pergunte ao administrador de 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 Elastic IP \(p. 742\)](#).
- Verifique a carga da CPU na instância. O servidor pode estar sobrecarregado. A AWS fornece automaticamente dados, como status de métricas e status de Amazon CloudWatch, que você pode usar para ver quanta carga de CPU estiver na sua instância e, caso necessário, ajusta como suas cargas são manuseadas. Para obter mais informações, consulte [Monitoramento das suas instâncias usando o CloudWatch \(p. 575\)](#).
 - 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 \(p. 247\)](#).

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 tiver executado sua instância de uma AMI mais antiga, isso pode não ser configurado 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: 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 [your key name].pem ec2-user@[public DNS address of your instance].compute-1.amazonaws.com
```

O exemplo 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: kex_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: bogus.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: bogus.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 SSH (MindTerm) para conectar à sua instância

- Se o Java não for ativado, o servidor não reconhecerá a chave do usuário. Para habilitar o Java, acesse [Como habilito o Java no meu navegador?](#) na documentação do Java.

Se você usar o PuTTY para conectar à sua instância

- Verifique se seu arquivo de chave privada (.pem) foi convertido para o formato reconhecido por PuTTY (.ppk). Para obter mais informações a conversão da sua chave privada, consulte [Conexão da sua instância do Linux no Windows usando PuTTY \(p. 444\)](#).

Note

No PuTTYgen, carregue seu 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. Digite o nome de usuário na caixa Nome do host na janela Configuração de PuTTY.
 - Para a AMI do Amazon Linux 2 ou do Amazon Linux, o nome de usuário é `ec2-user`.
 - Para um AMI do CentOS, o nome de usuário é `centos`.
 - Em uma AMI do Debian, o nome de usuário é `admin` ou `root`.
 - Para a AMI do Fedora, o nome de usuário é `ec2-user` ou `fedora`.
 - Para a AMI do RHEL, o nome de usuário é `ec2-user` ou `root`.
 - Para a AMI do SUSE, o nome de usuário é `ec2-user` ou `root`.
 - Para uma AMI do Ubuntu, o nome de usuário é `ubuntu`.
 - Caso contrário, se `ec2-user` e `root` não funcionarem, verifique com o provedor de 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 \(p. 720\)](#).

Erro: Chave do host não encontrada, permissão negada (publickey) ou Falha na autenticação, permissão negada

Se você se conectar à sua instância usando SSH e obtiver algum dos erros a seguir, `Host key not found in [directory]`, `Permission denied (publickey)` ou `Authentication failed, permission denied`, verifique se está se conectando com o nome de usuário apropriado para sua AMI e que especificou o arquivo de chave privada (`.pem`) apropriado para sua instância. Para clientes MindTerm, insira o nome de usuário na caixa Nome do usuário da janela Conectar à sua instância.

Os nomes de usuários adequados são os seguintes:

- Para a AMI do Amazon Linux 2 ou do Amazon Linux, o nome de usuário é `ec2-user`.
- Para um AMI do CentOS, o nome de usuário é `centos`.
- Em uma AMI do Debian, o nome de usuário é `admin` ou `root`.
- Para a AMI do Fedora, o nome de usuário é `ec2-user` ou `fedora`.
- Para a AMI do RHEL, o nome de usuário é `ec2-user` ou `root`.
- Para a AMI do SUSE, o nome de usuário é `ec2-user` ou `root`.
- Para uma AMI do Ubuntu, o nome de usuário é `ubuntu`.
- Caso contrário, se `ec2-user` e `root` não funcionarem, verifique com o provedor de 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 ec2-user@public-dns-hostname
```

Confirme se você está usando um arquivo de chave privada que corresponde ao par de chaves que selecionou ao executar a instância.

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. Selecione sua instância. Na guia Descrição, verifique o valor de Nome do par de chaves.
3. 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 [Conexão à sua instância do Linux se você perder sua chave privada \(p. 623\)](#).

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/ec2-user/.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 [Interrompa e inicie sua instância \(p. 458\)](#) e [Separação de um volume do Amazon EBS de uma instância \(p. 893\)](#).
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 [Associação de um volume do Amazon EBS a uma instância \(p. 863\)](#).
3. Conecte-se à instância temporária, crie um ponto de montagem e monte o volume associado. Para obter mais informações, consulte [Disponibilização de um volume do Amazon EBS para uso no Linux \(p. 864\)](#).
4. Na instância temporária, verifique as permissões do diretório `/home/ec2-user/` do volume associado. Se necessário, ajuste as permissões da seguinte forma:

```
[ec2-user ~]$ chmod 600 mount_point/home/ec2-user/.ssh/authorized_keys
```

```
[ec2-user ~]$ chmod 700 mount_point/home/ec2-user/.ssh
```

```
[ec2-user ~]$ chmod 700 mount_point/home/ec2-user
```

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!      @  
@@@@@@@
```

Amazon Elastic Compute Cloud
User Guide for Linux Instances

Erro: a chave privada deve começar com "----
BEGIN RSA PRIVATE KEY----" e terminar
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. Para corrigir o erro, execute o comando a seguir substituindo o caminho pelo seu arquivo de chave privada.

```
[ec2-user ~]$ chmod 0400 .ssh/my_private_key.pem
```

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 recursou nossa chave ou Não há métodos de autenticação compatíveis

Se você usar o PuTTY para se conectar à sua instância e obter algum dos erros a seguir, `Error: Server refused our key` ou `Error: No supported authentication methods available`, verifique se está se conectando com o nome de usuário apropriado para sua AMI. Digite o nome de usuário na caixa Nome do usuário na janela Configuração de PuTTY.

Os nomes de usuários adequados são os seguintes:

- Para a AMI do Amazon Linux 2 ou do Amazon Linux, o nome de usuário é `ec2-user`.
- Para um AMI do CentOS, o nome de usuário é `centos`.
- Em uma AMI do Debian, o nome de usuário é `admin` ou `root`.
- Para a AMI do Fedora, o nome de usuário é `ec2-user` ou `fedora`.
- Para a AMI do RHEL, o nome de usuário é `ec2-user` ou `root`.
- Para a AMI do SUSE, o nome de usuário é `ec2-user` ou `root`.
- Para uma AMI do Ubuntu, o nome de usuário é `ubuntu`.
- Caso contrário, se `ec2-user` e `root` não funcionarem, verifique com o provedor de AMI.

Você também deve verificar se seu arquivo de chave privada (.pem) foi convertido corretamente para o formato reconhecido por PuTTY (.ppk). Para obter mais informações a conversão da sua chave privada, consulte [Conexão da sua instância do Linux no Windows usando PuTTY \(p. 444\)](#).

Erro ao usar o MindTerm no navegador Safari

Se você usar o MindTerm para se conectar com sua instância e estiver usando o navegador Safari, pode obter o seguinte erro:

