aws

Guia do usuário

Amazon Elastic Compute Cloud

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon Elastic Compute Cloud: Guia do usuário

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

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

Table of Contents

O que é o Amazon EC2? ... 1
Atributos ... 1
Serviços relacionados ... 2
Acesso ao EC2 ... 4
Preços ... 5
Estimativas, faturamento e otimização de custos ... 6
Recursos ... 7
Tutorial de conceitos básicos ... 8
Etapa 1: executar uma instância ... 10
Etapa 2: conectar-se à instância ... 12
Etapa 3: limpar a instância ... 15
Próximas etapas ... 16
Práticas recomendadas ... 18
Imagens de máquina da Amazon ... 21
Características da AMI ... 23
Permissões de execução ... 23
Tipo do volume de raiz ... 24
Identificação do tipo de volume raiz da AMI ... 25
Tipos de virtualização ... 27
Encontrar uma AMI ... 29
Parâmetros do Systems Manager ... 32
Parâmetros públicos do Systems Manager ... 36
AMIs pagas no AWS Marketplace ... 39
Vender sua AMI no AWS Marketplace ... 40
Localizar uma AMI paga ... 40
Comprar uma AMI paga ... 42
Recuperar o código do produto ... 43
Usar suporte pago ... 44
Faturas para AMI pagas e compatíveis ... 45
Gerenciar suas assinaturas do ... 45
Ciclo de vida da AMI ... 47
Criar uma AMI ... 48
Criação de uma AMI baseada no Amazon S3 ... 58
Criar uma AMI usando o Sysprep do Windows ... 99

Copiar um AMI ... 116
Armazenar e restaurar uma AMI ... 135
Ancestralidade da AMI ... 145
Uso de AMIs ... 151
Defasar uma AMI ... 176
Desabilitar uma AMI ... 182
Cancelar o registro de uma AMI ... 188
Modos de inicialização ... 195
Requisitos para o modo de inicialização da UEFI ... 196
Parâmetro do modo de inicialização da AMI ... 198
Modo de inicialização do tipo de instância ... 200
Modo de inicialização da instância ... 203
Modo de inicialização do sistema operacional ... 205
Definir modo de inicialização da AMI ... 207
Variáveis UEFI ... 214
UEFI Secure Boot ... 214
Criptografia da AMI ... 232
Cenários de execução de instância ... 232
Cenários de cópia de imagem ... 236
AMIs compartilhadas ... 239
Provedor verificado ... 239
Encontrar AMIs compartilhadas ... 240
Preparar-se para usar AMIs compartilhadas para Linux ... 243
AMIs permitidas ... 244
Tornar sua AMI pública ... 265
Bloquear o acesso público para AMIs ... 269
Compartilhar uma AMI com organizações e unidades organizacionais ... 279
Compartilhar uma AMI com contas específicas da AWS ... 292
Cancelar o compartilhamento de uma AMI com sua conta ... 295
Recomendações para criar AMIs compartilhadas no Linux ... 297
Monitorar eventos da AMI ... 303
Detalhes do evento ... 304
availableEventos do ... 305
failedEventos do ... 306
deregisteredEventos do ... 306
disabledEventos do ... 307

Noções básicas sobre o faturamento da AMI 308
Campos de faturamento da AMI 308
Localizar informações de faturamento de AMI 311
Verificar cobranças da AMI em sua fatura 313
Cotas de AMI 313
Solicitar um aumento de cota para AMIs 315
Instâncias 316
Tipos de instância 317
Tipos de instâncias disponíveis 318
Especificações de hardware 319
Tipo de hipervisor 319
Tipos de virtualização de AMI 320
Processadores 320
Localizar um tipo de instância do 324
Localizador de tipo de instância do EC2 331
Recomendações do Compute Optimizer 333
Alterações no tipo de instância 337
Instâncias expansíveis 346
Instâncias de GPU 401
Instâncias Mac 416
Otimização de EBS 467
Opções de CPU 582
AMD SEV-SNP 833
Controle do estado do processador 841
Instâncias gerenciadas 845
Faturamento de instâncias gerenciadas 845
Identificar instâncias gerenciadas 846
Conceitos básicos das instâncias gerenciadas 848
Virtualização aninhada 848
Como funcionam 849
Considerações 849
Iniciar uma nova instância com a virtualização aninhada 849
Configurar uma instância existente para usar a virtualização aninhada 851
Opções de faturamento e compra 852
Instâncias sob demanda 853
Reserved Instances 856

Instâncias spot ... 927
Dedicated Hosts ... 1034
Dedicated Instances ... 1100
Capacity Reservations ... 1107
Modelos de execução ... 1259
Restrições ... 1260
Permissões ... 1261
Controlar a inicialização das instâncias ... 1268
Criar ... 1271
Modificar (gerenciar versões) ... 1287
Excluir ... 1292
Iniciar uma instância ... 1294
Tutoriais ... 1297
Referência de parâmetros de instâncias ... 1322
Usar o assistente de execução de instância ... 1337
Executar usando um modelo de execução ... 1341
Executar em uma instância existente ... 1348
Executar em uma AMI do AWS Marketplace ... 1350
Conecte-se à sua instância ... 1353
Pré-requisitos gerais de conexão ... 1355
Conectar-se à instância do Linux usando SSH ... 1360
Conectar-se à instância do Windows no usando RDP ... 1377
Conectar-se usando o Gerenciador de sessões ... 1387
Conecte-se usando um IP público e o EC2 Instance Connect ... 1388
Conecte-se usando um IP privado e uma instância do EC2 Conecte-se ao endpoint ... 1425
Alterações do estado de instâncias ... 1460
Faturamento por estado da instância ... 1461
Instâncias pendentes ... 1463
Instâncias interrompidas ... 1463
Instâncias hibernadas ... 1464
Instâncias de reinicialização ... 1465
Instâncias encerradas ... 1465
Diferenças entre os estados de instâncias ... 1466
Interromper e iniciar ... 1468
Hibernar ... 1489
Reinicializar ... 1520

Encerrar ... 1522
Retirada ... 1540
Recuperação automática de instâncias ... 1545
Conceitos principais da recuperação automática de instâncias ... 1547
Diferenças entre a recuperação automática simplificada e a recuperação baseada em ações do CloudWatch ... 1549
Crie um sistema resiliente ... 1550
Verificar se ocorreu a recuperação automática ... 1551
Recuperação automática simplificada ... 1553
Recuperação baseada em ações do CloudWatch ... 1558
Metadados da instância ... 1563
Categorias de metadados da instância ... 1564
Categorias de dados dinâmicos ... 1581
Acessar metadados de instância ... 1582
Configurar as opções de IMDS ... 1623
Executar comandos no lançamento ... 1652
Exemplo: valor de índice de execução da AMI ... 1680
Detectar se um host é uma instância do EC2 ... 1684
Inspecione o documento de identidade da instância ... 1685
Inspecione o UUID do sistema ... 1685
Inspecione o identificador de geração da máquina virtual do sistema ... 1687
Documentos de identidade da instância ... 1692
Recuperar o documento de identidade da instância ... 1694
Verificar documento de identidade da instância ... 1696
Certificados públicos ... 1707
Conformidade com STIG ... 1768
Configurações STIG ... 1769
Baixar scripts STIG ... 1789
Aplicar configurações STIG com o Systems Manager ... 1811
Sincronização do relógio ... 1814
Carimbo de data e hora de pacotes de hardware ... 1815
Segundos bissextos ... 1816
Usar o Serviço de Sincronização Temporal da Amazon local ... 1817
Usar o Serviço de Sincronização Temporal da Amazon público ... 1830
Comparação dos carimbos de data/hora das instâncias do Linux ... 1832
Alteração do fuso horário da instância ... 1834

EC2 Capacity Manager ... 1836
Recursos principais ... 1837
Habilitação do Capacity Manager ... 1837
Organização dos seus dados ... 1848
Navegando pelo Capacity Manager no console ... 1857
Exportação dos seus dados ... 1860
Gerenciamento de drivers de dispositivo ... 1863
Drivers de rede ... 1863
Drivers de gráficos ... 1864
Drivers de dispositivo de armazenamento ... 1864
Drivers AMD ... 1864
Drivers NVIDIA ... 1871
Instalar o driver do ENA no Windows ... 1917
Drivers PV do Windows ... 1938
AWSDrivers NVMe ... 1975
Configuração da instância do Windows ... 1987
Configurações de sistema específicas do Windows ... 1987
Drivers de dispositivos da AWS para instâncias do Windows ... 1988
Agentes de inicialização do Windows ... 1990
EC2 Fast Launch para Windows ... 2159
Alterar a senha de administrador do Windows ... 2184
Adicionar componentes do Sistema Windows ... 2185
Instalação do WSL no Windows ... 2190
Utilitários do Windows ... 2192
Atualizar instâncias do Windows ... 2194
Realizar uma atualização no local ... 2195
Realizar uma atualização automatizada ... 2200
Migrar para um tipo de instância baseada em Nitro ... 2212
Solucionar problemas de uma atualização ... 2221
Tutorial: conectar uma instância do EC2 a um banco de dados do RDS ... 2222
Objetivo do tutorial ... 2222
Contexto ... 2222
Arquitetura ... 2223
Considerações ... 2224
É hora de concluir o tutorial ... 2225
Custos ... 2225

Opção 1: conectar automaticamente usando o console do EC2 ... 2226
Opção 2: conectar automaticamente usando o console do RDS ... 2239
Opção 3: conectar manualmente ... 2251
Frotas ... 2263
Recursos e benefícios ... 2263
Que método de frota deve ser usado? ... 2264
Opções de configuração ... 2266
Tipos de solicitação ... 2267
Limite de gastos ... 2297
Seleção de tipo de instância baseada em atributos ... 2299
Ponderação de instâncias ... 2336
Estratégias de alocação ... 2339
Rebalanceamento de capacidade ... 2347
Reservas de capacidade ... 2353
Trabalhar com uma frota do EC2 ... 2354
Estados das solicitações da Frota do EC2 ... 2355
Pré-requisitos da Frota do EC2 ... 2356
Criar uma Frota do EC2. ... 2361
Marcar uma Frota do EC2 ... 2370
Descrever uma frota do EC2 ... 2373
Modificar uma Frota do EC2 ... 2377
Excluir uma Frota do EC2 ... 2379
Trabalhar com frotas spot ... 2384
Estados das solicitações de frota spot ... 2385
Permissões de frota spot ... 2386
Criar uma Frota spot ... 2397
Marcar uma frota spot ... 2407
Descrever uma frota spot ... 2416
Modificar uma solicitação de frota spot ... 2418
Cancelar (excluir) uma solicitação de frota spot ... 2420
Escalabilidade automática para frota spot ... 2423
Monitorar a frota ... 2434
Monitorar a frota usando o CloudWatch ... 2435
Monitorar a frota usando o EventBridge ... 2438
Tutoriais ... 2457
Tutorial: configurar o EC2 Fleet para usar ponderação de instâncias ... 2458

Tutorial: configurar o EC2 Fleet para usar instâncias sob demanda como a capacidade principal ... 2462
Tutorial: configurar o EC2 Fleet para executar instâncias sob demanda usando reservas de capacidade direcionadas ... 2464
Tutorial: configurar o EC2 Fleet para executar instâncias em blocos de capacidade ... 2471
Exemplo de configurações da CLI para frotas do EC2 ... 2473
Exemplo 1: Executar Instâncias spot como a opção de compra padrão ... 2474
Exemplo 2: Executar Instâncias on-demand como a opção de compra padrão ... 2475
Exemplo 3: Executar Instâncias on-demand como a capacidade principal ... 2475
Exemplo 4: Iniciar Instâncias sob demanda usando várias Reservas de Capacidade ... 2476
Exemplo 5: Iniciar Instâncias sob demanda usando Reservas de Capacidade quando a capacidade total de destino for maior que o número de Reservas de Capacidade não utilizadas ... 2480
Exemplo 6: Iniciar Instâncias sob demanda usando Reservas de Capacidade direcionadas ... 2483
Exemplo 7: Configurar o rebalanceamento de capacidade para executar a Instâncias spot de substituição ... 2487
Exemplo 8: iniciar instâncias spot em uma frota otimizada para capacidade ... 2489
Exemplo 9: iniciar instâncias spot em uma frota otimizada para capacidade com prioridades ... 2490
Exemplo 10: iniciar instâncias spot em uma frota otimizada para preço-capacidade ... 2491
Exemplo 11: configurar a seleção de tipo de instância baseada em atributos ... 2493
Exemplo de configurações da CLI para frotas spot ... 2494
Exemplo 1: zona de disponibilidade com o menor preço ... 2495
Exemplo 2: zona de disponibilidade com o menor preço em uma lista ... 2496
Exemplo 3: tipo de instância com o menor preço em uma lista ... 2498
Exemplo 4. Cancelar o preço da solicitação ... 2499
Exemplo 5: usar a estratégia de alocação diversificada ... 2501
Exemplo 6: usar ponderação de instâncias ... 2504
Exemplo 7: usar capacidade sob demanda ... 2506
Exemplo 8: configurar o rebalanceamento de capacidade ... 2507
Exemplo 9: usar uma frota otimizada para capacidade ... 2508
Exemplo 10: usar uma frota otimizada para capacidade com prioridades ... 2509
Exemplo 11: usar uma frota priceCapacityOptimized ... 2511
Exemplo 12: configurar a seleção de tipo de instância baseada em atributos ... 2512
Quotas da frota ... 2513

Solicitar um aumento de cota para a capacidade pretendida 2514
Redes 2516
A VPC abrange as zonas de disponibilidade e a zona Wavelength. 2517
Regiões 2518
Zonas de disponibilidade 2518
zonas locais 2520
Zonas do Wavelength 2521
AWS Outposts 2522
Endereçamento IP de instâncias 2525
Endereços IPv4 privados 2525
Endereços IPv4 públicos 2526
Otimização de endereço IPv4 público 2528
Endereços IPv6 2530
Vários endereços IP 2531
Hostnames de instância do EC2 2533
Endereços locais de link 2533
Endereços IPv4 2533
Endereços IPv6 2539
Endereços IP secundários 2545
Endereços IPv4 no Windows 2549
Nomes de host e domínios de instâncias do EC2 2557
Entendendo nomes de host e domínios de instâncias do EC2 2558
Tipos de nomes de host 2558
Traga seus próprios endereços IP 2574
Definições BYOIP 2575
Requisitos e cotas 2576
Disponibilidade regional 2577
Disponibilidade da zona local 2577
Pré-requisitos 2579
Integrar seu intervalo de endereços 2588
Usar o intervalo de endereços 2597
Endereços IP elásticos 2598
Definição de preço de endereços IP elásticos 2599
Noções básicas sobre endereços IP elásticos 2599
Cota de endereços IP elásticos 2601
Associar um endereço IP elástico 2601

Transferir endereço IP elástico ... 2607
Liberar um endereço IP elástico ... 2613
Usar DNS reverso para aplicações de e-mail ... 2614
Interfaces de rede ... 2618
Conceitos da interface de rede ... 2620
Placas de rede ... 2622
Endereços IP por interface de rede ... 2625
Criar uma interface de rede ... 2627
Anexos de interface de rede ... 2633
Gerenciar endereços IP ... 2637
Modificar atributos da interface de rede ... 2640
Várias interfaces de rede ... 2645
Interfaces de rede gerenciadas pelo solicitante ... 2648
Delegação de prefixo ... 2650
Excluir uma interface de rede ... 2660
Largura de banda de rede ... 2661
Largura de banda disponível da instância ... 2662
Ponderação de largura de banda ... 2665
Monitorar largura de banda da instância ... 2699
Redes avançadas ... 2700
Elastic Network Adapter (ENA) ... 2701
ENA Express ... 2772
Intel 82599 VF ... 2804
Melhor desempenho de rede ... 2817
Aprimorar a latência de rede no Linux ... 2828
Considerações sobre a performance do Nitro ... 2832
Otimizar a performance da rede no Windows ... 2841
Elastic Fabric Adapter ... 2843
Conceitos básicos de EFA ... 2844
Interfaces e bibliotecas compatíveis ... 2847
Tipos de instâncias compatíveis ... 2847
Sistemas operacionais compatíveis ... 2862
Limitações de EFA ... 2863
Preços do EFA ... 2864
Conceitos básicos do EFA e MPI ... 2864
Conceitos básicos do EFA e NCCL ... 2882

Maximize a largura de banda da rede ... 2906
Criar e anexar um EFA ... 2920
Desanexar e excluir um EFA ... 2925
Monitorar um EFA ... 2926
Verificar o instalador do EFA ... 2934
Notas da versão ... 2948
Topologia do EC2 ... 2973
Como funciona ... 2974
Pré-requisitos ... 2982
Exemplos ... 2984
Grupos de posicionamento ... 3000
Estratégias de posicionamento ... 3001
Criar um grupo de posicionamento. ... 3007
Alterar posicionamento de instâncias ... 3009
Excluir um grupo de posicionamento. ... 3011
Grupos de posicionamento compartilhados ... 3012
Grupos de posicionamento no AWS Outposts ... 3015
Conexão MTU ... 3016
Frames jumbo (9001 MTU) ... 3017
Path MTU Discovery ... 3018
Definir a MTU para as instâncias ... 3019
Solução de problemas ... 3025
Nuvens privadas virtuais ... 3025
Suas VPCs padrão ... 3026
VPCs não padrão ... 3027
Acesso à Internet ... 3028
Sub-redes compartilhadas ... 3028
Sub-redes somente IPv6 ... 3029
Redes secundárias ... 3029
O que são redes secundárias? ... 3030
Principais conceitos ... 3030
Arquitetura ... 3031
Considerações adicionais ... 3031
Introdução ... 3031
Gerenciar recursos de rede secundária ... 3034
Práticas recomendadas de projeto de rede ... 3035

Solução de problemas ... 3035
Cotas e limites ... 3036
Segurança ... 3038
Proteção de dados ... 3039
Segurança de dados do Amazon EBS ... 3040
Criptografia em repouso ... 3041
Criptografia em trânsito ... 3042
Segurança da infraestrutura ... 3044
Isolamento de rede ... 3044
Isolamento em hosts físicos ... 3045
Controlar o tráfego de rede ... 3045
Resiliência ... 3048
Validação de conformidade ... 3049
Identity and Access Management ... 3049
Políticas baseadas em identidade ... 3050
Exemplo de políticas para a API ... 3062
Políticas de exemplo para o console ... 3107
AWSPolíticas gerenciadas pela ... 3121
Funções do IAM ... 3129
Gerenciamento de atualizações ... 3141
Práticas recomendadas para instâncias do Windows ... 3142
Práticas recomendadas de segurança de alto nível ... 3142
Gerenciamento de atualizações ... 3143
Gerenciamento de configuração ... 3145
Gerenciamento de alterações ... 3147
Auditoria e responsabilidade para instâncias do Windows do Amazon EC2 ... 3147
Pares de chaves ... 3148
Criar um par de chaves ... 3150
Descrever seus pares de chaves ... 3157
Excluir o par de chaves ... 3162
Adicionar ou substituir uma chave pública na instância do Linux ... 3163
Verificar a impressão digital ... 3165
Grupos de segurança ... 3168
Visão geral ... 3169
Criar um grupo de segurança ... 3170
Alterar grupos de segurança da instância ... 3172

Exclua um grupo de segurança ... 3179
Acompanhamento da conexão ... 3180
Regras de grupo de segurança para diferentes casos de uso ... 3186
NitroTPM ... 3193
Requisitos ... 3194
Habilitar uma AMI do Linux para NitroTPM ... 3196
Certifique-se de que uma AMI esteja habilitada para o NitroTPM ... 3197
Habilitar ou interromper o uso do NitroTPM ... 3199
Verificar se uma instância está habilitada para o NitroTPM ... 3200
Recuperar a chave pública de endosso ... 3202
Atestação de instância do EC2 ... 3204
Integração com AWS KMS ... 3205
Atestação de ambientes de computação isolados ... 3206
Modelo de Responsabilidade Compartilhada da AWS ... 3206
AMIs atestáveis ... 3206
Preparar o AWS KMS para atestação ... 3216
Obter o atestado do NitroTPM ... 3217
Integração com o AWS KMS ... 3225
Isolar dados de seus próprios operadores ... 3226
Credential Guard para instâncias do Windows ... 3227
Pré-requisitos ... 3227
Inicialização de uma instância compatível ... 3228
Desabilitação da integridade da memória ... 3230
Ativação do Credential Guard ... 3230
Verificação se o Credential Guard está em execução ... 3232
AWS PrivateLink ... 3233
Criar um VPC endpoint de interface ... 3234
Criar uma política de endpoint ... 3234
Armazenamento ... 3236
Preço de armazenamento da AWS ... 3237
Amazon EBS ... 3238
Limites de volume do EBS ... 3239
Cartões EBS ... 3242
Armazenamento de instâncias do Amazon EC2 ... 3243
Persistência de dados ... 3245
Limites de volume de armazenamento de instância ... 3247

Volumes de armazenamento de instâncias SSD ... 3252
Adicionar volumes de armazenamento de instâncias ... 3256
Habilitar volume de troca para instâncias M1 e C1 ... 3265
Inicializar volumes de armazenamento de instância ... 3269
Estatísticas de performance detalhadas de volumes de armazenamento de instância ... 3270
Volumes raiz ... 3274
Instâncias com um volume raiz do Amazon EBS ... 3275
Instâncias com um volume raiz de armazenamento de instância (somente para instâncias do Linux) ... 3277
Manter o volume raiz após o encerramento da instância ... 3278
Substituir um volume raiz ... 3282
Nomes de dispositivos para volumes ... 3294
Nomes de dispositivos disponíveis ... 3294
Considerações sobre nomes de dispositivos ... 3297
Mapeamentos de dispositivos de blocos ... 3299
Conceitos de mapeamento de dispositivos de blocos ... 3300
Adicionar mapeamento de dispositivos de blocos a uma AMI ... 3304
Adicionar mapeamento de dispositivos de blocos a uma instância ... 3309
Como os volumes são anexados e mapeados para instâncias Windows ... 3318
Mapear discos NVMe para volumes ... 3319
Mapear discos não NVMe para volumes ... 3324
Prevenção de gravação interrompida ... 3334
Tamanhos de blocos compatíveis ... 3335
Requisitos ... 3336
Verificar compatibilidade de instâncias ... 3337
Configurar workload ... 3339
Snapshots do EBS do VSS ... 3340
O que é o VSS? ... 3341
Como funciona a solução de snapshots do Amazon EBS baseada no VSS ... 3342
Pré-requisitos do VSS ... 3343
Criar snapshots do VSS ... 3356
Solucionar problemas de snapshots do VSS ... 3367
Opções de restauração para a solução AWS VSS ... 3372
Histórico de versões ... 3373
Armazenamento de objetos, armazenamento de arquivos e armazenamento em cache de arquivos ... 3378

Amazon S3 ... 3379
Amazon EFS ... 3382
Amazon FSx ... 3386
Amazon File Cache ... 3392
Gerenciar recursos ... 3393
Selecionar uma região para os recursos ... 3393
Encontrar seus recursos ... 3395
Etapas do console ... 3395
Exemplos de linha de comando ... 3404
Visão global (entre regiões) ... 3408
AWS Global View ... 3408
Marcar com tag os recursos do ... 3412
Conceitos Básicos de Tags ... 3413
Marcar seus recursos com tag ... 3414
Restrições de tags ... 3415
Gerenciamento de tags e acesso ... 3416
Marcar com tag recursos para faturamento ... 3416
Marcar permissões de recursos ... 3417
Adicionar e remover tags ... 3420
Filtrar recursos por tag ... 3425
Visualizar tags usando metadados da instância ... 3427
Service Quotas ... 3433
Visualizar as cotas atuais ... 3433
Solicitar um aumento ... 3434
Restrição para e-mails enviados usando a porta 25 ... 3435
Monitorar recursos do ... 3436
Monitorar o status das instâncias ... 3437
Verificações do status ... 3438
Eventos de alteração de estado ... 3447
Eventos agendados ... 3450
Monitorar instâncias usando o CloudWatch ... 3489
Alarmes de instância ... 3490
Gerenciar o monitoramento detalhado ... 3492
métricas do CloudWatch ... 3495
Baixar e configurar o atendente do CloudWatch ... 3516
Estatísticas para métricas do ... 3521

Exibir os grafos de monitoramento ... 3530
Criar um alarme ... 3531
Criar alarmes para interromper, encerrar, reinicializar ou recuperar uma instância ... 3532
Automatizar usando o EventBridge ... 3545
Tipos de eventos do Amazon EC2 ... 3546
Log chamadas de API usando o CloudTrail ... 3546
Eventos de gerenciamento da API do Amazon EC2 no CloudTrail ... 3548
Exemplos de eventos da API do Amazon EC2 ... 3548
Auditar conexões realizadas com o EC2 Instance Connect ... 3550
Monitorar as aplicações .NET e SQL Server ... 3551
Acompanhar seu uso do nível gratuito ... 3552
Benefícios do nível gratuito antes e depois de 15 de julho de 2025 ... 3553
Rastrear o uso do nível gratuito para contas criadas antes de 15 de julho de 2025 ... 3554
Relatórios de uso e faturamento ... 3556
Instâncias ... 3557
Instâncias bare metal ... 3558
Hosts dedicados ... 3558
Dedicated Instances ... 3558
Otimização de EBS ... 3559
Reservas de capacidade ... 3559
Fazer o inventário de suas instâncias do EC2 ... 3559
Localização geográfica ... 3561
Especificações de hardware ... 3562
Imagens ... 3563
Endereços IP e nomes do host DNS ... 3565
Regras de grupos de segurança ... 3566
Dados do usuário ... 3568
Recursos relacionados ... 3569
Solução de problemas ... 3570
Problemas de inicialização de instâncias ... 3570
Nome de dispositivo inválido ... 3571
Limite de instâncias excedido ... 3572
Capacidade insuficiente da instância ... 3572
A configuração solicitada não é suportada atualmente. Verifique a documentação quanto às configurações compatíveis. ... 3573
A instância é encerrada imediatamente ... 3574

Permissões insuficientes 3575
Alto uso da CPU logo após a inicialização do Windows (somente para instâncias do Windows) 3576
Problemas de interrupção de instâncias 3577
Forçar a interrupção de uma instância 3578
(Opcional) Criar uma instância de substituição 3580
Problemas de encerramento de instâncias 3583
A instância é encerrada imediatamente 3583
Encerramento atrasado da instância 3583
Instância encerrada ainda sendo exibida 3586
Erro: a instância não pode ser encerrada. Modifique seu atributo de instância 'disableApiTermination' 3586
Instâncias executadas ou encerradas automaticamente 3586
Instâncias inacessíveis 3587
Reinicialização da instância 3587
Saída do console da instância 3587
Fazer uma captura de tela de uma instância inacessível 3588
Capturas de tela comuns para instâncias do Windows 3590
Recuperação da instância quando um computador host falhar 3600
A instância apareceu offline e foi reiniciada inesperadamente 3600
Problemas de SSH da instância do Linux 3601
Causas comuns de problemas de conexão 3602
Erro ao se conectar à sua instância: limite de tempo da conexão atingido 3604
Erro: não foi possível carregar a chave ... Esperando: QUALQUER CHAVE PRIVADA 3607
Erro: Chave do usuário não reconhecida pelo servidor 3608
Erro: permissão negada ou conexão fechada pela porta 22 de [instância] 3610
Erro: arquivo de chave privada desprotegido 3613
Erro: a chave privada deve começar com "-----BEGIN RSA PRIVATE KEY-----" e terminar com "-----END RSA PRIVATE KEY-----" 3614
Erro: falha na verificação de chaves do host 3615
Erro: o servidor recusou nossa chave ou não há métodos de autenticação compatíveis 3615
Não é possível fazer o ping da instância 3616
Erro: Server unexpectedly closed network connection (A conexão de rede foi fechada inesperadamente pelo servidor) 3617
Erro: falha na validação da chave do host para EC2 Instance Connect 3617
Não é possível conectar a uma instância Ubuntu usando o EC2 Instance Connect 3619

Perdi minha chave privada. Como posso me conectar à instância? 3620
Falhas nas verificações de status de instâncias do Linux 3627
Analisar informações de verificação de status 3628
Recuperar os logs do sistema 3629
Solução de problemas relacionados aos erros de log do sistema para instâncias do Linux 3630
Sem memória: encerrar processo 3631
ERRO: falha em mmu_update (falha na atualização do gerenciamento de memória) 3632
Erro de E/S (falha de dispositivo de blocos) 3633
ERRO DE E/S: nem disco local nem disco remoto (o dispositivo de blocos distribuído está quebrado) 3635
request_module: modprobe de loop descontrolado (modprobe do kernel legado do looping, em versões mais antigas do Linux) 3636
"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) 3637
"FATAL: Não foi possível carregar os módulos /lib/" ou "BusyBox" (módulos do kernel ausentes) 3638
ERRO Kernel inválido (kernel incompatível com EC2) 3640
fsck: Nenhum arquivo ou diretório ao tentar abrir… (Sistema de arquivos não encontrado) 3641
Erro geral ao montar os sistemas de arquivos (falha na montagem) 3643
VFS: Não foi possível montar o fs raiz em um bloco desconhecido (falta de correspondência no sistema de arquivos-raiz) 3646
Erro: não foi possível determinar o número principal/secundário do dispositivo raiz... (Incompatibilidade entre sistema de arquivos/dispositivo raiz) 3647
XENBUS: Dispositivo sem driver… 3648
…dias sem ser verificada, verificação forçada (verificação necessária para o sistema de arquivos) 3650
O fsck morreu com status de saída… (Dispositivo ausente) 3650
Prompt do GRUB (grubdom>) 3652
Acessando a interface eth0: O dispositivo eth0 tem um endereço MAC diferente do esperado, ignorando. (Endereço MAC hard-coded) 3655
Não foi possível carregar a Política do SELinux. A máquina está no modo de força. Parando agora. (Erro de configuração do SELinux) 3657
XENBUS: Excedido o limite de tempo para se conectar a dispositivos (tempo limite do Xenbus) 3658
Instância do Linux é inicializada com volume errado 3659
Problemas de RDP com instâncias do Windows 3661

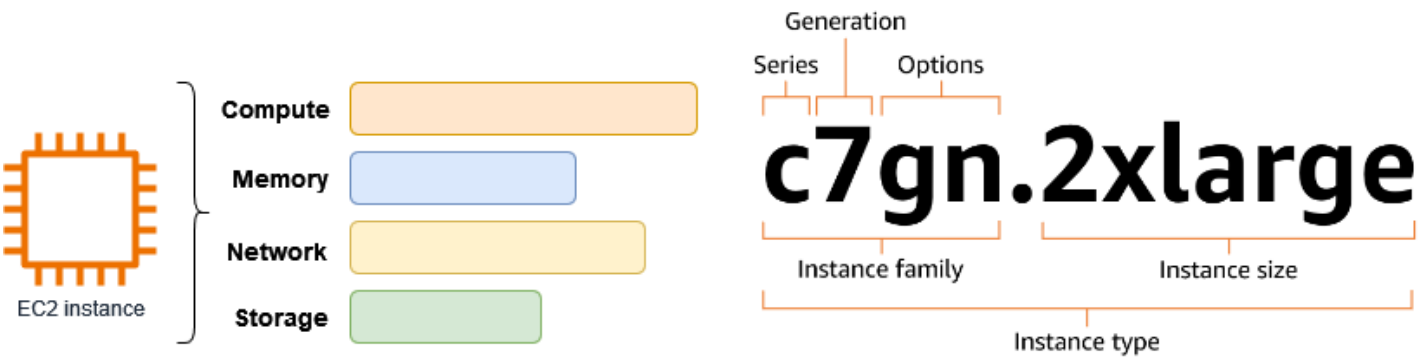
O Remote Desktop não pode se conectar ao computador remoto ... 3662
Erro ao usar o cliente RDP do macOS ... 3663
O RDP exibe uma tela preta em vez da área de trabalho ... 3664
Não foi possível fazer login remotamente em uma instância com um usuário que não é administrador ... 3664
Resolução de problemas do desktop remoto usando o AWS Systems Manager ... 3664
Habilitar a área de trabalho remota em uma instância do EC2 com o registro remoto ... 3669
Perdi minha chave privada. Como posso me conectar à minha instância do Windows? ... 3670
Problemas de inicialização de instâncias do Windows ... 3671
"A senha não está disponível" ... 3671
"A senha ainda não está disponível" ... 3672
"Não é possível recuperar a senha do Windows" ... 3673
"Esperando o serviço de metadados" ... 3673
"Não é possível ativar o Windows" ... 3677
"O Windows não é genuíno (0x80070005)" ... 3679
"Nenhum servidor de licença do servidor terminal disponível para fornecer uma licença" ... 3680
“Algumas configurações são gerenciadas pela sua organização” ... 3680
Problemas com instâncias do Windows ... 3681
Não é possível conectar o AWS Systems Manager Sessions Manager a uma instância do Windows Server 2025 ... 3681
Os volumes do EBS não são inicializados no Windows Server 2016 e 2019 ... 3682
Inicialize uma instância do EC2 Windows no Directory Services Restore Mode (DSRM) ... 3683
A instância perde a conectividade de rede ou as tarefas agendadas não são executadas quando esperado ... 3686
Não foi possível obter o resultado do console ... 3687
Windows Server 2012 R2 não disponível na rede ... 3687
Colisão de assinatura em disco ... 3688
Definir senha de administrador do Windows ... 3689
Redefinir a senha usando o EC2Launch v2 ... 3691
Redefinir a senha usando o EC2Launch ... 3696
Redefinir a senha usando o EC2Config ... 3702
Solução de problemas de Sysprep ... 3708
EC2Rescue para instâncias do Linux ... 3710
Instalar o EC2Rescue ... 3711
Executar comandos do EC2Rescue ... 3715
Desenvolver módulos do EC2Rescue ... 3717

EC2Rescue para instâncias do Windows 3724
Solucionar problemas usando a GUI do EC2Rescue 3726
Solucionar problemas usando a CLI do EC2Rescue 3733
Solucionar problemas usando o EC2Rescue e o Systems Manager 3742
Console de série do EC2 3746
Pré-requisitos 3746
Configurar o acesso ao Console de Série do EC2 3754
Conectar-se ao Console de Série do EC2 3765
Desconecte-se do Console de Série do EC2 3775
Solucionar problemas da instância usando o Console de Série do EC2 3776
Enviar interrupção para diagnóstico 3785
Tipos de instâncias compatíveis 3786
Pré-requisitos 3786
Enviar uma interrupção para diagnóstico 3789
Histórico do documento 3791
Histórico para 2018 e para os anos anteriores 3832

O que é o Amazon EC2?

O Amazon Elastic Compute Cloud (Amazon EC2) oferece uma capacidade de computação escalável sob demanda na Nuvem Amazon Web Services (AWS). O uso do Amazon EC2 reduz os custos de hardware para que você possa desenvolver e implantar aplicações com mais rapidez. É possível usar o Amazon EC2 para executar quantos servidores virtuais forem necessários, configurar a segurança e as redes e gerenciar o armazenamento. É possível adicionar capacidade (aumentar a escala verticalmente) para lidar com tarefas de computação pesada, como processos mensais ou anuais ou picos no tráfego do site. Quando o uso diminui, você pode reduzir a capacidade (reduzir a escala verticalmente) de novo.

Uma instância do EC2 é um servidor virtual na Nuvem AWS. Quando executa uma instância do EC2, o tipo de instância que você especifica determina o hardware disponível para sua instância. Cada tipo de instância oferece um equilíbrio diferente entre recursos de computação, memória, armazenamento e rede. Para obter mais informações, consulte o Guia de tipos de instância do Amazon EC2.



Recursos do Amazon EC2

O Amazon EC2 fornece os seguintes recursos de alto nível:

Instâncias

Servidores virtuais.

Imagens de máquina da Amazon (AMIs)

Os modelos pré-configurados para suas instâncias que empacotam os componentes de que você precisa para seu servidor (incluindo o sistema operacional e software adicional).

Tipos de instância

Várias configurações de capacidade de CPU, memória, armazenamento e redes e hardware gráfico para suas instâncias.

Volumes do Amazon EBS

Volumes de armazenamento persistentes para seus dados usando o Amazon Elastic Block Store (Amazon EBS).

Volumes de armazenamento de instâncias

Volumes de armazenamento para dados temporários que são excluídos quando você interrompe, hiberna ou encerra sua instância.

Pares de chaves

Proteja informações de login de suas instâncias. A AWS armazena a chave pública, e você armazena a chave privada em um lugar seguro.

Grupos de segurança

Um firewall virtual que permite especificar os protocolos, as portas e os intervalos de IP de origem que podem alcançar suas instâncias e os intervalos de IP de destino aos quais suas instâncias podem se conectar.

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

Serviços relacionados

Serviços para uso com o Amazon EC2

É possível usar outra Serviços da AWS com as instâncias que você implanta usando o Amazon EC2.

Amazon EC2 Auto Scaling

Ajuda a garantir que você tenha o número correto de instâncias do Amazon EC2 disponíveis para processar a carga da aplicação.

AWS Backup

Automatize o backup de suas instâncias do Amazon EC2 e dos volumes do Amazon EBS anexados a elas.

Amazon CloudWatch

Monitore suas instâncias e os volumes do Amazon EBS.

Elastic Load Balancing

Distribua automaticamente o tráfego de entrada da aplicação entre várias instâncias.

Amazon GuardDuty

Detecte o uso potencialmente não autorizado ou mal-intencionado de suas instâncias do EC2.

EC2 Image Builder

Automatize a criação, o gerenciamento e a implantação de imagens de servidor personalizadas, seguras e atualizadas.

AWS Launch Wizard

Dimensione, configure e implante recursos da AWS para aplicações de terceiros sem precisar identificar e provisionar recursos da AWS individuais manualmente.

AWS Systems Manager

Execute operações em grande escala em instâncias do EC2 com essa solução segura de gerenciamento de ponta a ponta.