```
Error connecting to your_instance_ip, reason:  
-> Key exchange failed: Host authentication failed
```

Você precisa atualizar as configurações de segurança do navegador para permitir que o Console de gerenciamento da AWS execute o plug-in do Java no modo inseguro.

Para permitir que o plug-in do Java execute no modo inseguro

1. No Safari, mantenha o console do Amazon EC2 aberto e escolha Safari, Preferências, Segurança.
2. Escolha Configurações do plug-in (ou Gerenciar configurações do website, nas versões mais antigas do Safari).
3. Escolha o plug-in do Java à esquerda.
4. Para Websites abertos no momento, selecione a URL do Console de gerenciamento da AWS e escolha Executar em modo desprotegido.
5. Quando solicitado, escolha Confiável na caixa de diálogo de advertência e escolha Concluído.

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.

Solução de problemas da parada da sua 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 há custo nenhum pelo uso da instância enquanto ela não estiver no estado `running`.

Force a interrupção da instância usando o console ou a AWS CLI.

- Para forçar a interrupção da instância usando o console, selecione a instância travada e escolha Actions (Ações), Instance State (Estado da instância), Stop (Parar) e Yes, Forcefully Stop (Sim, force a interrupção).
- Para forçar a interrupção 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 [Amazon EC2 forum](#). 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](#).

Criar uma instância de substituição

Para tentar resolver o problema enquanto você espera pela assistência do [Amazon EC2 forum](#) ou do [Atendimento ao cliente](#), crie uma instância de substituição. Crie uma AMI da instância travada e execute uma nova instância usando a nova AMI.

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 [Criação de uma AMI do Linux de uma instância \(p. 112\)](#)

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.

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 nos procedimentos anteriores, 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, selecione Instâncias, selecione a instância que acabou de executar, escolha Ações, Estado da instância e Parar.
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 Ações, Associar volume e associe-o na nova instância como volume do dispositivo 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 Ações, Estado da instância, Iniciar. Verifique se a instância está trabalhando.
9. Selecione a instância travada, escolha Ações, depois Estado da instância e Encerrar. Se a instância também ficar travada ao ser encerrada, o Amazon EC2 automaticamente forçará o encerramento dela dali a algumas horas.

Solução de problemas de encerramento (desativação) da sua 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`.

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 mais do que várias horas, publique uma solicitação de ajuda no [Amazon EC2 forum](#). 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.

Execute ou encerre automaticamente as instâncias

Se você encerrar todas as instâncias, poderá ver que nós executamos uma nova instância para você. Se você executar uma instância, poderá ver que nós encerramos uma de suas instâncias. Se parar uma

instância, poderá ver que nós encerramos a instância e executamos uma nova instância. Geralmente, esses comportamentos significam que você usou o Amazon EC2 Auto Scaling ou o Elastic Beanstalk para escalar seus recursos de computação automaticamente com base em critérios que você definiu.

Para obter mais informações, consulte [Guia do usuário do Amazon EC2 Auto Scaling](#) ou [Guia do desenvolvedor do AWS Elastic Beanstalk](#).

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.

Tópicos

- [Analizar informações de verificação de status \(p. 1039\)](#)
- [Recuperar os logs do sistema \(p. 1039\)](#)
- [Resolução de problemas dos erros no log do sistema para instâncias baseadas em Linux \(p. 1040\)](#)
- [Sem memória: encerrar processo \(p. 1041\)](#)
- [ERRO: falha em mmu_update \(falha na atualização do gerenciamento de memória\) \(p. 1041\)](#)
- [Erro de E/S \(Falha de dispositivo de blocos\) \(p. 1042\)](#)
- [ERRO DE E/S: nem disco local nem disco remoto \(o dispositivo de blocos distribuído está quebrado\) \(p. 1043\)](#)
- [request_module: modprobe de loop descontrolado \(modprobe do kernel legado do looping, em versões mais antigas do Linux\) \(p. 1044\)](#)
- ["FATAL: kernel antigo demais" e "fsck: Não existe esse arquivo ou diretório ao tentar abrir /dev" \(falta de correspondência entre o kernel e a AMI\) \(p. 1045\)](#)
- ["FATAL: Não foi possível carregar os módulos /lib/" ou "BusyBox" \(módulos do kernel ausentes\) \(p. 1045\)](#)
- [ERRO Kernel inválido \(kernel incompatível com EC2\) \(p. 1047\)](#)
- [request_module: modprobe de loop descontrolado \(modprobe do kernel legado do looping, em versões mais antigas do Linux\) \(p. 1048\)](#)
- [fsck: Nenhum arquivo ou diretório ao tentar abrir... \(Sistema de arquivos não encontrado\) \(p. 1049\)](#)
- [Erro geral ao montar os sistemas de arquivos \(falha na montagem\) \(p. 1050\)](#)
- [VFS: Não foi possível montar o fs raiz em um bloco desconhecido \(falta de correspondência no sistema de arquivos-raiz\) \(p. 1052\)](#)
- [Erro: não foi possível determinar o número principal/secundário do dispositivo raiz... \(Incompatibilidade entre sistema de arquivos/dispositivo raiz\) \(p. 1053\)](#)
- [XENBUS: Dispositivo sem driver... \(p. 1054\)](#)
- [...dias sem ser verificada, verificação forçada \(verificação necessária para o sistema de arquivos\) \(p. 1055\)](#)
- [O fsck morreu com status de saída... \(Dispositivo ausente\) \(p. 1055\)](#)
- [Prompt do GRUB \(grubdom>\) \(p. 1056\)](#)
- [Acessando a interface eth0: O dispositivo eth0 tem um endereço MAC diferente do esperado, ignorando. \(Endereço MAC hard-coded\) \(p. 1058\)](#)
- [Não foi possível carregar a Política do SELinux. A máquina está no modo de força. Parando agora. \(Erro de configuração do SELinux\) \(p. 1059\)](#)

- [XENBUS: Excedido o limite de tempo para se conectar a dispositivos \(tempo limite do Xenbus\) \(p. 1060\)](#)

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 que interrompem, encerram ou recuperam uma instância](#) no Guia do usuário do Amazon CloudWatch.
- Se você alterou o tipo de instância para uma [instância baseada em Nitro \(p. 179\)](#), as verificações de status falham se você migrou de uma instância que não possui os drivers ENA e NVMe necessários. Para obter mais informações, consulte [Compatibilidade para redimensionamento de instâncias \(p. 248\)](#).
- 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 [Amazon EC2 forum](#).
- 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 para 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 Ações, Estado da instância, Reiniciar. Pode demorar alguns minutos para sua instância reiniciar.
4. Verifique o problema ainda existe; em alguns casos, reiniciar pode resolver o problema.
5. Quando a instância estiver no estado `running`, escolha Ações, Configurações da instância, 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 publicar seu problema no [Amazon EC2 forum](#).

Resolução de problemas dos erros no log 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. 1041)
- ERRO: falha em mmu_update (falha na atualização do gerenciamento de memória) (p. 1041)

Erros do dispositivo

- Erro de E/S (Falha de dispositivo de blocos) (p. 1042)
- ERRO DE E/S: nem disco local nem disco remoto (o dispositivo de blocos distribuído está quebrado) (p. 1043)

Erros de kernel

- request_module: modprobe de loop descontrolado (modprobe do kernel legado do looping, em versões mais antigas do Linux) (p. 1044)
- "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. 1045)
- "FATAL: Não foi possível carregar os módulos /lib/" ou "BusyBox" (módulos do kernel ausentes) (p. 1045)
- ERRO Kernel inválido (kernel incompatível com EC2) (p. 1047)

Erros do sistema de arquivos

- request_module: modprobe de loop descontrolado (modprobe do kernel legado do looping, em versões mais antigas do Linux) (p. 1048)
- fsck: Nenhum arquivo ou diretório ao tentar abrir... (Sistema de arquivos não encontrado) (p. 1049)
- Erro geral ao montar os sistemas de arquivos (falha na montagem) (p. 1050)
- VFS: Não foi possível montar o fs raiz em um bloco desconhecido (falta de correspondência no sistema de arquivos-raiz) (p. 1052)
- Erro: não foi possível determinar o número principal/secundário do dispositivo raiz... (Incompatibilidade entre sistema de arquivos/dispositivo raiz) (p. 1053)
- XENBUS: Dispositivo sem driver... (p. 1054)
- ...dias sem ser verificada, verificação forçada (verificação necessária para o sistema de arquivos) (p. 1055)
- O fsck morreu com status de saída... (Dispositivo ausente) (p. 1055)

Erros do sistema operacional

- Prompt do GRUB (grubdom>) (p. 1056)

- Acessando a interface eth0: O dispositivo eth0 tem um endereço MAC diferente do esperado, ignorando. (Endereço MAC hard-coded) (p. 1058)
- Não foi possível carregar a Política do SELinux. A máquina está no modo de força. Parando agora. (Erro de configuração do SELinux) (p. 1059)
- XENBUS: Excedido o limite de tempo para se conectar a dispositivos (tempo limite do Xenbus) (p. 1060)

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	<p>Faça uma das coisas a seguir:</p> <ul style="list-style-type: none">• 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.• 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.
Com armazenamento de instâncias	<p>Faça uma das coisas a seguir:</p> <ul style="list-style-type: none">• 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.• 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.

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 contate 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">1. Pare a instância.2. Separe o volume.3. Tentativa de recuperar o volume. <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">4. Reassocie o volume à instância.5. Separe o volume.
Com armazenamento de instâncias	<p>Encerre a instância e execute uma nova instância.</p> <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)

OMB HIGHMEM available.

...
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>

Para este tipo de instância	Faça o seguinte
	1. Pare a instância. 2. Modifique os atributos de kernel e ramdisk para usar um kernel mais recente. 3. Inicie a instância.
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	Use o procedimento a seguir: 1. Pare a instância. 2. Modifique a configuração para usar um kernel mais recente. 3. Inicie a instância.
Com armazenamento de instâncias	Use o procedimento a seguir: 1. Crie uma AMI que use um kernel mais recente. 2. Encerre a instância. 3. Execute uma nova instância com base na AMI criada.

"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.

Amazon Elastic Compute Cloud
User Guide for Linux Instances
"FATAL: Não foi possível carregar os módulos /lib/" ou "BusyBox" (módulos do kernel ausentes)

```
[    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/sda1 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">1. Selecione o ramdisk corrigido para o volume do Amazon EBS.2. Pare a instância.3. Desanexe o volume e repare-o.4. Associe o volume à instância.5. Inicie a instância.6. Modifique a AMI para usar o ramdisk corrigido.
Com armazenamento de instâncias	<p>Use o procedimento a seguir:</p>

Para este tipo de instância	Faça o seguinte
	<ol style="list-style-type: none">1. Encerre a instância e execute uma nova instância com o ramdisk correto.2. Crie uma nova AMI com o ramdisk correto.

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/sdal 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/sdal 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	<p>Use o procedimento a seguir:</p> <ol style="list-style-type: none">1. Pare a instância.2. Substitua por um kernel em funcionamento.3. Instale um kernel de fallback.4. Modifique a AMI corrigindo o kernel.
Com armazenamento de instâncias	Use o procedimento a seguir:

Para este tipo de instância	Faça o seguinte
	<ol style="list-style-type: none">1. Encerre a instância e execute uma nova instância com o kernel correto.2. Crie uma AMI com o kernel correto.3. (Opcional) Procure assistência técnica para recuperação de dados usando o AWS Support.

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
request_module: runaway loop modprobe binfmt-464c
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">1. Pare a instância.2. Modifique os atributos de kernel e ramdisk para usar um kernel mais recente.3. Inicie a instância.

Para este tipo de instância	Faça o seguinte
Com armazenamento de instâncias	Encerre a instância e execute uma nova, especificando os parâmetros <code>-kernel</code> e <code>-ramdisk</code> .

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
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">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.2. Corrija o ramdisk para incluir o /etc/fstab modificado (se aplicável).3. Modifique as AMIs para usar um ramdisk mais recente. <p>O sexto campo do fstab define os requisitos de disponibilidade da montagem – um valor diferente 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.</p>
Com armazenamento de instâncias	<p>Use o procedimento a seguir:</p> <ol style="list-style-type: none">1. Encerre a instância e execute uma nova instância.2. Separe todos os volumes do Amazon EBS com erro e a instância de reinicialização.3. (Opcional) Procure assistência técnica para recuperação de dados usando o AWS Support.

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">Volume do Amazon EBS destacado ou com falha.Sistema de arquivos corrompido.Combinação malfeita de ramdisk e AMI (por exemplo, ramdisk Debian com AMI SUSE).
Com armazenamento de instâncias	<ul style="list-style-type: none">Uma unidade com falha.Um sistema de arquivos corrompido.Combinação malfeita de ramdisk e AMI (por exemplo, ramdisk Debian com AMI SUSE).

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">Pare a instância.Separar o volume de raiz.Associe o volume do dispositivo raiz a uma instância de trabalho conhecida.Execute uma verificação no sistema de arquivos (fsck -a /dev/...).Corrija todos os erros.Separar o volume de instância de trabalho conhecida.Associe o volume à instância parada.Inicie a instância.Verifique novamente o status da instância.

Para este tipo de instância	Faça o seguinte
Com armazenamento de instâncias	Faça uma das coisas a seguir: <ul style="list-style-type: none"> Execute uma nova instância. (Opcional) Procure assistência técnica para recuperação de dados usando o AWS Support.