Serviços adicionais de computação

É possível iniciar instâncias usando outro serviço de computação da AWS em vez de usar o Amazon EC2.

Amazon Lightsail

Crie sites ou aplicações da Web usando Amazon Lightsail uma plataforma em nuvem que fornece os recursos necessários para implantar seu projeto rapidamente, por um preço mensal baixo e previsível. Para comparar o Amazon EC2 e o Lightsail, consulte Amazon Lightsail ou Amazon EC2.

Amazon Elastic Container Service (Amazon ECS)

Implante, gerencie e escale aplicações em contêineres em um cluster de instâncias do EC2. Para obter mais informações, consulte Escolher um serviço de contêiner da AWS.

Amazon Elastic Kubernetes Service (Amazon EKS)

Execute as aplicações do Kubernetes na AWS. Para obter mais informações, consulte Escolher um serviço de contêiner da AWS.

Acessar o Amazon EC2

É possível criar e gerenciar as instâncias do Amazon EC2 usando as seguintes interfaces:

Console do Amazon EC2

Uma interface Web simples para criar e gerenciar instâncias e recursos 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.

AWS Command Line Interface

Permite interagir com serviços da AWS usando comandos no shell da linha de comando. É compatível com Windows, Mac e Linux. Para obter mais informações sobre a AWS CLI, consulte o Guia do usuário da AWS Command Line Interface. É possível encontrar os comandos do Amazon EC2 na AWS CLI Command Reference.

CloudFormation

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

SDKs da AWS

Se você preferir criar aplicações usando APIs específicas de uma linguagem em vez de enviar uma solicitação via HTTP ou HTTPS, a AWS fornece bibliotecas, código de exemplo, tutoriais e outros recursos para desenvolvedores de software. Essas bibliotecas fornecem funções básicas

que automatizam tarefas, como assinatura criptografada de suas solicitações, novas tentativas de solicitações e tratamento das respostas de erro, facilitando para que você comece rapidamente. Para obter mais informações, consulte Ferramentas para criar na AWS.

AWS Tools for PowerShell

Um conjunto de módulos do PowerShell criados com base na funcionalidade exposta pelo SDK for .NET. As ferramentas para PowerShell permitem que você execute scripts para operações em seus recursos da AWS usando a linha de comando do PowerShell. Para começar a usar, consulte o Guia do usuário da AWS Tools for PowerShell. É possível encontrar os cmdlets para o Amazon EC2, na AWS Tools for PowerShell Cmdlet Reference.

API de consulta

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.

Definição de preço do Amazon EC2

O Amazon EC2 fornece as seguintes opções de preços:

Nível gratuito

É possível começar gratuitamente com o Amazon EC2. Para explorar as opções do nível gratuito, consulte Nível gratuito da AWS.

Instâncias sob demanda

Pague pelas instâncias que você usar por segundo, com um mínimo de 60 segundos, sem qualquer compromisso de longo prazo ou pagamentos adiantados.

Savings Plans

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

Reserved Instances

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

Spot Instances

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

Hosts dedicados

Reduza os custos usando um servidor físico do EC2 totalmente dedicado ao seu uso, sob demanda ou como parte de um Savings Plan. É possível usar suas licenças de software existentes vinculadas ao servidor e obter ajuda para atender aos requisitos de conformidade.

Reservas de capacidade sob demanda

Reserve capacidade de computação para suas instâncias do EC2 em uma zona de disponibilidade específica por qualquer tempo de duração.

Cobrança por segundo

Elimina o custo de minutos e segundos não utilizados da sua fatura.

Para obter uma lista completa de cobranças e preços do Amazon EC2 e mais informações sobre modelos de compra, consulte Preço do Amazon EC2.

Estimativas, faturamento e otimização de custos

Para criar estimativas para seus casos de uso da AWS, use a AWS Pricing Calculator.

Para estimar o custo de transformar as workloads da Microsoft em uma arquitetura moderna que usa serviços de código aberto e nativos da nuvem implantados na AWS, use a Calculadora de Modernização da AWS para workloads da Microsoft.

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

Se tiver dúvidas sobre faturamento, contas e eventos da AWS, entre em contato com o Suporte da AWS.

Para calcular o custo de um exemplo de ambiente provisionado, consulte Centro de informações sobre economia da nuvem. Ao calcular o custo de um ambiente provisionado, lembre-se de incluir custos incidentais, como armazenamento de snapshots para volumes do EBS.

É possível otimizar o custo, a segurança e a performance do seu ambiente da AWS usando o AWS Trusted Advisor.

É possível usar o AWS Cost Explorer para analisar o custo e o uso das instâncias do EC2. É possível visualizar dados dos últimos 13 meses e prever o provável valor que você gastará nos próximos 12 meses. Para obter mais informações, consulte Análise do seu custo e utilização com o AWS Cost Explorer no Guia do usuário do AWS Cost Management.

Recursos

- Recursos do Amazon EC2
- AWS re:Post
- AWS Skill Builder
- Suporte do AWS
- Tutoriais práticos
- Hospedagem na Web
- Windows na AWS

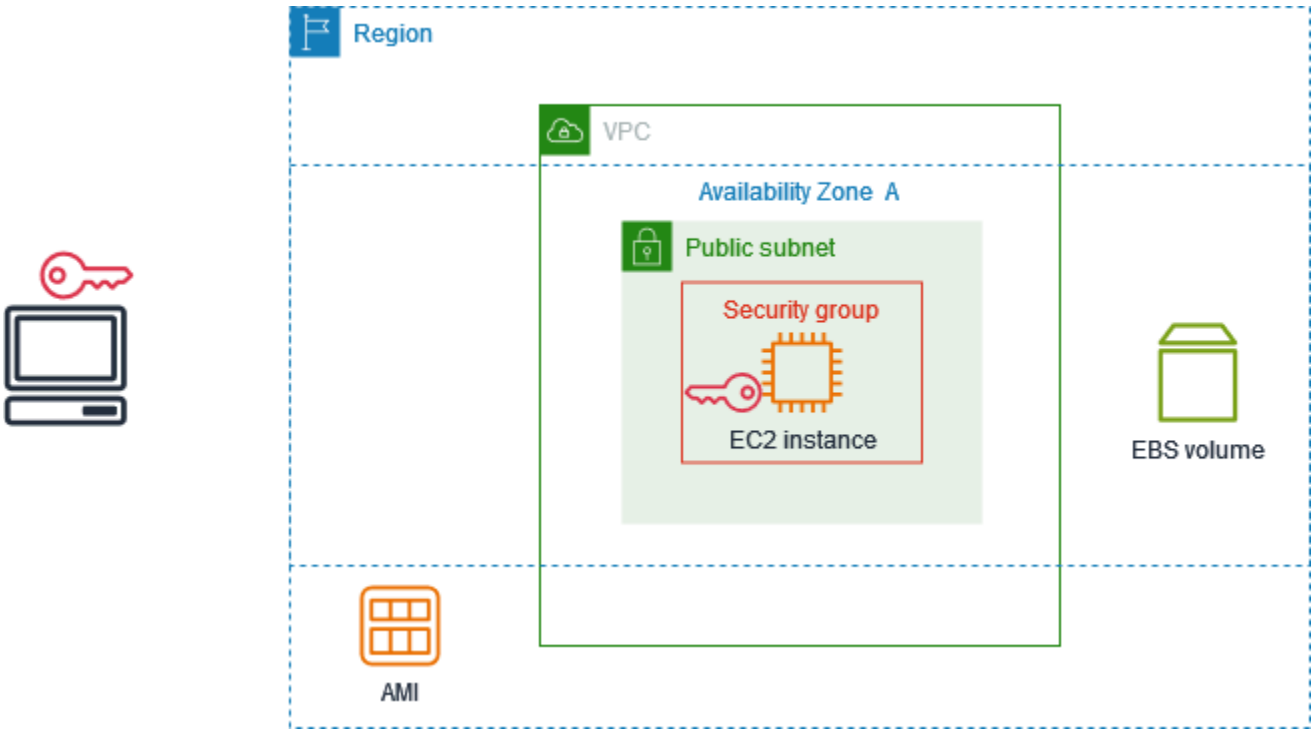
Comece a usar o Amazon EC2

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

Visão geral

O seguinte diagrama mostra os principais componentes que você usará neste tutorial:

- Uma imagem: um modelo que contém o software a ser executado na instância, como o sistema operacional.
- Um par de chaves: um conjunto de credenciais de segurança que você usa para provar a identidade ao realizar a conexão com a instância. A chave pública está na instância e a chave privada está no computador.
- Uma rede: uma nuvem privada virtual (VPC) é uma rede virtual dedicada à Conta da AWS. Para ajudar você a começar a usar rapidamente, a conta é equipada com uma VPC padrão em cada Região da AWS, e cada VPC padrão tem uma sub-rede padrão em cada zona de disponibilidade.
- Um grupo de segurança: atua como um firewall virtual para controlar o tráfego de entrada e de saída.
- Um volume do EBS: exigimos um volume raiz para a imagem. Como opção, é possível adicionar volumes de dados.



Custo para este tutorial

Ao criar sua Conta da AWS, comece a usar o Amazon EC2 gratuitamente com o Nível gratuito da AWS.

Caso tenha criado sua Conta da AWS antes de 15 de julho de 2025, ela tenha menos de 12 meses e ainda não tenha excedido os benefícios do nível gratuito para o Amazon EC2, você não pagará nada para concluir este tutorial, pois ajudamos a selecionar opções com os benefícios do nível gratuito. Caso contrário, você incorrerá em taxas de uso padrão do Amazon EC2 desde o momento em que executar a instância (mesmo que ela permaneça ociosa) até encerrá-la.

Caso tenha criado sua Conta da AWS em 15 de julho de 2025 ou após essa data, ela tenha menos de seis meses e não tenha usado todos os créditos, a conclusão deste tutorial não custará nada, pois ajudamos você a selecionar opções que estão dentro dos benefícios do nível gratuito.

Para obter informações sobre como determinar se você é elegível para o nível gratuito, consulte the section called “Acompanhar seu uso do nível gratuito”.

Tarefas

- Etapa 1: executar uma instância
- Etapa 2: conectar-se à instância
- Etapa 3: limpar a instância

- Próximas etapas

Etapa 1: executar uma instância

É possível iniciar uma instância do EC2 usando o Console de gerenciamento da AWS conforme descrito no procedimento a seguir. Este tutorial tem o objetivo de ajudar você a iniciar rapidamente sua primeira instância. Ele não abrange todas as opções possíveis.

Como iniciar 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, exibimos a Região da AWS atual. Por exemplo, Ohio. É possível usar a região selecionada ou, opcionalmente, selecionar uma região mais próxima de você.
3. No painel do console do EC2, no painel Executar instância, escolha Executar instância.
4. Em Name and tags (Nome e etiquetas), em Name (Nome), insira um nome descritivo para a instância.
5. Em Application and OS Images (Amazon Machine Image) (Imagens de aplicações e SO [imagem de máquina da Amazon]), faça o seguinte:
   a. Escolha Início rápido e, em seguida, selecione o sistema operacional (SO) da sua instância. Para sua primeira instância do Linux, recomendamos escolher o Amazon Linux.
   b. Em Imagem de máquina da Amazon (AMI), selecione uma AMI marcada como sendo elegível para o nível gratuito.
6. Em Tipo de instância, para Tipo de instância, selecione um tipo de instância marcado como elegível para o nível gratuito.
7. Em Par de chaves (login), para Nome do par de chaves, escolha um par de chaves existente ou selecione Criar novo par de chaves para criar seu primeiro par de chaves.

   > ⚠ Warning
   >
   > Se você escolher Prosseguir sem um par de chaves (não recomendado), não será possível realizar a conexão com a instância usando os métodos descritos neste tutorial.

8. Em Configurações de rede, observe que selecionamos a VPC padrão, selecionamos a opção de usar a sub-rede padrão em uma zona de disponibilidade que escolhemos para você e

configuramos um grupo de segurança com uma regra que permite conexões com a instância de qualquer origem (`0.0.0.0/0`).

> **Warning**
>
> Se especificar `0.0.0.0/0`, você habilitará o tráfego de qualquer endereço IP no mundo. Para os protocolos SSH e RDP, essa abordagem é aceitável por um período curto em um ambiente de teste, mas não é seguro em ambientes de produção. Em produção, certifique-se de autorizar o acesso somente a partir do endereço IP individual apropriado ou do intervalo de endereços.

Para sua primeira instância, recomendamos usar as configurações padrão. Caso contrário, é possível atualizar as configurações de rede da seguinte forma:

- (Opcional) Para usar uma sub-rede padrão específica, escolha Editar e, em seguida, selecione uma sub-rede.
- (Opcional) Para usar uma VPC diferente, escolha Editar e, em seguida, selecione uma VPC existente. Se a VPC não estiver configurada para acesso público por parte da Internet, você não conseguirá se conectar à instância.
- (Opcional) Para restringir o tráfego de conexão de entrada para uma rede específica, escolha Personalizado em vez de Qualquer lugar e insira o bloco CIDR da sua rede.
- (Opcional) Para usar um grupo de segurança diferente, escolha Selecionar grupo de segurança existente e escolha um grupo de segurança existente. Se o grupo de segurança não tiver uma regra que permita o tráfego de conexão da sua rede, você não conseguirá se conectar à instância. Para uma instância do Linux, você deve permitir o tráfego SSH. Para uma instância do Windows, você deve permitir o tráfego RDP.

9. Em Configurar armazenamento, observe que configuramos um volume raiz, mas nenhum volume de dados. Isto é suficiente para fins de teste.
10. Revise um resumo da configuração da instância no painel Summary (Resumo) e, quando você estiver pronto, escolha Launch instance (Iniciar instância).
11. Se a inicialização ocorrer com êxito, escolha o ID da instância na notificação de Êxito para abrir a página Instâncias e monitorar o status da inicialização.
12. Marque a caixa de seleção da instância. O estado inicial da instância é `pending`. Depois que a instância é iniciada, seu estado muda para `running`. Escolha a guia Status e alarmes.

Depois que a instância for aprovada nas verificações de status, ela estará pronta para receber solicitações de conexão.

Etapa 2: conectar-se à instância

O procedimento usado dependerá do sistema operacional da instância. Se você não puder se conectar à sua instância, consulte Solucionar problemas de conexão com a instância do Linux do Amazon EC2 para obter assistência.

Instâncias do Linux

É possível se conectar à instância do Linux usando qualquer cliente SSH. Se você estiver executando o Windows em seu computador, abra um terminal e execute o comando `ssh` para verificar se um cliente SSH está instalado. Se o comando não for encontrado, instale o OpenSSH para Windows.

Para se conectar à sua instância usando SSH

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 Conectar.
4. Na página Conectar-se à instância, escolha a guia Cliente SSH.
5. (Opcional) Se você criou um par de chaves ao iniciar a instância e fez download da chave privada (arquivo .pem) em um computador em execução no Linux ou no macOS, execute o comando chmod de exemplo para definir as permissões para a chave privada.
6. Copie o comando SSH de exemplo. Veja a seguir um exemplo em que *key-pair-name*.pem é o nome do arquivo de chave privada, *ec2-user* é o nome do usuário associado à imagem, e a string após o símbolo @ é o nome DNS público da instância.

   ```
   ssh -i key-pair-name.pem ec2-user@ec2-198-51-100-1.us-east-2.compute.amazonaws.com
   ```

7. Em uma janela de terminal do computador, execute o comando ssh que você salvou na etapa anterior. Se o arquivo de chave privada não estiver no diretório atual, você deverá especificar o caminho completo para o arquivo de chave neste comando.

   Esta é uma resposta de exemplo:

```
The authenticity of host 'ec2-198-51-100-1.us-east-2.compute.amazonaws.com
 (198-51-100-1)' can't be established.
ECDSA key fingerprint is l4UB/neBad9tvkgJf1QZWxheQmR59WgrgzEimCG6kZY.
Are you sure you want to continue connecting (yes/no)?
```

8. (Opcional) Verifique se a impressão digital no alerta de segurança corresponde à impressão digital da instância contida na saída do console ao iniciar uma instância pela primeira vez. Para obter a saída do console, escolha Ações, Monitorar e solucionar problemas e Obter log do sistema. Caso essas impressões digitais não correspondam, alguém pode estar tentando um ataque man-in-the-middle. Se corresponderem, continue para a próxima etapa.
9. Digite **`yes`**.

   Esta é uma resposta de exemplo:

```
Warning: Permanently added 'ec2-198-51-100-1.us-
east-2.compute.amazonaws.com' (ECDSA) to the list of known hosts.
```

Instâncias do Windows

Para você se conectar a uma instância do Windows, é necessário recuperar a senha de administrador inicial e inserir essa senha quando se conectar à instância. Após a execução da instância, leva alguns minutos para que a senha fique disponível. Sua conta precisa ter permissão para chamar a ação GetPasswordData. Para obter mais informações, consulte Exemplo de políticas para controlar o acesso à API do Amazon EC2.

O nome de usuário padrão correspondente à conta de administrador depende do idioma do sistema operacional (SO) contido na AMI. Para determinar o nome de usuário correto, identifique o idioma do sistema operacional e escolha o nome de usuário correspondente. Por exemplo, para um sistema operacional em inglês, o nome de usuário será `Administrator`, para um sistema operacional francês, será `Administrateur` e para um sistema operacional português, será `Administrador`. Se uma versão de idioma do sistema operacional não tiver um nome de usuário no mesmo idioma, escolha o nome de usuário `Administrator (Other)`. Para obter mais informações, consulte Nomes localizados da conta de administrador no Windows no site da Microsoft.

Recuperar a senha de administrador inicial

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 Conectar.
4. Na página Conectar à instância, escolha a guia Cliente RDP.
5. Em Nome de usuário, escolha o nome de usuário padrão para a conta do administrador. O nome de usuário escolhido deverá corresponder ao idioma do sistema operacional (SO) contido na AMI que você usou para executar a instância. Se não houver um nome de usuário no mesmo idioma do seu sistema operacional, escolha Administrador (Outro).
6. Escolha Obter senha.
7. Na página Obter senha do Windows, faça o seguinte:

    a. Escolha Fazer upload de arquivo de chave privada e localize o arquivo de chave privada (`.pem`) que especificou ao executar a instância. Selecione o arquivo e escolha Open (Abrir) para copiar todo o conteúdo do arquivo para essa janela.

    b. Escolha Descriptografar senha. A página Obter senha do Windows será fechada e a senha padrão do administrador para a instância será exibida em Senha, substituindo o link Obter senha exibido anteriormente.

    c. Copie e salve a senha em um lugar seguro. Essa senha é necessária para se conectar à instância.

O procedimento a seguir usa o cliente Remote Desktop Connection para Windows (MSTSC). Se você estiver usando um cliente RDP diferente, baixe o arquivo RDP e consulte a sua documentação para conhecer as etapas para estabelecer a conexão RDP.

Conectar-se a uma instância do Windows usando um cliente RDP

1. Na página Conectar-se a uma instância, escolha Baixar arquivo de área de trabalho remota. Quando o download do arquivo terminar, escolha Cancelar para retornar à página Instâncias. O arquivo RDP é baixado para a sua pasta `Downloads`.
2. Execute `mstsc.exe` para abrir o cliente RDP.
3. Expanda Mostrar opções, escolha Abrir e selecione o arquivo .rdp na pasta `Downloads`.
4. Por padrão, Computador é o nome DNS IPv4 público da instância, e Nome de usuário é a conta do administrador. Em vez disso, para se conectar à instância usando IPv6, substitua o nome DNS IPv4 público da instância pelo endereço IPv6. Analise as configurações padrão e altere-as conforme necessário.

5. Selecione Conectar. Se você receber um aviso de que o publicador da conexão remota é desconhecido, selecione Conectar para continuar.
6. Digite a senha que você salvou anteriormente e selecione OK.
7. Por causa da natureza de certificados autoassinados, talvez você receba um aviso indicando que não foi possível autenticar o certificado de segurança. Execute um destes procedimentos:
   - Se você confia no certificado, escolha Sim para realizar a conexão com a instância.
   - [Windows] Antes de continuar, compare a impressão digital do certificado com o valor no log do sistema para confirmar a identidade do computador remoto. Escolha Visualizar certificado e, em seguida, escolha Impressão digital na guia Detalhes. Compare esse valor com o valor de `RDPCERTIFICATE-THUMBPRINT` em Ações, Monitorar e solucionar problemas e Obter log do sistema.
   - [Mac OS X] Antes de continuar, compare a impressão digital do certificado com o valor no log do sistema para confirmar a identidade do computador remoto. Escolha Mostrar certificado, expanda Detalhes e selecione Impressões digitais de SHA1. Compare esse valor com o valor de `RDPCERTIFICATE-THUMBPRINT` em Ações, Monitorar e solucionar problemas e Obter log do sistema.
8. Se a conexão RDP tiver êxito, o cliente RDP exibirá a tela de login do Windows e, em seguida, a área de trabalho do Windows. Se, em vez disso, você receber uma mensagem de erro, consulte the section called “O Remote Desktop não pode se conectar ao computador remoto”. Ao finalizar a conexão RDP, será possível fechar o cliente RDP.

Etapa 3: limpar a instância

> **Warning**
>
> O encerramento de uma instância é permanente e irreversível.
> Depois de encerrar uma instância, não será mais possível se conectar a ela e ela não poderá ser recuperada. Todos os volumes anexados do Amazon EBS configurados para serem excluídos no encerramento também serão excluídos permanentemente e não poderão ser recuperados. Todos os dados armazenados em volumes de armazenamento de instância serão perdidos permanentemente. Para obter mais informações, consulte Como funciona o encerramento de uma instância.
> Antes de encerrar uma instância, certifique-se de ter feito backup de todos os dados que você precise reter após o encerramento no armazenamento persistente.

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.

Você deixará de incorrer em custos por essa instância ou em uso que conte para os limites do nível gratuito assim que o status da instância for alterado para `shutting down` ou `terminated`. Para manter sua instância para uso posterior, sem incorrer em custos ou uso que conte para os limites do nível gratuito, você pode interromper a instância agora e reiniciá-la posteriormente. Para obter mais informações, consulte Início e interrupção de instâncias do Amazon EC2.

Para encerrar sua instância

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

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

Próximas etapas

Depois de iniciar a instância, você pode querer explorar as seguintes etapas:

- Explore os principais conceitos do Amazon EC2 com os tutoriais introdutórios. Para obter mais informações, consulte Tutoriais para executar instâncias do EC2.
- Saiba como monitorar o uso do nível gratuito do Amazon EC2 usando o console. Para obter mais informações, consulte the section called “Acompanhar seu uso do nível gratuito”.
- Configure um alarme do CloudWatch para enviar uma notificação caso seu uso ultrapasse o nível gratuito (para contas criadas antes de 15 de julho de 2025). Para obter mais informações, consulte Tracking your Nível gratuito da AWS usage no AWS Billing User Guide.
- Adicione um volume do EBS. Para obter mais informações, consulte Criar um volume do Amazon EBS no Guia do usuário do Amazon EC2.
- Saiba como gerenciar remotamente a instância do EC2 utilizando o comando Run. Para obter mais informações, consulte Comando AWS Systems Manager Run no Guia do usuário do AWS Systems Manager.

- Saiba mais sobre as opções de compra de instâncias. Para obter mais informações, consulte Opções de faturamento e compra do Amazon EC2.
- Obtenha conselho sobre tipos de instâncias. Para obter mais informações, consulte Obtenha recomendações do localizador de tipo de instância do EC2.

Melhores práticas do Amazon EC2

Para garantir os resultados máximos com a execução do Amazon EC2, sugerimos executar as práticas recomendadas a seguir.

Segurança

- Gerencie o acesso a recursos e APIs da AWS usando federação de identidades com um provedor de identidades e perfis do IAM sempre que possível. Para obter mais informações, consulte Criar políticas do IAM no Guia do usuário do IAM.
- Implemente as regras menos permissivas para o security group.
- Corrija, atualize e proteja regularmente o sistema operacional e os aplicativos em sua instância. Para obter mais informações, consulte Gerenciamento de atualizações. Para obter diretrizes específicas para sistemas operacionais do Windows, consulte Práticas recomendadas de segurança para instâncias do Windows.
- Use o Amazon Inspector para descobrir e verificar automaticamente instâncias do Amazon EC2 em busca de vulnerabilidades de software e exposição não intencional da rede. Para obter mais informações, consulte o Guia do usuário do Amazon Inspector.
- Use controles do AWS Security Hub CSPM para monitorar seus recursos do Amazon EC2 em relação às melhores práticas e padrões de segurança. Para obter mais informações sobre o uso do Security Hub CSPM, consulte Controles do Amazon Elastic Compute Cloud no Guia do usuário do AWS Security Hub CSPM.

Armazenamento

- Compreenda como o tipo de volume raiz afeta a persistência de dados, o backup e a recuperação. Para obter mais informações, consulte Tipo do volume de raiz.
- 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 dados quando uma instância for encerrada.
- Use o armazenamento de instâncias disponível para que sua instância armazene dados temporários. Lembre-se de que os dados armazenados em um armazenamento de instâncias são excluídos quando você interrompe, hiberna ou encerra uma instância. Se você usar o armazenamento de instâncias para armazenamento de bancos de dados, verifique se você tem um cluster com um fator de replicação que garanta tolerância a falhas.

- Criptografe volumes e snapshots do EBS. Para obter mais informações, consulte Criptografia do Amazon EBS no Guia do usuário do Amazon EBS.

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 Usar metadados da instância para gerenciar a instância do EC2 e Marcar com tag os recursos do Amazon EC2.
- 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 Service Quotas do Amazon EC2.
- Use AWS Trusted Advisor para inspecionar seu ambiente da AWS e fazer recomendações quando houverem oportunidades para economizar dinheiro, melhorar a performance do sistema ou ajudar a corrigir falhas de segurança. Consulte mais informações em AWS Trusted Advisor no Guia de Usuário AWS Support.

Backup e recuperação

- Faça backup de seus volumes do EBS regularmente usando Snapshots do Amazon EBS e crie uma Imagem de máquina da Amazon (AMI) de sua instância para salvar a configuração como um modelo para executar futuras instâncias. Para obter mais informações sobre os serviços da AWS que ajudam a realizar esse caso de uso, consulte AWS Backup e o Amazon Data Lifecycle Manager.
- 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.
- Monitorar e responder a eventos. Para obter mais informações, consulte Monitorar recursos do Amazon EC2.
- Certifique-se de que você está preparado para lidar com failover. Para uma solução básica, é possível 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. Para uma solução automatizada, é possível usar o Amazon EC2 Auto Scaling. Para mais informações, consulte o Guia do usuário do Amazon EC2 Auto Scaling.

- Teste regularmente o processo de recuperação de suas instâncias e dos volumes do Amazon EBS para garantir que dados e serviços sejam restaurados com êxito.

Redes

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

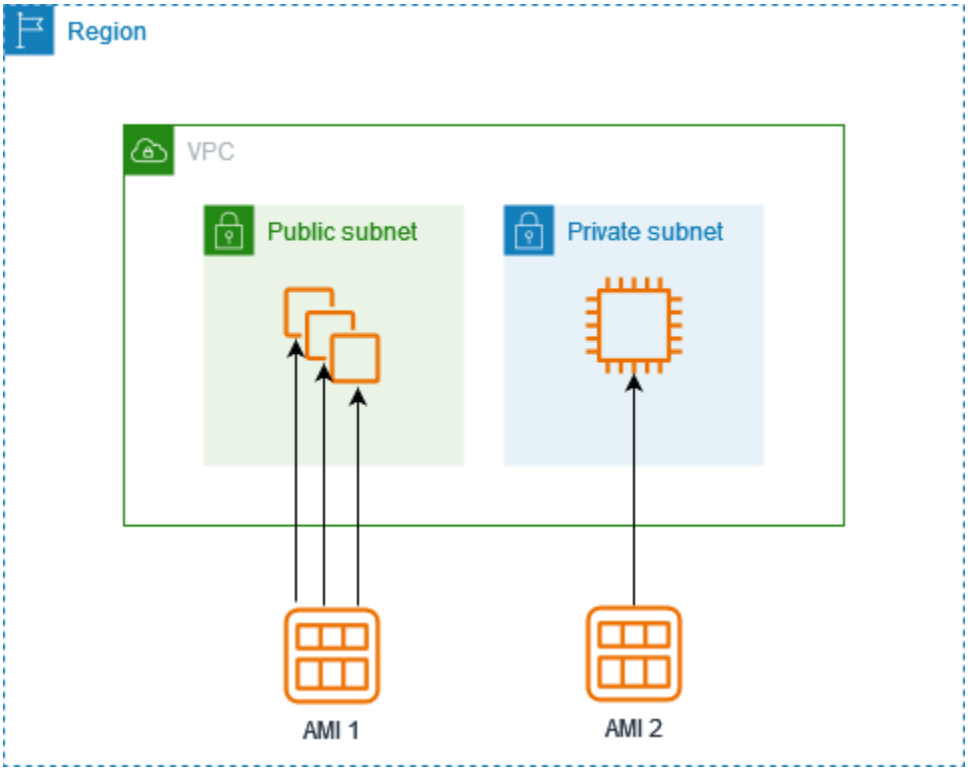
Imagens de máquina da Amazon no Amazon EC2

Uma Imagem de máquina da Amazon (AMI) é uma imagem que fornece o software necessário para configurar e inicializar uma instância do Amazon EC2. Cada AMI também contém um mapeamento de dispositivos de blocos que especifica os dispositivos de blocos a serem anexados às instâncias que você executa. Especifique uma AMI ao iniciar uma instância. Essa AMI deve ser compatível com o tipo de instância que você escolhe para a sua instância. É possível usar uma AMI fornecida pela AWS, uma AMI pública, uma AMI que alguém compartilhou com você ou uma AMI que você comprou no AWS Marketplace.

Uma AMI é específica para o seguinte:

- Região
- Sistema operacional
- Arquitetura do processador
- Tipo do volume de raiz
- Tipo de virtualização

É possível iniciar várias instâncias em uma única AMI quando precisar de várias instâncias com a mesma configuração. É possível usar AMIs diferentes para executar instâncias quando precisar de instâncias com configurações diferentes, conforme mostrado no diagrama a seguir.



É possível criar uma AMI de suas instâncias do Amazon EC2 e então usá-la para executar instâncias com a mesma configuração. É possível copiar uma AMI para outra região da AWS e usá-la para executar instâncias nessa região. Você também pode compartilhar uma AMI que você criou com outras contas para que elas possam executar instâncias com a mesma configuração. É possível vender sua AMI usando o AWS Marketplace.

Conteúdo

- Características e tipos de AMI no Amazon EC2
- Encontrar uma AMI que atenda aos requisitos da instância do EC2
- AMIs pagas no AWS Marketplace para instâncias do Amazon EC2
- Ciclo de vida da AMI do Amazon EC2
- Comportamento de execução da instância com modos de inicialização do Amazon EC2
- Usar criptografia com AMIs com EBS
- Saiba mais sobre o uso da AMI compartilhada no Amazon EC2
- Monitorar eventos da AMI usando o Amazon EventBridge
- Noções básicas sobre as informações de faturamento da AMI
- Cotas da AMI no Amazon EC2

Características e tipos de AMI no Amazon EC2

Ao executar uma instância, a AMI que você escolher deve ser compatível com o tipo de instância que você escolher. É possível selecionar uma AMI para uso com base nas seguintes características:

- Região
- Sistema operacional
- Arquitetura do processador
- Permissões de execução
- Tipo do volume de raiz
- Tipos de virtualização

Permissões de execução

As permissões de execução determinam quem pode usar uma AMI para executar instâncias. É possível pensar nas permissões de execução como compartilhar uma AMI — ao conceder permissões de execução, você está compartilhando a AMI com outros usuários. Somente o proprietário de uma AMI pode determinar 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, organizações ou unidades organizacionais (UOs) 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 Saiba mais sobre o uso da AMI compartilhada no Amazon EC2. Os desenvolvedores podem cobrar por suas AMIs. Para obter mais informações, consulte AMIs pagas no AWS Marketplace para instâncias do Amazon EC2.

Tipo do volume de raiz

Todas as AMIs são categorizadas como baseadas no Amazon EBS ou baseadas no Amazon S3.

- AMI baseada no Amazon EBS: o volume raiz de uma instância iniciada com a AMI corresponde a um volume do Amazon Elastic Block Store (Amazon EBS) criado a partir de um snapshot do Amazon EBS. Compatível com as AMIs do Linux e do Windows.
- AMI baseada no Amazon S3: o volume raiz de uma instância iniciada com a AMI corresponde a um volume de armazenamento de instância criado a partir de um modelo armazenado no Amazon S3. Compatível somente com as AMIs do Linux. As AMIs do Windows não são compatíveis com o armazenamento de instância para o volume raiz.

Para obter mais informações, consulte Volumes raiz para as instâncias do Amazon EC2.

> **Note**
>
> As AMIs baseadas no Amazon S3 estão no fim da vida útil e recomendamos não as usar em novos projetos. Elas são aceitas somente nos seguintes tipos de instância mais antigos: C1, C3, D2, I2, M1, M2, M3, R3 e X1.

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

Característica	AMI baseada no Amazon EBS	AMI baseada no Amazon S3
Volume raiz	Volume do EBS	Volumes de armazenamento de instâncias
Tempo de inicialização para uma instância	Geralmente menos que 1 minuto	Geralmente menos que 5 minutos
Persistência de dados	Por padrão, o volume raiz é excluído quando a instância é encerrada.* Os dados em todos os outros volumes do EBS persistem após o encerramento da instância, por padrão.	Os dados em qualquer volume do armazenamento de instâncias persistem apenas durante a vida útil da instância.

Característica	AMI baseada no Amazon EBS	AMI baseada no Amazon S3
Estado parado	Pode estar em um estado interrompido. Mesmo quando a instância é interrompida e não está em execução, o volume-raiz persiste no Amazon EBS.	Não pode estar em um estado interrompido; as instâncias estão em execução ou foram encerradas.
Modificações	O tipo de instância, o kernel, o disco da RAM e os dados do usuário podem ser alterados enquanto a instância está parada.	Os atributos de instância são fixos durante a vida útil de uma instância.
Cobranças	Você é cobrado pelo uso de instância, uso de volume do EBS; e pelo armazenamento da AMI como um snapshot do EBS.	Você é cobrado pelo uso da instância e pelo armazenamento da AMI no Amazon S3.
Criação/empacotamento da AMI	Usa um único comando/chamada	Requer instalação e uso de ferramentas de AMI

* Por padrão, os volumes raiz do EBS têm o sinalizador `DeleteOnTermination` definido como `true`. Para obter informações sobre como alterar esse sinalizador para que o volume persista depois do encerramento, consulte Manter um volume raiz do Amazon EBS após o encerramento de uma instância do Amazon EC2.

** Compatível apenas com `io2` EBS Block Express. Para obter mais informações, consulte Volumes SSD do Block Express com IOPS provisionadas no Guia do usuário do Amazon EBS.

Identificação do tipo de volume raiz determinado pela AMI

A AMI que você usa para executar uma instância do EC2 determina o tipo de volume raiz. O volume raiz de uma instância do EC2 é um volume do EBS ou um volume de armazenamento de instância.

Instâncias baseadas em Nitro são compatíveis somente com volumes raiz do EBS. Os seguintes tipos de instância de geração anterior são os únicos tipos de instância compatíveis com volumes raiz de armazenamento de instância: C1, C3, D2, I2, M1, M2, M3, R3 e X1.

Console

Para identificar o tipo de volume raiz determinado por uma AMI

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha AMIs e, em seguida, selecione a AMI.
3. Na guia Details (Detalhes), marque o valor de Root Device Type (Tipo de dispositivo raiz) da seguinte maneira:
   - `ebs`: instâncias iniciadas usando esta AMI receberão um volume raiz do EBS.
   - `instance store`: instâncias iniciadas usando esta AMI receberão um volume raiz de armazenamento de instância.

AWS CLI

Para identificar o tipo de volume raiz determinado por uma AMI

Use o comando describe-images.

```
aws ec2 describe-images \
    --image-ids ami-0abcdef1234567890 \
    --query Images[].RootDeviceType
```

O seguinte é um exemplo de saída.

```
ebs
```

PowerShell

Para identificar o tipo de volume raiz determinado por uma AMI

Use o cmdlet Get-EC2Image.

```
(Get-EC2Image `
    -ImageId ami-0abcdef1234567890).RootDeviceType.Value
```

O seguinte é um exemplo de saída.

```
ebs
```

Tipos de virtualização

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

A tabela a seguir compara AMIs de HVM e PV.

Característica	HVM	PV
Descrição	As AMIs HVM são apresentadas com um conjunto totalmente virtualizado de hardware e inicialização ao executar o registro de inicialização mestre do dispositivo de blocos raiz da sua imagem. Esse tipo de virtualização permite a execução de um sistema operacional diretamente em uma máquina virtual, sem qualquer modificação, como se tivesse sido executada em hardware bare metal. O sistema do host Amazon EC2 emula algum ou todos os hardwares subjacentes apresentados ao guest.	As AMIs PV são inicializadas com um bootloader especial chamado PV-GRUB, que começa o ciclo de inicialização e encadeia e carrega o kernel especificado no arquivo `menu.lst` da sua imagem. Os convidados paravirtuais podem ser executados em hardware de host que não é explicitamente compatível para virtualização. Para obter mais informações sobre o PV-GRUB e seu uso no Amazon EC2, consulte User provided kernels.
Tipos de instâncias compatíveis	Todos os tipos de instância da geração atual são compatíveis com AMIs HVM.	Os seguintes tipos de instância da geração anterior são compatíveis com AMIs

Característica	HVM	PV
		PV: C1, C3, M1, M3, M2 e T1. Os tipos de instância da geração atual não são compatíveis com AMIs PV.
Suporte para extensões de hardware	Os guests HVM podem aproveitar as extensões de hardware que fornecem acesso rápido ao hardware subjacente no sistema host. Eles são necessários para usar rede aperfeiçoada e processamento de GPU. Para passar instruções à rede especializada e aos dispositivos de GPU, o SO precisa ter acesso à plataforma de hardware nativa; a virtualização de HVM fornece esse acesso. Para obter mais informações, consulte Redes aperfeiçoadas para instâncias do Amazon EC2.	Não, eles não podem se beneficiar de extensões de hardware especiais, como rede aperfeiçoada ou processamento de GPU.
Como encontrar	Verifique se o tipo de virtualização da AMI está definido como `hvm` usando o console ou o comando describe-images.	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 performance no armazenamento e na E/S de rede usando-os. Com esses drivers de PV em HVM, os convidados recebem performance igual, ou melhor, que os guests paravirtuais.