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.

```

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/sda1 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"> Dispositivo não associado corretamente. O dispositivo raiz não foi associado no ponto correto do dispositivo. O sistema de arquivos não está no formato esperado. Uso do kernel de legado (por exemplo, 2.6.16-XenU). Uma atualização de kernel recente na sua instância (atualização defeituosa ou bug de atualização)
Com armazenamento de instâncias	Falha no dispositivo de hardware.

Ações sugeridas

Para este tipo de instância	Faça o seguinte
Baseado em Amazon EBS	Faça uma das coisas a seguir: <ul style="list-style-type: none"> Pare e reinicie a instância. Modifique o volume do dispositivo raiz para associar no ponto correto do dispositivo, possível /dev/sda1 em vez de /dev/sda.

Para este tipo de instância	Faça o seguinte
	<ul style="list-style-type: none"> • Pare e modifique para usar o kernel moderno. • Consulte a documentação para sua distribuição Linux para verificar bugs conhecidos da atualização. Altere ou reinstale o kernel.
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	Use o procedimento a seguir: <ol style="list-style-type: none"> 1. Pare a instância. 2. Separe o volume. 3. Corrija o problema de mapeamento de dispositivos. 4. Inicie a instância.

Para este tipo de instância	Faça o seguinte
	5. Modifique a AMI para abordar os problemas de mapeamento de dispositivos.
Com armazenamento de instâncias	Use o procedimento a seguir: 1. Crie nova AMI com a correção apropriada (mapeie o dispositivo de blocos corretamente). 2. Encerre a instância e execute uma nova a partir da AMI criada.

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	Use o procedimento a seguir: 1. Pare a instância. 2. Separe o volume. 3. Corrija o problema de mapeamento de dispositivos. 4. Inicie a instância. 5. Modifique a AMI para abordar os problemas de mapeamento de dispositivos.

Para este tipo de instância	Faça o seguinte
Com armazenamento de instâncias	Use o procedimento a seguir: <ol style="list-style-type: none"> 1. Crie uma AMI com a correção apropriada (mapeie o dispositivo de blocos corretamente). 2. Encerre a instância e execute uma nova usando a AMI criada.

...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">• Pare a instância, associe o volume a uma instância em execução existente.• Execute manualmente verificações de consistência.• Conserte o ramdisk para incluir utilitários relevantes.• Modifique os parâmetros de ajuste do sistema de arquivos para remover os requisitos de consistência (não recomendados).
Com armazenamento de instâncias	<p>Teste uma ou mais das opções a seguir para resolver o problema:</p> <ul style="list-style-type: none">• Reempacote o ramdisk com as ferramentas corretas.• Modifique os parâmetros de ajuste do sistema de arquivos para remover os requisitos de consistência (não recomendados).• Encerre a instância e execute uma nova instância.• (Opcional) Procure assistência técnica para recuperação de dados usando o AWS Support.

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">• Arquivo de configuração do GRUB ausente.

Tipo de instância	Possíveis causas
	<ul style="list-style-type: none"> • Imagem incorreta de GRUB usada, esperando arquivo de configuração do GRUB em um local diferente. • 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).
Com armazenamento de instâncias	<ul style="list-style-type: none"> • Arquivo de configuração do GRUB ausente. • Imagem incorreta de GRUB usada, esperando arquivo de configuração do GRUB em um local diferente. • 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).

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"> 1. Modifique as AMIs de origem para criar um arquivo de configuração GRUB no local padrão (/boot/grub/menu.lst). 2. Verifique se sua versão do GRUB oferece suporte ao tipo de sistema de arquivos e atualize o GRUB, se necessário. 3. Escolha a imagem de GRUB adequada, (unidade hd0-1st ou hd00 – 1º unidade, 1ª partição). 4. Encerre a instância e execute uma nova usando a AMI criada. <p>Opção 2: Corrija a instância existente:</p> <ol style="list-style-type: none"> 1. Pare a instância. 2. Separe o sistema de arquivos-raiz. 3. Associe o sistema de arquivos raiz para uma instância de trabalho conhecida. 4. Monte o sistema de arquivos. 5. Crie o arquivo de configuração do GRUB. 6. Verifique se sua versão do GRUB oferece suporte ao tipo de sistema de arquivos e atualize o GRUB, se necessário. 7. Separe o sistema de arquivos. 8. Associe à instância original.

Para este tipo de instância	Faça o seguinte
	<p>9. Modifique o atributo do kernel para usar a imagem adequada do GRUB (1º disco ou 1ª partição no 1º disco). 10 Inicie a instância.</p>
Com armazenamento de instâncias	<p>Opção 1: Modifique a AMI e reexecute a instância:</p> <ol style="list-style-type: none">1. Crie a nova AMI com um arquivo de configuração GRUB no local padrão (/boot/grub/menu.lst).2. Escolha a imagem de GRUB adequada, (unidade hd0-1st ou hd00 – 1º unidade, 1ª partição).3. Verifique se sua versão do GRUB oferece suporte ao tipo de sistema de arquivos e atualize o GRUB, se necessário.4. Encerre a instância e execute uma nova usando a AMI criada. <p>Opção 2: Encerre a instância e execute uma nova, especificando o kernel correto.</p> <p>Note</p> <p>Para recuperar dados da instância existente, entre em contato com o AWS Support.</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>Faça uma das coisas a seguir:</p> <ul style="list-style-type: none">Modifique a AMI para remover o hard code e reexecute a instância.Modifique a instância para remover o endereço MAC hard-coded. <p>OU</p> <p>Use o procedimento a seguir:</p> <ol style="list-style-type: none">Pare a instância.Separe o volume de raiz.Associe o volume a outra instância e modifique o volume para remover o endereço MAC hard-coded.Associe o volume à instância original.Inicie a instância.
Com armazenamento de instâncias	<p>Faça uma das coisas a seguir:</p> <ul style="list-style-type: none">Modifique a instância para remover o endereço MAC hard-coded.Encerre a instância e execute uma nova instância.

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">1. Pare a instância com falha.2. Separe o volume do dispositivo raiz da instância com falha.3. Associe o volume do dispositivo raiz a outra instância do Linux em execução (posteriormente chamada de instância de recuperação).4. Conecte-se à instância de recuperação e monte o volume do dispositivo raiz da instância falha.5. 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. <p>Note</p> <p>Em alguns sistemas, você desabilita o SELinux configurando <code>SELINUX=disabled</code> no arquivo <code>/mount_point/etc/sysconfig/selinux</code>, onde <code>mount_point</code> é o local onde você montou o volume da sua instância de recuperação.</p> <ol style="list-style-type: none">6. Desmonte e separe o volume do dispositivo raiz da instância de recuperação e reassocie-o à instância original.7. Inicie a instância.
Com armazenamento de instâncias	<p>Use o procedimento a seguir:</p> <ol style="list-style-type: none">1. Encerre a instância e execute uma nova instância.2. (Opcional) Procure assistência técnica para recuperação de dados usando o AWS Support.

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	Faça uma das coisas a seguir: <ul style="list-style-type: none">• Modifique a AMI e a instância para usar um kernel moderno e reexecutar a instância.• Reinicie a instância.
Com armazenamento de instâncias	Faça uma das coisas a seguir: <ul style="list-style-type: none">• Encerre a instância.• Modifique as AMIs para usar um kernel moderno e execute uma nova instância usando essa AMI.

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 painel de status dos serviços que impediu a execução bem-sucedida do processo de recuperação. Consulte <http://status.aws.amazon.com/> para obter as informações mais recentes sobre a 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 do status do sistema de instância persistir, recomendamos que você inicie e pare manualmente a instância. Para obter mais informações, consulte [Interrompa e inicie sua instância \(p. 458\)](#).

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.

Como obter a saída do console

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.

Da mesma forma, a capacidade para reiniciar instâncias que de outra forma seriam inalcançáveis é valiosa para solução de problemas e gerenciamento geral de instâncias.

As instâncias do EC2 não têm um monitor físico pelo qual você pode ver a saída do console. Eles também carecem de controles físicos que permitem a você iniciá-los, reinicializá-los ou desativá-los. Em vez disso, você executa essas tarefas com a API do Amazon EC2 e com a interface de linha de comando (CLI).

Reinicialização da instância

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 [Reinicialize sua instância \(p. 467\)](#).

Warning

Para instâncias do Windows, essa operação executa um "hard reboot" que pode realizar a corrupção de dados.

Saída do console da instância

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 output exibe 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 é compatível somente em tipos de instância que usam o hypervisor Nitro. 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.

Para obter a saída do console 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 Instâncias e selecione a instância.
3. Selecione Ações, Configurações da instância, Obter log do sistema.

Para obter a saída do console 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 [Acessando o Amazon EC2 \(p. 3\)](#).

- [get-console-output](#) (AWS CLI)
- [Get-EC2ConsoleOutput](#) (AWS Tools para Windows PowerShell)

Para mais informações sobre erros comuns do log do sistema, consulte [Resolução de problemas dos erros no log do sistema para instâncias baseadas em Linux \(p. 1040\)](#).

Faça uma captura de tela da instância inatingível

Se você não conseguir alcançar sua instância via SSH ou RDP, pode fazer uma captura de tela da sua instância e vê-la como imagem. Isso dá visibilidade quanto ao status da instância e permite uma solução de problemas mais rápida.

Não há custo de transferência de dados custos para essa captura de tela. A imagem é gerada em formato JPG, não maior que 100 KB.

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. Selecione Ações, Configurações da instância.
5. Selecione Obter captura de tela da instância.

Clique com o botão direito sobre a imagem para baixá-la 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 [Acessando 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 parada de 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 [Interrompa e inicie sua instância \(p. 458\)](#).

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 [Criação de uma AMI em Linux com armazenamento de instâncias \(p. 115\)](#).

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 /.

Histórico do documento

A tabela a seguir descreve adições importantes na documentação do Amazon EC2. Também atualizamos a documentação com frequência para abordar os comentários enviados por você.

Current API version: 2016-11-15 (Versão da API atual: 2016-11-15)

Recurso	Versão da API	Descrição	Data de lançamento
Placement groups de partição	15/11/2016	Os placement groups de partição distribuem instâncias entre partições lógicas, garantindo que instâncias em uma partição não compartilhem hardware subjacente com instâncias em outras partições. Para obter mais informações, consulte Placement groups de partição (p. 794) .	20 de dezembro de 2018
Instâncias p3dn.24xlarge	15/11/2016	As novas instâncias p3dn.xlarge 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 Hibernar sua instância (p. 461) .	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 Amazon Elastic Inference (p. 534) .	28 de novembro de 2018
Instâncias com 100 Gbps de largura de banda de rede	15/11/2016	As novas instâncias C5n podem utilizar até 100 Gbps de largura de banda de rede.	26 de novembro de 2018
Instâncias com processadores baseados em Arm	15/11/2016	As novas instâncias A1 fornecem economias de custo significativas e são ideais para cargas de trabalho 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 seu aplicativo. Para obter mais informações, consulte Criação da solicitação de Frota spot (p. 320) .	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	14 de novembro de 2018

Recurso	Versão da API	Descrição	Data de lançamento
		instâncias executadas na resposta da API e não toma nenhuma ação adicional permitindo que você controle se e quando as instâncias são executadas. Para obter mais informações, consulte Tipos de solicitação de Frota do EC2 (p. 415) .	
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, aplicativos de negócios e muito mais.	6 de novembro de 2018
Informações sobre economias do Spot	15/11/2016	É possível visualizar a economia feita com o uso de Instâncias spot para uma única Frota spot ou para todas as Instâncias spot. Para obter mais informações, consulte Economia na compra das Instâncias spot (p. 305) .	5 de novembro de 2018
Suporte do console para otimização de opções de CPU	15/11/2016	Ao executar uma instância, você pode otimizar as opções de CPU para atender a cargas de trabalho ou necessidades de negócios específicas usando o console do Amazon EC2. Para obter mais informações, consulte Otimizar opções de CPU (p. 495) .	31 de outubro de 2018
Suporte do console para criação de um modelo de execução usando uma instância	15/11/2016	Você pode criar um modelo de execução usando uma instância como a base para um novo modelo de execução usando o console do Amazon EC2. Para obter mais informações, consulte Criação de um modelo de execução (p. 399) .	30 de outubro de 2018
Reservas de capacidade sob demanda	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 Reservas de capacidade sob demanda (p. 376) .	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 trazer o intervalo de endereços para a AWS, ele aparece em sua conta como um grupo de endereços. Você pode criar um endereço IP elástico de seu grupo de endereços e usá-lo com seus recursos da AWS. Para obter mais informações, consulte Traga seus próprios endereços IP (BYOIP) (p. 738) .	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

Recurso	Versão da API	Descrição	Data de lançamento
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 Atribuição de Hosts dedicados (p. 360) .	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 desempenho bare metal com acesso direto ao hardware do host. Para obter mais informações, consulte Instâncias otimizadas para memória (p. 223) .	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 adicional para ações de escalabilidade programadas para o Frota spot	15/11/2016	Aumentar ou diminuir a capacidade atual da frota com base em data e hora. Para obter mais informações, consulte Escalar o Frota spot usando a escalabilidade programada (p. 341) .	20 de setembro de 2018
Instâncias T3	15/11/2016	As instâncias T3 são o tipo de instância de uso geral com capacidade de intermitência de última geração que fornecem a um nível de linha de base de desempenho de CPU a capacidade de intermitência para uso de CPU a qualquer momento, pelo tempo que for necessário. Para obter mais informações, consulte Instâncias de desempenho com capacidade de intermitência (p. 189) .	21 de agosto de 2018
Estratégias de alocação para Frotas do EC2	15/11/2016	Você pode especificar se a capacidade sob demanda é atendida pelo preço (preço mais baixo primeiro) ou prioridade (prioridade mais alta primeiro). Você pode especificar o número de grupos spot para os quais alocar sua capacidade spot de destino. Para obter mais informações, consulte Estratégias de alocação para Instâncias spot (p. 416) .	26 de julho de 2018
Estratégias de alocação para Frotas spot	15/11/2016	Você pode especificar se a capacidade sob demanda é atendida pelo preço (preço mais baixo primeiro) ou prioridade (prioridade mais alta primeiro). Você pode especificar o número de grupos spot para os quais alocar sua capacidade spot de destino. Para obter mais informações, consulte Estratégia de alocação para Instâncias spot (p. 299) .	26 de julho de 2018

Recurso	Versão da API	Descrição	Data de lançamento
Instâncias R5 e R5d	15/11/2016	As instâncias R5 e R5d são ideais para bancos de dados de alto desempenho, caches na memória distribuídos e análises na memória. As instâncias R5d vêm com volumes de armazenamento de instâncias do NVMe. Para obter mais informações, consulte Instâncias otimizadas para memória (p. 223) .	25 de julho de 2018
Instâncias z1d	15/11/2016	Essas instâncias são projetadas para aplicativos que exigem alto desempenho por núcleo com uma grande quantidade de memória, como a automação de design eletrônico (EDA) e bancos de dados relacionais. Essas instâncias vêm com volumes de armazenamento de instâncias do NVMe. Para obter mais informações, consulte Instâncias otimizadas para memória (p. 223) .	25 de julho de 2018
Automação do ciclo de vida do snapshot	15/11/2016	Você pode usar o Gerenciador de ciclo de vida de dados da Amazon para automatizar a criação e a exclusão de snapshots para seus volumes do EBS. Para obter mais informações, consulte Automação do ciclo de vida de snapshot do Amazon EBS (p. 907) .	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 cargas de trabalho ou necessidades de negócios específicos. Para obter mais informações, consulte Criação de um modelo de execução (p. 399) .	11 de julho de 2018
Marcação de Hosts dedicados	15/11/2016	Você pode marcar seus Hosts dedicados. Para obter mais informações, consulte Marcação de Host dedicados (p. 365) .	3 de julho de 2018
Instâncias i3.metal	15/11/2016	As instâncias i3.metal fornecem aos aplicativos acesso direto aos recursos físicos do servidor host, como os processadores e a memória. Para obter mais informações, consulte Instâncias otimizadas para armazenamento (p. 231) .	17 de maio de 2018
Obter a saída mais recente do console	15/11/2016	Você pode recuperar a saída mais recente do console para alguns tipos de instância usando o comando get-console-output da AWS CLI.	9 de maio de 2018
Otimizar as opções de CPU	15/11/2016	Ao executar uma instância, você pode otimizar as opções de CPU para atender a cargas de trabalho ou necessidades de negócios específicas: Para obter mais informações, consulte Otimizar opções de CPU (p. 495) .	8 de maio de 2018

Recurso	Versão da API	Descrição	Data de lançamento