Encontrar uma AMI que atenda aos requisitos da instância do EC2

Uma AMI inclui os componentes e as aplicações, como o sistema operacional e o tipo de volume raiz, necessários para iniciar uma instância. Para executar uma instância, você precisa encontrar uma AMI atenda às suas necessidades.

Ao selecionar uma AMI, considere os seguintes requisitos que você pode ter para as instâncias que deseja iniciar:

- A região da AWS da AMI já que os IDs da AMI são exclusivos de cada região.
- O sistema operacional (por exemplo, Linux ou Windows).
- A arquitetura (por exemplo, 32 bits, 64 bits ou ARM de 64 bits).
- O tipo de volume raiz (por exemplo, Amazon EBS ou armazenamento de instância).
- O provedor (por exemplo, Amazon Web Services).
- Software adicional (por exemplo, SQL Server).

Console

É possível selecionar uma AMI da lista ao usar o assistente de inicialização de instâncias, ou pesquisar todas as AMIs disponíveis usando a página Imagens.

Como encontrar uma AMI do Quick Start usando o assistente de inicialização de instâncias

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. Os IDs da AMI são exclusivos de cada região da AWS.
3. No painel do console, selecione Launch instance (Executar instância).
4. Em Application and OS Images (Amazon Machine Image) (Imagens de aplicações e SO [imagem de máquina da Amazon]), escolha Quick Start (Início rápido), escolha o sistema

operacional (SO) para sua instância e, em Amazon Machine Image (AMI) (Imagem de máquina da Amazon [AMI]), selecione uma das AMIs mais usadas na lista. Caso não veja a AMI que deseja usar, escolha Browse more AMIs (Pesquisar mais AMIs) para navegar pelo catálogo completo de AMIs. Para obter mais informações, consulte Imagens de aplicações e sistemas operacionais (imagem de máquina da Amazon).

Para encontrar uma AMI usando a página de AMIs

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. Os IDs da AMI são exclusivos de cada região da AWS.
3. No painel de navegação, selecione AMIs.
4. (Opcional) Use as opções de filtro e pesquisa para restringir o escopo da lista de AMIs exibidas e ver somente as AMIs correspondentes ao seu critério.

   Por exemplo, para listar todas as AMIs fornecidas pela AWS, escolha Imagens públicas. Em seguida, use as opções de pesquisa para aumentar o escopo da lista de AMIs exibidas. Escolha a barra de Pesquisa e, no menu, escolha Owner alias (Alias do proprietário), depois o operador = e, em seguida, o valor amazon. Para encontrar AMIs que correspondam a uma plataforma específica, por exemplo, Linux ou Windows, escolha novamente a barra Pesquisar para escolher Plataforma, depois o operador = e, em seguida, o sistema operacional na lista fornecida.
5. (Opcional) Escolha o ícone Preferências para definir quais atributos da imagem serão exibidos, como o tipo do volume raiz. Como alternativa, é possível selecionar uma AMI na lista e visualizar suas propriedades na guia Details (Detalhes).
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 Tipo do volume de raiz.
7. Para iniciar uma instância a partir dessa AMI, selecione-a e escolha Iniciar instância a partir da imagem. Para obter informações sobre como iniciar uma instância usando o console, consulte Executar uma instância do EC2 usando o assistente de inicialização de instâncias no console. Se você não estiver pronto para executar a instância agora, anote o ID da AMI para consultar depois.

AWS CLI

Use o comando describe-images para encontrar uma AMI que atenda aos seus requisitos. Por padrão, esse comando retorna todas as AMIs públicas, de sua propriedade e compartilhadas com você.

Para encontrar uma AMI de propriedade da Amazon

Use o comando describe-images com a opção `--owners`.

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

Para encontrar uma AMI do Windows

Adicione o seguinte filtro para exibir somente AMIs do Windows.

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

Para encontrar uma AMI baseada no EBS

Adicione o seguinte filtro para exibir somente AMIs baseadas no Amazon EBS.

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

PowerShell

Use o cmdlet Get-EC2Image para encontrar uma AMI que atenda aos seus requisitos. Por padrão, esse cmdlet retorna todas as AMIs públicas, de sua propriedade ou compartilhadas com você.

Para encontrar uma AMI de propriedade da Amazon

Use o comando Get-EC2Instance com o parâmetro `-Owner`.

```
Get-EC2Image -Owner amazon
```

Para encontrar uma AMI do Windows

Adicione o seguinte filtro para exibir somente AMIs do Windows.

```
-Filter @{Name="platform"; Values="windows"}
```

Para mais exemplos, consulte Find an Amazon Machine Image Using Windows PowerShell no Guia do usuário do AWS Tools for PowerShell.

Recursos relacionados

Para obter mais informações sobre AMIs para um sistema operacional específico, consulte o seguinte:

- Amazon Linux 2023: AL2023 on Amazon EC2 no Guia do usuário do Amazon Linux 2023
- Ubuntu: Amazon EC2 AMI Locator no site sobre o Ubuntu da Canonical
- RHEL: Red Hat Enterprise Linux Images (AMI) Available on Amazon Web Services (AWS) no site da Red Hat
- Windows Server: Referência da AMI do Windows da AWS

Para obter informações sobre AMIs que você pode assinar no AWS Marketplace, consulte AMIs pagas no AWS Marketplace para instâncias do Amazon EC2.

Para obter informações sobre como usar o Systems Manager para ajudar seus usuários a encontrar a AMI mais recente que devem usar ao iniciar uma instância, consulte o seguinte:

- Referência às AMIs usando parâmetros do Systems Manager
- Referência às AMIs mais recentes usando parâmetros públicos do Systems Manager

Referência às AMIs usando parâmetros do Systems Manager

Quando você inicia uma instância usando o assistente de inicialização de instâncias do EC2 no console do Amazon EC2, pode selecionar uma AMI da lista ou selecionar um parâmetro do AWS Systems Manager que aponta para um ID de AMI (descrito nesta seção). Se usar o código de automação para executar as instâncias, será possível especificar o parâmetro do Systems Manager em vez do ID de AMI.

Um parâmetro do Systems Manager é um par de chave-valor definido pelo cliente que pode ser criado no repositório de parâmetros do Systems Manager. O repositório de parâmetros fornece um armazenamento central para externalizar os valores de configuração da aplicação. Para obter mais

informações, consulte o Parameter Store do AWS Systems Manager no Guia do usuário do AWS Systems Manager.

Ao criar um parâmetro que aponte para um ID de AMI, especifique o tipo de dado como `aws:ec2:image`. Especificar esse tipo de dado garante que, quando o parâmetro for criado, modificado ou validado, o valor dele será validado como um ID da AMI. Para obter mais informações, consulte Suporte a parâmetro nativo para IDs de imagem de máquina da Amazon no Guia do usuário do AWS Systems Manager.

Tópicos

- Casos de uso
- Permissões
- Limitações
- Executar uma instância usando um parâmetro de Systems Manager

Casos de uso

Ao usar os parâmetros do Systems Manager para apontar para IDs de AMI, é mais fácil para os usuários selecionar a AMI correta ao iniciar instâncias. Os parâmetros do Systems Manager também podem simplificar a manutenção do código de automação.

Mais fácil para os usuários

Se você precisar que as instâncias sejam iniciadas usando uma AMI específica, e se essa AMI for atualizada regularmente, recomendamos que você exija que os usuários selecionem um parâmetro do Systems Manager para localizar a AMI. Exigir que os usuários selecionem um parâmetro do Systems Manager garante que a AMI mais recente seja usada para iniciar instâncias.

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

Simplificar a manutenção do código de automação

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

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

Permissões

Se você usar parâmetros do Systems Manager que direcionem para IDs de AMI no assistente de inicialização de instâncias, deverá adicionar as seguintes permissões à política do IAM:

- `ssm:DescribeParameters`: concede permissão para visualizar e selecionar os parâmetros do Systems Manager.
- `ssm:GetParameters`: concede permissão para recuperar os valores dos parâmetros do Systems Manager.

Também é possível restringir o acesso a parâmetros específicos do Systems Manager. Para obter mais informações e exemplos de políticas do IAM, consulte Exemplo: uso do assistente de início de instância do EC2.

Limitações

As AMIs e os parâmetros do Systems Manager são específicos da região. Para usar o mesmo nome de parâmetro do Systems Manager entre regiões, crie um parâmetro do Systems Manager em cada região com o mesmo nome (por exemplo, `golden-ami`). Em cada região, aponte o parâmetro do Systems Manager para uma AMI nessa região.

Os nomes dos parâmetros diferenciam maiúsculas de minúsculas. As barras invertidas para o nome do parâmetro só são necessárias quando o parâmetro faz parte de uma hierarquia, por exemplo, `/amis/production/golden-ami`. Será possível omitir a barra invertida se o parâmetro não fizer parte de uma hierarquia.

Executar uma instância usando um parâmetro de Systems Manager

Quando você inicia uma instância, em vez de especificar um ID de AMI, pode especificar um parâmetro do Systems Manager que aponta para um ID de AMI.

Para especificar o parâmetro no programa, use a sintaxe a seguir, onde `resolve:ssm` é o prefixo padrão e `parameter-name` é o nome exclusivo do parâmetro.

```
resolve:ssm:parameter-name
```

Os parâmetros do Systems Manager são compatíveis com versão. Cada iteração de um parâmetro recebe um número de versão exclusivo. É possível referenciar a versão do parâmetro como se segue, onde `version` é o número exclusivo da versão. Por padrão, a versão mais recente do parâmetro é usada quando nenhuma versão é especificada.

```
resolve:ssm:parameter-name:version
```

Para iniciar uma instância usando um parâmetro público fornecido pela AWS, consulte Referência às AMIs mais recentes usando parâmetros públicos do Systems Manager.

Console

Para encontrar uma AMI usando um parâmetro do Systems Manager

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Na barra de navegação, selecione a região na qual executar as instâncias. Selecione qualquer região que estiver disponível para você, independentemente do seu local.
3. No painel do console, selecione Launch instance (Executar instância).
4. Em Application and OS Images (Amazon Machine Image) (Imagens de aplicações e sistemas operacionais [imagem de máquina da Amazon]), escolha Browse more AMIs (Procurar mais AMIs).
5. Escolha o botão de seta à direita da barra de pesquisa e escolha Search by Systems Manager parameter (Pesquisar por parâmetro do Systems Manager).
6. Em Systems Manager parameter (Parâmetro do Systems Manager), selecione um parâmetro. O ID da AMI correspondente é exibido abaixo de Currently resolves to (Resolve atualmente para).
7. Escolha Pesquisar. As AMIs correspondentes ao ID da AMI são exibidas na lista.

8. Selecione a AMI na lista e escolha Select (Selecionar).

Para obter mais informações sobre como iniciar uma instância usando o assistente de inicialização de instância, consulte Executar uma instância do EC2 usando o assistente de inicialização de instâncias no console.

AWS CLI

Para iniciar uma instância usando um parâmetro de Systems Manager

Use o comando run-instances com a opção `--image-id`. Este exemplo usa um parâmetro do Systems Manager denominado **`golden-ami`**, que especifica um ID de AMI.

```
--image-id resolve:ssm:/golden-ami
```

É possível criar versões de um parâmetro do Systems Manager. O exemplo a seguir especifica a versão 2 do parâmetro **`golden-ami`**.

```
--image-id resolve:ssm:/golden-ami:2
```

PowerShell

Para iniciar uma instância usando um parâmetro de Systems Manager

Use o cmdlet New-EC2Instance com o parâmetro `-ImageId`. Este exemplo usa um parâmetro do Systems Manager denominado **`golden-ami`**, que especifica um ID de AMI.

```
-ImageId "resolve:ssm:/golden-ami"
```

É possível criar versões de um parâmetro do Systems Manager. O exemplo a seguir especifica a versão 2 do parâmetro **`golden-ami`**.

```
-ImageId "resolve:ssm:/golden-ami:2"
```

Referência às AMIs mais recentes usando parâmetros públicos do Systems Manager

O AWS Systems Manager fornece parâmetros públicos para as AMIs públicas mantidas pela AWS. É possível usar os parâmetros públicos ao iniciar instâncias para garantir que está usando as AMIs

mais recentes. Por exemplo, o parâmetro público `/aws/service/ami-amazon-linux-latest/al2023-ami-kernel-default-arm64` está disponível em todas as regiões e sempre direciona para a versão mais recente da AMI do Amazon Linux 2023 para a arquitetura de arm64 em uma determinada região.

Os parâmetros públicos estão disponíveis ao usar os seguintes caminhos:

- Linux – `/aws/service/ami-amazon-linux-latest`
- Windows – `/aws/service/ami-windows-latest`

Para obter mais informações, consulte Trabalhar com parâmetros públicos no Guia do usuário do AWS Systems Manager

Listar as AMIs do Amazon Linux

AWS CLI

Para listar as AMIs do Linux na região atual da AWS

Use o seguinte comando get-parameters-by-path. O valor do parâmetro `--path` é específico para as AMIs do Linux.

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

PowerShell

Para listar as AMIs do Linux na região atual da AWS

Use o cmdlet Get-SSMParametersByPath.

```
Get-SSMParametersByPath `
    -Path "/aws/service/ami-amazon-linux-latest" | `
    Sort-Object Name | Format-Table Name
```

Listar as AMIs do Windows

AWS CLI

Para listar as AMIs do Windows na região atual da AWS

Use o seguinte comando get-parameters-by-path. O valor do parâmetro `--path` é específico para as AMIs do Windows.

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

PowerShell

Para listar as AMIs do Windows na região atual da AWS

Use o cmdlet Get-SSMParametersByPath.

```
Get-SSMParametersByPath `
    -Path "/aws/service/ami-windows-latest" | `
    Sort-Object Name | Format-Table Name
```

Iniciar uma instância usando um parâmetro público

Para especificar o parâmetro público ao iniciar uma instância, use a seguinte sintaxe: `resolve:ssm:`*`public-parameter`*, onde `resolve:ssm` é o prefixo padrão e *`public-parameter`* é o caminho e o nome do parâmetro público.

AWS CLI

Como executar uma instância usando um parâmetro público

Use o comando run-instances com a opção `--image-id`. O exemplo especifica um parâmetro público do Systems Manager para o ID da imagem com a finalidade de iniciar uma instância usando a mais nova AMI do Amazon Linux 2023

```
--image-id resolve:ssm:/aws/service/ami-amazon-linux-latest/al2023-ami-kernel-default-x86_64
```

PowerShell

Como executar uma instância usando um parâmetro público

Use o cmdlet New-EC2Instance com o parâmetro `-ImageId`. O exemplo especifica um parâmetro público do Systems Manager para o ID da imagem com a finalidade de iniciar uma instância usando a mais nova AMI do Windows Server 2022.

```
-ImageId "resolve:ssm:/aws/service/ami-windows-latest/Windows_Server-2022-English-Full-Base"
```

Para obter mais exemplos que usam parâmetros do Systems Manager, consulte Query for the latest Amazon Linux AMI IDs Using AWS Systems Manager Parameter Store e Query for the Latest Windows AMI Using AWS Systems Manager Parameter Store.

AMIs pagas no AWS Marketplace para instâncias do Amazon EC2

Uma AMI paga é uma AMI que está listada para venda no AWS Marketplace. O AWS Marketplace é uma loja online na qual é possível adquirir o software executado na AWS, incluindo as AMIs usadas na execução da instância do EC2. As AMIs do AWS Marketplace são organizadas em categorias, como Ferramentas para desenvolvedores, o que permite que você encontre produtos para atender às suas necessidades. Para obter mais informações sobre o AWS Marketplace, consulte o site do AWS Marketplace.

É possível comprar AMIs no AWS Marketplace de terceiros, incluindo AMIs equipadas com contratos de serviço de organizações como a Red Hat. Além disso, é possível criar uma AMI e vendê-la no AWS Marketplace para outros usuários do Amazon EC2. 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 Saiba mais sobre o uso da AMI compartilhada no Amazon EC2.

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 de acordo com as taxas de uso padrão dos serviços Web relacionados, por exemplo, a taxa por hora para a execução de um tipo de instância m5.small no Amazon EC2. Taxas adicionais também podem ser cobradas. O proprietário da AMI paga pode confirmar se uma determinada instância foi executada usando essa AMI paga.

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

Conteúdo

- Vender sua AMI no AWS Marketplace
- Localizar uma AMI paga
- Comprar uma AMI paga no AWS Marketplace
- Recuperar o código do produto do AWS Marketplace da sua instância
- Usar suporte pago para as ofertas compatíveis do AWS Marketplace
- Faturas para AMI pagas e compatíveis
- Gerenciar suas assinaturas do AWS Marketplace

Vender sua AMI no AWS Marketplace

É possível vender a AMI usando o AWS Marketplace. O AWS Marketplace oferece uma experiência de compras organizada. Além disso, o AWS Marketplace também oferece suporte a recursos da AWS, como AMIs baseadas no Amazon EBS, instâncias reservadas e instâncias spot.

Para obter informações sobre como vender a AMI no AWS Marketplace, consulte Como vender no AWS Marketplace.

Localizar uma AMI paga

Uma AMI paga é uma Imagem de máquina da Amazon (AMI) que está disponível para compra. Uma AMI paga também tem um código de produto. É possível encontrar AMIs que estão disponíveis para compra no AWS Marketplace.

Console

Para encontrar uma AMI paga

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. Execute um destes procedimentos:
   - Se você souber o código do produto, escolha Product Code (Código do produto), = e depois insira o código do produto.
   - Se você não souber o código do produto, na barra de pesquisa, especifique o seguinte filtro: Owner alias=aws-marketplace. Especifique filtros adicionais conforme necessário.
5. Salve o ID da AMI.

AWS CLI

Para encontrar uma AMI paga

Use o seguinte comando describe-images.

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

A saída incluirá um grande número de imagens. É possível especificar filtros para ajudar você a determinar de qual AMI precisa. Após encontrar uma AMI, especifique seu ID no comando a seguir para obter o código do produto.

```
aws ec2 describe-images \
    --image-ids ami-0abcdef1234567890 \
    --query Images[*].ProductCodes[].ProductCodeId
```

O seguinte é um exemplo de saída.

```
[
    "cdef1234abc567def8EXAMPLE"
]
```

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 \
    --filters "Name=product-code,Values=cdef1234abc567def8EXAMPLE" \
    --query "sort_by(Images, &CreationDate)[-1].[ImageId]"
```

PowerShell

Para encontrar uma AMI paga

Use o cmdlet Get-EC2Image.

```
Get-EC2Image -Owner aws-marketplace
```

A saída incluirá um grande número de imagens. É possível especificar filtros para ajudar você a determinar de qual AMI precisa. Após encontrar uma AMI, especifique seu ID no comando a seguir para obter o código do produto.

```
(Get-EC2Image -ImageId ami-0abcdef1234567890).ProductCodes
```

O seguinte é um exemplo de saída.

```
ProductCodeId             ProductCodeType
-------------             ---------------
cdef1234abc567def8EXAMPLE 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.

```
(Get-EC2Image -Owner aws-marketplace -Filter @{"Name"="product-
code";"Value"="cdef1234abc567def8EXAMPLE"} | sort CreationDate -Descending | Select-
Object -First 1).ImageId
```

Comprar uma AMI paga no AWS Marketplace

Você deve primeiro se inscrever em (comprar) uma AMI paga para poder executar uma instância do Amazon EC2 usando a AMI.

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

Comprar uma AMI paga usando o console

É possível comprar uma AMI paga usando o assistente de execução do Amazon EC2. Para obter mais informações, consulte Executar uma instância do Amazon EC2 em uma AMI do AWS Marketplace.

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, é necessário estar cadastrado para usar o serviço Amazon EC2 e ter assinado o produto do qual iniciar a instância. É possível usar um dos seguintes métodos para se inscrever em produtos no AWS Marketplace:

- Site do AWS Marketplace: é possível executar o software pré-configurado rapidamente com o recurso de implantação de um clique. Para obter mais informações, consulte AMI-based products no AWS Marketplace.
- Assistente de execução do Amazon EC2: é possível procurar uma AMI e executar uma instância diretamente do assistente. Para obter mais informações, consulte Executar uma instância do Amazon EC2 em uma AMI do AWS Marketplace.

Recuperar o código do produto do AWS Marketplace da sua instância

Recupere o código do produto do AWS Marketplace para sua instância usando os metadados da instância. Se a instância tiver um código de produto, o Amazon EC2 o retornará. Para obter mais informações sobre como recuperar os metadados, consulte Acessar metadados de instância para uma instância do EC2.

IMDSv2

Linux

Execute o seguinte comando em sua instância Linux.

```
TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
    && curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/product-codes
```

Windows

Execute os seguintes cmdlets na sua instância Windows.

```
[string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds"
 = "21600"} `
    -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} `
    -Method GET -Uri http://169.254.169.254/latest/meta-data/product-codes
```

IMDSv1

Linux

Execute o seguinte comando em sua instância Linux.

```
curl http://169.254.169.254/latest/meta-data/product-codes
```

Windows

Execute o seguinte comando em sua instância Windows.

```
Invoke-RestMethod -Uri http://169.254.169.254/latest/meta-data/product-codes
```

Usar suporte pago para as ofertas compatíveis do AWS Marketplace

O Amazon EC2 também permite que desenvolvedores ofereçam suporte para o software (ou AMI derivadas). Os desenvolvedores podem criar produtos de suporte nos quais é possível se cadastrar para usar. Durante o cadastro no produto de suporte, o desenvolvedor oferece a você um código de produto, que é necessário 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.

Limitações

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

AWS CLI

Para associar um código de produto à sua AMI

Use o comando modify-image-attribute.

```
aws ec2 modify-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --product-codes "cdef1234abc567def8EXAMPLE"
```

PowerShell

Para associar um código de produto à sua AMI

Use o cmdlet Edit-EC2ImageAttribute.

```
Edit-EC2ImageAttribute `
    -ImageId ami-0abcdef1234567890 `
    -ProductCode "cdef1234abc567def8EXAMPLE"
```

Faturas para AMI pagas e compatíveis

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

Gerenciar suas assinaturas do AWS Marketplace

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

Verificar os detalhes da assinatura do

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 Instruções de uso para exibir as instruções específicas sobre o uso do produto, por exemplo, um nome de usuário para se conectar à instância em execução.

Cancelamento de assinaturas

> **Note**
>
> - O cancelamento de uma assinatura não encerra as instâncias executadas com essa AMI. Continuaremos cobrando suas instâncias em execução até que elas sejam encerradas. É necessário encerrar todas as instâncias executadas com a AMI para interromper o faturamento da assinatura.
> - 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 por meio do assistente de inicialização no console do Amazon EC2.

Para cancelar a assinatura do AWS Marketplace

1. Para interromper a cobrança da assinatura, certifique-se de ter encerrado todas as instâncias em execução referentes à assinatura.

   > **Warning**
   >
   > O encerramento de uma instância é permanente e irreversível.
   > Depois de encerrar uma instância, não será mais possível se conectar a ela e ela não poderá ser recuperada. Todos os volumes anexados do Amazon EBS configurados para serem excluídos no encerramento também serão excluídos permanentemente e não poderão ser recuperados. Todos os dados armazenados em volumes de armazenamento de instância serão perdidos permanentemente. Para obter mais informações, consulte Como funciona o encerramento de uma instância.
   > Antes de encerrar uma instância, certifique-se de ter feito backup de todos os dados que você precise reter após o encerramento no armazenamento persistente.

   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 Estado da instância e Encerrar (excluir) instância.

d. Quando a confirmação for solicitada, escolha Encerrar (excluir).

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.

Ciclo de vida da AMI do Amazon EC2

Uma Imagem de máquina da Amazon (AMI) é uma imagem que contém a configuração de software necessária para configurar e inicializar uma instância. Especifique uma AMI ao iniciar uma instância. É possível usar as AMIs fornecidas pela Amazon ou criar as suas próprias AMIs. A AMI deve estar localizada na Região da AWS em que você deseja iniciar a instância.

O ciclo de vida de uma AMI inclui sua criação, cópia, descontinuação, desabilitação e exclusão (cancelamento do registro).

Criar AMIs. Embora a Amazon forneça AMIs que podem ser usadas para iniciar as suas instâncias, você pode criar próprias AMIs personalizadas, de acordo com as suas necessidades. Para criar uma AMI personalizada, inicie uma instância em uma AMI existente, personalize a instância (por exemplo, instale software e defina as configurações do sistema operacional) e depois crie uma AMI na instância. Todas as personalizações da instância são salvas na nova AMI para que as instâncias iniciadas na nova AMI incluam essas personalizações.

AMIs atestáveis. Para criar uma AMI compatível com a atestação de instância do EC2, consulte AMIs atestáveis.

Copiar AMIs. É possível usar uma AMI para iniciar uma instância apenas na Região da AWS em que a AMI está localizada. Se você precisar iniciar instâncias com a mesma configuração em várias regiões, copie a AMI para as outras regiões.

Descontinuar AMIs. Para marcar uma AMI como superada ou desatualizada, você pode definir uma data de descontinuação imediata ou futura. As AMIs descontinuadas não constam das listagens de AMIs, mas os usuários e serviços podem continuar usando as AMIs descontinuadas se souberem seu ID.

Desabilitar AMIs. Para impedir temporariamente o uso de uma AMI, você pode desabilitá-la. Quando uma AMI é desabilitada, ela não pode ser usada para inicializar novas instâncias. No entanto, se você reabilitar a AMI, ela poderá ser usada para inicializar instâncias novamente. Observação: a desabilitação de uma AMI não afeta as instâncias existentes que já foram inicializadas a partir dela.

Cancelar (excluir) o registro de AMIs. Quando não precisar mais de uma AMI, será possível cancelar seu registro, evitando que ela seja usada para iniciar novas instâncias. Se a AMI atender a uma regra de retenção, ela será movida para a Lixeira, onde poderá ser restaurada antes que o período de retenção expire, depois do que será excluída permanentemente. Se não atender a nenhuma regra de retenção, ela será imediatamente excluída de modo permanente. Observe que cancelar o registro de uma AMI não afeta as instâncias que foram inicializadas na AMI.

Automatizar o ciclo de vida da AMI. É possível usar Amazon Data Lifecycle Manager para automatizar a criação, a retenção, a cópia, a defasagem e a exclusão de AMIs baseadas no Amazon EBS e seus snapshots de backup. Você também pode usar o EC2 Image Builder para automatizar a criação, o gerenciamento e a implantação das AMIs personalizadas. Para obter mais informações, consulte Automate backups with Amazon Data Lifecycle Manager no Amazon EBS User Guide e no EC2 Image Builder User Guide.

Conteúdo

- Criação de uma AMI baseada no Amazon EBS
- Criação de uma AMI baseada no Amazon S3
- Criar uma AMI do Amazon EC2 usando o Sysprep do Windows
- Copiar uma AMI do Amazon EC2
- Armazenar e restaurar uma AMI usando o S3
- Use a ancestralidade da AMI para rastrear a origem de uma AMI
- Gerenciar e monitorar o uso de AMIs
- Descontinuar uma AMI do Amazon EC2
- Desabilitar uma AMI do Amazon EC2
- Cancelar o registro de uma AMI do Amazon EC2

Criação de uma AMI baseada no Amazon EBS

É possível criar sua própria AMI baseada no Amazon EBS com uma instância do Amazon EC2 ou com o snapshot do volume raiz de uma instância do Amazon EC2.

Para criar uma AMI baseada no Amazon EBS com uma instância, comece executando uma instância usando uma AMI baseada no Amazon EBS existente. Essa AMI pode ser uma que você obteve do AWS Marketplace, criada usando VM Import/Export ou qualquer outra AMI que você possa acessar. Depois de personalizar a instância para atender aos seus requisitos específicos, crie e registre uma nova AMI. É possível usar a nova AMI para executar novas instâncias com suas personalizações.

> **Note**
>
> Para criar uma AMI compatível com a atestação de instância do EC2, consulte AMIs atestáveis.

Os procedimentos descritos abaixo funcionam para instâncias do Amazon EC2 baseada em volumes do Amazon Elastic Block Store (Amazon EBS) criptografados (incluindo o volume raiz), bem como para volumes descriptografados.

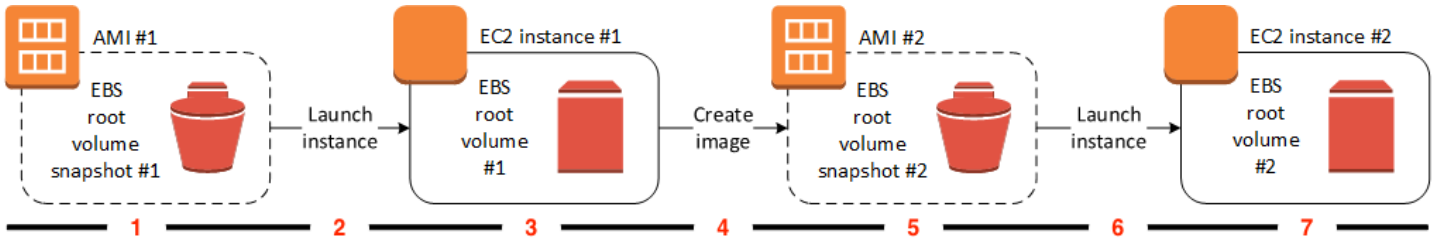
O processo de criação de AMIs é diferente para AMIs baseadas no Amazon S3. Para obter mais informações, consulte Criação de uma AMI baseada no Amazon S3.

Conteúdo

- Visão geral da criação de AMI usando uma instância
- Criação de uma AMI usando uma instância
- Criar uma AMI de um snapshot

Visão geral da criação de AMI usando uma instância

O diagrama a seguir resume o processo de criação de uma AMI baseada no Amazon EBS a partir de uma instância do EC2 em execução: comece com uma AMI existente, inicie uma instância, personalize-a, crie uma nova AMI a partir dela e, por fim, inicie uma instância de sua nova AMI. Os números no diagrama correspondem aos números na descrição a seguir.



1 – AMI #1: comece com uma AMI existente

Encontre uma AMI existente semelhante à AMI que você deseja criar. Pode ser uma AMI que você obteve do AWS Marketplace, uma AMI que você criou usando VM Import/Export ou qualquer outra AMI que você possa acessar. Você personalizará essa AMI para suas necessidades.

No diagrama, EBS root volume snapshot #1 (Snapshot do volume raiz do EBS #1) indica que a AMI é uma AMI baseada no Amazon EBS e que as informações sobre o volume raiz são armazenadas neste snapshot.

2 – iniciar instância a partir da AMI existente

A maneira de configurar uma AMI é iniciar uma instância a partir da AMI na qual você gostaria de basear sua nova AMI e, em seguida, personalizar a instância (indicado em 3 no diagrama). Em seguida, você vai criar uma nova AMI que inclua as personalizações (indicado em 4 no diagrama).

3 – instância do EC2 #1: personalize a instância

Conecte-se à sua instância e personalize-a para suas necessidades. Sua nova AMI incluirá essas personalizações.

É possível executar qualquer uma destas ações em sua instância para personalizá-la:

- Instalar o software e aplicações
- Copiar dados
- Reduzir o tempo de inicialização excluindo arquivos temporários e desfragmentando o disco rígido
- Anexar volumes adicionais do EBS

4 – Crie a imagem

Quando você cria uma AMI a partir de uma instância, 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. Se qualquer volume anexado à instância estiver criptografado, a nova AMI só será iniciada com êxito em instâncias com suporte para a criptografia do Amazon EBS.

Dependendo do tamanho dos volumes, pode levar vários minutos para que o processo de criação da AMI se complete (às vezes até 24 horas). É possível achar mais eficiente 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.)

5 – AMI #2: nova AMI

Após a conclusão do processo, você terá novos AMI e snapshot (snapshot #2) criados a partir do volume raiz da instância. Se você adicionou volumes de armazenamento de instância ou volumes do EBS à instância, além do volume raiz, o mapeamento de dispositivos de blocos para a nova AMI conterá informações sobre esses volumes.

O Amazon EC2 registra automaticamente a AMI para você.

6 – inicie uma instância a partir da nova AMI

É possível usar a nova AMI para iniciar uma instância.

7 – instância do EC2 #2: nova instância

Quando você inicia uma instância usando a nova AMI, o Amazon EC2 cria um novo volume do EBS para o volume raiz da instância usando o snapshot. Se você adicionou volumes de armazenamento de instância ou volumes do EBS ao personalizar a instância, 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 iniciadas usando a nova AMI também incluirão, de forma automática, informações sobre esses volumes. Os volumes de armazenamento de instâncias especificados no mapeamento de dispositivos de blocos para a nova instância são novos e não contêm dados dos volumes de armazenamento de instâncias da instância usada para criar a AMI. Os dados nos volumes do EBS persistem. Para obter mais informações, consulte Mapeamento de dispositivos de blocos para volumes em instâncias do Amazon EC2.

Ao criar uma nova instância de uma AMI com suporte do EBS, é necessário inicializar o volume raiz todo o armazenamento adicional EBS antes de colocá-lo em produção. Para obter mais informações, consulte Inicializar volumes do Amazon EBS no Guia do usuário do Amazon EBS.

Criação de uma AMI usando uma instância

Caso já tenha uma instância, você pode criar uma AMI dela.

Console

Criar uma AMI

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 da qual a AMI será criada e escolha Actions (Ações), Image and templates (Imagem e modelos), Create image (Criar imagem).

   > **Tip**
   >
   > Se essa opção está desabilitada, sua instância não é uma instância baseada no Amazon EBS.

4. Na página Create image (Criar imagem), especifique as seguintes informações:

   a. Em Image name (Nome da imagem), insira um nome exclusivo para a imagem com até 127 caracteres.

   b. Em Image description (Descrição da imagem), insira uma descrição opcional da imagem, com até 255 caracteres.

   c. Em Reinicializar instância, mantenha a caixa de seleção marcada (o padrão) ou desmarque-a.

      - Se Reinicializar instância estiver desmarcado, quando o Amazon EC2 criar a nova AMI, ele reinicializará a instância para que ela possa obter snapshots dos volumes anexados enquanto os dados estiverem em repouso, a fim de garantir um estado consistente.
      - Se Inicializar instância estiver desmarcado, quando o Amazon EC2 criar a nova AMI, ele não fechará e reinicializará a instância.

> **Warning**
>
> Se você desmarcar Inicializar instância, não poderemos garantir a integridade do sistema de arquivos da imagem criada.

d. Volumes da instância: você pode modificar o volume raiz e adicionar volumes do Amazon EBS e volumes com armazenamento de instância, como mostrado a seguir:

   i. O volume raiz é definido na primeira linha.

      - Para alterar o tamanho do volume raiz, em Size (Tamanho), insira o valor necessário.
      - Se você selecionar Delete on Termination (Excluir ao encerrar), quando encerrar a instância criada a partir desta AMI, o volume do EBS será excluído. Se você não selecionar Delete on Termination (Excluir ao encerrar), quando encerrar a instância, o volume do EBS não será excluído. Para obter mais informações, consulte Preservação de dados quando uma instância for encerrada.

   ii. Para adicionar o volume do EBS; escolha Add volume (Adicionar volume) (que acrescenta uma nova linha). Em Tipo de armazenamento, escolha EBS e preencha os campos da linha. Quando você executa uma instância da nova AMI, os volumes adicionais são anexados automaticamente à instância. Os volumes vazios devem ser formatados e montados. Os volumes baseados em um snapshot devem ser montados.

   iii. Para adicionar um volume de armazenamento de instância, consulte Adicionar volumes de armazenamento de instância a uma AMI do Amazon EC2. 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.

e. Destino do snapshot: se os volumes da instância estiverem em uma zona local que seja compatível com snapshots locais do EBS, escolha onde criar os snapshots da AMI:

   - Região da AWS: crie snapshots na região principal da zona local dos volumes.
   - Zona local da AWS: crie snapshots na mesma zona local dos volumes.

> **Note**
>
> Essa opção aparece somente em zonas locais compatíveis com snapshots locais do EBS e apenas se a instância foi criada em uma zona local. Se o volume estiver em uma região, essa opção não aparecerá e o snapshot será criado automaticamente na mesma região que o volume. Para obter mais informações, consulte Local snapshots in Local Zones no Guia do usuário do Amazon EBS.

> **Important**
>
> Todos os snapshots dos volumes da instância devem estar no mesmo local. Verifique a localização dos snapshots existentes. Se algum snapshot existente estiver em um local diferente do destino selecionado, a criação da AMI falhará.

f. Tags: é possível marcar a AMI e os snapshots com as mesmas tags ou pode marcá-los com tags diferentes.

- Para marcar a AMI e os snapshots com as mesmas tags, escolha Tag image and snapshots together (Marcar Imagem e snapshots juntos). As mesmas tags são aplicadas à AMI e a cada snapshot criado.
- Para marcar a AMI e os snapshots com tags diferentes, escolha Tag image and snapshots separately (Marcar imagem e snapshots separadamente). Diferentes tags são aplicadas à AMI e aos snapshots criados. No entanto, todos os snapshots obtêm as mesmas tags; não é possível marcar cada snapshot com uma tag diferente.

(Opcional) Para adicionar uma tag, escolha Add tag (Adicionar tag) e digite a chave e o valor da tag. Repita esse procedimento para cada tag.

g. Quando você estiver pronto para criar a AMI, escolha Create image (Criar imagem).