Frota do EC2	15/11/2016	Você pode usar a Frota do EC2 para executar um grupo de instâncias 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. Para obter mais informações, consulte Executar uma frota de EC2 (p. 412) .	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 Como Frota spot funciona (p. 298) .	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 Criação de um snapshot do Amazon EBS (p. 898) .	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 Como alterar o placement group de uma instância (p. 799) .	1 de março de 2018
IDs mais longos de recursos	15/11/2016	Você pode habilitar o formato de ID mais longo para outros tipos de recursos. Para obter mais informações, consulte IDs de recursos (p. 993) .	9 de fevereiro de 2018
Melhorias no desempenho da rede	15/11/2016	As instâncias de fora de um placement group de cluster podem agora se beneficiar de uma maior largura de banda para enviar ou receber tráfego de rede entre as outras instâncias ou o Amazon S3. Para obter mais informações, consulte Recursos de redes e armazenamento (p. 180) .	24 de janeiro de 2018
Marcar endereços IP elásticos	15/11/2016	Você pode marcar seus endereços IP elásticos. Para obter mais informações, consulte Marcar um endereço IP elástico (p. 744) .	21 de dezembro de 2017
Amazon Linux 2	15/11/2016	O Amazon Linux 2 é uma nova versão do Amazon Linux. Ele proporciona uma base de alto desempenho, estável e segura para seus aplicativos. Para obter mais informações, consulte Amazon Linux (p. 158) .	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 Definição da hora de sua instância do Linux (p. 491) .	29 de novembro de 2017
T2 ilimitada	15/11/2016	As instâncias T2 ilimitadas podem apresentar uma intermitência acima da linha de base pelo tempo que for necessário. Para obter mais informações, consulte Instâncias de desempenho com capacidade de intermitência (p. 189) .	29 de novembro de 2017

Recurso	Versão da API	Descrição	Data de lançamento
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 Execução de uma instância a partir de um modelo de execução (p. 398) .	29 de novembro de 2017
Posicionamento disseminado	15/11/2016	Os placement groups de distribuição são recomendados para aplicativos com uma pequena quantidade de instâncias críticas que devem ser mantidas separadasumas das outras. Para obter mais informações, consulte Placement groups de distribuição (p. 795) .	29 de novembro de 2017
Instâncias H1	15/11/2016	As instâncias H1 são projetadas para cargas de trabalho de big data de alto desempenho. Para obter mais informações, consulte Instâncias otimizadas para armazenamento (p. 231) .	28 de novembro de 2017
Instâncias M5	15/11/2016	As instâncias M5 são a última geração de instâncias de computação para uso 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 Como colocar em hibernação Instâncias spot interrompidas (p. 350) .	28 de novembro de 2017
Rastreamento do destino da frota spot	15/11/2016	Você pode configurar políticas de escalabilidade de rastreamento de destino para a frota spot. Para obter mais informações, consulte Dimensionamento da Frota spot usando as políticas de rastreamento de destino (p. 338) .	17 de novembro de 2017
A frota spot é integrada ao Elastic Load Balancing	15/11/2016	Você pode anexar um ou mais load balancers a uma frota spot.	10 de novembro de 2017
Instâncias X1e	15/11/2016	As instâncias X1e são ideais para bancos de dados de alto desempenho, bancos de dados de memória e outros aplicativos empresariais que consomem muita memória. Para obter mais informações, consulte Instâncias otimizadas para memória (p. 223) .	28 de novembro de 2017
Instâncias C5	15/11/2016	As instâncias C5 são desenvolvidas para aplicativos de computação pesada. Para obter mais informações, consulte Instâncias otimizadas para computação (p. 219) .	6 de novembro de 2017

Recurso	Versão da API	Descrição	Data de lançamento
Mesclagem e divisão do Instâncias reservadas conversíveis	15/11/2016	Você pode trocar (mesclar) dois ou mais Instâncias reservadas conversíveis por um novo Instância reservada convertível. Você também pode usar o processo de modificação para dividir um Instância reservada convertível em reservas menores. Para obter mais informações, consulte Trocar Instâncias reservadas conversíveis (p. 285) .	6 de novembro de 2017
Instâncias P3	15/11/2016	As instâncias P3 são a última geração de instâncias GPU otimizadas para computação. Para obter mais informações, consulte Linux Instâncias de computação acelerada (p. 237) .	25 de outubro de 2017
Modificar a locação da VPC	15/11/2016	Você pode alterar o atributo de locação da instância da VPC de <code>dedicated</code> para <code>default</code> . Para obter mais informações, consulte Alterar a locação de uma VPC (p. 376) .	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 Comportamento da interrupção (p. 349) .	18 de setembro de 2017
Marcar gateways NAT	15/11/2016	Você pode marcar o gateway NAT. Para obter mais informações, consulte Marcação dos seus recursos (p. 1004) .	7 de setembro de 2017
Descrições de regras do security group	15/11/2016	Você pode adicionar descrições às regras do security group. Para obter mais informações, consulte Regras de security groups (p. 627) .	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 Recuperar um endereço IP elástico (p. 746) .	11 de agosto de 2017
Marcar instâncias de frota Spot	15/11/2016	Você pode configurar sua frota Spot para marcar automaticamente as instâncias que ela executa.	24 de julho de 2017
Instâncias G3	15/11/2016	As instâncias G3 fornecem uma plataforma de alto desempenho, econômica, para aplicativos gráficos 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 Linux Instâncias de computação acelerada (p. 237) .	13 de julho de 2017

Recurso	Versão da API	Descrição	Data de lançamento
Atualização do tutorial do SSL/TLS	15/11/2016	Configure o suporte ao SSL/TLS no servidor web do EC2 usando o Let's Encrypt. Para obter mais informações, consulte Tutorial: Configurar o servidor web Apache no Amazon Linux 2 para usar SSL/TLS (p. 65) .	25 de abril de 2017
Instâncias F1	15/11/2016	As instâncias F1 representam a próxima geração de instâncias de computação acelerada. Para obter mais informações, consulte Linux Instâncias de computação acelerada (p. 237) .	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 Marcação dos seus recursos (p. 1004) . 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, Permissões em nível de recursos para marcação (p. 678) .	28 de março de 2017
Instâncias I3	15/11/2016	As instâncias I3 representam a próxima geração de instâncias otimizadas para armazenamento. Para obter mais informações, consulte Instâncias otimizadas para armazenamento (p. 231) .	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 Como modificar o tamanho, o desempenho ou o tipo de um volume do EBS (p. 882) .	13 de fevereiro de 2017
Anexar uma função da IAM	15/11/2016	Você pode anexar, desanexar ou substituir uma função da IAM para uma instância existente. Para obter mais informações, consulte Funções do IAM para Amazon EC2 (p. 712) .	9 de fevereiro de 2017
Instâncias spot dedicadas	15/11/2016	Você pode executar instâncias spot em hardware de único locatário em uma nuvem privada virtual (VPC). Para obter mais informações, consulte Como especificar a locação para suas Instâncias spot (p. 308) .	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 Endereçamento IP de instâncias do Amazon EC2 (p. 723) .	1º de dezembro de 2016

Recurso	Versão da API	Descrição	Data de lançamento
Instâncias R4	15/09/2016	As instâncias R4 representam a próxima geração de instâncias otimizadas para memória. As instâncias R4 são ideais para cargas de trabalho com uso intensivo de memória e sensíveis à latência, como business intelligence (BI), mineração de dados e análise, bancos de dados em memória, cache de memória de escala web distribuída e processamento em tempo real do desempenho de aplicativos de big data não estruturado. Para obter mais informações, consulte Instâncias otimizadas para memória (p. 223)	30 de novembro de 2016
Novos tipos de instância t2.xlarge e t2.2xlarge	15/09/2016	As instâncias T2 são projetadas para fornecer desempenho base moderado e capacidade de intermitência para obter desempenho significativamente mais alto conforme necessário para sua carga de trabalho. São destinadas para aplicativos que precisam de capacidade de resposta, alto desempenho por períodos de tempo limitados e de baixo custo. Para obter mais informações, consulte Instâncias de desempenho com capacidade de intermitência (p. 189) .	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 Linux Instâncias de computação acelerada (p. 237) .	29 de setembro de 2016
Instâncias m4.16xlarge	01/04/2016	Expande o intervalo da família M4 de finalidade geral com a introdução de instâncias m4.16xlarge, com 64 vCPUs e 256 GiB de RAM.	6 de setembro de 2016
Escalabilidade automática para frota spot		Agora você pode configurar políticas de escalabilidade para a frota de spot. Para obter mais informações, consulte Escalabilidade automática da Frota spot (p. 337) .	1 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 Tipos de rede avançada (p. 768) .	28 de junho de 2016