5. Para visualizar o status da AMI enquanto ela estiver sendo criada:

a. No painel de navegação, selecione AMIs.

b. Defina o filtro como Owned by me (De minha propriedade) e encontre a AMI na lista.

Inicialmente, o status será `pending`, mas deverá mudar para `available` após alguns minutos.

6. (Opcional) Para visualizar o snapshot que foi criado para a nova AMI:

   a. Anote o ID da AMI que você localizou na etapa anterior.

   b. No painel de navegação, escolha Snapshots.

   c. Defina o filtro como Owned by me (De minha propriedade) e, em seguida, localize o snapshot da novo ID da AMI na coluna Description (Descrição).

      Ao iniciar uma instância com essa AMI, o Amazon EC2 usa esse snapshot para criar o volume raiz da instância.

AWS CLI

Criar uma AMI

Use o comando create-image.

```
aws ec2 create-image \
    --instance-id i-1234567890abcdef0 \
    --name "my-web-server" \
    --description "My web server image" \
    --no-reboot
```

PowerShell

Criar uma AMI

Use o cmdlet New-EC2Image.

```
New-EC2Image `
    -InstanceId i-1234567890abcdef0 `
    -Name "my-web-server" `
    -Description "My web server image" `
    -NoReboot $true
```

Criar uma AMI de um snapshot

Caso você tenha um snapshot do volume raiz de uma instância, será possível criar uma AMI usando esse snapshot.

> **Note**
>
> Na maioria dos casos, as AMIs para Windows, Red Hat, SUSE e SQL Server exigem que as informações corretas de licenciamento estejam presentes na AMI. Para obter mais informações, consulte Noções básicas sobre as informações de faturamento da AMI. Ao criar uma AMI de um snapshot, a operação `RegisterImage` obtém as informações de faturamento corretas dos metadados do snapshot, mas isso exige que os metadados apropriados estejam presentes. Para verificar se as informações de cobrança corretas foram aplicadas, verifique o campo Detalhes da plataforma na nova AMI. Se o campo estiver vazio ou não corresponder ao código esperado do sistema operacional (por exemplo, Windows, Red Hat, SUSE ou SQL), a criação da AMI não teve êxito e você deverá descartá-la e seguir as instruções em Criação de uma AMI usando uma instância.

Console

Criar uma AMI de um snapshot

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Snapshots.
3. Selecione o snapshot do qual a AMI será criada e escolha Actions, (Ações), Create image from snapshot (Criar imagem do snapshot).
4. Na página Criar imagem de um snapshot, especifique as seguintes informações:
   a. Em Image name (Nome da imagem), insira um nome descritivo para a imagem.
   b. Em Description (Descrição), insira uma breve descrição da imagem.
   c. Em Architecture (Arquitetura), escolha a arquitetura da imagem. Escolha i386 para 32 bits, x86_64 para 64 bits, arm64 para ARM de 64 bits ou x86_64 para macOS de 64 bits.
   d. Em Nome do dispositivo raiz, insira o nome do dispositivo que será usado para o volume raiz. Para obter mais informações, consulte Nomes de dispositivos para volumes em instâncias do Amazon EC2.

e. Em Virtualization type (Tipo de virtualização), escolha o tipo de virtualização a ser usado por instâncias iniciadas partir dessa AMI. Para obter mais informações, consulte Tipos de virtualização.

f. (Somente para virtualização paravirtual) Em Kernel ID (ID do kernel), selecione o kernel do sistema operacional para a imagem. Se você estiver usando um snapshot do volume raiz de uma instância, selecione o mesmo ID de kernel da instância original. Se não tiver certeza, use o kernel padrão.

g. (Somente para virtualização paravirtual) Ema RAM disk ID (ID do disco de RAM), selecione o disco de RAM para a imagem. Se você selecionar um kernel específico, pode precisar selecionar um disco de RAM específico com os drivers que ofereçam suporte a ele.

h. Em Modo de inicialização, escolha o modo de inicialização para a imagem ou escolha Usar padrão para que, quando uma instância for iniciada com essa AMI, ela seja inicializada com o modo de inicialização com suporte para o tipo de instância. Para obter mais informações, consulte Definir o modo de inicialização de uma AMI do Amazon EC2.

i. (Opcional) Em Mapeamentos de dispositivos de blocos, personalize o volume raiz e adicione os demais volumes de dados.

   Para cada volume, é possível especificar o tamanho, o tipo, as características de performance, o comportamento de exclusão ao término e o status da criptografia. Para o volume da raiz, o tamanho não pode ser menor do que o tamanho do snapshot. Para o tipo de volume, o SSD de uso geral `gp3` é a seleção padrão.

j. (Opcional) Em Tags, você pode adicionar uma ou mais tags à nova AMI. (Opcional) Para adicionar uma tag, escolha Add tag (Adicionar tag) e digite a chave e o valor da tag. Repita esse procedimento para cada tag.

k. Quando você estiver pronto para criar a AMI, escolha Create image (Criar imagem).

5. (Somente para Windows, Red Hat, SUSE e SQL Server) Para verificar se as informações de cobrança corretas foram aplicadas, verifique o campo Detalhes da plataforma na nova AMI. Se o campo estiver vazio ou não corresponder ao código esperado do sistema operacional (por exemplo, Windows ou Red Hat), a criação da AMI não teve êxito e você deverá descartá-la e seguir as instruções em Criação de uma AMI usando uma instância.

AWS CLI

Para criar uma AMI a partir de um snapshot usando a AWS CLI

Use o comando register-image.

```
aws ec2 register-image \
    --name my-image \
    --root-device-name /dev/xvda \
    --block-device-mappings DeviceName=/dev/
xvda,Ebs={SnapshotId=snap-0db2cf683925d191f}
```

PowerShell

Para criar uma AMI a partir de um snapshot usando o PowerShell

Use o cmdlet Register-EC2Image.

```
$block = @{SnapshotId=snap-0db2cf683925d191f}
Register-EC2Image `
    -Name my-image `
    -RootDeviceName /dev/xvda `
    -BlockDeviceMapping @{DeviceName="/dev/xvda";Ebs=$block}
```

Criação de uma AMI baseada no Amazon S3

A AMI especificada no momento da inicialização da instância define o tipo do volume raiz para a instância.

Para criar uma AMI do Linux baseada no Amazon S3, comece com uma instância iniciada a partir de uma AMI do Linux baseada no Amazon S3 existente. Depois de personalizar a instância para atender às suas necessidades, empacote o volume e registre uma nova AMI, que é possível usar para executar novas instâncias com essas personalizações.

Não é possível criar uma AMI do Windows baseada no Amazon S3, já que as AMIs do Windows não permitem usar armazenamento de instância como volume raiz.

> **Important**
>
> Somente os seguintes tipos de instância são compatíveis com um volume de armazenamento de instância como volume raiz e exigem uma AMI baseada no Amazon S3: C1, C3, D2, I2, M1, M2, M3, R3 e X1.

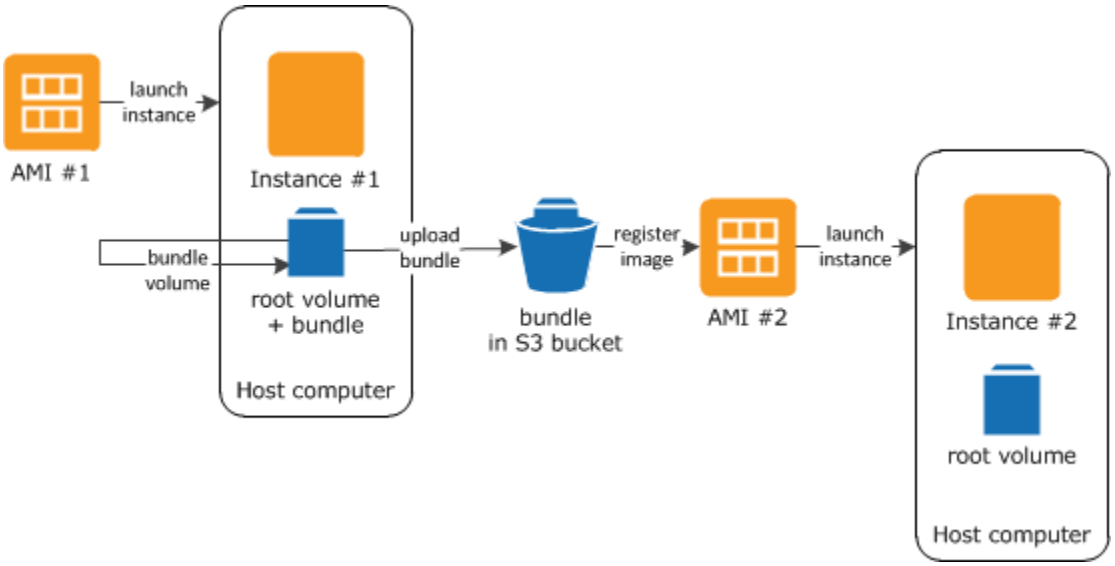
O processo de criação da AMI é diferente para AMIs baseadas no Amazon EBS. Para obter mais informações, consulte Criação de uma AMI baseada no Amazon EBS.

Conteúdo

- Visão geral da criação de uma AMI
- Pré-requisitos
- Criar uma AMI de uma instância do Linux da Amazon
- Configurar as ferramentas de AMIs do Amazon EC2
- Referência de ferramentas de AMI do Amazon EC2
- Conversão da AMI baseada no Amazon S3 em uma AMI baseada no EBS

Visão geral da criação de uma AMI

O diagrama apresentado a seguir resume o processo de criação de uma AMI usando uma instância com volume raiz de armazenamento de instância.



Primeiro, execute uma instância de uma AMI semelhante à AMI que você deseja criar. É possível conectá-la à sua instância e personalizá-la. Quando a instância estiver configurada da forma como você deseja, é possível 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.

> **Note**
>
> Para fazer upload de objetos em um bucket do S3 da AMI do Linux baseada no Amazon S3, é necessário que as ACLs estejam habilitadas no bucket. Caso contrário, o Amazon EC2 não poderá definir ACLs nos objetos a serem carregados. Se o bucket de destino usar a configuração imposta pelo proprietário do bucket para propriedade de objeto do S3, isso não funcionará, porque as ACLs estarão desabilitadas. Para obter mais informações, consulte Controlar a propriedade de objetos e desabilitar ACLs para seu bucket.

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 de uma AMI do Amazon EC2.

Se além do volume raiz, você adicionar volumes de armazenamento de instância à sua instância, o mapeamento de dispositivos de blocos da nova AMI conterá informações sobre esses volumes, e os mapeamentos de dispositivos de blocos das instâncias que você iniciar usando a nova AMI conterão automaticamente informações sobre esses volumes. Para obter mais informações, consulte Mapeamento de dispositivos de blocos para volumes em instâncias do Amazon EC2.

Pré-requisitos

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

- Instale as ferramentas da AMI. Para obter mais informações, consulte Configurar as ferramentas de AMIs do Amazon EC2.
- Instale o AWS CLI. Para obter mais informações, consulte Conceitos básicos do AWS CLI.
- Verifique se você tem um bucket do S3 para o pacote e se o bucket tem ACLs habilitadas. Para obter mais informações sobre a configuração de ACLs, consulte Configuração de ACLs.
  - Para criar um bucket do S3 usando o Console de gerenciamento da AWS, abra o console do Amazon S3 em https://console.aws.amazon.com/s3/ e escolha Criar bucket.
  - Para criar um bucket do S3 com a AWS CLI, é possível usar o comando mb. Se a versão instalada das ferramentas da AMI for 1.5.18 ou posterior, também será possível usar o comando `ec2-upload-bundle` para criar o bucket do S3. Para obter mais informações, consulte ec2-upload-bundle.

- Certifique-se de que os arquivos em seu pacote não estejam criptografados no bucket do S3. Caso precise de criptografia para sua AMI, será possível usar uma AMI baseada no EBS em vez disso. Para obter mais informações, consulte Usar criptografia com AMIs com EBS.
- Verifique se você tem seu ID de conta da AWS. Para obter mais informações, consulte Visualizar identificadores de Conta da AWS no Guia de referência de gerenciamento de contas da AWS.
- Certifique-se de ter credenciais para usar o AWS CLI. Para obter mais informações, consulte Credenciais de acesso e autenticação para o AWS CLI no Guia do usuário do AWS Command Line Interface.
- Verifique se você tem um certificado x.509 e a chave privada correspondente.
  - Se você precisar criar um certificado X.509, consulte Gerenciar certificados de assinatura. 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, é possível instalar softwares e aplicações, copiar dados, excluir arquivos temporários e modificar a configuração do Linux.

Criar uma AMI de uma instância do Linux da Amazon

Os procedimentos apresentados a seguir explicam como criar uma AMI usando uma instância com um volume raiz de armazenamento de instância que está executando o Amazon Linux 1. Eles podem não funcionar para instâncias em execução em outras distribuições do Linux.

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 usando uma instância do Amazon Linux com volume raiz de armazenamento de instância

Este procedimento pressupõe que você atendeu aos pré-requisitos de Pré-requisitos.

Nos comandos a seguir, substitua cada *espaço reservado para entrada do usuário* por suas próprias informações.

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. 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, é possível 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 em 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, associar e montar um novo volume do Amazon EBS para armazenar o pacote. Para obter mais informações, consulte Criar um volume do Amazon EBS no Guia do usuário do Amazon EC2.

a. Execute o comando ec2-bundle-vol como raiz. Na maioria dos comandos, é possível usar sudo para ganhar permissões elevadas, mas neste caso, é necessário 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 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.

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 para volumes em instâncias do Amazon EC2.

a. Crie um backup do seu arquivo `image.manifest.xml`.

```
[ec2-user ~]$ sudo cp /tmp/image.manifest.xml /tmp/image.manifest.xml.bak
```

b. Reformate o arquivo `image.manifest.xml` para que seja mais fácil ler e editar.

```
[ec2-user ~]$ sudo xmllint --format /tmp/image.manifest.xml.bak > /tmp/
image.manifest.xml
```

c. Edite os mapeamentos de dispositivos de blocos em `image.manifest.xml` com um editor de texto. O exemplo abaixo mostra uma nova entrada para o volume do armazenamento de instâncias `ephemeral1`.

> **Note**
>
> Para obter uma lista dos arquivos excluídos, consulte ec2-bundle-vol.

```
<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 da seguinte forma.

```
[ec2-user ~]$ ec2-upload-bundle -b amzn-s3-demo-bucket/bundle_folder/bundle_name -
m /tmp/image.manifest.xml -a your_access_key_id -s your_secret_access_key
```

> **Important**
>
> Para registrar a AMI em uma região diferente de US East (N. Virginia), é preciso especificar tanto a região de destino com a opção `--region` quanto um caminho do bucket que já exista na região de destino, ou um caminho de bucket exclusivo que possa ser criado na região de destino.

5. (Opcional) Depois de o pacote ser carregado para o Amazon S3, é possível 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, 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 amzn-s3-demo-
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, especifique essa região novamente para esse comando.

Configurar as ferramentas de AMIs do Amazon EC2

Você pode usar as ferramentas da AMI para criar e gerenciar AMIs do Linux baseadas no Amazon S3. Para usar as ferramentas, é necessário 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.

```
[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.

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

Para configurar as ferramentas da AMI usando o arquivo .zip

1. Instale o Ruby e descompacte usando o gerenciador de pacotes para sua distribuição do Linux, como apt-get. Por exemplo:

```
[ec2-user ~]$ sudo apt-get update -y && sudo apt-get install -y ruby unzip
```

2. Baixe o arquivo .zip usando uma ferramenta como wget ou curl. Por exemplo:

```
[ec2-user ~]$ wget https://s3.amazonaws.com/ec2-downloads/ec2-ami-tools.zip
```

3. Descompacte os arquivos em um diretório de instalação apropriado, como `/usr/local/ec2`.

```
[ec2-user ~]$ sudo mkdir -p /usr/local/ec2
$ sudo unzip ec2-ami-tools.zip -d /usr/local/ec2
```

Observe que o arquivo .zip contém uma pasta ec2-ami-tools-*x.x.x*, em que *x.x.x* é o número da versão das ferramentas (por exemplo, `ec2-ami-tools-1.5.7`).

4. Ajuste a variável de ambiente `EC2_AMITOOL_HOME` para o diretório de instalação para as ferramentas. Por exemplo:

```
[ec2-user ~]$ export EC2_AMITOOL_HOME=/usr/local/ec2/ec2-ami-tools-x.x.x
```

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

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

6. É possível verificar a instalação das suas ferramentas da AMI usando o comando ec2-ami-tools-version.

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

Gerenciar certificados de assinatura

Determinados comandos nas ferramentas da AMI exigem a assinatura de um certificado (também conhecido como certificado X.509). É necessário criar o certificado e, então, carregá-lo para a AWS. Por exemplo, é possível usar uma ferramenta de terceiros, como OpenSSL, para criar o certificado.

Para criar um certificado de assinatura

1. Instale e configure o OpenSSL.
2. Crie uma chave privada usando o comando `openssl genrsa` e salve a saída em um arquivo `.pem`. Recomendamos que você crie uma chave RSA de 2048 ou 4096 bits.

   ```
   openssl genrsa 2048 > private-key.pem
   ```
3. Gere um certificado usando o comando `openssl req`.

   ```
   openssl req -new -x509 -nodes -sha256 -days 365 -key private-key.pem -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 0FHPLP4ZULTHYPMSYEX704BEXAMPLE
```

Referência de ferramentas de AMI do Amazon EC2

É possível usar os comandos das ferramentas da AMI para criar e gerenciar AMIs do Linux baseadas no Amazon S3. Para configurar as ferramentas, consulte Configurar as ferramentas de AMIs do Amazon EC2.

Para obter mais informações sobre as chaves de acesso, consulte Gerenciamento de chaves de acesso de usuários do IAM no Guia do usuário do IAM.

Comandos

- ec2-ami-tools-version
- ec2-bundle-image
- ec2-bundle-vol
- ec2-delete-bundle
- ec2-download-bundle
- ec2-migrate-manifest
- ec2-unbundle
- ec2-upload-bundle
- Opções comuns de ferramentas da AMI

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

Cria uma AMI do Linux baseada no Amazon S3 usando uma imagem do sistema operacional gerada em um arquivo 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.

Obrigatório: sim

`-k, --privatekey` path

O caminho para um arquivo de chave RSA codificado por PEM. Será necessário especificar essa chave para desfazer esse pacote e, assim, mantê-lo em um lugar seguro. Observe que a chave não precisa estar registrada na conta da AWS.

Obrigatório: sim

`-u, --user` account

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

Obrigatório: sim

`-i, --image` path

O caminho até imagem para fazer o pacote.

Obrigatório: sim

`-d, --destination` path

O diretório no qual o pacote deve ser criado.

Padrão: `/tmp`

Exigido: Não

`--ec2cert` path

O caminho até o certificado de chave pública X.509 do Amazon EC2 usado para criptografar o manifesto da imagem.

As regiões `us-gov-west-1` e `cn-north-1` usam um certificado de chave pública não padrão e o caminho para esse certificado deve ser especificado com essa opção. O caminho para o certificado varia de acordo com o método de instalação das ferramentas da AMI. Para o Amazon Linux, os certificados estão localizados em `/opt/aws/amitools/ec2/etc/ec2/amitools/`. Se você tiver instalado as ferramentas da AMI do arquivo RPM ou ZIP em Configurar as ferramentas de AMIs do Amazon EC2, os certificados estarão localizados em `$EC2_AMITOOL_HOME/etc/ec2/amitools/`.

Obrigatório: apenas para as regiões `us-gov-west-1` e `cn-north-1`.

`-r, --arch` architecture

Arquitetura da imagem. Se você não tiver fornecido a arquitetura na linha de comando, ela será solicitada quando o empacotamento for iniciado.

Valores válidos: `i386` | `x86_64`

Exigido: Não

`--productcodes` code1,code2,...

Os códigos de produto para associar à imagem no momento do registro, separado por vírgulas.

Exigido: Não

`-B, --block-device-mapping` mapping

Define como dispositivos de blocos são expostos a uma instância dessa AMI, caso esse tipo de instância seja compatível com o dispositivo especificado.

Especifique uma lista separada por vírgulas de pares de valor-chave, nos quais cada chave é um nome virtual e cada valor é o nome do dispositivo correspondente. Os nomes virtuais incluem o seguinte:

- `ami` — o dispositivo do sistema de arquivos raiz, como visto pela instância
- `root` — o dispositivo do sistema de arquivos raiz, como visto pelo kernel
- `swap` — o dispositivo de troca, como visto pela instância
- `ephemeralN` — o enésimo volume de armazenamento de instâncias

Exigido: Não

`-p, --prefix` prefix

O prefixo do nome dos arquivos de AMI em pacote.

Padrão: O nome de arquivo de imagem. Por exemplo: se o caminho da imagem for `/var/spool/my-image/version-2/debian.img`, o prefixo padrão será `debian.img`.

Exigido: Não

`--kernel` kernel_id

Suspenso. Use register-image para configurar o kernel.

Exigido: Não

`--ramdisk` ramdisk_id

Suspenso. Use register-image para configurar o disco RAM, se necessário.

Obrigatório: 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 do Linux baseada no Amazon S3 ao compactar, criptografar e assinar uma cópia do volume 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 baseada no Amazon S3.

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.

Obrigatório: sim

`-k, --privatekey` path

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

Obrigatório: sim

`-u, --user` account

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

Obrigatório: sim

`-d, --destination` destination

O diretório no qual o pacote deve ser criado.

Padrão: `/tmp`

Exigido: Não

`--ec2cert` path

O caminho até o certificado de chave pública X.509 do Amazon EC2 usado para criptografar o manifesto da imagem.

As regiões `us-gov-west-1` e `cn-north-1` usam um certificado de chave pública não padrão e o caminho para esse certificado deve ser especificado com essa opção. O caminho para o certificado varia de acordo com o método de instalação das ferramentas da AMI. Para o Amazon Linux, os certificados estão localizados em `/opt/aws/amitools/ec2/etc/ec2/amitools/`. Se você tiver instalado as ferramentas da AMI do arquivo RPM ou ZIP em Configurar as ferramentas de AMIs do Amazon EC2, 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.

Obrigatório: 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 '/'

Obrigatório: sim

`-a, --access-key` access_key_id

O ID da chave de acesso da AWS.

Obrigatório: sim

`-s, --secret-key` secret_access_key

A chave de acesso secreta da AWS.

Obrigatório: sim

`-t, --delegation-token` token

O token de delegação para repassar à solicitação da AWS. Para obter mais informações, consulte Credenciais de segurança temporárias no Guia do usuário do IAM.

Obrigatório: Somente quando você usar credenciais temporárias de segurança.

Padrão: O valor da variável de ambiente `AWS_DELEGATION_TOKEN` (se definida).

`--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`*versão*

A versão da assinatura a ser usada ao assinar a solicitação.

Valores válidos: `2` | `4`

Padrão: `4`

Exigido: Não

`-m, --manifest`*path*

O caminho até o arquivo manifesto.

Obrigatório: Especifique `--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: Especifique `--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.

Obrigatório: 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 amzn-s3-demo-bucket -a your_access_key_id -
s your_secret_access_key
Deleting files:
amzn-s3-demo-bucket/image.manifest.xml
amzn-s3-demo-bucket/image.part.00
amzn-s3-demo-bucket/image.part.01
amzn-s3-demo-bucket/image.part.02
amzn-s3-demo-bucket/image.part.03
amzn-s3-demo-bucket/image.part.04
amzn-s3-demo-bucket/image.part.05
amzn-s3-demo-bucket/image.part.06
Continue? [y/n]
y
Deleted amzn-s3-demo-bucket/image.manifest.xml
Deleted amzn-s3-demo-bucket/image.part.00
Deleted amzn-s3-demo-bucket/image.part.01
Deleted amzn-s3-demo-bucket/image.part.02
Deleted amzn-s3-demo-bucket/image.part.03
Deleted amzn-s3-demo-bucket/image.part.04
Deleted amzn-s3-demo-bucket/image.part.05
Deleted amzn-s3-demo-bucket/image.part.06
ec2-delete-bundle complete.
```

ec2-download-bundle

Descrição

Realiza download das AMIs do Linux baseadas no Amazon S3 especificadas usando o 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 '/'.

Obrigatório: sim

`-a, --access-key` access_key_id

O ID da chave de acesso da AWS.

Obrigatório: sim

`-s, --secret-key` secret_access_key

A chave de acesso secreta da AWS.

Obrigatório: sim

`-k, --privatekey` path

A chave privada usada para descriptografar o manifesto.

Obrigatório: sim

`--url` url

O URL do serviço Amazon S3.

Padrão: `https://s3.amazonaws.com/`

Exigido: Não

`--region` region

A região a ser usada na assinatura da solicitação.

Padrão: `us-east-1`

Obrigatório: Sim se estiver usando a assinatura versão 4

`--sigv` version

A versão da assinatura a ser usada ao assinar a solicitação.

Valores válidos: `2` | `4`

Padrão: `4`

Exigido: Não

`-m, --manifest` file

O nome do arquivo manifesto (sem o caminho). Recomendamos que você especifique o manifesto (`-m`) ou um prefixo (`-p`).

Exigido: Não

`-p, --prefix` prefix

O prefixo do nome dos arquivos de AMI em pacote.

Padrão: `image`

Exigido: Não

`-d, --directory` directory

O diretório no qual o pacote baixado é salvo. O diretório deve existir.

Padrão: O diretório de trabalho atual.

Exigido: Não

`--retry`

Tenta novamente mais uma vez todos os erros de Amazon S3, até cinco vezes por operação.

Obrigatório: 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 `amzn-s3-demo-bucket` do Amazon S3.

```
[ec2-user ~]$ mkdir bundled
[ec2-user ~]$ ec2-download-bundle -b amzn-s3-demo-bucket/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 amzn-s3-demo-bucket to mybundle/
image.manifest.xml ...
Downloading part image.part.00 from amzn-s3-demo-bucket/bundles/bundle_name to
 mybundle/image.part.00 ...
Downloaded image.part.00 from amzn-s3-demo-bucket
Downloading part image.part.01 from amzn-s3-demo-bucket/bundles/bundle_name to
 mybundle/image.part.01 ...
Downloaded image.part.01 from amzn-s3-demo-bucket
Downloading part image.part.02 from amzn-s3-demo-bucket/bundles/bundle_name to
 mybundle/image.part.02 ...
Downloaded image.part.02 from amzn-s3-demo-bucket
Downloading part image.part.03 from amzn-s3-demo-bucket/bundles/bundle_name to
 mybundle/image.part.03 ...
Downloaded image.part.03 from amzn-s3-demo-bucket
Downloading part image.part.04 from amzn-s3-demo-bucket/bundles/bundle_name to
 mybundle/image.part.04 ...
Downloaded image.part.04 from amzn-s3-demo-bucket
Downloading part image.part.05 from amzn-s3-demo-bucket/bundles/bundle_name to
 mybundle/image.part.05 ...
Downloaded image.part.05 from amzn-s3-demo-bucket
Downloading part image.part.06 from amzn-s3-demo-bucket/bundles/bundle_name to
 mybundle/image.part.06 ...
Downloaded image.part.06 from amzn-s3-demo-bucket
```

ec2-migrate-manifest

Descrição

Modifica uma AMI do Linux baseada no Amazon S3 (por exemplo, o certificado, o kernel e o disco de RAM) para que a AMI se torne compatível com 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.

Obrigatório: sim

`-k, --privatekey` path

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

Obrigatório: sim

`--manifest` path

O caminho até o arquivo manifesto.

Obrigatório: sim

`-a, --access-key` access_key_id

O ID da chave de acesso da AWS.

Obrigatório: Obrigatório se estiver usando o mapeamento automático.

`-s, --secret-key` secret_access_key

A chave de acesso secreta da AWS.

Obrigatório: Obrigatório se estiver usando o mapeamento automático.

`--region` region

A região a pesquisar no arquivo de mapeamento.

Obrigatório: Obrigatório se estiver usando o mapeamento automático.

`--no-mapping`

Desabilita o mapeamento automático de kernels e discos RAM.

Durante a migração, o Amazon EC2 substitui o kernel e o disco RAM no arquivo manifesto por um kernel e disco RAM projetados para a região de destino. A menos que o parâmetro `--no-mapping` seja fornecido, `ec2-migrate-bundle` poderá usar as operações `DescribeRegions` e `DescribeImages` para executar mapeamentos automatizados.

Obrigatório: Obrigatório se não fornecer as opções `-a`, `-s` e `--region` usadas para mapeamento automático.

`--ec2cert` path

O caminho até o certificado de chave pública X.509 do Amazon EC2 usado para criptografar o manifesto da imagem.

As regiões `us-gov-west-1` e `cn-north-1` usam um certificado de chave pública não padrão e o caminho para esse certificado deve ser especificado com essa opção. O caminho para o certificado varia de acordo com o método de instalação das ferramentas da AMI. Para o Amazon Linux, os certificados estão localizados em `/opt/aws/amitools/ec2/etc/ec2/amitools/`. Se você tiver instalado as ferramentas da AMI do arquivo ZIP em Configurar as ferramentas de AMIs do Amazon EC2, 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 User provided kernels no Amazon Linux 2 User Guide.

Obrigatório: 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 User provided kernels no Amazon Linux 2 User Guide.

Obrigatório: 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 usando uma AMI do Linux baseada no Amazon S3.

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.

Obrigatório: sim

`-m, --manifest` path

O caminho até o arquivo manifesto.

Obrigatório: sim

`-s, --source` source_directory

O diretório que contém o pacote.

Padrão: O diretório atual.

Exigido: Não

`-d, --destination` destination_directory

O diretório no qual o pacote da AMI deve ser desfeito. O diretório de destino deve existir.

Padrão: O diretório atual.

Obrigatório: 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 baseada no Amazon S3 para o Amazon S3 e define as listas de controle de acesso (ACLs) apropriadas nos objetos carregados. Para obter mais informações, consulte Criação de uma AMI baseada no Amazon S3.

> **Note**
>
> Para fazer upload de objetos em um bucket do S3 da AMI do Linux baseada no Amazon S3, é necessário que as ACLs estejam habilitadas no bucket. Caso contrário, o Amazon EC2 não poderá definir ACLs nos objetos a serem carregados. Se o bucket de destino usar a

configuração imposta pelo proprietário do bucket para propriedade de objeto do S3, isso não funcionará, porque as ACLs estarão desabilitadas. Para obter mais informações, consulte Controlar a propriedade de objetos e desabilitar ACLs para seu bucket.

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. Além disso, se o bucket não existir e a versão das ferramentas da AMI for 1.5.18 ou posterior, esse comando definirá as ACLs para o bucket.

Obrigatório: Sim

`-a, --access-key` access_key_id

Seu ID de chave de acesso da AWS.

Obrigatório: sim

`-s, --secret-key` secret_access_key

Sua chave de acesso secreta da AWS.

Obrigatório: sim

`-t, --delegation-token` token

O token de delegação para repassar à solicitação da AWS. Para obter mais informações, consulte Credenciais de segurança temporárias no Guia do usuário do IAM.

Obrigatório: Somente quando você usar credenciais temporárias de segurança.

Padrão: O valor da variável de ambiente `AWS_DELEGATION_TOKEN` (se definida).

`-m, --manifest` path

O caminho até o arquivo manifesto. O arquivo manifesto é criado durante o processo de empacotamento e pode ser localizado no diretório que contém o pacote.

Obrigatório: sim

`--url` url

Suspenso. Use a opção `--region` a menos que seu bucket esteja restrito ao local `EU` (e não `eu-west-1`). A marca `--location` é uma única forma de destinar essa restrição específica de local.

O URL do serviço de endpoint do Amazon S3.

Padrão: `https://s3.amazonaws.com/`

Exigido: Não

`--region` region

A região a ser usada na assinatura da solicitação para o bucket do S3 de destino.

- Se o bucket não existir e você não especificar uma região, a ferramenta criará o bucket sem uma restrição de local (em `us-east-1`).
- Se o bucket não existir e você especificar uma região, a ferramenta criará o bucket na região especificada.
- Se o bucket existir e você não especificar uma região, a ferramenta usará o local do bucket.
- Se o bucket existir e você especificar `us-east-1` como região, a ferramenta usará o local real do bucket sem nenhuma mensagem de erro e todos os arquivos correspondentes serão substituídos.
- Se o bucket existir e você especificar uma região (além de `us-east-1`) que não corresponde ao local real do bucket, a ferramenta sairá com um erro.

Se seu bucket estiver restrito ao local `EU` (e não `eu-west-1`), use a marca `--location`. A marca `--location` é uma única forma de destinar essa restrição específica de local.

Padrão: `us-east-1`

Obrigatório: Sim se estiver usando a assinatura versão 4

`--sigv` version

A versão da assinatura a ser usada ao assinar a solicitação.

Valores válidos: `2` | `4`

Padrão: `4`

Exigido: Não

`--acl` acl

A política de lista de controle de acesso da imagem empacotada.

Valores válidos: `public-read` | `aws-exec-read`

Padrão: `aws-exec-read`

Exigido: Não

`-d, --directory` directory

O diretório que contém as partes da AMI empacotadas.

Padrão: O diretório que contém o arquivo manifesto (veja a opção `-m`).

Exigido: Não

`--part` part

Inicia a transferência da parte especificada e de todas as partes subsequentes. Por exemplo, `--part 04`.

Exigido: Não

`--retry`

Tenta novamente mais uma vez todos os erros de Amazon S3, até cinco vezes por operação.

Exigido: Não

`--skipmanifest`

Não faz upload do manifesto.

Exigido: Não

`--location` location

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`.

Obrigatório: 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 amzn-s3-demo-bucket/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 amzn-s3-demo-bucket ...
Uploaded image.part.00
Uploaded image.part.01
Uploaded image.part.02
Uploaded image.part.03
Uploaded image.part.04
Uploaded image.part.05
Uploaded image.part.06
Uploaded image.part.07
```

```
Uploaded image.part.08
Uploaded image.part.09
Uploaded image.part.10
Uploaded image.part.11
Uploaded image.part.12
Uploaded image.part.13
Uploaded image.part.14
Uploading manifest ...
Uploaded manifest.
Bundle upload completed.
```

Opções comuns de ferramentas da AMI

A maioria das ferramentas da AMI aceita os parâmetros opcionais a seguir.

`--help, -h`

Exibe a mensagem de ajuda.

`--version`

Exibe a notificação de versão e direitos autorais.

`--manual`

Exibe a entrada manual.

`--batch`

Executa no modo em lote, suprimindo prompts interativos.

`--debug`

Exibe informações que podem ser úteis ao resolver problemas.

Conversão da AMI baseada no Amazon S3 em uma AMI baseada no EBS

É possível converter uma AMI do Linux de sua propriedade, que é baseada no Amazon S3, em uma AMI do Linux baseada no Amazon EBS.

> **Important**
>
> Não é possível converter uma AMI que não lhe pertença.

Para converter uma AMI baseada no Amazon S3 em uma AMI baseada no Amazon EBS

1. Execute uma instância do Amazon Linux a partir de uma AMI baseada no Amazon EBS. Para obter mais informações, consulte Executar uma instância do EC2 usando o assistente de inicialização de instâncias no console. As instâncias do Amazon Linux têm a AWS CLI e as ferramentas da AMI pré-instaladas.
2. Faça upload da chave privada X.509 usada para criar a AMI baseada no Amazon S3 para a 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. 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. Configure as variáveis de ambiente para usar o AWS CLI. Para obter mais informações, consulte Environment variables.

   a. (Recomendado) Defina as variáveis de ambiente para sua chave de acesso, chave secreta e token de sessão da AWS.

   ```
   [ec2-user ~]$ export AWS_ACCESS_KEY_ID=your_access_key_id
   [ec2-user ~]$ export AWS_SECRET_ACCESS_KEY=your_secret_access_key
   [ec2-user ~]$ export AWS_SESSION_TOKEN=your_session_token
   ```

   b. Defina as variáveis de ambiente para sua chave de acesso da AWS e uma chave secreta.

   ```
   [ec2-user ~]$ export AWS_ACCESS_KEY_ID=your_access_key_id
   [ec2-user ~]$ export AWS_SECRET_ACCESS_KEY=your_secret_access_key
   ```

4. Prepare um volume do Amazon Elastic Block Store (Amazon EBS) para sua nova AMI.

a. Crie um o volume do EBS vazio na mesma zona de disponibilidade que sua instância usando o comando create-volume. Observe o ID do volume na saída do comando.

> **Important**
>
> Esse volume do EBS deve ter tamanho igual ou superior ao volume do dispositivo raiz do armazenamento de instâncias original.

```
aws ec2 create-volume \
    --size 10 \
    --region us-west-2 \
    --availability-zone us-west-2b
```

b. Associe o volume à sua instância baseada no Amazon EBS usando o comando attach-volume.

```
aws ec2 attach-volume \
    --volume-id vol-01234567890abcdef \
    --instance-id i-1234567890abcdef0 \
    --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.

```
[ec2-user ~]$ ec2-download-bundle -b amzn-s3-demo-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.

a. Altere os diretórios para a pasta de pacotes.

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

b. Execute o comando ec2-unbundle.

```
[ec2-user bundle]$ ec2-unbundle -m image.manifest.xml --privatekey /path/to/pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem
```

8. Copie os arquivos da imagem não empacotada para o novo volume do EBS.

```
[ec2-user bundle]$ sudo dd if=/tmp/bundle/image of=/dev/sdb bs=1M
```

9. Teste o volume quanto a quaisquer novas partições não empacotadas.

```
[ec2-user bundle]$ sudo partprobe /dev/sdb1
```

10. Liste os dispositivos de blocos para encontrar o nome do dispositivo para montar.

```
[ec2-user bundle]$ lsblk
NAME         MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
/dev/sda    202:0    0   8G  0 disk
##/dev/sda1 202:1    0   8G  0 part /
/dev/sdb    202:80   0  10G  0 disk
##/dev/sdb1 202:81   0  10G  0 part
```

Neste exemplo, a partição a montar é `/dev/sdb1`, mas o nome do seu dispositivo provavelmente será diferente. Se seu volume não estiver particionado, o dispositivo para montar será semelhante a `/dev/sdb` (sem um dígito final de partição do dispositivo).