Suporte avançado para visualização e modificação de IDs mais longos	01/04/2016	Agora você pode visualizar e modificar as configurações de IDs mais longos para outros usuários do IAM funções do IAM ou usuários root. Para obter mais informações, consulte IDs de recursos (p. 993) .	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 Cópia de um snapshot do Amazon EBS (p. 902) .	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 Faça uma captura de tela da instância inatingível (p. 1063) .	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 aplicativos de computação de alta performance (HPC). Para obter mais informações, consulte Instâncias otimizadas para memória (p. 223) .	18 de maio de 2016
Dois novos tipos de volume do EBS	01/10/2015	Agora você pode criar HDD otimizado para throughput (st1) e volumes de disco rígido frio (sc1). Para obter mais informações, consulte Tipos de volume do Amazon EBS (p. 844) .	19 de abril de 2016
Inclusão de novas métricas NetworkPacketsIn e NetworkPacketsOut para o Amazon EC2		Inclusão de novas métricas NetworkPacketsIn e NetworkPacketsOut para o Amazon EC2. Para obter mais informações, consulte Métricas de instância (p. 577) .	23 de março de 2016
Métricas do CloudWatch para frota spot		Agora você pode obter as métricas do CloudWatch para sua frota spot. Para obter mais informações, consulte Métricas do CloudWatch para Frota spot (p. 334) .	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 Instâncias reservadas programadas (p. 289) .	13 de janeiro de 2016
IDs mais longos de recursos	01/10/2015	Gradualmente, estamos introduzindo IDs de comprimento mais longo para alguns tipos de recursos do Amazon EC2 e do Amazon EBS. Durante o período de aceitação, você pode habilitar o formato mais longo de ID para tipos de recursos compatíveis. Para obter mais informações, consulte IDs de recursos (p. 993) .	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 Habilitação do suporte a DNS do ClassicLink (p. 819) .	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 desempenho base moderado e capacidade de intermitência para obter desempenho significativamente mais alto conforme necessário para sua carga de trabalho. São destinadas para aplicativos que precisam de capacidade de resposta, alto desempenho por períodos de tempo limitados e de baixo custo. Para obter mais informações, consulte Instâncias de desempenho com capacidade de intermitência (p. 189) .	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 Hosts dedicados (p. 356) .	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 Como especificar a duração para suas Instâncias spot (p. 307) .	6 de outubro de 2015
Solicitação de modificação de frota spot	01/10/2015	Agora você pode modificar a capacidade de destino de sua solicitação de frota spot. Para obter mais informações, consulte Modificação da solicitação de Frota spot (p. 324) .	29 de setembro de 2015
Estratégia diversificada de alocação de frota spot	15/04/2015	Agora você pode alocar instâncias spot em vários grupos spot usando uma única solicitação de frota spot. Para obter mais informações, consulte Estratégia de alocação para Instâncias spot (p. 299) .	15 de setembro de 2015
Importância da instância de frota spot	15/04/2015	Agora você pode definir as unidades de capacidade com que cada tipo de instância contribui para o desempenho de seu aplicativo, e ajustar a sugestão de preço para cada grupo spot de forma correspondente. Para obter mais informações, consulte Peso da instância da Frota spot (p. 300) .	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 Crie alarmes para parar, encerrar, reiniciar ou recuperar uma instância (p. 595) .	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 desempenho base moderado e capacidade de intermitência para obter desempenho significativamente mais alto conforme necessário para sua carga de trabalho. São destinadas para aplicativos que precisam de capacidade de resposta, alto desempenho por períodos de tempo limitados e de baixo custo. Para obter mais informações, consulte Instâncias de desempenho com capacidade de intermitência (p. 189) .	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
Frotas spot	15/04/2015	Você pode gerenciar uma coleção ou uma frota de instâncias spot em vez de gerenciar solicitações separadas de instâncias spot. Para obter mais informações, consulte Como Frotas spot funcionam (p. 298) .	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 Como migrar um endereço IP elástico do EC2-Classic (p. 810) .	15 de maio de 2015
Importar VMs com vários discos como AMIs	01/03/2015	O processo de VM Import agora oferece suporte à importação de VMs com vários discos como AMIs. Para obter mais informações, consulte Como importar uma VM como uma imagem usando o VM Import/Export no Guia do usuário de VM Import/Export.	23 de abril de 2015
Novo tipo de instância <code>g2.8xlarge</code>		A nova instância <code>g2.8xlarge</code> tem suporte de quatro GPUs NVIDIA de alto desempenho, tornando-a ideal para cargas de trabalho de computação de GPU incluindo renderização em grande escala, transcodificação, Machine Learning e outras cargas de trabalho 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>A próxima geração de instâncias do Amazon EC2 com armazenamento denso que são otimizadas para aplicativos 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/desempenho na família de armazenamento denso. Habilitadas por processadores de 2,4 GHz Intel® Xeon® E5 2676v3 (Haswell), as instâncias D2 melhoram as instâncias HS1 fornecendo poder computacional adicional, mais memória e redes avançadas. Além disso, as instâncias D2 estão disponíveis em quatro tamanhos de instância com opções de armazenamento de 6, 12, 24 e 48 TB.</p> <p>Para obter mais informações, consulte Instâncias otimizadas para armazenamento (p. 231).</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 Recuperar sua instância (p. 476).</p>	12 de janeiro de 2015
Instâncias C4		<p>A próxima geração de instâncias otimizadas para computação que fornecem desempenho muito alto 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 o mais alto desempenho de processador entre as instâncias do EC2. Idealmente, essas instâncias são ideais para aplicativos web de alto tráfego, veiculação de anúncios, processamento em lote, codificação de vídeo, análises distribuídas, física de alta energia, análise de genoma e dinâmica de fluidos computacional.</p> <p>Para obter mais informações, consulte Instâncias otimizadas para computação (p. 219).</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 ClassicLink (p. 812) .	7 de janeiro de 2015
Avisos de encerramento de instâncias spot		<p>A melhor maneira de proteger-se contra a interrupção de instâncias spot é configurar o aplicativo para ser tolerante a falhas. Além disso, você pode tirar proveito dos avisos de encerramento de instâncias spot, que fornecem um aviso de dois minutos antes de o Amazon EC2 encerrar a instância spot</p> <p>Para obter mais informações, consulte Avisos de interrupção de Instância spots (p. 352).</p>	5 de janeiro de 2015
Suporte à paginação de <code>DescribeVolumes</code>	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 DescribeVolumes no Amazon EC2 API Reference.	23 de outubro de 2014
Instâncias T2	15/06/2014	As instâncias T2 são projetadas para fornecer desempenho base moderado e capacidade de intermitência para obter desempenho significativamente mais alto conforme necessário para sua carga de trabalho. São destinadas para aplicativos que precisam de capacidade de resposta, alto desempenho por períodos de tempo limitados e de baixo custo. Para obter mais informações, consulte Instâncias de desempenho com capacidade de intermitência (p. 189) .	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
Amazon EBSVolumes do Finalidade geral (SSD)	01/05/2014	Os volumes Finalidade geral (SSD) oferecem armazenamento econômico ideal para uma ampla variedade de cargas de trabalho. Esses volumes proporcionam latências de milissegundos de um dígito, capacidade de intermitência de 3.000 IOPS por períodos estendidos e um desempenho basal de 3 IOPS/GiB. Os volumes do Finalidade geral (SSD) podem variar de 1 GiB a 1 TiB. Para obter mais informações, consulte Volumes do Finalidade geral (SSD) (gp2) (p. 847) .	16 de junho de 2014

Recurso	Versão da API	Descrição	Data de lançamento
Criptografia de Amazon EBS	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 não utilizados no momento, criptografando seus dados usando chaves gerenciadas pela Amazon. 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 Amazon EBS Encryption (p. 926) .	21 de maio de 2014
Instâncias R3	01/02/2014	<p>Instâncias otimizadas para memória de próxima geração com a melhor faixa de preços por GiB de RAM e de alto desempenho. Idealmente, essas instâncias são ideais para bancos de dados relacionais e NoSQL, soluções de análise na memória, computação científica e outros aplicativos com consumo intensivo de memória que podem se beneficiar de mais memória vCPU, alto desempenho de computação e dos recursos de rede avançada das instâncias R3.</p> <p>Para obter mais informações sobre as especificações de hardware para cada tipo de instância do Amazon EC2, veja Tipos de instâncias do Amazon EC2.</p>	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 Relatórios de uso do Amazon EC2 (p. 1015) .	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 para cada tipo de instância do Amazon EC2, veja Tipos de instâncias 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 desempenho 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 desempenho de pacotes por segundo (PPS) significativamente mais alta. Para obter mais informações, consulte Instâncias otimizadas para armazenamento (p. 231) .	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 Guia do usuário de VM Import/Export .	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 Como controlar o acesso aos recursos do Amazon EC2 (p. 641) .	20 de novembro de 2013