11. Crie um ponto de montagem para o novo volume do EBS e monte o volume.

```
[ec2-user bundle]$ sudo mkdir /mnt/ebs
[ec2-user bundle]$ sudo mount /dev/sdb1 /mnt/ebs
```

12. Abra o arquivo `/etc/fstab` no volume do EBS com seu editor de texto favorito (como o vim ou o nano) e remova todas as entradas dos volumes de armazenamento de instâncias (temporários). Como o volume do EBS é montado em `/mnt/ebs`, o arquivo `fstab` é localizado em `/mnt/ebs/etc/fstab`.

```
[ec2-user bundle]$ sudo nano /mnt/ebs/etc/fstab
#
LABEL=/     /           ext4    defaults,noatime  1   1
tmpfs       /dev/shm    tmpfs   defaults        0   0
devpts      /dev/pts    devpts  gid=5,mode=620  0   0
sysfs       /sys        sysfs   defaults        0   0
proc        /proc       proc    defaults        0   0
```

```
/dev/sdb        /media/ephemeral0       auto    defaults,comment=cloudconfig    0
     2
```

Neste exemplo, a última linha deve ser removida.

13. Desmonte o volume e separe-o da instância.

```
[ec2-user bundle]$ sudo umount /mnt/ebs
[ec2-user bundle]$ aws ec2 detach-volume --volume-id vol-01234567890abcdef --
region us-west-2
```

14. Crie uma AMI a partir do novo volume do EBS, da seguinte forma.

    a. Crie um snapshot do novo volume do EBS.

    ```
    [ec2-user bundle]$ aws ec2 create-snapshot --region us-west-2 --description
     "your_snapshot_description" --volume-id vol-01234567890abcdef
    ```

    b. Verifique se seu snapshot está concluído.

    ```
    [ec2-user bundle]$ aws ec2 describe-snapshots --region us-west-2 --snapshot-
    id snap-0abcdef1234567890
    ```

    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. Nesta etapa, você precisará do ID da AMI correspondente à AMI original que é baseada no Amazon S3.

    ```
    [ec2-user bundle]$ aws ec2 describe-images --region us-west-2 --image-
    id ami-0abcdef1234567890 --output text
    IMAGES x86_64 amazon/amzn-ami-pv-2013.09.2.x86_64-s3 ami-8ef297be amazon
     available public machine aki-fc8f11cc instance-store paravirtual xen
    ```

    Neste exemplo, arquitetura é `x86_64` e o ID da imagem do kernel é `aki-fc8f11cc`. Use os valores a seguir na próxima etapa. Se a saída do comando acima também listar um ID `ari`, anote isso também.

    d. Registre sua nova AMI com o ID do snapshot do seu novo volume do EBS e os valores da etapa anterior. Se a saída do comando anterior listou um ID `ari`, inclua-o no comando seguinte com `--ramdisk-id` *`ari_id`*.

    ```
    [ec2-user bundle]$ aws ec2 register-image --region us-west-2 --
    name your_new_ami_name --block-device-mappings DeviceName=device-
    ```

```
name,Ebs={SnapshotId=snap-0abcdef1234567890} --virtualization-type paravirtual
 --architecture x86_64 --kernel-id aki-fc8f11cc --root-device-name device-name
```

15. (Opcional) Depois de ter testado que pode executar uma instância a partir da nova AMI, é possível excluir o volume do EBS criado para esse procedimento.

```
aws ec2 delete-volume --volume-id vol-01234567890abcdef
```

Criar uma AMI do Amazon EC2 usando o Sysprep do Windows

A ferramenta Preparação do sistema da Microsoft (Sysprep do Windows) cria uma versão generalizada do sistema operacional, com a configuração do sistema específica da instância removida antes de capturar uma nova imagem.

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

Você também pode usar o Sysprep do Windows para criar uma AMI padronizada usando os agentes de inicialização do Windows: EC2Launch v2, EC2Launch e EC2Config.

> **Important**
>
> Não use o Sysprep do Windows para criar um backup da instância. O Sysprep do Windows remove informações específicas do sistema; a remoção dessas informações pode ter consequências não intencionais para um backup da instância.

Para solucionar problemas do Sysprep do Windows, consulte Solucionar problemas de Sysprep com instâncias do Windows do Amazon EC2.

Conteúdo

- Fases do Sysprep do Windows
- Antes de começar
- Criar uma AMI usando o Sysprep do Windows com o EC2Launch v2
- Criar uma AMI usando o Sysprep do Windows com o EC2Launch
- Criar uma AMI usando o Sysprep do Windows com o EC2Config

Fases do Sysprep do Windows

O Sysprep do Windows é executado nas seguintes fases:

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

  > **Note**
  >
  > Quando você executa o Sysprep do Windows com os agentes de inicialização do Windows, o sistema impede que os drivers sejam removidos porque, por padrão, `PersistAllDeviceInstalls` é definida como verdadeira.

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

Antes de começar

- Antes da execução do Sysprep do Windows, recomendamos que você remova todas as contas de usuário locais e todos os perfis de conta, exceto uma única conta de administrador em que o Sysprep do Windows será executado. Caso execute o Sysprep do Windows com contas e perfis adicionais, poderá ocorrer um comportamento inesperado, inclusive a perda de dados de perfil ou a falha de conclusão do Sysprep do Windows.
- Saiba mais em Visão geral do Sysprep.
- Saiba quais perfis do servidor são compatíveis com o Sysprep.

Criar uma AMI usando o Sysprep do Windows com o EC2Launch v2

Quando você cria uma imagem de uma instância com o agente EC2Launch v2 instalado, ele realiza tarefas específicas à medida que a imagem é preparada. Isso inclui trabalhar com o Sysprep do Windows. Para obter mais informações, consulte the section called “Fases do Sysprep do Windows”.

Conteúdo

- Ações do Sysprep do Windows
- Após Sysprep
- Executar o Sysprep do Windows com o EC2Launch v2

Ações do Sysprep do Windows

O Sysprep do Windows e o EC2Launch v2 executam as ações a seguir na preparação de uma imagem.

1. Quando você escolhe Shutdown with Sysprep (Desligar com Sysprep) na caixa de diálogo EC2Launch settings (Configurações do EC2Launch), o sistema executa o comando `ec2launch sysprep`.
2. O EC2Launch v2 edita o conteúdo do arquivo `unattend.xml` lendo o valor do registro em `HKEY_USERS\.DEFAULT\Control Panel\International\LocaleName`. O arquivo está localizado no seguinte diretório: `C:\ProgramData\Amazon\EC2Launch\sysprep`.
3. O sistema executa o `BeforeSysprep.cmd`. Esse comando cria uma chave de registro da seguinte maneira:

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

   A chave de registro desabilita as conexões RDP até serem re-habilitadas. Desabilitar as conexões RDP é uma medida de segurança necessária, pois, na primeira sessão de inicialização após o Sysprep do Windows ser executado, há um breve período no qual o RDP permite conexões e a senha do Administrador fica em branco.
4. O serviço do EC2Launch v2 chama o Sysprep do Windows ao executar o seguinte comando:

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

Generalizar a fase

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

Fase especializada

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

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

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

  Se você não tiver personalizações específicas do perfil do usuário que deseja transferir para a nova imagem, altere essa configuração para `False`. O Sysprep do Windows removerá todos os perfis de usuário (isso economiza tempo e espaço em disco).
- TimeZone: o fuso horário é definido como Coordinated Universal Time (UTC – Tempo universal coordenado), por padrão.
- Comando síncrono com pedido 1: o sistema executa o comando a seguir, que habilita a conta do administrador e especifica o requisito de senha:

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

- Comando síncrono com pedido 2: o sistema vasculha a senha do administrador. Essa medida de segurança foi criada para impedir que a instância seja acessível após a conclusão do Sysprep do Windows, caso você não tenha configurado a tarefa `setAdminAccount`.

  O sistema executa o seguinte comando no diretório local do agente de inicialização (`C:\Program Files\Amazon\EC2Launch\`).

  ```
  EC2Launch.exe internal randomize-password --username Administrator
  ```

- Para habilitar conexões de área de trabalho remota, o sistema define a chave de registro `fDenyTSConnections` do Terminal Server como false.

Fase OOBE

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

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

O Windows está sendo configurado. SysprepState=IMAGE_STATE_UNDEPLOYABLE

2. O sistema executa o EC2Launch v2.

Após Sysprep

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

```
Windows sysprep configuration complete.
```

Depois, o EC2Launch v2 executa as ações a seguir:

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

Para obter mais informações sobre o EC2Launch v2, consulte Usar o agente do EC2Launch v2 para realizar tarefas durante a execução da instância EC2 Windows.

Executar o Sysprep do Windows com o EC2Launch v2

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

1. No console do Amazon EC2, localize uma AMI que você deseja duplicar.
2. Execute e conecte-se à sua instância do Windows.
3. Personalizar configurações

    a. No menu Start (Iniciar) do Windows, procure e escolha Amazon EC2Launch settings (Configurações do Amazon EC2Launch). Para obter mais informações sobre as opções e configurações na caixa de diálogo Amazon EC2Launch settings (Configurações do Amazon EC2Launch), consulte Definição das configurações do EC2Launch v2 para instâncias do Windows.

    b. Se você fez alterações, escolha Salvar antes de desligar.

4. Selecione Desligar com Sysprep ou Desligar sem Sysprep.

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

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

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

Criar uma AMI usando o Sysprep do Windows com o EC2Launch

Quando você cria uma imagem de uma instância com o agente EC2Launch instalado, ele realiza tarefas específicas à medida que a imagem é preparada. Isso inclui trabalhar com o Sysprep do Windows. Para obter mais informações, consulte the section called “Fases do Sysprep do Windows”.

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

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

Conteúdo

- Arquivos de resposta e em lotes do EC2Launch para o Sysprep do Windows
- Executar o Sysprep do Windows com o EC2Launch
- Para atualizar rotas de metadados/KMS para o Server 2016 e posterior ao iniciar uma AMI personalizada

Arquivos de resposta e em lotes do EC2Launch para o Sysprep do Windows

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

`Unattend.xml`

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

`BeforeSysprep.cmd`

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

`SysprepSpecialize.cmd`

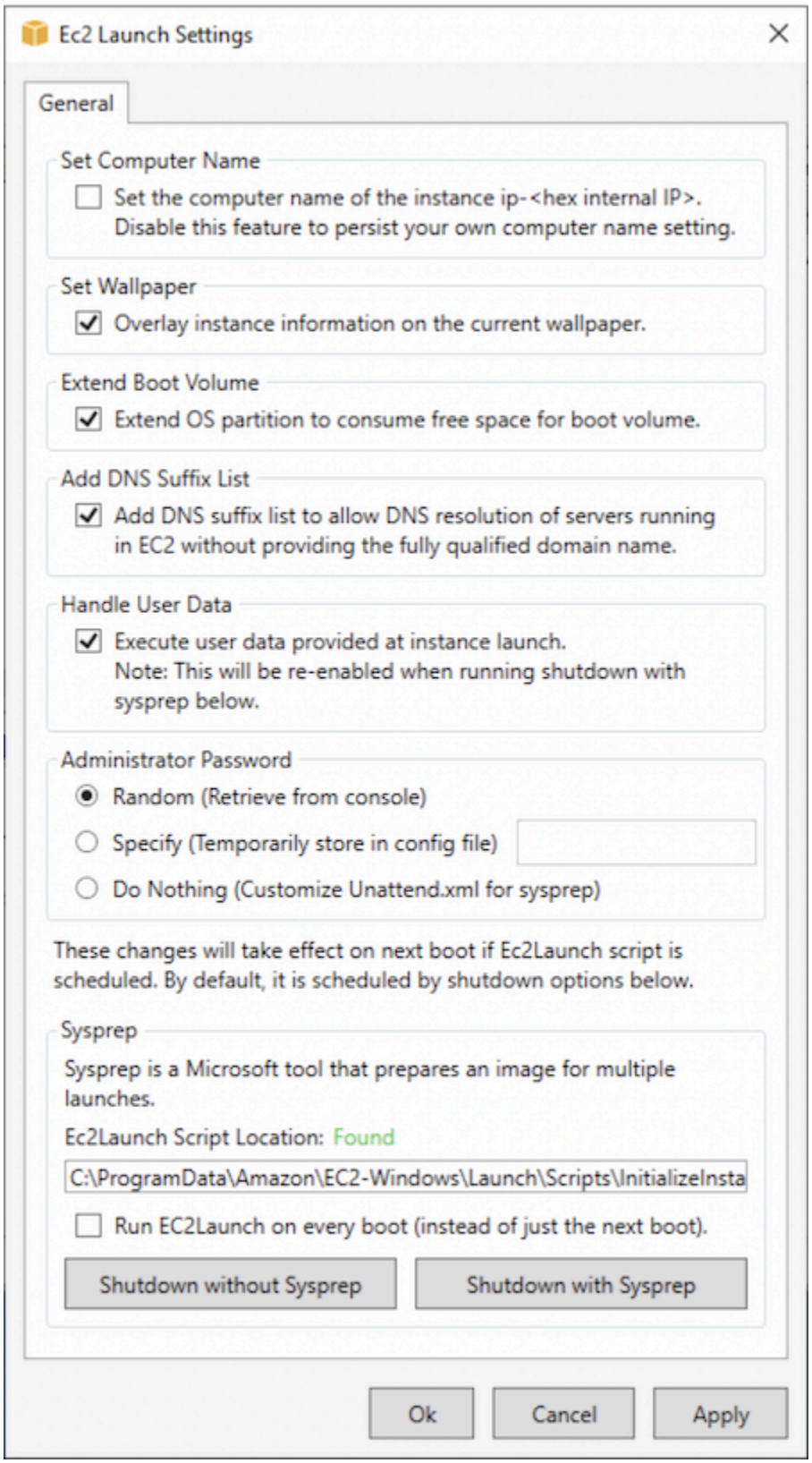
Personalize esse arquivo em lotes para executar comandos durante a fase de especialização do Sysprep do Windows.

Executar o Sysprep do Windows com o EC2Launch

Na instalação completa do Windows Server 2016 e posterior (com uma experiência de desktop), é possível executar o Sysprep do Windows com o EC2Launch manualmente ou usando a aplicação Configurações do EC2Launch.

Executar o Sysprep do Windows usando a aplicação Configurações do EC2Launch

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



5. Selecione ou limpe as opções conforme for necessário. Essas configurações são armazenadas no arquivo `LaunchConfig.json`.

6. Em Administrator password, faça uma das seguintes ações:

   - Escolha Random. O EC2Launch gera uma senha e criptografa-a usando a chave de usuário. O sistema desativa essa configuração depois da execução da instância, portanto, essa senha persistirá se a instância for reinicializada ou parada e iniciada.
   - Escolha Specify e digite a senha que atende aos requisitos do sistema. A senha é armazenada em `LaunchConfig.json` como texto não criptografado e será excluída depois que o Sysprep do Windows definir a senha de administrador. Se você fechar agora, a senha será definida imediatamente. O EC2Launch criptografa a senha usando a chave de usuário.
   - Escolha DoNothing e especifique uma senha no arquivo `unattend.xml`. Se você não especificar uma senha em `unattend.xml`, a conta de administrador ficará desativada.

7. Escolha Shutdown with Sysprep (Desligar com Sysprep).

Executar o Sysprep do Windows manualmente usando o EC2Launch

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

   Para `adminPasswordType`, especifique um dos seguintes valores:

   `Random`

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

   `Specify`

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

`DoNothing`

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

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

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

Para atualizar rotas de metadados/KMS para o Server 2016 e posterior ao iniciar uma AMI personalizada

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

- Execute a GUI EC2LaunchSettings (C:\ProgramData\Amazon\EC2-Windows\Launch\Settings\Ec2LaunchSettings.exe) e selecione a opção para encerrar com o Sysprep do Windows.
- Execute EC2LaunchSettings e desligue sem o Sysprep do Windows antes de criar a AMI. Isso configura as tarefas de inicialização do EC2 para serem executadas na próxima inicialização, que definirá as rotas com base na sub-rede da instância.
- Reprograme manualmente as tarefas de inicialização do EC2 antes de criar uma AMI do PowerShell.

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

- Para atualizar as rotas em uma instância em execução que está passando por ativação do Windows ou comunicação com falhas de metadados de instância, consulte "Não é possível ativar o Windows".

Criar uma AMI usando o Sysprep do Windows com o EC2Config

Quando você cria uma imagem de uma instância com o serviço EC2Config instalado, ele realiza tarefas específicas à medida que a imagem é preparada. Isso inclui trabalhar com o Sysprep do Windows. Para obter mais informações, consulte the section called "Fases do Sysprep do Windows".

Conteúdo

- Ações do Sysprep do Windows
- Após Sysprep
- Executar o Sysprep do Windows com o serviço do EC2Config

Ações do Sysprep do Windows

O Sysprep do Windows e o serviço do EC2Config executam as ações a seguir na preparação de uma imagem.

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

   O arquivo `BundleConfig.xml` inclui as seguintes configurações. É possível alterar essas configurações:

   - AutoSysprep: indica se o Sysprep do Windows deve ser usado automaticamente. Você não precisará mudar esse valor se estiver executando o Sysprep do Windows pela caixa de diálogo de propriedades do serviço do EC2. O valor padrão é `No`.

- SetRDPCertificate: define um certificado autoassinado para o servidor de Desktop Remoto. Isso permite que você use com segurança o Remote Desktop Protocol (RDP) para se conectar à instância. Altere o valor para `Yes` se as novas instâncias precisarem usar um certificado. Essa configuração não é usada com instâncias Windows Server 2012 porque esses sistemas operacionais podem gerar seus próprios certificados. O valor padrão é `No`.
- SetPasswordAfterSysprep: define uma senha aleatória em uma instância recém-executada, criptografa-a com a chave de execução do usuário e gera a senha criptografada no console. Altere o valor para `No` se novas instâncias não precisarem ser definidas com uma senha criptografada aleatória. O valor padrão é `Yes`.
- PreSysprepRunCmd: o local do comando para execução. Por padrão, o comando está localizado no seguinte diretório:: `C:\Program Files\Amazon\Ec2ConfigService\Scripts\BeforeSysprep.cmd`

3. O sistema executa o `BeforeSysprep.cmd`. Esse comando cria uma chave de registro da seguinte maneira:

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

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

4. O serviço do EC2Config chama o Sysprep do Windows ao executar o seguinte comando:

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

Generalizar a fase

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

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

- DoNotCleanUpNonPresentDevices: essa configuração retém informações de plug and play para dispositivos que não estão presentes no momento.

- O Sysprep do Windows fecha o SO à medida que se prepara para criar a AMI. O sistema executa uma nova instância ou inicia a instância original.

Fase especializada

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

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

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

  Se você não tiver personalizações específicas do perfil do usuário que deseja transferir para a nova imagem, altere essa configuração para falso. O Sysprep do Windows removerá todos os perfis de usuário; isso economiza tempo e espaço em disco.
- TimeZone: o fuso horário é definido como Coordinated Universal Time (UTC – Tempo universal coordenado), por padrão.
- Comando síncrono com pedido 1: o sistema executa o comando a seguir, que habilita a conta do administrador e especifica o requisito de senha.

  net user Administrator /ACTIVE:YES /LOGONPASSWORDCHG:NO /EXPIRES:NEVER /PASSWORDREQ:YES
- Comando síncrono com pedido 2: o sistema vasculha a senha do administrador. Essa medida de segurança é criada para impedir que a instância fique acessível após o Sysprep do Windows ser concluído, caso você não tenha habilitado a configuração ec2setpassword.

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

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

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

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

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

Fase OOBE

1. Usando o arquivo de resposta do serviço EC2Config, o sistema especifica as seguintes configurações:
   - <InputLocale>en-US</InputLocale>
   - <SystemLocale>en-US</SystemLocale>
   - <UILanguage>en-US</UILanguage>
   - <UserLocale>en-US</UserLocale>
   - <HideEULAPage>true</HideEULAPage>
   - <HideWirelessSetupInOOBE>true</HideWirelessSetupInOOBE>
   - <NetworkLocation>Other</NetworkLocation>
   - <ProtectYourPC>3</ProtectYourPC>
   - <BluetoothTaskbarIconEnabled>false</BluetoothTaskbarIconEnabled>
   - <TimeZone>UTC</TimeZone>
   - <RegisteredOrganization>Amazon.com</RegisteredOrganization>
   - <RegisteredOwner>Amazon</RegisteredOwner>

   > **Note**
   >
   > Durante as fases de generalização e especialização, o serviço EC2Config monitora o status do SO. Se o EC2Config detectar que o sistema operacional está na fase Sysprep, ele publicará a seguinte mensagem no log do sistema: EC2ConfigMonitorState: 0 O Windows está sendo configurado. SysprepState=IMAGE_STATE_UNDEPLOYABLE

2. Após a conclusão da fase OOBE, o sistema executa `SetupComplete.cmd` a partir do seguinte local: `C:\Windows\Setup\Scripts\SetupComplete.cmd`. Na AMIs públicas da Amazon

antes de abril de 2015 este arquivo estava vazio e não executava nada na imagem. Em AMIs públicas posteriores a abril de 2015, o arquivo inclui o seguinte valor: call "C:\Program Files \Amazon\Ec2ConfigService\Scripts\PostSysprep.cmd".

3. O sistema executa `PostSysprep.cmd`, que realiza as seguintes operações:
   - Define a senha do Administrador para não expirar. Se a senha expirou, os Administradores podem não conseguir fazer login.
   - Define o nome da máquina MSSQLServer (se instalada) para que o nome esteja em sincronia com a AMI.

Após Sysprep

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

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

O EC2Config então executa as ações a seguir:

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

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

Para obter mais informações sobre plug-ins do Windows, consulte Usar o serviço EC2Config para realizar tarefas durante a execução da instância herdada do sistema operacional Windows do EC2.

Executar o Sysprep do Windows com o serviço do EC2Config

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

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

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

- Manter existente: a senha existente para a conta do Administrador não muda quando o Sysprep do Windows é executado ou o EC2Config é reiniciado. É importante recordar essa senha, pois você não poderá recuperá-la depois.

8. Escolha OK.

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

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

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

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

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

Copiar uma AMI do Amazon EC2

Quando precisar de uma configuração consistente de instância do Amazon EC2 em várias regiões, será possível usar uma única imagem de máquina da Amazon (AMI) como modelo para inicializar todas as instâncias. No entanto, as AMIs são recursos específicos de uma região. Para inicializar uma instância em uma determinada Região da AWS, a AMI precisará estar localizada nessa região.

Portanto, para usar a mesma AMI em várias regiões, você precisará copiá-la da região de origem para cada região de destino.

O método usado para copiar uma AMI dependerá de você estar copiando entre regiões dentro da mesma partição ou entre diferentes partições:

- Cópia entre regiões: copie AMIs entre regiões na mesma partição, por exemplo, entre regiões na partição comercial. Esse método de cópia está descrito neste tópico.
- Cópia entre partições:: copie AMIs de uma partição da para outra partição, por exemplo, da partição comercial para a partição AWS GovCloud (US). Para obter informações sobre esse método de cópia, consulte Armazenar e restaurar uma AMI.
- Cópia entre contas: crie uma cópia de uma AMI que outra Conta da AWS tenha compartilhado com a sua Conta da AWS. Esse método de cópia está descrito neste tópico.

O tempo necessário para concluir a operação de cópia da AMI entre regiões e entre contas é apresentado com base no melhor esforço. Se precisar controlar o tempo de conclusão, será possível especificar uma janela de conclusão que varia de 15 minutos a 48 horas, garantindo que sua AMI seja copiada dentro do prazo exigido. Cobranças adicionais são aplicáveis a operações de cópia de AMI baseadas em tempo. Para obter mais informações, consulte Cópias baseadas em tempo, no Guia do usuário do Amazon EBS.

Conteúdo

- Considerações
- Custos
- Conceder permissões para copiar AMIs do Amazon EC2
- Copiar um AMI
- Parar uma operação de cópia de AMI pendente
- Como funciona a cópia de uma AMI do Amazon EC2

Considerações

- Permissão para copiar AMIs: é possível usar políticas do IAM para conceder ou negar aos usuários permissão para copiar AMIs. A partir de 28 de outubro de 2024, você pode especificar permissões no nível do recurso para a ação `CopyImage` na AMI de origem. As permissões no nível do recurso da nova AMI estão disponíveis como antes.

- Permissões de execução e permissões de bucket do Amazon S3: a AWS não copia permissões de execução nem permissões de bucket do Amazon S3 da AMI de origem para a nova AMI. Após a conclusão da operação de cópia, você pode aplicar permissões de inicialização e permissões de bucket do Amazon S3 à nova AMI.
- Tags: é possível copiar somente as tags de AMI definidas pelo usuário que você anexou à AMI de origem. Tags do sistema (prefixadas com `aws:`) e tags definidas pelo usuário anexadas por outras Contas da AWS não serão copiadas. Ao copiar uma AMI, você pode anexar novas tags à nova AMI e seus snapshots de suporte.
- Cotas para cópias de AMI baseadas em tempo: depois que você atingir sua cota cumulativa de throughput para cópias de snapshot, as solicitações subsequentes de cópias de AMI baseadas no tempo vão falhar. Para obter mais informações, consulte Cotas para cópias baseadas em tempo, no Guia do Usuário do Amazon EBS.
- Cópias de origem-destino compatíveis: a localização da AMI de origem determina se você pode copiá-la e os destinos permitidos para a nova AMI:
  - Se a AMI de origem estiver em uma região, será possível copiá-la dentro dessa região para outra região, para um Outpost associado a essa região ou para uma zona local na região.
  - Se a AMI de origem estiver em uma zona local, será possível copiá-la dentro dessa zona local para a região principal dessa zona local ou para outras zonas locais específicas com a mesma região principal.
  - Se a AMI de origem estiver em, um Outpost, você não poderá copiá-la.
- Parâmetros da CLI para origem e destino: ao usar a CLI, os seguintes parâmetros são compatíveis para especificar o local de origem da AMI a ser copiada e o destino da nova AMI. Observe que a operação de cópia deve ser iniciada na região de destino; se você omitir o parâmetro `--region`, o destino assumirá a região padrão configurada em suas configurações da AWS CLI.

Origem para destino	Parâmetro de origem	Parâmetro de destino
Região para região	`--source-region`	`--region`
Região para Outpost	`--source-region`	`--destination-outpost-arn` (o ARN do Outpost)
Região para zona local	`--source-region`	`--destination-availability-zone` (o nome da zona local) ou `--destina`

Origem para destino	Parâmetro de origem	Parâmetro de destino
	Deve ser a região principal da zona local.	`tion-availability-zone-id` (o ID da zona local)
Zona local para região	`--source-region` Deve ser a região principal da zona local. A zona local de origem é assumida da localização da ID da AMI de origem especific ada.	`--region` Deve ser a região principal da zona local.
Zona local para zona local	`--source-region` Deve ser a região principal da zona local. A zona local de origem é assumida da localização da ID da AMI de origem especific ada.	`--destination-avai lability-zone` (o nome da zona local) ou `--destina tion-availability-zone-id` (o ID da zona local)

Custos

Não há cobrança pela cópia de uma AMI quando não houver nenhum tempo de conclusão especificado. No entanto, há cobranças adicionais para operações de cópia de AMI baseadas em tempo. Para obter mais informações, consulte Cópias baseadas em tempo, no Guia do usuário do Amazon EBS.

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

Conceder permissões para copiar AMIs do Amazon EC2

Para copiar uma AMI baseada no EBS ou no Amazon S3, são necessárias as seguintes permissões do IAM:

- `ec2:CopyImage`: para copiar a AMI. Para AMIs baseadas no EBS, ele também concede permissão para copiar os snapshots de suporte da AMI.
- `ec2:CreateTags`: para marcar a AMI de destino. Para AMIs baseadas no EBS, ele também concede permissão para marcar os snapshots de apoio da AMI de destino.

Se você estiver copiando uma AMI baseada em uma instância armazenada, as seguintes permissões adicionais do IAM serão necessárias:

- `s3:CreateBucket`: para criar o bucket do S3 na região de destino da nova AMI
- `s3:PutBucketOwnershipControls`: para habilitar ACLs para o bucket do S3 recém-criado para que os objetos possam ser gravados com a `aws-exec-read` ACL pré-configurada
- `s3:GetBucketAcl`: para ler as ACLs para o bucket de origem
- `s3:ListAllMyBuckets`: para encontrar um bucket do S3 existente para AMIs na região de destino
- `s3:GetObject`: para ler os objetos no bucket de origem
- `s3:PutObject`: para escrever os objetos no bucket de destino
- `s3:PutObjectAcl`: para escrever as permissões para os novos objetos no bucket de destino

> **Note**
>
> A partir de 28 de outubro de 2024, você pode especificar permissões no nível do recurso para a ação `CopyImage` na AMI de origem. As permissões no nível do recurso da AMI de destino estão disponíveis como antes. Para obter mais informações, consulte CopyImage na tabela em Ações definidas pelo Amazon EC2 na Referência de autorização do serviço.

Exemplo de política do IAM para copiar uma AMI baseada em EBS e marcar a AMI e os snapshots de destino

O exemplo de política a seguir concede a você permissão para copiar qualquer AMI baseada no EBS e marcar a AMI de destino e seus snapshots de apoio.

> **Note**
>
> A partir de 28 de outubro de 2024, você pode especificar snapshots no elemento `Resource`. Para obter mais informações, consulte CopyImage na tabela em Ações definidas pelo Amazon EC2 na Referência de autorização do serviço.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [{
        "Sid": "PermissionToCopyAllImages",
        "Effect": "Allow",
        "Action": [
            "ec2:CopyImage",
            "ec2:CreateTags"
        ],
        "Resource": [
            "arn:aws:ec2:*::image/*",
            "arn:aws:ec2:*::snapshot/*"
        ]
    }]
}
```

Exemplo de política do IAM para copiar uma AMI baseada no EBS, mas negar a marcação de novos snapshots.

A permissão `ec2:CopySnapshot` é concedida automaticamente quando você recebe a permissão `ec2:CopyImage`. A permissão para marcar os novos snapshots de apoio pode ser negada explicitamente, anulando o efeito `Allow` da ação `ec2:CreateTags`.

O exemplo de política a seguir concede a você permissão para copiar qualquer AMI baseada no EBS, mas proíbe a marcação de novos snapshots de apoio da AMI de destino.

JSON

```
{
    "Version":"2012-10-17",
```

```
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ec2:CopyImage",
                "ec2:CreateTags"
            ],
            "Resource": [
                "arn:aws:ec2:*::image/*",
                "arn:aws:ec2:*::snapshot/*"
            ]
        },
        {
            "Effect": "Deny",
            "Action": "ec2:CreateTags",
            "Resource": "arn:aws:ec2:::snapshot/*"
        }
    ]
}
```

Exemplo de política do IAM para copiar uma AMI baseada no Amazon S3 e adicionar marcação à AMI de destino

A política de exemplo apresentada a seguir concede permissão para copiar qualquer AMI baseada no Amazon S3 no bucket de origem especificado para a região indicada e adicionar etiquetas à AMI de destino.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [{
            "Sid": "PermissionToCopyAllImages",
            "Effect": "Allow",
            "Action": [
                "ec2:CopyImage",
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:*::image/*"
        },
        {
            "Effect": "Allow",
```

```
            "Action": "s3:ListAllMyBuckets",
            "Resource": [
                "arn:aws:s3:::*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": "s3:GetObject",
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-source-bucket/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:CreateBucket",
                "s3:GetBucketAcl",
                "s3:PutObjectAcl",
                "s3:PutObject"
            ],
            "Resource": [
                "arn:aws:s3:::amis-for-111122223333-in-us-east-2-hash"
            ]
        }
    ]
}
```

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

> **Note**
>
> Você precisa da permissão `s3:CreateBucket` apenas na primeira vez em que copiar uma AMI baseada no Amazon S3 para uma região específica. Depois disso, o bucket do Amazon S3 que foi criado na região será usado para armazenar todas as AMIs futuras que você copiar para essa região.

Copiar um AMI

É possível copiar uma AMI de sua propriedade ou uma AMI compartilhada com você de outra conta. Para obter as combinações de origem e destino compatíveis, consulte Considerações.

Console

Copiar uma AMI

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.
3. No painel de navegação, selecione AMIs para exibir a lista de AMIs disponíveis para você na região.
4. Caso não veja a AMI que deseja copiar, selecione um filtro diferente. É possível filtrar por AMIs Pertencentes a mim, Imagens privadas, Imagens públicas e Imagens desabilitadas.
5. Selecione a AMI para copiar e escolha Ações, Copiar AMI.
6. Na página Copy imagem de máquina da Amazon (AMI), especifique as seguintes informações:

   a. AMI copy name (Nome da cópia da AMI): o nome da nova AMI. É possível incluir informações do sistema operacional no nome, pois o Amazon EC2 não fornece essas informações ao exibir detalhes sobre a AMI.

   b. AMI copy description: (Descrição da cópia da AMI): por padrão, a descrição inclui informações sobre a AMI de origem, de forma que você possa distinguir uma cópia da original. É possível alterar essa descrição conforme necessário.

   c. Destination region (Região de destino): a região para a qual a AMI deve ser copiada. Para obter mais informações, consulte Cópia entre regiões e Cópia entre contas.

   d. Copiar tags: marque essa caixa de seleção para incluir as tags de AMI definidas pelo usuário ao copiar a AMI. Tags do sistema (prefixadas com `aws:`) e tags definidas pelo usuário anexadas por outras Contas da AWS não serão copiadas.

   e. Cópia com base emtempo: você pode especificar se a operação de cópia será concluída dentro de um prazo específico ou com base no melhor esforço, da seguinte forma:

      - Para concluir a cópia dentro de um prazo específico:
        - Selecione Habilitar cópia com base em tempo.

- Em Duração da conclusão, insira o número de minutos (em incrementos de 15 minutos) permitidos para a operação de cópia. A duração da conclusão é aplicável a todos os snapshots associados à AMI.

  Para obter mais informações, consulte Cópias baseadas em tempo, no Guia do usuário do Amazon EBS.

- Para concluir a cópia com base no melhor esforço:
  - Deixe a opção Habilitar cópia com base no tempo desmarcada.

f. (Somente AMIs baseadas no EBS) Criptografar snapshots do EBS de uma cópia da AMI: marque essa caixa de seleção para criptografar os snapshots de destino ou para recriptografá-los usando uma chave diferente. Se a opção de criptografar por padrão estiver habilitada, a caixa de seleção Criptografar snapshots do EBS da cópia da AMI estará selecionada e não poderá ser desmarcada. Para obter mais informações, consulte Criptografar e copiar.

g. (Somente AMIs baseadas no EBS) Chave do KMS: a chave do KMS usada para criptografar os snapshots de destino.

h. Tags: é possível marcar a nova AMI e os novos snapshots com as mesmas tags ou pode marcá-los com tags diferentes.

- Para marcar a nova AMI e novos os snapshots com as mesmas tags, escolha Marcar imagem e snapshots juntos. As mesmas tags são aplicadas à nova AMI e a cada snapshot criado.
- Para marcar a nova AMI e os snapshots com tags diferentes, escolha Marcar imagem e snapshots separadamente. Diferentes tags são aplicadas à nova AMI e aos snapshots criados. Observe, no entanto, que todos os novos snapshots criados recebem as mesmas tags; não é possível marcar cada snapshot com uma tag diferente.

(Opcional) Para adicionar uma tag, escolha Add tag (Adicionar tag) e digite a chave e o valor da tag. Repita esse procedimento para cada tag.

i. Quando estiver com tudo pronto para copiar a AMI, escolha Copiar AMI.

O status inicial da nova AMI é `Pending`. A operação de cópia da AMI estará concluída quando o status for `Available`.