Instâncias C3	15/10/2013	Instâncias otimizadas para computação que fornecem desempenho muito alto 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 desempenho 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 para cada tipo de instância do Amazon EC2, veja Tipos de instâncias 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 assistente de execução do Amazon EC2. Para obter mais informações, consulte Executar uma instância do AWS Marketplace (p. 410) .	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, streaming de aplicativos com consumo intensivo de gráficos e outras cargas de trabalho do servidor que exigem potência de processamento paralelo massivo. Para obter mais informações, consulte Linux Instâncias de computação acelerada (p. 237) .	4 de novembro de 2013
Novo assistente de execução		Há um novo assistente de execução reprojetado do EC2. Para obter mais informações, consulte Execução de uma instância usando o assistente de execução de instância (p. 391) .	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 Modificar Instâncias reservadas (p. 278) .	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 Modificar Instâncias reservadas (p. 278) .	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 Como atribuir um endereço IPv4 público durante a execução da instância (p. 728) .	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 IAM Políticas do Amazon EC2 (p. 643) .	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 Cópia de um snapshot do Amazon EBS (p. 902) .	11 de junho de 2013
Nova página Tags		Há uma nova página Tags no console do Amazon EC2. Para obter mais informações, consulte Marcação dos seus recursos do Amazon EC2 (p. 1003) .	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 Amazon EBS – instâncias otimizadas (p. 916).</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 Cópia de uma AMI (p. 150).</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 a alto desempenho da CPU e da rede. Essas instâncias são ideais para análise na memória, análise de gráficos e aplicativos 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 alto desempenho 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 Cópia de um snapshot do Amazon EBS (p. 902).</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 Provisioned IOPS SSD. Para obter mais informações, consulte Como monitorar volumes com o CloudWatch (p. 868). Novas verificações de status também adicionadas para volumes do Provisioned IOPS SSD. Para obter mais informações, consulte Como monitorar volumes com verificações de status (p. 873).</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 para cada tipo de instância do Amazon EC2, veja Tipos de instâncias do Amazon EC2 .	31 de outubro de 2012
Status da solicitação da instância Spot	01/10/2012	O status da solicitação da instância spot facilita determinar o estado de suas solicitações de 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
Loja de instâncias reservadas do Amazon EC2	15/08/2012	O Marketplace de instâncias reservadas corresponde 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 alto desempenho previsível para cargas de trabalho com uso intensivo de E/S, como aplicativos de banco de dados que dependem de tempos de resposta consistentes e rápidos. Para obter mais informações, consulte Tipos de volume do Amazon EBS (p. 844) .	31 de julho de 2012
Instâncias de E/S alta para o Amazon EC2	15/06/2012	As instâncias de E/S alta fornecem desempenho muito alto 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"> • Chaves de acesso da AWS para aplicativos que executam em instâncias do Amazon EC2. • Rotação automática das chaves de acesso da AWS na instância do Amazon EC2. • Permissões granulares para aplicativos que executam em instâncias do Amazon EC2 que fazem solicitações para seus serviços da AWS. 	

Recurso	Versão da API	Descrição	Data de lançamento
Os recursos de instâncias spot que facilitam a familiarização e o manuseio de potenciais interrupções.		<p>Agora você pode gerenciar suas Instâncias spot da seguinte forma:</p> <ul style="list-style-type: none"> • Fazer sugestões de preço para instâncias spot usando configurações de execução de Auto Scaling, e configurar uma programação para fazer sugestões de preço para instâncias spot. Para obter mais informações, consulte Como executar instâncias spot em seu grupo do Auto Scaling no Guia do usuário do Amazon EC2 Auto Scaling. • Obter notificações quando as instâncias forem executadas ou encerradas. • Usar modelos do AWS CloudFormation para executar instâncias spot em uma pilha com recursos da AWS. 	7 de junho de 2012
Exportação de instâncias do EC2 e time stamps para verificações de status para o Amazon EC2	01/05/2012	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
AMIs do AWS Marketplace	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 Interfaces de rede elástica (p. 747) .	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 Monitoramento do status de suas instâncias (p. 565) .	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	Adicionadas 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). Executando instâncias spot em uma VPC, os usuários de instâncias spot podem usufruir dos 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 Guia do usuário de VM Import/Export .	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 Como habilitar seus próprios kernels do Linux (p. 169) .	20 de junho de 2011
Alterações na definição de preço de zonas de disponibilidade de instâncias spot	15/05/2011	Adicionadas 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 quando você consulta as solicitações de instâncias 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 Como controlar o acesso aos recursos do Amazon EC2 (p. 641) .	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 Como habilitar seus próprios kernels do Linux (p. 169) .	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. 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 Instâncias dedicadas (p. 371) .	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 Instâncias reservadas (p. 253) .	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. Para obter mais informações, consulte AMIs para instâncias de computação acelerada baseadas em GPU (p. 242) .	15 de março de 2011
Informações de metadados	01/01/2011	Adicionadas informações sobre os metadados para refletir as alterações na versão 2011-01-01. Para obter mais informações, consulte Metadados da instância e dados do usuário (p. 516) e Categorias de metadados da instância (p. 523) .	11 de março de 2011

Recurso	Versão da API	Descrição	Data de lançamento
Amazon EC2 VM Import Connector para VMware vCenter		Adicionadas informações sobre o Amazon EC2 VM Import Connector para o dispositivo virtual VMware vCenter (conector). O conector é um plug-in para VMware vCenter que está integrado a VMware vSphere Client e fornece uma interface gráfica de usuário que pode ser usada para importar as máquinas virtuais do VMware para o Amazon EC2.	3 de março de 2011
Forçar desanexação de volume		Agora você pode usar o Console de Gerenciamento da AWS para forçar a desanexação de um volume do Amazon EBS de uma instância. Para obter mais informações, consulte Separação de um volume do Amazon EBS de uma instância (p. 893) .	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 Habilitação da proteção contra o encerramento de uma instância (p. 472) .	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 Guia do usuário de VM Import/Export .	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 Listagem e filtragem dos seus recursos (p. 999) e Marcação dos seus recursos do Amazon EC2 (p. 1003) .	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 Como garantir idempotência 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 aplicativos. Para obter mais informações, consulte Instâncias de desempenho com capacidade de intermitência (p. 189) .	8 de setembro de 2010

Recurso	Versão da API	Descrição	Data de lançamento
AWS Identity and Access Management para o Amazon EC2		O Amazon EC2 agora se integra com o AWS Identity and Access Management (IAM). Para obter mais informações, consulte Como controlar o acesso aos recursos do Amazon EC2 (p. 641) .	2 de setembro de 2010
Instâncias em cluster	15/06/2010	O Amazon EC2 oferece instâncias de computação em cluster para aplicativos de computação de alta performance (HPC). Para obter mais informações sobre as especificações de hardware para cada tipo de instância do Amazon EC2, veja Tipos de instâncias 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 do Amazon CloudWatch para volumes do Amazon EBS		O monitoramento do Amazon CloudWatch agora está disponível automaticamente para volumes do Amazon EBS. Para obter mais informações, consulte Como monitorar volumes com o CloudWatch (p. 868) .	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 para cada tipo de instância do Amazon EC2, veja Tipos de instâncias do Amazon EC2 .	22 de fevereiro de 2010

AWS Glossary

For the latest AWS terminology, see the [AWS Glossary](#) in the AWS General Reference.