AWS CLI

Para copiar uma AMI de uma região para outra

Use o comando copy-image (Copiar imagem). Especifique as regiões de origem e de destino. Especifique a região de origem usando o parâmetro `--source-region`. É possível especificar a região de destino usando o parâmetro `--region` (ou omitir esse parâmetro para assumir a região padrão configurada em suas configurações da AWS CLI).

```
aws ec2 copy-image \
    --source-image-id ami-0abcdef1234567890 \
    --source-region us-west-2 \
    --name my-ami \
    --region us-east-1
```

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

Para copiar uma AMI de uma região para uma zona local

Use o comando copy-image (Copiar imagem). Você deve especificar a origem e o destino. Especifique a região de origem usando o parâmetro `--source-region`. Você especifica a zona local de destino usando o parâmetro `--destination-availability-zone` (você pode usar `--destination-availability-zone-id` em vez disso). Observe que você só pode copiar uma AMI de uma região para uma zona local dentro dessa mesma região.

```
aws ec2 copy-image \
    --source-image-id ami-0abcdef1234567890 \
    --source-region cn-north-1 \
    --destination-availability-zone cn-north-1-pkx-1a \
    --name my-ami \
    --region cn-north-1
```

Para copiar uma AMI de uma zona local para uma região

Use o comando copy-image (Copiar imagem). Você deve especificar a origem e o destino. Especifique a região de origem usando o parâmetro `--source-region`. Você especifica a região de destino usando o parâmetro `--region` (ou omite esse parâmetro para assumir a região padrão configurada em suas configurações da AWS CLI). A zona local de origem é assumida da localização da ID da AMI de origem especificada. Observe que você só pode copiar uma AMI de uma zona local para sua região principal.

```
aws ec2 copy-image \
    --source-image-id ami-0abcdef1234567890 \
    --source-region cn-north-1 \
    --name my-ami \
    --region cn-north-1
```

Para copiar uma AMI de uma zona local para outra

Use o comando copy-image (Copiar imagem). Você deve especificar a origem e o destino. Você especifica a região de origem da zona local usando o parâmetro `--source-region`. Você especifica a zona local de destino usando o parâmetro `--destination-availability-zone` (você pode usar `--destination-availability-zone-id` em vez disso). A zona local de origem é assumida da localização da ID da AMI de origem especificada. Você especifica a região principal da zona local de destino usando o parâmetro `--region` (ou omite esse parâmetro para assumir a região padrão configurada em suas configurações da AWS CLI).

```
aws ec2 copy-image \
    --source-image-id ami-0abcdef1234567890 \
    --source-region cn-north-1 \
    --destination-availability-zone cn-north-1-pkx-1a \
    --name my-ami \
    --region cn-north-1
```

PowerShell

Para copiar uma AMI de uma região para outra

Use o cmdlet Copy-EC2Image. Especifique as regiões de origem e de destino. Especifique a região de origem usando o parâmetro `-SourceRegion`. É possível especificar a região de destino usando o parâmetro `-Region` ou o cmdlet Set-AWSDefaultRegion.

```
Copy-EC2Image `
    -SourceImageId ami-0abcdef1234567890 `
    -SourceRegion us-west-2 `
    -Name my-ami `
    -Region us-east-1
```

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

Para copiar uma AMI de uma região para uma zona local

Use o cmdlet Copy-EC2Image. Você deve especificar a origem e o destino. Especifique a região de origem usando o parâmetro `-SourceRegion`. Você especifica a zona local de destino usando o parâmetro `-DestinationAvailabilityZone` (você pode usar `-DestinationAvailabilityZoneId` em vez disso). Observe que você só pode copiar uma AMI de uma região para uma zona local dentro dessa mesma região.

```
Copy-EC2Image `
    -SourceImageId ami-0abcdef1234567890 `
    -SourceRegion cn-north-1 `
    -DestinationAvailabilityZone cn-north-1-pkx-1a `
    -Name my-ami `
    -Region cn-north-1
```

Para copiar uma AMI de uma zona local para uma região

Use o cmdlet Copy-EC2Image. Você deve especificar a origem e o destino. Especifique a região de origem usando o parâmetro `-SourceRegion`. É possível especificar a região de destino usando o parâmetro `-Region` ou o cmdlet Set-AWSDefaultRegion. A zona local de origem é assumida da localização da ID da AMI de origem especificada. Observe que você só pode copiar uma AMI de uma zona local para sua região principal.

```
Copy-EC2Image `
    -SourceImageId ami-0abcdef1234567890 `
    -SourceRegion cn-north-1 `
    -Name my-ami `
    -Region cn-north-1
```

Para copiar uma AMI de uma zona local para outra

Use o cmdlet Copy-EC2Image. Você deve especificar a origem e o destino. Você especifica a região de origem da zona local usando o parâmetro `-SourceRegion`. Você especifica a zona local de destino usando o parâmetro `-DestinationAvailabilityZone` (você pode usar `-DestinationAvailabilityZoneId` em vez disso). A zona local de origem é assumida da localização da ID da AMI de origem especificada. É possível especificar a região principal da zona local de destino usando o parâmetro `-Region` ou o cmdlet Set-AWSDefaultRegion.

```
Copy-EC2Image `
    -SourceImageId ami-0abcdef1234567890 `
    -SourceRegion cn-north-1 `
    -DestinationAvailabilityZone cn-north-1-pkx-1a `
```

```
    -Name my-ami `
    -Region cn-north-1
```

Parar uma operação de cópia de AMI pendente

É possível interromper uma cópia pendente de uma AMI usando os procedimentos a seguir.

Console

Para interromper uma operação de cópia de AMI

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 Ações e Cancelar registro da AMI.
5. Quando a confirmação for solicitada, escolha Deregister AMI (Cancelar registro da AMI).

AWS CLI

Para interromper uma operação de cópia de AMI

Use o comando deregister-image.

```
aws ec2 deregister-image --image-id ami-0abcdef1234567890
```

PowerShell

Para interromper uma operação de cópia de AMI usando

Use o cmdlet Unregister-EC2Image.

```
Unregister-EC2Image -ImageId ami-0abcdef1234567890
```

Como funciona a cópia de uma AMI do Amazon EC2

Copiar uma AMI de origem resulta em uma nova AMI idêntica, mas separada, que também é chamada de AMI de destino. A AMI de destino tem o próprio ID de AMI exclusivo. É possível

alterar ou cancelar o registro da AMI de origem sem afetar a AMI de destino. O inverso também é verdadeiro.

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

Conteúdo

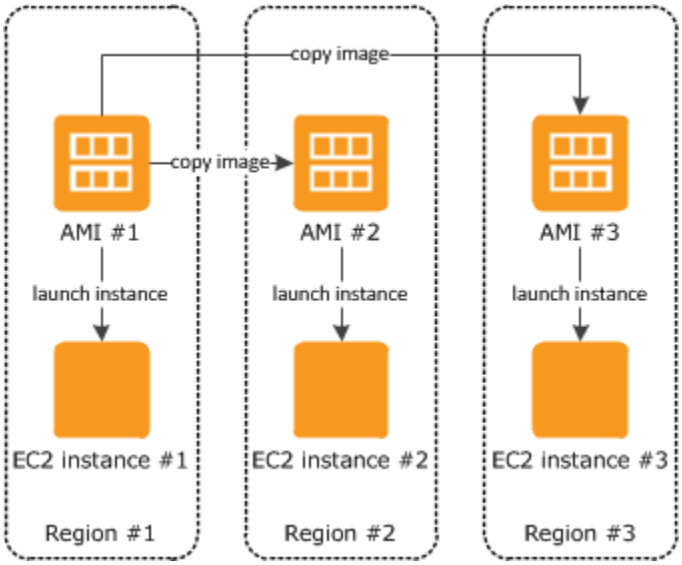
- Cópia entre regiões
- Cópia entre contas
- Operações de cópia de AMI baseadas no tempo
- Criptografar e copiar

Cópia entre regiões

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

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

O diagrama a seguir mostra as relações entre uma AMI de origem e duas AMIs copiadas em regiões diferentes, assim como as instâncias do EC2 executadas por 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 uma AMI baseada no Amazon S3 para uma região pela primeira vez, criamos um bucket do Amazon S3 para as AMIs copiadas para essa região. Todas as AMIs baseadas no Amazon S3 que você copia para essa região são armazenadas neste 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, atualize todas as string de conexão com o banco de dados ou dados de configuração de aplicação para apontarem para os recursos apropriados. Caso contrário, as instâncias executadas pela nova AMI na região de destino ainda poderão usar os recursos da região de origem, o que pode afetar a performance e o custo.

Limitações

- Regiões de destino estão limitadas a 300 operações de cópia de AMI simultâneas. Isso também é aplicável a operações de cópia de AMI baseadas no tempo.
- 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.

Cópia entre contas

Se uma AMI de outra Conta da AWS for compartilhada com a sua Conta da AWS, será possível copiar a AMI compartilhada. Isso é conhecido como cópia entre contas. A AMI que é compartilhada

com você é a AMI de origem. Quando copia a AMI de origem, você cria uma nova AMI. A nova AMI geralmente é chamada de AMI de destino.

Custos da AMI

- Para a AMI compartilhada, a cobrança pelo armazenamento na região é lançada na conta da AMI compartilhada.
- Se copiar uma AMI compartilhada com sua conta, você será o proprietário da AMI de destino na sua conta.
  - As taxas de transferência padrão do Amazon EBS ou do Amazon S3 são cobradas do proprietário da AMI de origem.
  - O armazenamento da AMI de destino na região de destino é cobrado de você.

Permissões de recursos

Para copiar uma AMI compartilhada com você de outra conta, o proprietário da AMI de origem precisará conceder permissão de leitura para o armazenamento que suporta a AMI e não apenas para a própria AMI. O armazenamento corresponde ao snapshot do EBS associado, no caso de uma AMI baseada no Amazon EBS, ou a um bucket do S3 associado, no caso de uma AMI baseada no Amazon S3. Se a AMI compartilhada tiver snapshots criptografados, o proprietário deve compartilhar a chave ou as chaves com você. Para obter mais informações sobre a concessão de permissões de recursos para snapshots do EBS, consulte Compartilhar um snapshot do Amazon EBS com outras Contas da AWS no Guia do usuário do Amazon EBS. Para buckets do S3, consulte Gerenciamento de identidade e acesso no Amazon S3 no Guia do usuário do Amazon S3.

> **Note**
>
> As tags anexadas à AMI de origem não são copiadas entre contas para a AMI de destino.

Operações de cópia de AMI baseadas no tempo

Quando você inicia uma operação de cópia de AMI baseada no tempo para uma AMI baseada no EBS com um único snapshot associado, ela se comporta da mesma maneira que uma operação individual de cópia de snapshot baseada no tempo, e as mesmas limitações de throughput são aplicáveis.

Quando você inicia uma operação de cópia de AMI baseada no tempo para uma AMI baseada no EBS com vários snapshots associados, ela se comporta da mesma maneira que operações simultâneas de cópia de snapshot baseadas no tempo, e as mesmas limitações de throughput são aplicáveis. Cada snapshot associado resulta em uma solicitação de cópia de snapshot separada, cada qual contribuindo para sua cota cumulativa de throughput de cópias de snapshots. A duração da conclusão que você especifica é aplicável a cada snapshot associado.

Para obter mais informações, consulte Cópias baseadas em tempo, no Guia do usuário do Amazon EBS.

Criptografar e copiar

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

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

> **Note**
>
> A criptografia durante a ação `CopyImage` se aplica somente a AMIs baseadas no Amazon EBS. Por não usar snapshots, uma AMI baseada no Amazon S3 não pode ter o status de criptografia alterado por meio da cópia.

Ao copiar uma AMI sem especificar parâmetros de criptografia, o snapshot de apoio é copiado com seu status de criptografia original por padrão. Portanto, se a AMI de origem for apoiada por um snapshot não criptografado, o snapshot de destino resultante também não será criptografado. Da mesma forma, se o snapshot da AMI de origem for criptografado, o snapshot de destino resultante também será criptografado pela mesma chave do AWS KMS. Em AMIs apoiadas por vários

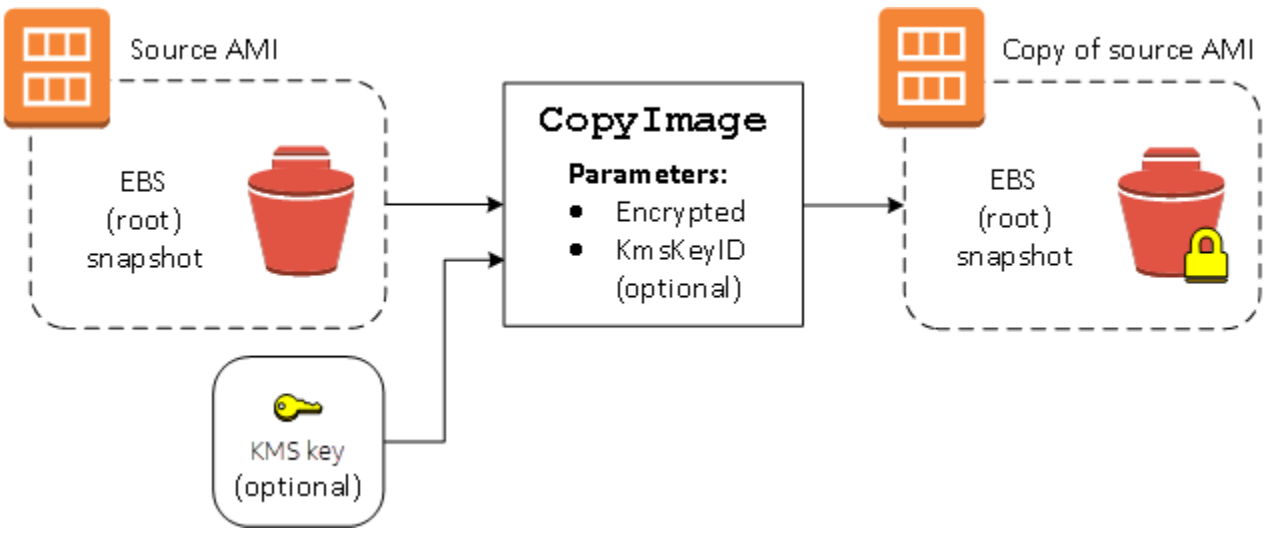
snapshots, cada snapshot de destino preserva o estado de criptografia do snapshot de origem correspondente.

Para alterar o estado de criptografia dos snapshots de destino de apoio durante uma cópia da AMI, você pode especificar parâmetros de criptografia. O exemplo a seguir mostra um caso não padrão, em que os parâmetros de criptografia são especificados com a ação `CopyImage` para alterar o estado de criptografia da AMI de destino.

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

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

> **Note**
>
> Habilitar a criptografia por padrão tem o mesmo efeito que configurar o parâmetro `Encrypted` como `true` para todos os snapshots na AMI.



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

Para obter mais informações sobre como copiar AMIs com snapshots criptografados, consulte Usar criptografia com AMIs com EBS.

Armazenar e restaurar uma AMI usando o S3

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

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

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

Para obter mais informações sobre as partições da AWS, consulte *`partição`* na página Nomes do recurso da Amazon (ARN) no Guia do usuário do IAM.

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

Conteúdo

- Casos de uso
- Limitações
- Custos
- Como o armazenamento e a restauração de uma AMI funciona
- Criar uma tarefa de armazenamento de imagem

Casos de uso

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

- Copiar uma AMI entre partições da AWS
- Fazer cópias de arquivamento de AMIs

Copiar uma AMI entre partições da AWS

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

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

- Armazene a AMI em um bucket do S3 na região atual usando `CreateStoreImageTask`. Neste exemplo, o bucket do S3 está localizado em `us-east-2`.
- Monitore o andamento da tarefa de armazenamento usando `DescribeStoreImageTasks`. O objeto fica visível no bucket do S3 quando a tarefa é concluída.
- Copie o objeto da AMI armazenado para um bucket do S3 na partição de destino usando um procedimento de sua escolha. Neste exemplo, o bucket do S3 está localizado em `us-gov-east-1`.

> **Note**
>
> Como você precisa de credenciais diferentes da AWS para cada partição, você não pode copiar um objeto S3 diretamente de uma partição para outra. O processo para copiar um objeto S3 entre partições está fora do escopo desta documentação. Fornecemos os processos de cópia a seguir como exemplos, mas use o processo de cópia que atenda aos seus requisitos de segurança.
>
> - Para copiar uma AMI entre partições, o processo de cópia pode ser tão simples quanto o seguinte: baixe o objeto do bucket de origem para um host intermediário (por exemplo, uma instância do EC2 ou um laptop) e carregue o objeto do host intermediário no bucket de destino. Para cada etapa do processo, use as credenciais da AWS para a partição.
> - Para um uso mais sustentável, considere desenvolver uma aplicação que gerencia as cópias, potencialmente usando downloads e uploads de várias partesdo S3.

- Restaure a AMI do bucket do S3 na partição de destino usando `CreateRestoreImageTask`. Neste exemplo, o bucket do S3 está localizado em `us-gov-east-1`.

- Monitore o andamento da tarefa de restauração descrevendo a AMI para verificar quando seu estado se torna disponível. Também é possível monitorar as porcentagens de progresso dos snapshots que compõem a AMI restaurada descrevendo os instantâneos.

Fazer cópias de arquivamento de AMIs

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

Limitações

- Para armazenar uma AMI, sua Conta da AWS deve possuir a AMI e seus snapshots, ou a AMI e seus snapshots devem ser compartilhados diretamente com sua conta. Você não pode armazenar uma AMI se ela for compartilhada publicamente apenas.
- Somente AMIs baseadas no EBS podem ser armazenadas usando essas APIs.
- Não há suporte a AMIs paravirtuais (PV).
- O tamanho de uma AMI (antes da compactação) que pode ser armazenada é limitado a 5.000 GB.
- Cota em solicitações de imagem de armazenamento: 1.200 GB de trabalho de armazenamento (dados de snapshots) em andamento.
- Cota em solicitações de imagem de restauração: 600 GB de trabalho de restauração (dados de snapshots) em andamento.
- Durante a tarefa de armazenamento, os snapshots não devem ser excluídos e a entidade principal do IAM que faz o armazenamento deve ter acesso aos snapshots, caso contrário o processo de armazenamento apresentará falha.
- Não é possível criar várias cópias de uma AMI no mesmo bucket do S3.
- Uma AMI armazenada em um bucket do S3 não pode ser restaurada com seu ID de AMI original. É possível mitigar isso usando Alias de AMI.
- Atualmente, as APIs de armazenamento e restauração só são compatíveis se for utilizada a AWS Command Line Interface, os AWS SDKs e a API do Amazon EC2. Não é possível armazenar e restaurar uma AMI usando o console do Amazon EC2.

Custos

Quando você armazena e restaura AMIs usando o S3, é cobrado pelos serviços usados pelas APIs de armazenamento e restauração e pela transferência de dados. As APIs usam o S3 e a API direta do EBS (usadas internamente por essas APIs para acessar os dados do snapshot). Para obter mais informações, consulte Definição de preço do Amazon S3 e Definição de preço do Amazon EBS.

Como o armazenamento e a restauração de uma AMI funciona

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

- `CreateStoreImageTask` – Armazena a AMI em um bucket do S3
- `DescribeStoreImageTasks` – Fornece o andamento da tarefa de armazenamento da AMI
- `CreateRestoreImageTask` – Restaura a AMI de um bucket do S3

Como as APIs funcionam

- CreateStoreImageTask
- DescriboesToreImageTasks
- CreateRestoreImageTask
- Caminhos do arquivo

CreateStoreImageTask

A API `CreateStoreImageTask` armazena uma AMI como um único objeto em um bucket do S3.

A API cria uma tarefa que lê todos os dados da AMI e seus snapshots e, a seguir, usa um multipart upload do S3 para armazenar os dados em um objeto do S3. A API leva todos os componentes da AMI, incluindo a maioria dos metadados de AMI não específicos da região e todos os snapshots do EBS contidos na AMI, e os empacota em um único objeto no S3. Os dados são compactados como parte do processo de upload para reduzir a quantidade de espaço usado no S3; portanto, o objeto no S3 pode ser menor do que a soma dos tamanhos dos snapshots na AMI.

Se houver tags de AMI e de snapshot visíveis para a conta chamando essa API, elas serão preservadas.

O objeto no S3 tem o mesmo ID que a AMI, mas com uma extensão `.bin`. Os dados a seguir também são armazenados como tags de metadados do S3 no objeto do S3: nome da AMI, descrição

da AMI, data de registro da AMI, conta de proprietário da AMI e um timestamp para a operação de armazenamento.

O tempo necessário para concluir a tarefa depende do tamanho da AMI. Também depende de quantas outras tarefas estão em andamento porque as tarefas estão em fila. É possível acompanhar o andamento da tarefa chamando a API `DescribeStoreImageTasks`.

A soma dos tamanhos de todas as AMIs em andamento é limitada a 1.200 GB de dados de snapshot do EBS por conta. A criação de tarefas adicionais será rejeitada até que as tarefas em andamento sejam inferiores ao limite. Por exemplo, se uma AMI com 200 GB de dados de snapshot e outra AMI com 400 GB de dados de snapshot estiverem sendo armazenadas no momento, outra solicitação será aceita, pois o total em andamento é de 600 GB, que é inferior ao limite. Mas se uma única AMI com 1.200 GB de dados de snapshot estiver sendo armazenada no momento, outras tarefas serão rejeitadas até que a tarefa seja concluída.

DescriboesToreImageTasks

A API `DescribeStoreImageTasks` descreve o andamento das tarefas de armazenamento de uma AMI. É possível descrever tarefas para AMIs especificadas. Se você não especificar AMIs, receberá uma lista paginada de todas as tarefas de imagem de armazenamento que foram processadas nos últimos 31 dias.

Para cada tarefa de AMI, a resposta indica se a tarefa é `InProgressCompleted` ou `Failed`. Para tarefas `InProgress`, a resposta mostra um andamento estimado como uma porcentagem.

As tarefas são listadas em ordem cronológica inversa.

No momento, somente as tarefas do mês anterior podem ser visualizadas.

CreateRestoreImageTask

A API `CreateRestoreImageTask` inicia uma tarefa que restaura uma AMI de um objeto do S3 que foi criado anteriormente usando uma solicitação `CreateStoreImageTask`.

A tarefa de restauração pode ser executada na mesma região ou em uma região diferente daquela em que a tarefa de armazenamento foi executada.

O bucket do S3 a partir do qual o objeto da AMI será restaurado deve estar na mesma região em que a tarefa de restauração é solicitada. A AMI será restaurada nessa região.

A AMI é restaurada com seus metadados, como o nome, a descrição e os mapeamentos de dispositivos de blocos correspondentes aos valores da AMI armazenada. O nome deve ser exclusivo

para AMIs na região dessa conta. Se você não fornecer um nome, a nova AMI obterá o mesmo nome da AMI original. A AMI obtém um novo ID de AMI que é gerado no momento do processo de restauração.

O tempo necessário para a conclusão da tarefa de restauração da AMI depende do tamanho da AMI. Também depende de quantas outras tarefas estão em andamento porque as tarefas estão em fila. É possível visualizar o andamento da tarefa descrevendo a AMI (describe-images) ou seus snapshots do EBS (describe-snapshots). Se a tarefa falhar, a AMI e os snapshots serão movidos para um estado com falha.

A soma dos tamanhos de todas as AMIs em andamento é limitada a 600 GB (com base no tamanho após a restauração) de dados de snapshot do EBS por conta. A criação de tarefas adicionais será rejeitada até que as tarefas em andamento sejam inferiores ao limite.

Caminhos do arquivo

É possível usar caminhos de arquivo ao armazenar e restaurar AMIs, da seguinte forma:

- Ao armazenar uma AMI no S3, o caminho do arquivo pode ser adicionado ao nome do bucket. Internamente, o sistema separa o caminho do nome do bucket e, em seguida, adiciona o caminho à chave do objeto que é gerada para armazenar a AMI. O caminho completo do objeto é mostrado na resposta da chamada de API.
- Ao restaurar a AMI, como um parâmetro de chave de objeto está disponível, o caminho pode ser adicionado ao início do valor da chave do objeto.

Exemplo: nome do bucket com caminho de arquivo anexado

Ao armazenar a AMI, especifique o caminho do arquivo após o nome do bucket.

```
amzn-s3-demo-bucket/path1/path2
```

A chave do objeto resultante é mostrada a seguir.

```
path1/path2/ami-0abcdef1234567890.bin
```

Ao restaurar a AMI, especifique o nome do bucket e a chave do objeto. Para obter exemplos, consulte the section called “Criar uma tarefa de armazenamento de imagem”.

Criar uma tarefa de armazenamento de imagem

Quando você armazena uma AMI em um bucket do S3, uma tarefa de armazenamento de imagem é criada. É possível usar a tarefa de armazenamento de imagem para monitorar o andamento e o resultado do processo.

Conteúdo

- Proteger suas AMIs
- Permissões para armazenar e restaurar AMIs usando o S3
- Criar uma tarefa de armazenamento de imagem
- Criar uma tarefa de restauração de imagem

Proteger suas AMIs

É importante garantir que o bucket do S3 esteja configurado com segurança suficiente para proteger o conteúdo da AMI e que a segurança seja mantida enquanto os objetos da AMI permanecerem no bucket. Se isso não puder ser feito, o uso dessas APIs não é recomendado. Não permita acesso público ao bucket do S3. Recomendamos que você ative a Criptografia do lado do servidor para os buckets do S3 nos quais você armazena as AMIs, embora não seja necessário.

Para obter informações sobre como definir as configurações de segurança apropriadas para os buckets do S3, consulte os seguintes tópicos de segurança:

- Bloquear o acesso público ao armazenamento do Amazon S3
- Definir o comportamento padrão da criptografia para os buckets do Amazon S3
- Qual política de bucket do S3 devo usar para seguir a regra s3-bucket-ssl-requests-only do AWS Config?
- Habilitar o log de acesso ao servidor do Amazon S3

Quando os snapshots da AMI são copiados para o objeto S3, os dados são copiados em conexões TLS. É possível armazenar AMIs com snapshots criptografados, mas os snapshots são descriptografados como parte do processo de armazenamento.

Permissões para armazenar e restaurar AMIs usando o S3

Caso as entidades principais do IAM armazenem ou restaurem AMIs usando o Amazon S3, você precisará conceder a elas as permissões necessárias.

A política de exemplo a seguir inclui todas as ações necessárias para permitir que uma entidade principal do IAM execute as tarefas de armazenamento e restauração.

Também é possível criar políticas do IAM que concedam às entidades principais acesso apenas a recursos específicos. Para obter mais exemplos de políticas, consulte Gerenciamento de acesso para recursos da AWS no Guia do usuário do IAM.

> **Note**
>
> Se os snapshots que compõem a AMI estiverem criptografados ou se a conta estiver habilitada para criptografia por padrão, seu principal do IAM deverá ter permissão para usar a chave KMS.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:DeleteObject",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:PutObject",
                "s3:PutObjectTagging",
                "s3:AbortMultipartUpload",
                "ebs:CompleteSnapshot",
                "ebs:GetSnapshotBlock",
                "ebs:ListChangedBlocks",
                "ebs:ListSnapshotBlocks",
                "ebs:PutSnapshotBlock",
                "ebs:StartSnapshot",
                "ec2:CreateStoreImageTask",
                "ec2:DescribeStoreImageTasks",
                "ec2:CreateRestoreImageTask",
                "ec2:GetEbsEncryptionByDefault",
                "ec2:DescribeTags",
                "ec2:CreateTags"
            ],
```

```
            "Resource": "*"
        }
    ]
}
```

Criar uma tarefa de armazenamento de imagem

Para armazenar uma AMI em um bucket do S3, comece criando uma tarefa de armazenamento de imagem. O tempo necessário para concluir a tarefa depende do tamanho da AMI. É possível acompanhar o andamento da tarefa até que ela tenha êxito ou falhe.

AWS CLI

Para criar a tarefa de armazenamento de imagem

Use o comando create-store-image-task.

```
aws ec2 create-store-image-task \
    --image-id ami-0abcdef1234567890 \
    --bucket amzn-s3-demo-bucket
```

O seguinte é um exemplo de saída.

```
{
  "ObjectKey": "ami-0abcdef1234567890.bin"
}
```

Para descrever o andamento de uma tarefa de armazenamento de AMI

Use o comando describe-store-image-tasks.

```
aws ec2 describe-store-image-tasks \
    --image-ids ami-0abcdef1234567890 \
    --query StoreImageTaskResults[].StoreTaskState \
    --output text
```

O seguinte é um exemplo de saída.

```
InProgress
```

PowerShell

Para criar a tarefa de armazenamento de imagem

Use o cmdlet New-EC2StoreImageTask.

```
New-EC2StoreImageTask `
    -ImageId ami-0abcdef1234567890 `
    -Bucket amzn-s3-demo-bucket
```

O seguinte é um exemplo de saída.

```
ObjectKey         : ami-0abcdef1234567890.bin
```

Para descrever o andamento de uma tarefa de armazenamento de AMI

Use o cmdlet Get-EC2StoreImageTask.

```
(Get-EC2StoreImageTask -ImageId ami-0abcdef1234567890).StoreTaskState
```

O seguinte é um exemplo de saída.

```
InProgress
```

Criar uma tarefa de restauração de imagem

É necessário especificar um nome para a AMI restaurada. O nome deve ser exclusivo para AMIs na região dessa conta. A AMI restaurada obtém um novo ID de AMI.

AWS CLI

Para criar uma tarefa de armazenamento de imagem

Use o comando create-restore-image-task.

```
aws ec2 create-restore-image-task \
    --object-key ami-0abcdef1234567890.bin \
    --bucket amzn-s3-demo-bucket \
    --name "my-restored-ami"
```

O seguinte é um exemplo de saída.

```
{
   "ImageId": "ami-1234567890abcdef0"
}
```

PowerShell

Para criar uma tarefa de armazenamento de imagem

Use o cmdlet New-EC2RestoreImageTask.

```
New-EC2RestoreImageTask `
    -ObjectKey ami-0abcdef1234567890.bin `
    -Bucket amzn-s3-demo-bucket `
    -Name "my-restored-ami"
```

O seguinte é um exemplo de saída.

```
ImageId         : ami-1234567890abcdef0
```

Use a ancestralidade da AMI para rastrear a origem de uma AMI

A ancestralidade da AMI ajuda você a rastrear a origem de uma AMI retornando os IDs e as regiões de todas as AMIs ancestrais. Quando você cria ou copia uma AMI, a nova AMI retém o ID e a região de sua AMI de origem (principal). Isso permite que você rastreie a cadeia de AMIs até a AMI raiz.

Benefícios principais

O uso dos ancestrais de AMI é útil para que você:

- Rastreie os derivados de AMI para garantir a conformidade com as políticas internas.
- Identifique AMIs potencialmente vulneráveis quando um problema de segurança for encontrado em uma AMI ancestral.
- Mantenha a visibilidade das origens da AMI em várias regiões.

Tópicos

- Como funciona a ascendência da AMI

- Considerações
- Visualizar ascendência de AMI
- Identificar a AMI de origem

Como funciona a ascendência da AMI

A ascendência da AMI identifica a AMI principal que foi usada para criar a AMI especificada, a principal da principal e assim por diante, até a AMI raiz. Como isso funciona:

- Cada AMI exibe o ID e a região de sua AMI de origem (principal).
- Começando com a AMI selecionada, a lista de entradas de ascendência exibe cada AMI principal em sequência.
- A lista de entradas de ascendência remonta até chegar à AMI raiz. A AMI raiz é uma das seguintes:
  - Uma AMI pública de um provedor verificado (identificada pelo alias do proprietário, que é `amazon` ou `aws-marketplace`).
  - Uma AMI sem ancestral registrado. Por exemplo, ao usar RegisterImage para criar uma AMI diretamente de um conjunto de snapshots, não há nenhuma AMI de origem para rastrear, diferente da criação de uma AMI a partir de uma instância.
  - Uma AMI cuja AMI de origem é de uma partição diferente.
  - A 50ª AMI da lista. O número máximo de AMI em uma lista de ancestrais é 50.

Considerações

- O ID e a região da AMI de origem só estão disponíveis para AMIs criadas usando CreateImage, CopyImage ou CreateRestoreImageTask.
- Nas AMIs criadas utilizando CreateImage (cria uma AMI usando uma instância), o ID da AMI de origem é o ID da AMI utilizada para iniciar a instância.
- As informações de origem da AMI não estão disponíveis para:
  - AMIs criadas usando RegisterImage porque foram criadas a partir de instantâneos.
  - Para algumas AMIs mais antigas.
- As informações da AMI de origem são preservadas quando:
  - As AMIs são copiadas em todas as regiões.
  - As AMIs de origem são canceladas (excluídas).

  - Você não tem acesso às AMI de origem.
- Cada lista de ascendência é limitada a 50 AMIs.

Visualizar ascendência de AMI

É possível visualizar a ascendência de uma AMI usando os seguintes métodos.

Console

Para visualizar a ascendência de uma AMI

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione AMIs.
3. Selecione uma AMI e escolha a guia Ancestralidade da AMI.
4. A tabela de entradas de ancestralidade da AMI lista todas as AMIs na lista de ancestralidade.
   - ID da AMI — O identificador de cada AMI na lista de ancestralidade. A primeira entrada na tabela é a AMI selecionada, seguida por seus ancestrais.
   - ID da AMI de origem — A ID da AMI a partir da qual a AMI na coluna ID da AMI foi criada. Um traço (-) indica o fim da lista de ascendência da AMI.
   - Região da AMI de origem — Região da AWS Onde a AMI de origem está localizada.
   - Nível de ascendência — A posição na lista de ascendência, onde:
     - 0 (AMI de entrada) indica a AMI selecionada cuja ascendência você deseja conhecer.
     - Números crescentes mostram ancestrais mais antigos.
     - ***n*** (AMI original) indica a AMI raiz, com o número indicando até onde vai a lista de ancestrais.
   - Data de criação — Quando a AMI foi criada, no formato UTC.
   - Alias do proprietário — O alias do proprietário da AMI (por exemplo, `amazon`). Um traço (-) indica que a AMI não tem alias de proprietário.

AWS CLI

Para visualizar a ascendência de uma AMI

Use o comando get-image-ancestry e especifique o ID da AMI.

```
aws ec2 get-image-ancestry \
    --image-id ami-1111111111EXAMPLE \
    --region us-east-1
```

O seguinte é um exemplo de saída. A saída lista as AMIs em ordem de ascendência: a primeira entrada é a AMI especificada (de entrada), seguida pela principal, principal da principal e assim por diante, e termina com a AMI raiz.

```
{
    "ImageAncestryEntries": [
        {
            "CreationDate": "2025-01-17T18:37:50.000Z",
            "ImageId": "ami-1111111111EXAMPLE", // Input AMI
            "SourceImageId": "ami-2222222222EXAMPLE",
            "SourceImageRegion": "us-east-1"

        },
        {
            "CreationDate": "2025-01-17T18:37:50.000Z",
            "ImageId": "ami-2222222222EXAMPLE", // Parent AMI
            "SourceImageId": "ami-3333333333EXAMPLE",
            "SourceImageRegion": "us-east-1"
        },
        ...
        {
            "CreationDate": "2025-01-17T18:37:50.000Z",
            "ImageId": "ami-8888888888EXAMPLE", // Root AMI
            "ImageOwnerAlias": "aws-marketplace",
            "SourceImageId": "ami-9999999999EXAMPLE",
            "SourceImageRegion": "us-east-2"
        }
    ]
}
```

PowerShell

Para visualizar a ancestralidade de uma AMI

Use o cmdlet Get-EC2ImageAncestry.

```
Get-EC2ImageAncestry -ImageId ami-1111111111EXAMPLE
```

O seguinte é um exemplo de saída. A saída lista as AMIs em ordem de ascendência: a primeira entrada é a AMI especificada (de entrada), seguida pela principal, pela principal da principal e assim por diante, e termina com a AMI raiz.

```
ImageAncestryEntries : {
    @{
        CreationDate = "2025-01-17T18:37:50.000Z"
        ImageId = "ami-1111111111EXAMPLE"    # Input AMI
        SourceImageId = "ami-2222222222EXAMPLE"
        SourceImageRegion = "us-east-1"
    },
    @{
        CreationDate = "2025-01-17T18:37:50.000Z"
        ImageId = "ami-2222222222EXAMPLE"    # Parent AMI
        SourceImageId = "ami-3333333333EXAMPLE"
        SourceImageRegion = "us-east-1"
    },
    ...
    @{
        CreationDate = "2025-01-17T18:37:50.000Z"
        ImageId = "ami-8888888888EXAMPLE"    # Root AMI
        ImageOwnerAlias = "aws-marketplace"
        SourceImageId = "ami-9999999999EXAMPLE"
        SourceImageRegion = "us-east-2"
    }
}
```

Identificar a AMI de origem

Se você precisar identificar apenas a AMI principal imediata (de origem) usada para criar uma AMI, use os métodos a seguir.

Console

Para identificar a AMI de origem usada para criar a AMI selecionada

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione AMIs.
3. Selecione a AMI para visualizar os detalhes.

As informações da AMI de origem aparecem nos seguintes campos: ID da AMI de origem e Região da AMI de origem

AWS CLI

Para identificar a AMI de origem usada para criar a AMI especificada

Use o comando describe-images.

```
aws ec2 describe-images \
    --region us-east-1 \
    --image-ids ami-0abcdef1234567890 \
    --query "Images[].{ID:SourceImageId,Region:SourceImageRegion}"
```

O seguinte é um exemplo de saída.

```
[
    {
        "ID": "ami-0abcdef1234567890",
        "Region": "us-west-2"
    }
}
```

PowerShell

Para identificar a AMI de origem usada para criar a AMI especificada

Use o cmdlet Get-EC2Image.

```
Get-EC2Image -ImageId ami-0abcdef1234567890 | Select SourceImageId,
 SourceImageRegion
```

O seguinte é um exemplo de saída.

```
SourceImageId           SourceImageRegion
-------------           -----------------
ami-0abcdef1234567890 us-west-2
```

Gerenciar e monitorar o uso de AMIs

A AWS fornece vários recursos para ajudar você a gerenciar e monitorar o uso de AMIs de forma eficaz. É possível rastrear quais contas estão usando suas AMIs compartilhadas, identificar quando elas foram usadas pela última vez e descobrir quais recursos em sua Conta da AWS estão referenciando AMIs específicas.

A tabela a seguir fornece uma visão geral dos recursos para gerenciar e monitorar o uso de AMIs:

Recurso	Caso de uso	Benefícios principais
Relatórios de uso de AMIs	Obtenha visibilidade sobre quais Contas da AWS estão usando suas AMIs e o quanto cada AMI está sendo usada.	• Identifique as Contas da AWS e os tipos de recursos que referenciam suas AMIs para que você possa cancelar o registro ou desabilitar as AMIs com segurança. • Identifique AMIs não utilizadas para o cancelamento do registro para reduzir custos de armazenamento. • Identifique suas AMIs mais usadas.
Último rastreamento usado	Verifique quando sua AMI foi usada pela última vez.	• Identifique as AMIs não utilizadas para que você possa cancelar o registro das AMIs com segurança. • Identifique AMIs não utilizadas para o cancelame

Recurso	Caso de uso	Benefícios principais
		nto do registro para reduzir custos de armazenamento.
Verificação de referência de AMIs	Garanta que seus recursos da AWS estejam usando as AMIs compatíveis mais recentes.	• Audite o uso de AMIs em sua conta. • Verifique onde as AMIs específicas estão sendo referenciadas. • Mantenha a conformidade atualizando seus recursos para referenciar as AMIs mais recentes.

Tópicos

- Visualizar seu uso de AMIs
- Verificar quando uma AMI do Amazon EC2 foi usada pela última vez
- Identificar seus recursos que referenciam AMIs específicas

Visualizar seu uso de AMIs

Se você compartilhar suas imagens de máquina da Amazon (AMI) com outras Contas da AWS, seja com Contas da AWS específicas, organizações, unidades organizacionais (UOs) ou publicamente, você poderá ver como essas AMIs são usadas criando relatórios de uso de AMIs. Os relatórios fornecem visibilidade sobre:

- Quais Contas da AWS estão usando suas AMIs em instâncias do EC2 ou modelos de inicialização
- Quantas instâncias do EC2 ou modelos de reinicialização estão referenciando cada AMI

Os relatórios de uso de AMIs ajudam você a gerenciar suas AMIs com mais eficiência:

- Identifique as Contas da AWS e os tipos de recursos que referenciam suas AMIs para que você possa cancelar o registro ou desabilitar as AMIs com segurança.
- Identifique AMIs não utilizadas para o cancelamento do registro para reduzir custos de armazenamento.
- Identifique suas AMIs mais usadas.

Conteúdo

- Como funcionam os relatórios de uso de AMIs
- Criar um relatório de uso de AMIs
- Visualizar relatórios de uso de AMIs
- Excluir um relatório de uso de AMI
- Cotas de relatórios

Como funcionam os relatórios de uso de AMIs

Ao criar um relatório de uso de AMIs, especifique:

- A AMI a ser relatada.
- As Contas da AWS a serem verificadas (contas específicas ou todas as contas).
- Os tipos de recursos a serem verificados (instâncias do EC2, modelos de inicialização ou ambos).
- Para modelos de inicialização, o número de versões a serem verificadas (o padrão é as 20 versões mais recentes).

O Amazon EC2 cria um relatório separado para cada AMI. Cada relatório fornece:

- Uma lista das Contas da AWS usando a AMI.
- Uma contagem dos recursos que referenciam a AMI por tipo de recurso por conta. Observe que, para modelos de inicialização, se uma AMI for referenciada em várias versões de um modelo de inicialização, a contagem será de apenas um.

> **Important**
>
> Quando você gera um relatório de uso de AMIs, ele pode não conter a atividade mais recente. A atividade da instância das últimas 24 horas e a atividade do modelo de inicialização dos últimos dias podem não aparecer no relatório.

O Amazon EC2 exclui automaticamente um relatório 30 dias após ser criado. Você pode baixar os relatórios no console do EC2 para reter localmente.

Criar um relatório de uso de AMIs

Para ver como sua AMI está sendo usada, primeiro você deve criar um relatório de uso de AMIs, especificando as contas e os tipos de recursos a serem relatados. Depois que o relatório for criado, será possível visualizar o conteúdo do relatório. Você também pode baixar os relatórios no console do EC2.

Console

Para criar um relatório de uso de AMIs

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione AMIs.
3. Selecione uma AMI e escolha Ações, Uso de AMIs, Visualizar meu uso de AMIs.
4. Na página Criar meu relatório de uso de AMIs, faça o seguinte:
   a. Em Tipos de recursos, selecione um ou mais tipos de recursos a serem relatados.
   b. Em IDs de contas, siga um destes procedimentos:
      - Escolha Especificar IDs de contas e depois Adicionar ID de conta para cada conta a ser relatada.
      - Escolha Incluir todas as contas para gerar relatórios sobre todas as contas.
   c. Escolha Criar meu relatório de uso de AMIs.
5. Na página AMI, escolha a guia Meu uso de AMIs.
6. Escolha um ID de relatório para visualizar seus detalhes.

AWS CLI

Para criar um relatório de uso de AMIs para uma lista de contas

Use o comando create-image-usage-report com os seguintes parâmetros obrigatórios:

- `--image-id`: o ID da AMI sobre a ser relatada.
- `--resource-types`: os tipos de recursos a serem verificados. No exemplo a seguir, os tipos de recursos a serem verificados são instâncias do EC2 e modelos de inicialização. Além disso, o número de versões do modelo de inicialização a serem verificadas também é especificado (`version-depth=100`).

Para relatar contas específicas, use o parâmetro `--account-ids` para especificar o ID de cada conta a ser relatada.

```
aws ec2 create-image-usage-report \
    --image-id ami-0abcdef1234567890 \
    --account-ids 111122223333 444455556666 123456789012 \
    --resource-types ResourceType=ec2:Instance \
      'ResourceType=ec2:LaunchTemplate,ResourceTypeOptions=[{OptionName=version-
depth,OptionValues=100}]'
```

Para criar um relatório de uso de AMIs de todas as contas

Para relatar todas as contas usando a AMI especificada, use o mesmo comando, mas omita o parâmetro `--account-ids`.

```
aws ec2 create-image-usage-report \
    --image-id ami-0abcdef1234567890 \
    --resource-types ResourceType=ec2:Instance \
      'ResourceType=ec2:LaunchTemplate,ResourceTypeOptions=[{OptionName=version-
depth,OptionValues=100}]'
```

O seguinte é um exemplo de saída.

```
{
    "ReportId": "amiur-00b877d192f6b02d0"
}
```

Para monitorar o status da criação do relatório

Use o comando describe-image-usage-reports e especifique o ID do relatório.

```
aws ec2 describe-image-usage-reports --report-ids amiur-00b877d192f6b02d0
```

O seguinte é um exemplo de saída. O valor inicial do campo `State` é `pending`. Para poder visualizar as entradas do relatório, o estado deve ser `available`.

```
{
    "ImageUsageReports": [
        {
            "ImageId": "ami-0e9ae3dc21c2b3a64",
            "ReportId": "amiur-abcae3dc21c2b3999",
            "ResourceTypes": [
                {"ResourceType": "ec2:Instance"}
            ],
            "State": "pending",
            "CreationTime": "2025-09-29T13:27:12.322000+00:00",
            "ExpirationTime": "2025-10-28T13:27:12.322000+00:00"
        }
    ]
}
```

PowerShell

Para criar um relatório de uso de AMIs para uma lista de contas

Use o cmdlet New-EC2ImageUsageReport com os seguintes parâmetros obrigatórios:

- `-ImageId`: o ID da AMI sobre a ser relatada.
- `-ResourceType`: os tipos de recursos a serem verificados. No exemplo a seguir, os tipos de recursos a serem verificados são instâncias do EC2 e modelos de inicialização. Além disso, o número de versões do modelo de inicialização a serem verificadas também é especificado (`'version-depth' = 100`).

Para relatar contas específicas, use o parâmetro `-AccountId` para especificar o ID de cada conta a ser relatada.

```
New-EC2ImageUsageReport `
    -ImageId ami-0abcdef1234567890 `
    -AccountId 111122223333 444455556666 123456789012 `
```

```
    -ResourceType @(
        @{ResourceType = 'ec2:Instance'},
        @{ResourceType = 'ec2:LaunchTemplate'ResourceTypeOptions = @{'version-depth'
 = 100}
        })
```

Para criar um relatório de uso de AMIs de todas as contas

Para relatar todas as contas usando a AMI especificada, use o mesmo comando, mas omita o parâmetro `-AccountId`.

```
New-EC2ImageUsageReport `
    -ImageId ami-0abcdef1234567890 `
    -ResourceType @(
        @{ResourceType = 'ec2:Instance'},
        @{ResourceType = 'ec2:LaunchTemplate'ResourceTypeOptions = @{'version-depth'
 = 100}
        })
```

O seguinte é um exemplo de saída.

```
ReportId
--------
amiur-00b877d192f6b02d0
```

Para monitorar o status da criação do relatório

Use o comando Get-EC2ImageUsageReport e especifique o ID do relatório.

```
Get-EC2ImageUsageReport -ReportId amiur-00b877d192f6b02d0
```

O seguinte é um exemplo de saída. O valor inicial do campo `State` é `pending`. Para poder visualizar as entradas do relatório, o estado deve ser `available`.

```
ImageUsageReports
-----------------
{@{ImageId=ami-0e9ae3dc21c2b3a64; ReportId=amiur-abcae3dc21c2b3999;
 ResourceTypes=System.Object[]; State=pending; CreationTime=2025-09-29;
 ExpirationTime=2025-10-28}}
```

Visualizar relatórios de uso de AMIs

Você pode ver todos os relatórios de uso que criou para uma AMI nos últimos 30 dias. O Amazon EC2 exclui automaticamente um relatório 30 dias após ser criado.

Para cada relatório, você pode ver as Contas da AWS que estão usando a AMI, e para cada conta, uma contagem dos recursos que referenciam a AMI por tipo de recurso. Você também pode ver quando a criação do relatório foi iniciada. Essas informações só estão disponíveis quando o relatório está no estado Concluído (console) ou `available` (AWS CLI).

> **Important**
>
> Quando você gera um relatório de uso de AMIs, ele pode não conter a atividade mais recente. A atividade da instância das últimas 24 horas e a atividade do modelo de inicialização dos últimos dias podem não aparecer no relatório.

Console

Para visualizar um relatório de uso de AMIs

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione AMIs.
3. Selecione uma AMI.
4. Escolha a guia Meus relatórios de uso.

   A lista de relatórios mostra:

   - Todos os relatórios gerados nos últimos 30 dias para a AMI selecionada.
   - Para cada relatório, a coluna Hora de início do relatório mostra a data em que o relatório foi criado.
5. Escolha o ID do relatório para visualizar seu conteúdo.
6. Para voltar à guia Meus relatórios de uso na página de detalhes da AMI, escolha Exibir todos os relatórios dessa AMI.

AWS CLI

Para listar todos os relatórios de uso de AMIs para a AMI especificada

Use o comando describe-image-usage-reports e especifique o ID da AMI para obter uma lista de seus relatórios.

```
aws ec2 describe-image-usage-reports --image-ids ami-0abcdef1234567890
```

O seguinte é um exemplo de saída. Cada ID de relatório é listado junto com os tipos de recursos que foram verificados e as datas de criação e expiração do relatório. Você pode usar essas informações para identificar os relatórios cujas entradas você deseja visualizar.


```
{
  "ImageUsageReports": [
    {
      "ImageId": "ami-0abcdef1234567890",
      "ReportId": "amiur-1111111111111111",
      "ResourceTypes": [
        {
          "ResourceType": "ec2:Instance"
        }
      ],
      "State": "available",
      "CreationTime": "2025-09-29T13:27:12.322000+00:00",
      "ExpirationTime": "2025-10-28T13:27:12.322000+00:00",
      "Tags": []
    },
    {
      "ImageId": "ami-0abcdef1234567890",
      "ReportId": "amiur-2222222222222222",
      "ResourceTypes": [
        {
          "ResourceType": "ec2:Instance"
        },
        {
          "ResourceType": "ec2:LaunchTemplate"
        }
      ],
      "State": "available",
      "CreationTime": "2025-10-01T13:27:12.322000+00:00",
      "ExpirationTime": "2025-10-30T13:27:12.322000+00:00",
      "Tags": []
    }
  ],
  "NextToken": "opaque"
```

```
}
```

Para visualizar o conteúdo de um relatório de uso de AMI para a AMI especificada

Use o comando describe-image-usage-report-entries e especifique o ID da AMI. A resposta retorna todos os relatórios da AMI especificada, mostrando as contas que usaram a AMI e suas contagens de recursos.

```
aws ec2 describe-image-usage-report-entries --image-ids ami-0abcdef1234567890
```

O seguinte é um exemplo de saída.

```
{
  "ImageUsageReportEntries": [
    {
      "ImageId": "ami-0abcdef1234567890",
      "ResourceType": "ec2:Instance",
      "AccountId": "123412341234",
      "UsageCount": 15,
      "ReportCreationTime": "2025-09-29T13:27:12.322000+00:00",
      "ReportId": "amiur-1111111111111111"
    },
    {
      "ImageId": "ami-0abcdef1234567890",
      "ResourceType": "ec2:Instance",
      "AccountId": "123412341234",
      "UsageCount": 2,
      "ReportCreationTime": "2025-10-01T13:27:12.322000+00:00",
      "ReportId": "amiur-2222222222222222"
    },
    {
      "ImageId": "ami-0abcdef1234567890",
      "ResourceType": "ec2:Instance",
      "AccountId": "001100110011",
      "UsageCount": 39,
      "ReportCreationTime": "2025-10-01T13:27:12.322000+00:00",
      "ReportId": "amiur-2222222222222222"
    }
  ],
  "NextToken": "opaque"
}
```

Para visualizar o conteúdo de um relatório de uso de AMI do relatório especificado

Use o comando describe-image-usage-report-entries e especifique o ID do relatório. A resposta retorna todas as entradas do relatório especificado, mostrando as contas que usaram a AMI e suas contagens de recursos.

```
aws ec2 describe-image-usage-report-entries --report-ids amiur-1111111111111111
```

O seguinte é um exemplo de saída.

```
{
  "ImageUsageReportEntries": [
    {
      "ImageId": "ami-0abcdef1234567890",
      "ResourceType": "ec2:Instance",
      "AccountId": "123412341234",
      "UsageCount": 15,
      "ReportCreationTime": "2025-09-29T13:27:12.322000+00:00",
      "ReportId": "amiur-1111111111111111"
    },
    {
      "ImageId": "ami-0abcdef1234567890",
      "ResourceType": "ec2:LaunchTemplate",
      "AccountId": "123412341234",
      "UsageCount": 4,
      "ReportCreationTime": "2025-09-29T13:27:12.322000+00:00",
      "ReportId": "amiur-1111111111111111"
    },
    {
      "ImageId": "ami-0abcdef1234567890",
      "ResourceType": "ec2:LaunchTemplate",
      "AccountId": "001100110011",
      "UsageCount": 2,
      "ReportCreationTime": "2025-09-29T13:27:12.322000+00:00",
      "ReportId": "amiur-1111111111111111"
    }
  ],
  "NextToken": "opaque"
}
```

PowerShell

Para listar todos os relatórios de uso de AMIs para a AMI especificada

Use o cmdlet Get-EC2ImageUsageReport e especifique o ID da AMI para obter uma lista de seus relatórios.

```
Get-EC2ImageUsageReport -ImageId ami-0abcdef1234567890
```

O seguinte é um exemplo de saída. Cada ID de relatório é listado junto com os tipos de recursos que foram verificados e as datas de criação e expiração do relatório. Você pode usar essas informações para identificar os relatórios cujas entradas você deseja visualizar.

```
@{
    ImageUsageReports = @(
        @{
            ImageId = "ami-0abcdef1234567890"
            ReportId = "amiur-1111111111111111"
            ResourceTypes = @(
                @{
                    ResourceType = "ec2:Instance"
                }
            )
            State = "available"
            CreationTime = "2025-09-29T13:27:12.322000+00:00"
            ExpirationTime = "2025-10-28T13:27:12.322000+00:00"
        },
        @{
            ImageId = "ami-0abcdef1234567890"
            ReportId = "amiur-2222222222222222"
            ResourceTypes = @(
                @{
                    ResourceType = "ec2:Instance"
                }
            )
            State = "available"
            CreationTime = "2025-09-30T13:27:12.322000+00:00"
            ExpirationTime = "2025-10-29T13:27:12.322000+00:00"
        },
        @{
            ImageId = "ami-0abcdef1234567890"
            ReportId = "amiur-3333333333333333"
            ResourceTypes = @(
                @{
                    ResourceType = "ec2:Instance"
                }
            )
```

```
            State = "available"
            CreationTime = "2025-10-01T13:27:12.322000+00:00"
            ExpirationTime = "2025-10-30T13:27:12.322000+00:00"
        }
    )
    NextToken = "opaque"
}
```

Para visualizar o conteúdo de um relatório de uso de AMI para a AMI especificada

Use o cmdlet Get-EC2ImageUsageReportEntry e especifique o ID da AMI. A resposta retorna todos os relatórios da AMI especificada, mostrando as contas que usaram a AMI e suas contagens de recursos.

```
Get-EC2ImageUsageReportEntry -ImageId ami-0abcdef1234567890
```

O seguinte é um exemplo de saída.

```
ImageUsageReportEntries : {@{
    ImageId = "ami-0abcdef1234567890"
    ResourceType = "ec2:Instance"
    AccountId = "123412341234"
    UsageCount = 15
    ReportCreationTime = "2025-09-29T13:27:12.322000+00:00"
    ReportId = "amiur-1111111111111111"
    }, @{
    ImageId = "ami-0abcdef1234567890"
    ResourceType = "ec2:Instance"
    AccountId = "123412341234"
    UsageCount = 7
    ReportCreationTime = "2025-09-30T13:27:12.322000+00:00"
    ReportId = "amiur-2222222222222222"
    }...}
NextToken : opaque
```

Para visualizar o conteúdo de um relatório de uso de AMI do relatório especificado

Use o cmdlet Get-EC2ImageUsageReportEntry e especifique o ID do relatório. A resposta retorna todas as entradas do relatório especificado, mostrando as contas que usaram a AMI e suas contagens de recursos.

```
Get-EC2ImageUsageReportEntry -ReportId amiur-1111111111111111
```

O seguinte é um exemplo de saída.

```
ImageUsageReportEntries : {@{
    ImageId = "ami-0abcdef1234567890"
    ResourceType = "ec2:Instance"
    AccountId = "123412341234"
    UsageCount = 15
    ReportCreationTime = "2025-09-29T13:27:12.322000+00:00"
    ReportId = "amiur-11111111111111111"
    }, @{
    ImageId = "ami-0abcdef1234567890"
    ResourceType = "ec2:LaunchTemplate"
    AccountId = "123412341234"
    UsageCount = 4
    ReportCreationTime = "2025-09-29T13:27:12.322000+00:00"
    ReportId = "amiur-11111111111111111"
    }, @{
    ImageId = "ami-0abcdef1234567890"
    ResourceType = "ec2:LaunchTemplate"
    AccountId = "************"
    UsageCount = 2
    ReportCreationTime = "2025-09-29T13:27:12.322000+00:00"
    ReportId = "amiur-11111111111111111"
    }}
NextToken : opaque
```

Excluir um relatório de uso de AMI

O Amazon EC2 exclui automaticamente um relatório 30 dias após ser criado. Você pode excluí-lo manualmente antes desse período.

Console

Para excluir um relatório de uso de AMI

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

4. Escolha a guia Meu uso de AMIs.
5. Escolha o botão Excluir ao lado do relatório a ser excluído.

AWS CLI

Para excluir um relatório de uso de AMI

Use o comando delete-image-usage-report e especifique o ID do relatório.

```
aws ec2 delete-image-usage-report --report-id amiur-0123456789abcdefg
```

PowerShell

Para excluir um relatório de uso de AMI

Use o cmdlet Remove-EC2ImageUsageReport e especifique o ID do relatório.

```
Remove-EC2ImageUsageReport -ReportId amiur-0123456789abcdefg
```

Cotas de relatórios

As cotas a seguir se aplicam à criação de relatórios de uso de AMIs. Estas cotas são aplicáveis por Região da AWS.

Descrição	Quota
Relatórios de uso de AMIs em andamento (`pending`) por Conta da AWS	2.000
Relatórios de uso de AMIs em andamento (`pending`) por AMI	1

Verificar quando uma AMI do Amazon EC2 foi usada pela última vez

O Amazon EC2 rastreia a data e a hora quando a AMI foi usada a última vez para executar uma instância. Se tiver uma AMI que não tenha sido usada para executar uma instância há muito tempo, considere se a AMI é uma boa candidata para cancelamento de registro ou defasagem.

Considerações

- Quando uma AMI é usada para iniciar uma instância, há um atraso de 24 horas antes que o uso seja incluído em relatórios.
- Você precisa ser o proprietário da AMI para obter a hora da última execução.
- Os dados de uso das AMIs estão disponíveis a partir de abril de 2017.

Console

Como visualizar a última hora de início de uma AMI

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação à esquerda, selecione AMIs.
3. Na barra de filtros, escolha Owned by me (Sou proprietário).
4. Marque a caixa de seleção da AMI.
5. Na guia Detalhes, encontre Hora da última inicialização.

AWS CLI

Para visualizar a hora da última inicialização descrevendo a AMI

Use o comando describe-images. Se `LastLaunchedTime` não estiver presente na saída, verifique se você é o proprietário da AMI.

```
aws ec2 describe-images \
    --image-id ami-0abcdef1234567890 \
    --query Images[].LastLaunchedTime \
    --output text
```

O seguinte é um exemplo de saída.

```
2025-02-17T20:22:19Z
```

Para visualizar o atributo da hora de última inicialização de uma AMI

Use o comando describe-image-attribute. Você precisa ser o proprietário da AMI especificada.

```
aws ec2 describe-image-attribute \
```

```
    --image-id ami-0abcdef1234567890 \
    --attribute lastLaunchedTime \
    --query LastLaunchedTime.Value \
    --output text
```

O seguinte é um exemplo de saída.

```
2025-02-17T20:22:19Z
```

PowerShell

Para visualizar a hora da última inicialização descrevendo a AMI

Use o cmdlet Get-EC2Image. Se `LastLaunchedTime` não estiver presente na saída, verifique se você é o proprietário da AMI.

```
(Get-EC2Image -ImageId ami-0abcdef1234567890).LastLaunchedTime
```

O seguinte é um exemplo de saída.

```
2025-02-17T20:22:19Z
```

Para visualizar o atributo da hora de última inicialização de uma AMI

Use o cmdlet Get-EC2ImageAttribute. Você precisa ser o proprietário da AMI especificada.

```
(Get-EC2ImageAttribute `
    -ImageId ami-0abcdef1234567890 `
    -Attribute LastLaunchedTime).LastLaunchedTime
```

O seguinte é um exemplo de saída.

```
2025-02-17T20:22:19Z
```

Identificar seus recursos que referenciam AMIs específicas

É possível identificar seus recursos da AWS que referenciam imagens de máquina da Amazon (AMIs) específicas, independentemente de as AMIs serem públicas ou privadas ou de quem as

possui. Essa visibilidade ajuda você a garantir que seus recursos usem as mais recentes AMIs compatíveis.

Benefícios principais

A verificação das referências de AMIs ajuda para que você:

- Audite o uso de AMIs em sua conta.
- Verifique onde as AMIs específicas estão sendo referenciadas.
- Mantenha a conformidade atualizando seus recursos para referenciar as AMIs mais recentes.

Tópicos

- Recursos compatíveis
- Como funcionam as verificações de referência de AMIs
- Permissões obrigatórias do IAM
- Etapas para verificar as referências de AMIs

Recursos compatíveis

As referências de AMIs podem ser verificadas em:

- Instâncias do EC2
- Modelos de execução
- Parâmetros do SSM
- Fórmulas de imagens do Image Builder
- Fórmulas de contêineres do Image Builder

Como funcionam as verificações de referência de AMIs

Operação básica

Ao executar uma verificação de referência de AMIs:

- Especifique quais AMIs devem ser verificadas.
- Escolha quais tipos de recursos serão verificados.

- Receba uma lista de seus recursos que referenciam AMIs específicas.

Seleção do tipo de recurso

No console, você seleciona os tipos de recursos a serem verificados.

Na CLI, você especifica os tipos de recursos a serem verificados usando um ou os dois dos seguintes parâmetros da CLI:

- `IncludeAllResourceTypes`: verifica todos os tipos de recursos compatíveis.
- `ResourceTypes`: verifica os tipos de recursos especificados.

Definir o escopo de respostas

É possível definir o escopo de respostas para instâncias do EC2 e modelos de inicialização personalizando os valores de `ResourceTypeOptions` usando o parâmetro `ResourceTypes`. Tanto o console quanto o parâmetro `IncludeAllResourceTypes` usam valores de opção padrão. Quando `ResourceTypes` e `IncludeAllResourceTypes` são usados juntos, os valores das opções de `ResourceTypes` têm precedência sobre os padrões.

Os seguintes valores padrão são usados:

Tipo de recurso	Opção de escopo (**`OptionName`**)	Finalidade	Valores padrão para **`OptionValue`** e o console
Instâncias do EC2	`state-name`	Filtrar por estado da instância	`pending`, `running`, `shutting-down`, `terminated`, `stopping`, `stopped` (todos os estados)
Modelos de execução	`version-depth`	Especifique o número de versões do modelo de inicialização a serem verificadas (começando pela versão mais recente)	`10` (versões mais recentes)

Permissões obrigatórias do IAM

Para usar a API DescribeImageReferences para identificar seus recursos que referenciam AMIs específicas, você precisa das seguintes permissões do IAM para descrever os recursos:

- `ec2:DescribeInstances`
- `ec2:DescribeLaunchTemplates`
- `ec2:DescribeLaunchTemplateVersions`
- `ssm:DescribeParameters`
- `ssm:GetParameters`
- `imagebuilder:ListImageRecipes`
- `imagebuilder:ListContainerRecipes`
- `imagebuilder:GetContainerRecipe`

Exemplo de política do IAM para usar a API DescribeImageReferences

O exemplo de política a seguir concede a você as permissões para usar a API DescribeImageReferences, que inclui as permissões para descrever instâncias do EC2, modelos de inicialização, parâmetros do Systems Manager, fórmulas de imagens do Image Builder e fórmulas de contêineres do Image Builder.

JSON

```
{
 "Version":"2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": "ec2:DescribeImageReferences",
   "Resource": "*"
  },
  {
   "Effect": "Allow",
   "Action": [
    "ec2:DescribeInstances",
    "ec2:DescribeLaunchTemplates",
    "ec2:DescribeLaunchTemplateVersions",
    "ssm:DescribeParameters",
```

```
    "ssm:GetParameters",
    "imagebuilder:ListImageRecipes",
    "imagebuilder:ListContainerRecipes",
    "imagebuilder:GetContainerRecipe"
   ],
   "Resource": "*",
   "Condition": {
    "ForAnyValue:StringEquals": {
     "aws:CalledVia": [
      "ec2-images.amazonaws.com"
     ]
    }
   }
  }
 ]
}
```

Important

É altamente recomendável usar a política gerenciada `AmazonEC2ImageReferencesAccessPolicy` da AWS em vez de criar a política você mesmo. Criar uma política do IAM personalizada que forneça somente as permissões necessárias requer tempo e experiência, e exigirá atualizações à medida que novos tipos de recursos forem disponibilizados.

A política gerenciada `AmazonEC2ImageReferencesAccessPolicy`:

- Concede todas as permissões necessárias para usar a API DescribeImageReferences, que inclui as permissões para descrever instâncias do EC2, modelos de inicialização, parâmetros do Systems Manager e fórmulas de imagens e de contêineres do Image Builder.
- É automaticamente compatível com novos tipos de recursos à medida que ficam disponíveis (especialmente importante ao usar o parâmetro `IncludeAllResourceTypes`).

É possível anexar a política `AmazonEC2ImageReferencesAccessPolicy` às identidades do IAM (usuários, grupos e perfis).

Para visualizar as permissões incluídas nessa política, consulte AmazonEC2ImageReferencesAccessPolicy na Referência de políticas gerenciadas pela AWS.

Etapas para verificar as referências de AMIs

Use os procedimentos a seguir para identificar quais dos seus recursos da AWS estão referenciando AMIs específicas.

Console

Para identificar recursos referenciando AMIs específicas

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione AMIs.
3. Selecione uma ou mais AMIs para verificar as referências.
4. Escolha Ações, Uso de AMIs, Visualizar recursos referenciados.
5. Na página Visualizar recursos referenciando AMIs selecionadas:
   a. Em Tipos de recursos, selecione um ou mais tipos de recursos.
   b. Escolha Visualizar recursos.
6. A seção Recursos referenciando AMIs selecionadas é exibida. A lista exibe os recursos que referenciam AMIs específicas. Cada linha fornece as seguintes informações:
   - ID da AMI: o ID da AMI referenciada.
   - Tipo de recurso: o tipo de recurso do recurso que referencia a AMI.
   - ID do recurso: o ID do recurso que referencia a AMI.

AWS CLI

Para verificar as referências de AMIs para tipos de recursos específicos

Use o comando describe-image-references com o parâmetro `--resource-types`. O exemplo a seguir verifica as instâncias do EC2 (definição do escopo por estado da instância), modelos de inicialização (considerando as 20 versões mais recentes de modelos de inicialização) e outros tipos de recursos específicos.

```
aws ec2 describe-image-references \
    --image-ids ami-0abcdef1234567890 ami-1234567890abcdef0 \
    --resource-types \
        'ResourceType=ec2:Instance,ResourceTypeOptions=[{OptionName=state-
name,OptionValues=[running,pending]}]' \
        'ResourceType=ec2:LaunchTemplate,ResourceTypeOptions=[{OptionName=version-
depth,OptionValues=[20]}]' \
        'ResourceType=ssm:Parameter' \
        'ResourceType=imagebuilder:ImageRecipe' \
        'ResourceType=imagebuilder:ContainerRecipe'
```

O seguinte é um exemplo de saída.

```
{
    "ImageReferences": [
        {
            "ImageId": "ami-0abcdef1234567890",
            "ResourceType": "ec2:Instance",
            "Arn": "arn:aws:ec2:us-east-1:123456789012:instance/i-1234567890abcdef0"
        },
        {
            "ImageId": "ami-1234567890abcdef0",
            "ResourceType": "ec2:LaunchTemplate",
            "Arn": "arn:aws:ec2:us-east-1:123456789012:launch-template/
lt-1234567890abcdef0"
        }
    ]
}
```

Para verificar as referências de AMIs para todos os tipos de recursos compatíveis

Use o comando describe-image-references com o parâmetro `--include-all-resource-types`.

```
aws ec2 describe-image-references \
    --image-ids ami-0abcdef1234567890 ami-1234567890abcdef0 \
    --include-all-resource-types
```

Para verificar as referências de AMIs para todos os tipos de recursos compatíveis e opções específicas

Use o comando describe-image-references com os parâmetros `--include-all-resource-types` e `--resource-types`. Este exemplo verifica todos os tipos de recursos ao definir o escopo da resposta das instâncias do EC2 para as instâncias em execução ou pendentes.

```
aws ec2 describe-image-references \
    --image-ids ami-0abcdef1234567890 ami-1234567890abcdef0 \
    --include-all-resource-types \
    --resource-types
 'ResourceType=ec2:Instance,ResourceTypeOptions=[{OptionName=state-
name,OptionValues=[running,pending]}]'
```

PowerShell

Para verificar as referências de AMIs para tipos de recursos específicos

Use o cmdlet Get-EC2ImageReference com o parâmetro `-ResourceType`. O exemplo a seguir verifica as instâncias do EC2 (definição do escopo por estado da instância), modelos de inicialização (considerando as 20 versões mais recentes de modelos de inicialização) e outros tipos de recursos específicos.

```
Get-EC2ImageReference `
    -ImageId 'ami-0abcdef1234567890', 'ami-1234567890abcdef0' `
    -ResourceType @(
        @{
            ResourceType = 'ec2:Instance'
            ResourceTypeOptions = @(
                @{
                    OptionName = 'state-name'
                    OptionValues = @('running', 'pending')
                }
            )
        },
        @{
            ResourceType = 'ec2:LaunchTemplate'
            ResourceTypeOptions = @(
                @{
                    OptionName = 'version-depth'
                    OptionValues = @('20')
                }
            )
        },
        @{
```

```
            ResourceType = 'ssm:Parameter'
        },
        @{
            ResourceType = 'imagebuilder:ImageRecipe'
        },
        @{
            ResourceType = 'imagebuilder:ContainerRecipe'
        }
    )
```

Para verificar as referências de AMIs para todos os tipos de recursos compatíveis

Use o cmdlet Get-EC2ImageReference com o parâmetro `-IncludeAllResourceTypes`.

```
Get-EC2ImageReference `
    -ImageId 'ami-0abcdef1234567890', 'ami-1234567890abcdef0' `
    -IncludeAllResourceTypes
```

Para verificar as referências de AMIs para todos os tipos de recursos compatíveis e opções específicas

Use o cmdlet Get-EC2ImageReference com os parâmetros `-IncludeAllResourceTypes` e `-ResourceType`. Este exemplo verifica todos os tipos de recursos ao definir o escopo da resposta das instâncias do EC2 para as instâncias em execução ou pendentes.

```
Get-EC2ImageReference `
    -ImageId 'ami-0abcdef1234567890', 'ami-1234567890abcdef0' `
    -IncludeAllResourceTypes `
    -ResourceType @(
        @{
            ResourceType = 'ec2:Instance'
            ResourceTypeOptions = @(
                @{
                    OptionName = 'state-name'
                    OptionValues = @('running', 'pending')
                }
            )
        }
    )
```

Descontinuar uma AMI do Amazon EC2

É possível defasar uma AMI para indicar que ela está desatualizada e não deve ser usada. Também é possível especificar uma data de defasagem futura para uma AMI, indicando quando a AMI estará desatualizada. Por exemplo, é possível defasar uma AMI cuja manutenção não está mais ativa ou pode defasar uma AMI que foi substituída por uma versão mais recente. Por padrão, as AMIs defasadas não aparecem nas listagens de AMI, impedindo que novos usuários usem AMIs desatualizadas. No entanto, os usuários existentes e os serviços de inicialização, como modelos de inicialização e grupos do Auto Scaling, podem continuar usando uma AMI defasada especificando seu ID. Para excluir a AMI, de modo que usuários e serviços não possam usá-la, é necessário cancelar o registro dela.

Depois que uma AMI estiver defasada:

- Para usuários de AMI, a AMI defasada não aparece nas chamadas de API DescribeImages, a menos que você especifique o ID dela ou especifique que AMIs defasadas devem ser exibidas. Os proprietários da AMI continuam a ver AMIs defasadas nas chamadas de API DescribeImages.
- Para usuários de AMI, a AMI defasada não está disponível para seleção no console do EC2. Por exemplo, uma AMI defasada não é exibida no catálogo da AMI no assistente de inicialização de instância. Os proprietários da AMI continuam a ver AMIs defasadas no console do EC2.
- Para os usuários da AMI, se você souber o ID de uma AMI defasada, poderá continuar a iniciar instâncias usando a AMI defasada com a API, a CLI ou os SDKs.
- Os serviços de inicialização, como modelos de inicialização e grupos do Auto Scaling, podem continuar referenciando a AMIs defasadas.
- As instâncias do EC2 que foram iniciadas usando uma AMI que posteriormente é defasada não são afetadas e podem ser interrompidas, iniciadas e reinicializadas.

É possível defasar AMIs privadas e públicas.

Conteúdo

- Custos
- Considerações
- Defasar uma AMI
- Descrever AMIs defasadas
- Cancelar a descontinuação da AMI

Custos

Quando você defasar uma AMI, a AMI não será excluída. O proprietário da AMI continuará pagando pelos snapshots da AMI. Para parar de pagar pelos instantâneos, o proprietário da AMI deve excluir a AMI cancelando o registro dela.

Considerações

- Para defasar uma AMI, é necessário ser o proprietário da AMI.
- AMIs que não tenham sido usadas recentemente para iniciar uma instância podem ser boas candidatas para descontinuação ou cancelamento de registro. Para obter mais informações, consulte the section called “Verificar quando uma AMI foi usada pela última vez”.
- É possível criar políticas de AMI apoiadas pelo EBS Amazon Data Lifecycle Manager para automatizar a descontinuação das AMIs apoiadas pelo EBS. Para obter mais informações, consulte Create AMI lifecycle policies.
- Por padrão, a data de descontinuação de todas as AMIs públicas é definida como dois anos a partir da data de criação da AMI. É possível definir a data de descontinuação para antes de dois anos. Para cancelar a data de descontinuação ou adiá-la para uma data posterior, você deve tornar a AMI privada compartilhando-a somente com contas específicas da AWS.

Defasar uma AMI

É possível defasar uma AMI em uma data e hora específicas. É necessário ser o proprietário da AMI.

O limite superior para a data de descontinuação é daqui a 10 anos, exceto para AMIs públicas, em que o limite superior é de 2 anos após a data de criação. Você não pode especificar uma data no passado.

Console

Para descontinuar uma AMI em uma data específica

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No navegador à esquerda, escolha AMIs.
3. Na barra de filtros, escolha Owned by me (Sou proprietário).
4. Selecione a AMI e escolha Actions (Ações), Manage AMI Deprecation (Gerenciar descontinuação da AMI). É possível selecionar várias AMIs para definir a mesma data de descontinuação de várias AMIs de uma só vez.

5. Marque a caixa de seleção Habilitar e insira a data e a hora de descontinuação.
6. Escolha Salvar.

AWS CLI

Para descontinuar uma AMI em uma data específica

Usar o comando disable-image-deprecation. Se você especificar um valor para segundos, o Amazon EC2 arredondará os segundos para o minuto mais próximo.

```
aws ec2 enable-image-deprecation \
    --image-id ami-0abcdef1234567890 \
    --deprecate-at "2025-04-15T13:17:12.000Z"
```

PowerShell

Para descontinuar uma AMI em uma data específica

Use o cmdlet Enable-EC2ImageDeprecation. Se você especificar um valor para segundos, o Amazon EC2 arredondará os segundos para o minuto mais próximo.

```
Enable-EC2ImageDeprecation `
    -ImageId ami-0abcdef1234567890 `
    -DeprecateAt 2025-04-15T13:17:12.000Z
```

Descrever AMIs defasadas

É possível visualizar a data e a hora de descontinuação de uma AMI e filtrar as AMIs por data de substituição.

Console

Para visualizar a data de descontinuação de uma AMI

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No navegador, escolha AMIs e, em seguida, selecione a AMI.
3. Selecione o campo Hora da descontinuação (se você marcou a caixa de seleção ao lado da AMI, ele estará localizado na guia Detalhes). O campo mostra a data e a hora de descontinuação da AMI. Se o campo estiver vazio, a AMI não estará descontinuada.

Para filtrar AMIs por data de descontinuação

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No navegador à esquerda, escolha AMIs.
3. Na barra de filtros, escolha Owned by me (Sou proprietário) ou Private images (Imagens privadas) (as imagens privadas incluem AMIs compartilhadas com você e de sua propriedade).
4. Na Search bar (Barra de pesquisa), insira **`Deprecation time`** (à medida que você insere as letras, o filtro Deprecation time (Hora da descontinuação) aparece) e, em seguida, escolha um operador e uma data e hora.

AWS CLI

Quando você descreve todas as AMIs, os resultados dependerão se você é usuário da AMI ou proprietário da AMI.

- Usuário da AMI: por padrão, quando você descreve todas as AMIs, as AMIs descontinuadas compartilhadas com você, mas das quais você não é proprietário, são excluídas. Para incluir AMIs descontinuadas nos resultados, especifique a opção `--include-deprecated`.
- Proprietário da AMI: quando você descreve todas as AMIs, todas as AMIs das quais você é proprietário, inclusive AMIs descontinuadas, são incluídas. Você não pode usar a opção `--no-include-deprecated` para excluir as AMIs descontinuadas de sua propriedade.

Para incluir as AMIs descontinuadas ao descrever todas as AMIs de uma conta

Use o seguinte comando describe-images.

```
aws ec2 describe-images
    --owners 123456789012 \
    --include-deprecated
```

Para descrever as AMIs descontinuadas da sua conta

Use o seguinte comando describe-images.

```
aws ec2 describe-images \
    --owners self \
    --query "Images[?DeprecationTime!=null].ImageId" \
```

```
    --output text
```

O seguinte é um exemplo de saída.

```
ami-0abcdef1234567890
```

Para descrever a data de descontinuação de uma AMI

Use o seguinte comando describe-images. Se `DeprecationTime` não estiver presente na saída, a AMI não será descontinuada nem será definida para descontinuação em uma data futura.

```
aws ec2 describe-images \
    --image-ids ami-0abcdef1234567890 \
    --query Images[].DeprecationTime \
    --output text
```

O seguinte é um exemplo de saída.

```
2025-05-01T00:00:00.000Z
```

PowerShell

Para listar as AMIs descontinuadas da sua conta

Use o cmdlet Get-EC2Image.

```
(Get-EC2Image -Owner self | Where-Object {$_.DeprecationTime -ne $null}).ImageId
```

O seguinte é um exemplo de saída.

```
ami-0abcdef1234567890
```

Para descrever a data de descontinuação de uma AMI

Use o cmdlet Get-EC2Image. Se `DeprecationTime` não estiver presente na saída, a AMI não será descontinuada nem será definida para descontinuação em uma data futura.

```
(Get-EC2Image -ImageId ami-0abcdef1234567890).DeprecationTime
```

O seguinte é um exemplo de saída.

```
2025-05-01T00:00:00.000Z
```

Cancelar a descontinuação da AMI

É possível cancelar a descontinuação de uma AMI, o que remove a data e a hora de descontinuação. É necessário ser o proprietário da AMI para executar esse procedimento.

Console

Para cancelar a descontinuação de uma AMI

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No navegador à esquerda, escolha AMIs.
3. Na barra de filtros, escolha Owned by me (Sou proprietário).
4. Selecione a AMI e escolha Actions (Ações), Manage AMI Deprecation (Gerenciar descontinuação da AMI). É possível selecionar várias AMIs para cancelar a descontinuação de várias AMIs de uma só vez.
5. Desmarque a caixa de seleção Habilitar e escolha Salvar.

AWS CLI

Para cancelar a descontinuação de uma AMI

Use o seguinte comando disnable-image-deprecation.

```
aws ec2 disable-image-deprecation --image-id ami-0abcdef1234567890
```

PowerShell

Para cancelar a descontinuação de uma AMI

Use o cmdlet Disable-EC2ImageDeprecation.

```
Disable-EC2ImageDeprecation -ImageId ami-0abcdef1234567890
```

Desabilitar uma AMI do Amazon EC2

Você pode desabilitar uma AMI para evitar que ela seja usada em execuções de instâncias. Não é possível executar novas instâncias por meio de uma AMI desabilitada. Você pode reabilitar uma AMI desabilitada para que ela possa ser usada novamente em execuções de instâncias.

É possível desabilitar AMIs privadas e públicas.

Para reduzir os custos de armazenamento de AMIs baseadas no EBS desabilitadas, que são usadas raramente, mas que precisam ser retidas a longo prazo, você pode arquivar os snapshots a elas associados. Para obter mais informações, consulte Arquivar snapshots do Amazon EBS no Guia do usuário do Amazon EC2.

Conteúdo

- Como funciona a desabilitação de AMI
- Custos
- Pré-requisitos
- Permissões obrigatórias do IAM
- Desabilitar uma AMI
- Descrever AMIs desabilitadas
- Reabilitar uma AMI desabilitada

Como funciona a desabilitação de AMI

> **Warning**
>
> Ao desabilitar uma AMI, todas as permissões de execução são removidas.

Quando uma AMI é desabilitada:

- O estado da AMI muda para `disabled`.
- Uma AMI desabilitada não pode ser compartilhada. Se uma AMI era pública ou compartilhada, ela se tornará privada. Se uma AMI era compartilhada com uma Conta da AWS, organização ou unidade organizacional, elas perderão o acesso à AMI desabilitada.

- Por padrão, uma AMI desabilitada não é exibida nas chamadas da API DescribeImages.
- Uma AMI desabilitada não é exibida no filtro De minha propriedade do console. Para encontrar AMIs desabilitadas, use o filtro Imagens desabilitadas do console.
- Não é possível selecionar uma AMI desabilitada para execuções de instâncias no console do EC2. Por exemplo, uma AMI desabilitada não é exibida no catálogo de AMIs do assistente de execução da instância nem ao criar um modelo de execução.
- Os serviços de execução, como modelos de execução e grupos do Auto Scaling, podem continuar fazendo referência a AMIs desabilitadas. As execuções subsequentes de instâncias com base em uma AMI desabilitada vão falhar. Por isso, recomendamos atualizar os modelos de execução e os grupos do Auto Scaling para fazer referência somente às AMIs disponíveis.
- As instâncias do EC2 que eram executadas usando uma AMI que mais tarde foi desabilitada não serão afetadas e poderão ser interrompidas, iniciadas e reinicializadas.
- Não é possível excluir snapshots associados a AMIs desabilitadas. Tentar excluir um snapshot associado resulta no erro `snapshot is currently in use`.

Quando uma AMI é reabilitada:

- O estado da AMI muda para `available`, e ela pode ser usada para executar instâncias.
- A AMI pode ser compartilhada.
- Contas da AWS, organizações e unidades organizacionais que perderam o acesso à AMI quando ela foi desabilitada não recuperam o acesso automaticamente, mas a AMI pode ser compartilhada com elas de novo.

Custos

Quando você desabilita uma AMI, ela não é excluída. Se a AMI for uma AMI baseada no EBS, você continua pagando pelos snapshots do EBS da AMI. Se você quiser manter a AMI, talvez consiga reduzir os custos de armazenamento arquivando os snapshots. Para obter mais informações, consulte Arquivar snapshots do Amazon EBS no Guia do usuário do Amazon EC2. Se não quiser manter a AMI e seus snapshots, é preciso cancelar o registro da AMI e excluir os snapshots. Para obter mais informações, consulte Cancelar o registro de uma AMI.

Pré-requisitos

Para desabilitar ou reabilitar uma AMI, é preciso ser o proprietário da AMI.

Permissões obrigatórias do IAM

Para desabilitar e reabilitar uma AMI, é necessário ter as seguintes permissões do IAM:

- `ec2:DisableImage`
- `ec2:EnableImage`

Desabilitar uma AMI

Você pode desabilitar uma AMI usando o console do EC2 ou a AWS Command Line Interface (AWS CLI). É necessário ser o proprietário da AMI para executar esse procedimento.

Console

Desabilitar uma AMI

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação à esquerda, selecione AMIs.
3. Na barra de filtros, escolha Owned by me (Sou proprietário).
4. Selecione a AMI e escolha Ações, Desativar a AMI. É possível selecionar várias AMIs para serem desabilitadas de uma vez.
5. Na janela Desativar AMI, escolha Desativar AMI.

AWS CLI

Desabilitar uma AMI

Use o seguinte comando disable-image:

```
aws ec2 disable-image --image-id ami-0abcdef1234567890
```

PowerShell

Desabilitar uma AMI

Use o cmdlet Disable-EC2Image.

```
Disable-EC2Image -ImageId ami-0abcdef1234567890
```

Descrever AMIs desabilitadas

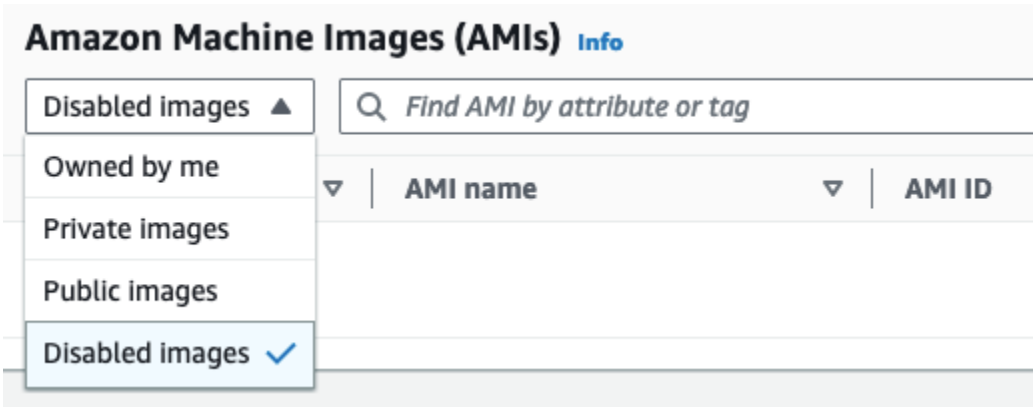
É possível visualizar as AMIs desabilitadas no console do EC2 usando a AWS CLI.

Você precisa ser o proprietário da AMI para ver as AMIs desabilitadas. Como as AMIs desabilitadas se tornam privadas, você não poderá ver as AMIs desabilitadas se não for o proprietário.

Console

Visualizar AMIs desabilitadas

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação à esquerda, selecione AMIs.
3. Na barra de filtro, escolha Imagens desabilitadas.



AWS CLI

Por padrão, quando você descreve todas as AMIs, as AMIs desabilitadas não são incluídas nos resultados. Para incluir AMIs desabilitadas nos resultados, especifique a opção `--include-disabled`. O campo `State` para uma AMI será `disabled` se a AMI estiver desabilitada.

Para incluir as AMIs desabilitadas ao descrever todas as AMIs de uma conta

Use o seguinte comando describe-images:

```
aws ec2 describe-images \
    --owners 123456789012 \
    --include-disabled
```

Para listar as AMIs desabilitadas da sua conta

Use o seguinte comando describe-images:

```
aws ec2 describe-images \
    --owners self \
    --include-disabled \
    --filters Name=state,Values=disabled \
    --query Images[].ImageId \
    --output text
```

O seguinte é um exemplo de saída.

```
ami-0abcdef1234567890
```

Para descrever o status de uma AMI

Use o seguinte comando describe-images: Se `DeprecationTime` não estiver presente na saída, a AMI não será descontinuada nem será definida para descontinuação em uma data futura.

```
aws ec2 describe-images \
    --image-ids ami-0abcdef1234567890 \
    --query Images[].State \
    --output text
```

O seguinte é um exemplo de saída.

```
disabled
```

PowerShell

Por padrão, quando você descreve todas as AMIs, as AMIs desabilitadas não são incluídas nos resultados. Para incluir AMIs desabilitadas nos resultados, é necessário especificar o parâmetro `-IncludeDisabled`. O campo `State` para uma AMI será `disabled` se a AMI estiver desabilitada.

Para listar as AMIs desabilitadas da sua conta

Use o cmdlet Get-EC2Image.

```
(Get-EC2Image `
```

```
    -Owner self `
    -IncludeDisabled $true | Where-Object {$_.State -eq "disabled"}).ImageId
```

O seguinte é um exemplo de saída.

```
ami-0abcdef1234567890
```

Para descrever o status de uma AMI

Use o cmdlet Get-EC2Image.

```
(Get-EC2Image -ImageId ami-0abcdef1234567890).State.Value
```

O seguinte é um exemplo de saída.

```
disabled
```

Reabilitar uma AMI desabilitada

Você pode reabilitar uma AMI desabilitada. É necessário ser o proprietário da AMI para executar esse procedimento.

Console

Reabilitar uma AMI desabilitada

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação à esquerda, selecione AMIs.
3. Na barra de filtro, escolha Imagens desabilitadas.
4. Selecione a AMI e escolha Ações, Habilitar a AMI. É possível selecionar várias AMIs para reabilitá-las ao mesmo tempo.
5. Na janela Habilitar AMI, escolha Habilitar.

AWS CLI

Reabilitar uma AMI desabilitada

Use o seguinte comando enable-image:

```
aws ec2 enable-image --image-id ami-0abcdef1234567890
```

PowerShell

Reabilitar uma AMI desabilitada

Use o cmdlet Enable-EC2Image.

```
Enable-EC2Image -ImageId ami-0abcdef1234567890
```

Cancelar o registro de uma AMI do Amazon EC2

Quando você cancela o registro de uma AMI, o Amazon EC2 a exclui permanentemente. Depois de cancelar o registro de uma AMI, você não poderá usá-la para executar novas instâncias. Considere cancelar o registro de uma AMI quando não pretender mais usá-la.

Para se proteger contra o cancelamento acidental ou mal-intencionado de uma AMI, é possível ativar a proteção contra cancelamento de registro. Se você cancelar acidentalmente o registro de uma AMI baseada no EBS, poderá usar a Lixeira para restaurá-la somente se o fizer dentro do período de tempo permitido antes que ela seja excluída permanentemente.

Ao cancelar o registro de uma AMI, é possível excluir ao mesmo tempo os snapshots associados. No entanto, se um snapshot estiver associado a várias AMIs, ele não será excluído, mesmo se especificado para exclusão, mas o registro da AMI ainda será cancelado. Qualquer snapshot não excluído continuará a gerar custos de armazenamento.

O cancelamento do registro de uma AMI não afetará nenhuma instância que já tenha sido iniciada pela AMI. Essas instâncias poderão continuar sendo usadas. Por padrão, o cancelamento do registro de uma AMI também não afeta os snapshots criados durante o processo de criação da AMI. Você continuará incorrendo em custos de uso para essas instâncias e em custos de armazenamento para os snapshots. Assim, para evitar incorrer em custos extras, recomendamos encerrar quaisquer instâncias e excluir quaisquer snapshots desnecessários. É possível excluir os snapshots automaticamente durante o cancelamento do registro ou manualmente após o cancelamento do registro. Para obter mais informações, consulte Evite custos com recursos não utilizados.

Para instâncias iniciadas a partir de uma AMI cujo registro é posteriormente cancelado, você ainda pode visualizar algumas informações de alto nível sobre a AMI usando o comando `describe-instance-image-metadata` AWS CLI. Para obter mais informações, consulte describe-instance-image-metadata.

Conteúdo

- Considerações
- Cancelar o registro de uma AMI
- Evite custos com recursos não utilizados
- Proteger uma AMI do Amazon EC2 de cancelamento de registro

Considerações

- Você não pode cancelar o registro de uma AMI que não pertença à sua conta.
- Você não pode cancelar o registro de uma AMI gerenciada pelo serviço AWS Backup usando o Amazon EC2. Em vez disso, use o AWS Backup para excluir os pontos de recuperação correspondentes no cofre de backup. Para obter mais informações, consulte Exclusão de namespaces no Guia do desenvolvedor do AWS Backup.

Cancelar o registro de uma AMI

É possível cancelar o registro de AMIs baseadas no EBS e de AMIs baseadas no Amazon S3. Para AMIs baseadas em EBS, é possível excluir ao mesmo tempo os snapshots associados. No entanto, se um snapshot estiver associado a outras AMIs, ele não será excluído, mesmo se especificado para exclusão.

Console

Para cancelar o registro de uma AMI

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione AMIs.
3. Na barra de filtros, escolha Pertencentes a mim para listar suas AMIs disponíveis ou escolha Imagens desabilitadas para listar suas AMIs desabilitadas.
4. Selecione a AMI para cancelar o registro.
5. Escolha Actions (Ações) e Deregister AMI (Cancelar registro da AMI).

6. (Opcional) Para excluir os snapshots associados durante o cancelamento do registro, marque a caixa de seleção Excluir snapshots associados.

> **Note**
>
> Se um snapshot estiver associado a outras AMIs, ele não será excluído mesmo se a caixa de seleção estiver marcada.

7. Escolha Cancelar registro da AMI.

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

AWS CLI

Para cancelar o registro de uma AMI

Use o seguinte comando deregister-image.

```
aws ec2 deregister-image --image-id ami-0abcdef1234567890
```

Para cancelar o registro de uma AMI e excluir seus snapshots associados

Use o comando deregister-image a seguir e especifique o parâmetro `--delete-associated-snapshots`. Observe que, se um snapshot estiver associado a outras AMIs, ele não será excluído, mesmo que você especifique esse parâmetro.

```
aws ec2 deregister-image \
    --image-id ami-0abcdef1234567890 \
    --delete-associated-snapshots
```

PowerShell

Para cancelar o registro de uma AMI

Use o cmdlet Unregister-EC2Image.

```
Unregister-EC2Image -ImageId ami-0abcdef1234567890
```

Para cancelar o registro de uma AMI e excluir seus snapshots associados

Use o cmdlet Unregister-EC2Image e especifique o parâmetro -DeleteAssociatedSnapshots. Observe que, se um snapshot estiver associado a outras AMIs, ele não será excluído, mesmo que você especifique esse parâmetro.

```
Unregister-EC2Image `
    -ImageId ami-0abcdef1234567890 `
    -DeleteAssociatedSnapshots
```

Evite custos com recursos não utilizados

O cancelamento do registro de uma AMI não exclui, por padrão, todos os recursos associados a ela. Esses recursos incluem os snapshots das AMIs baseadas no EBS e os arquivos armazenados no Amazon S3 das AMIs baseadas no Amazon S3. Quando o registro de uma AMI for cancelado, isso não encerrará nem interromperá nenhuma instância já iniciada via AMI.

Você continuará incorrendo em custos para armazenar os snapshots e os arquivos, e incorrerá em custos para qualquer instância em execução.

Para evitar incorrer nestes tipos de custos extras, recomendamos excluir quaisquer recursos desnecessários.

AMIs apoiadas pelo EBS

- Exclua os snapshots associados ao mesmo tempo que cancela o registro da AMI. Para obter mais informações, consulte Cancelar o registro de uma AMI.
- Se você cancelar o registro de uma AMI sem excluir seus snapshots associados, você poderá excluir os snapshots manualmente. O snapshot do volume raiz da instância criado durante a criação da AMI tem o seguinte formato de descrição:

```
Created by CreateImage(i-1234567890abcdef0) for ami-0abcdef1234567890
```

- Se você não precisar mais das instâncias que foram inicializadas pela AMI, poderá interrompê-las ou encerrá-las. Para listar as instâncias, filtre pelo ID da AMI.

AMIs baseadas no Amazon S3

- Exclua o pacote no Amazon S3 usando o comando ec2-delete-bundle (ferramentas de AMI).

- Se o bucket do Amazon S3 estiver vazio após a exclusão do pacote e você não tiver mais finalidade para esse bucket, você poderá excluir o bucket.
- Se você não precisar mais das instâncias que foram inicializadas pela AMI, poderá encerrá-las. Para listar as instâncias, filtre pelo ID da AMI.

Proteger uma AMI do Amazon EC2 de cancelamento de registro

É possível ativar a proteção contra cancelamento de registro em uma AMI para evitar exclusão acidental ou mal-intencionada. Quando a proteção contra cancelamento do registro estiver ativada, o registro da AMI não poderá ser cancelado por nenhum usuário, independente das permissões do IAM de cada um. Para cancelar o registro da AMI, desative primeiro a proteção contra cancelamento de registro na AMI.

Ao ativar a proteção contra cancelamento de registro em uma AMI, você terá a opção de incluir um período de espera de 24 horas. Esse período de espera é o tempo durante o qual a proteção contra cancelamento de registro permanece em vigor após você desativá-la. Durante esse período de espera, o registro da AMI não poderá ser cancelado. Quando o período de espera terminar, o registro da AMI poderá ser cancelado.

A proteção contra cancelamento de registro é desativada por padrão em todas as AMI novas e existentes.

Ativar a proteção contra cancelamento do registro

Use os procedimentos a seguir para ativar a proteção contra cancelamento de registro.

Console

Para ativar a proteção contra cancelamento do registro

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione AMIs.
3. Na barra de filtros, escolha Pertencentes a mim para listar suas AMIs disponíveis ou escolha Imagens desabilitadas para listar suas AMIs desabilitadas.
4. Selecione a AMI na qual você deseja ativar a proteção contra cancelamento de registro e, em seguida, escolha Ações, Gerenciar proteção contra cancelamento de registro da AMI.

5. Na caixa de diálogo Gerenciar proteção contra cancelamento de registro da AMI, é possível ativar a proteção contra cancelamento de registro com ou sem um período de espera. Escolha uma das seguintes opções:

   - Habilitar com período de espera de 24 horas: com um período de espera, o registro da AMI não poderá ser cancelado por 24 horas quando a proteção de cancelamento de registro estiver desativada.
   - Habilitar sem período de espera: sem um período de espera, o registro da AMI poderá ser cancelado imediatamente quando a proteção contra cancelamento de registro estiver desativada.

6. Selecione Salvar.

AWS CLI

Para ativar a proteção contra cancelamento do registro

Use o comando enable-image-deregistration-protection. Para habilitar o período de espera opcional, inclua a opção `--with-cooldown`.

```
aws ec2 enable-image-deregistration-protection \
    --image-id ami-0abcdef1234567890 \
    --with-cooldown
```

PowerShell

Para ativar a proteção contra cancelamento do registro

Use o cmdlet Enable-EC2ImageDeregistrationProtection. Para habilitar o período de espera opcional, defina o parâmetro `-WithCooldown` como `true`.

```
Enable-EC2ImageDeregistrationProtection `
    -ImageId ami-0abcdef1234567890 `
    -WithCooldown $true
```

Desativar a proteção contra cancelamento do registro

Use os procedimentos a seguir para desativar a proteção contra cancelamento de registro.

Se você optou por incluir um período de espera de 24 horas ao ativar a proteção contra cancelamento de registro para a AMI, quando a proteção contra cancelamento de registro for desativada, o registro da AMI não poderá ser cancelado imediatamente. Esse período de espera é o período de 24 horas durante o qual a proteção contra cancelamento de registro permanece em vigor após você desativá-la. Durante esse período de espera, o registro da AMI não poderá ser cancelado. Quando o período de espera terminar, o registro da AMI poderá ser cancelado.

Console

Para desativar a proteção contra cancelamento do registro

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione AMIs.
3. Na barra de filtros, escolha Pertencentes a mim para listar suas AMIs disponíveis ou escolha Imagens desabilitadas para listar suas AMIs desabilitadas.
4. Selecione a AMI na qual você deseja desativar a proteção contra cancelamento de registro e, em seguida, escolha Ações, Gerenciar proteção contra cancelamento de registro da AMI.
5. Na caixa de diálogo Gerenciar proteção contra cancelamento de registro da AMI, escolha Desabilitar.
6. Escolha Salvar.

AWS CLI

Para desativar a proteção contra cancelamento do registro

Use o comando disnable-image-deregistration-protection.

```
aws ec2 disable-image-deregistration-protection --image-id ami-0abcdef1234567890
```

PowerShell

Para desativar a proteção contra cancelamento do registro

Use o cmdlet Disable-EC2ImageDeregistrationProtection.

```
Disable-EC2ImageDeregistrationProtection -ImageId ami-0abcdef1234567890
```

Comportamento de execução da instância com modos de inicialização do Amazon EC2

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

No Amazon EC2, há suporte para duas variantes do software do modo de inicialização: Unified Extensible Firmware Interface (UEFI) e BIOS legado.

Possíveis parâmetros do modo de inicialização em uma AMI

Uma AMI pode ter um dos seguintes valores de parâmetro de modo de inicialização: `uefi`, `legacy-bios` ou `uefi-preferred`. O parâmetro de modo de inicialização da AMI é opcional. Para AMIs sem parâmetro de modo de inicialização, as instâncias executadas a partir delas usam o valor de modo de inicialização padrão do tipo de instância.

Objetivo do parâmetro de modo de inicialização da AMI

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

Parâmetro de modo de inicialização preferencial UEFI

É possível criar AMIs que suportem UEFI e Legacy BIOS usando o parâmetro `uefi-preferred` do modo de inicialização. Quando o parâmetro de modo de inicialização é definido como `uefi-preferred`, e se o tipo de instância oferecer suporte a UEFI, a instância será iniciada em UEFI. Se o tipo de instância não for compatível com UEFI, ela será iniciada em BIOS legado.

> **Warning**
>
> Alguns recursos, como o UEFI Secure Boot, só estão disponíveis em instâncias que inicializadas em UEFI. Quando você usa o parâmetro do modo de inicialização `uefi-preferred` da AMI com um tipo de instância que não ofereça suporte a UEFI, a instância será iniciada como BIOS legado e o recurso dependente de UEFI será desativado. Se você confia na disponibilidade de um recurso dependente de UEFI, defina o parâmetro do modo de inicialização da AMI como `uefi`.

Modos de inicialização padrão para tipos de instância

- Tipos de instância Graviton: UEFI
- Tipos de instância Intel e AMD: BIOS legado

Suporte para zonas

A inicialização UEFI não é compatível com as zonas do Wavelength.

Tópicos do modo de inicialização

- Requisitos para executar uma instância do EC2 no modo de inicialização da UEFI
- Determinar o parâmetro do modo de inicialização de uma AMI do Amazon EC2
- Determinar os modos de inicialização compatíveis de um tipo de instância do EC2
- Determinar o modo de inicialização de uma instância do EC2
- Determinar o modo de inicialização do sistema operacional para a instância do EC2
- Definir o modo de inicialização de uma AMI do Amazon EC2
- Variáveis da UEFI para instâncias do Amazon EC2
- UEFI Secure Boot para instâncias do Amazon EC2

Requisitos para executar uma instância do EC2 no modo de inicialização da UEFI

O modo de inicialização de uma instância é determinado pela configuração da AMI, pelo sistema operacional incluído nela e pelo tipo de instância. Para executar uma instância no modo de inicialização da UEFI, você deve atender aos requisitos a seguir.

AMI

A AMI deve ser configurada para a UEFI da seguinte forma:

- Sistema operacional: o sistema operacional contido na AMI deve ser configurado para usar UEFI; caso contrário, a inicialização da instância falhará. Para obter mais informações, consulte Determinar o modo de inicialização do sistema operacional para a instância do EC2.
- Parâmetro de modo de inicialização da AMI: o parâmetro de modo de inicialização da AMI deve ser definido como `uefi` ou `uefi-preferred`. Para obter mais informações, consulte Determinar o parâmetro do modo de inicialização de uma AMI do Amazon EC2.

Linux: as seguintes AMIs do Linux são compatíveis com UEFI:

- Amazon Linux 2023
- Amazon Linux 2 (somente instâncias do tipo Graviton)

Para outras AMIs do Linux, você deve configurar a AMI e importá-la por meio do VM Import/Export ou do CloudEndure.

Windows: as seguintes AMIs do Windows oferecem suporte para a UEFI:

- Windows_Server-2025-* (com exceção de AMIs com o prefixo de nome `BIOS-`)
- TPM-Windows_Server-2022-English-Full-Base
- TPM-Windows_Server-2022-English-Core-Base
- TPM-Windows_Server-2019-English-Full-Base
- TPM-Windows_Server-2019-English-Core-Base
- TPM-Windows_Server-2016-English-Full-Base
- TPM-Windows_Server-2016-English-Core-Base

Tipo de instância

Todas as instâncias criadas no AWS Nitro System são compatíveis com a UEFI e o BIOS herdado, exceto as seguintes: instâncias bare metal, DL1, G4ad, P4, u-3tb1, u-6tb1, u-9tb1, u-12tb1, u-18tb1, u-24tb1 e VT1. Para obter mais informações, consulte the section called “Modo de inicialização do tipo de instância”.

A tabela a seguir mostra que o modo de inicialização de uma instância (indicado pela coluna Modo de inicialização da instância resultante) é determinado por uma combinação do parâmetro do modo de inicialização da AMI (coluna 1), a configuração do modo de inicialização do sistema operacional contida na AMI (coluna 2) e o suporte ao modo de inicialização do tipo de instância (coluna 3).

Parâmetro do modo de inicialização da AMI	Configuração do modo de inicialização do sistema operacional	Suporte ao modo de inicialização do tipo de instância	Modo de inicialização da instância resultante
UEFI	UEFI	UEFI	UEFI
BIOS legado	BIOS legado	BIOS legado	BIOS legado

Parâmetro do modo de inicialização da AMI	Configuração do modo de inicialização do sistema operacional	Suporte ao modo de inicialização do tipo de instância	Modo de inicialização da instância resultante
UEFI preferencial	UEFI	UEFI	UEFI
UEFI preferencial	UEFI	UEFI e BIOS legado	UEFI
UEFI preferencial	BIOS legado	BIOS legado	BIOS legado
UEFI preferencial	BIOS legado	UEFI e BIOS legado	BIOS legado
Nenhum modo de inicialização especificado - ARM	UEFI	UEFI	UEFI
Nenhum modo de inicialização especificado - x86	BIOS legado	UEFI e BIOS legado	BIOS legado

Determinar o parâmetro do modo de inicialização de uma AMI do Amazon EC2

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

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

Console

Para determinar o parâmetro de modo de inicialização de uma AMI

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha AMIs e, em seguida, selecione a AMI.
3. Inspecione o campo Modo de inicialização.

- Um valor de uefi indica que a AMI é compatível com a UEFI.
- Um valor de uefi-preferred indica que a AMI é compatível tanto com a UEFI quanto a BIOS legada.
- Se não houver valor, as instâncias iniciadas na AMI usam o valor padrão do tipo de instância.

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

Ao executar uma instância usando o assistente de instância de execução, na etapa de selecionar uma AMI, verifique o campo Boot mode (Modo de inicialização). Para obter mais informações, consulte Imagens de aplicações e sistemas operacionais (imagem de máquina da Amazon).

AWS CLI

Para determinar o parâmetro de modo de inicialização de uma AMI

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

```
aws ec2 describe-images \
    --region us-east-1 \
    --image-id ami-0abcdef1234567890 \
    --query Images[].BootMode \
    --output text
```

O seguinte é um exemplo de saída.

```
uefi
```

Na saída, um valor de `uefi` indica que a AMI oferece suporte a UEFI. Um valor de `uefi-preferred` indica que a AMI oferece suporte tanto a UEFI quanto a BIOS legado. Se não houver valor, as instâncias iniciadas na AMI usam o valor padrão do tipo de instância.

PowerShell

Para determinar o parâmetro de modo de inicialização de uma AMI

Use o cmdlet Get-EC2Image para determinar o modo de inicialização de uma AMI.

```
Get-EC2Image -Region us-east-1 `
```

```
    -ImageId ami-0abcdef1234567890 | Format-List Name, BootMode, TpmSupport
```

O seguinte é um exemplo de saída.

```
Name       : TPM-Windows_Server-2016-English-Full-Base-2023.05.10
BootMode   : uefi
TpmSupport : v2.0
```

No saída, o valor `BootMode` indica o modo de inicialização da AMI. Um valor de `uefi` indica que a AMI oferece suporte a UEFI. Um valor de `uefi-preferred` indica que a AMI oferece suporte tanto a UEFI quanto a BIOS legado. Se não houver valor, as instâncias iniciadas na AMI usam o valor padrão do tipo de instância.

Determinar os modos de inicialização compatíveis de um tipo de instância do EC2

É possível determinar os modos de inicialização com suporte em um tipo de instância.

O console do Amazon EC2 não exibe os modos de inicialização com suporte em um tipo de instância.

AWS CLI

Use o comando describe-instance-types para determinar os modos de inicialização com suporte em um tipo de instância. O parâmetro `--query` filtra a saída para retornar apenas modelos de inicialização compatíveis.

O exemplo a seguir mostra que o tipo de instância especificado oferece suporte a ambos os modos de inicialização de UEFI e BIOS legado.

```
aws ec2 describe-instance-types \
    --instance-types m5.2xlarge \
    --query "InstanceTypes[*].SupportedBootModes"
```

O seguinte é um exemplo de saída.

```
[
    [
        "legacy-bios",
```

```
        "uefi"
    ]
]
```

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

```
aws ec2 describe-instance-types \
    --instance-types t2.xlarge \
    --query "InstanceTypes[*].SupportedBootModes"
```

O seguinte é um exemplo de saída.

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

PowerShell

Use o cmdlet Get-EC2InstanceType para determinar os modos de inicialização com suporte em um tipo de instância.

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

```
Get-EC2InstanceType -InstanceType m5.2xlarge | Format-List InstanceType,
 SupportedBootModes
```

O seguinte é um exemplo de saída.

```
InstanceType       : m5.2xlarge
SupportedBootModes : {legacy-bios, uefi}
```

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

```
Get-EC2InstanceType -InstanceType t2.xlarge | Format-List InstanceType,
 SupportedBootModes
```

O seguinte é um exemplo de saída.

```
InstanceType       : t2.xlarge
SupportedBootModes : {legacy-bios}
```

Para determinar os tipos de instância que são compatíveis com a UEFI

É possível determinar os tipos de instância que são compatíveis com UEFI. O console do Amazon EC2 não exibe o suporte a UEFI de um tipo de instância.

AWS CLI

Os tipos de instância disponíveis variam de acordo com a Região da AWS. Para ver os tipos de instâncias disponíveis com suporte a UEFI em uma região, use o comando describe-instance-types. Inclua o parâmetro `--filters` para definir o escopo dos resultados para os tipos de instância com suporte a UEFI e o parâmetro `--query` para definir o escopo da saída para o valor de `InstanceType`.

```
aws ec2 describe-instance-types \
    --filters Name=supported-boot-mode,Values=uefi \
    --query "InstanceTypes[*].[InstanceType]" --output text | sort
```

PowerShell

Os tipos de instância disponíveis variam de acordo com a Região da AWS. Para ver os tipos de instâncias disponíveis que oferecem suporte a UEFI em uma região, use o cmdlet Get-EC2InstanceType.

```
Get-EC2InstanceType | `
 Where-Object {$_.SupportedBootModes -Contains "uefi"} | `
 Sort-Object InstanceType | `
 Format-Table InstanceType -GroupBy CurrentGeneration
```

Para determinar os tipos de instância que são compatíveis com o UEFI Secure Boot e variáveis persistentes não voláteis

Instâncias bare metal não são compatíveis com o UEFI Secure Boot e variáveis não voláteis, portanto, esses exemplos as excluem da saída. Para obter informações sobre o UEFI Secure Boot, consulte UEFI Secure Boot para instâncias do Amazon EC2.

AWS CLI

Use o comando describe-instance-types e exclua as instâncias bare metal da saída.

```
aws ec2 describe-instance-types \
    --filters Name=supported-boot-mode,Values=uefi Name=bare-metal,Values=false \
    --query "InstanceTypes[*].[InstanceType]" \
    --output text | sort
```

PowerShell

Use o cmdlet Get-EC2InstanceType e exclua as instâncias bare metal da saída.

```
Get-EC2InstanceType | `
    Where-Object { `
        $_.SupportedBootModes -Contains "uefi" -and `
        $_.BareMetal -eq $False
        } | `
    Sort-Object InstanceType  | `
    Format-Table InstanceType, SupportedBootModes, BareMetal, `
        @{Name="SupportedArchitectures";
 Expression={$_.ProcessorInfo.SupportedArchitectures}}
```

Determinar o modo de inicialização de uma instância do EC2

O modo de inicialização de uma instância é exibido no campo Modo de inicialização no console do Amazon EC2 e pelo parâmetro `currentInstanceBootMode` na AWS CLI.

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

- Uma AMI com um parâmetro de modo de inicialização `uefi` cria uma instância com um parâmetro `currentInstanceBootMode` de `uefi`.
- Uma AMI com um parâmetro de modo de inicialização `legacy-bios` cria uma instância com um parâmetro `currentInstanceBootMode` de `legacy-bios`.
- Uma AMI com um parâmetro de modo de inicialização `uefi-preferred` cria uma instância com um parâmetro `currentInstanceBootMode` de `uefi` se o tipo de instância oferecer suporte a UEFI, caso contrário, cria uma instância com um parâmetro `currentInstanceBootMode` de `legacy-bios`.

- Uma AMI sem valor de parâmetro no modo de inicialização cria uma instância com um valor de parâmetro `currentInstanceBootMode` que é dependente se a arquitetura da AMI é ARM ou x86, e do modo de inicialização com suporte pelo tipo de instância. O modo de inicialização padrão é `uefi` nos tipos de instância Graviton e `legacy-bios` nos tipos de instância Intel e AMD.

Console

Para determinar o modo de inicialização de uma instância

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

AWS CLI

Para determinar o modo de inicialização de uma instância

Use o comando describe-instances para determinar o modo de inicialização de uma instância. Você também pode determinar o modo de inicialização da AMI que foi usada para criar a instância.

```
aws ec2 describe-instances \
    --region us-east-1 \
    --instance-ids i-1234567890abcdef0 \
    --query Reservations[].Instances[].BootMode \
    --output text
```

O seguinte é um exemplo de saída.

```
uefi
```

PowerShell

Para determinar o modo de inicialização de uma instância

Use o cmdlet Get-EC2Image para determinar o modo de inicialização de uma instância. Você também pode determinar o modo de inicialização da AMI que foi usada para criar a instância.

```
(Get-EC2Instance `
```

```
    -InstanceId i-1234567890abcdef0).Instances | Format-List BootMode,
 CurrentInstanceBootMode, InstanceType, ImageId
```

O seguinte é um exemplo de saída.

```
BootMode                : uefi
CurrentInstanceBootMode : uefi
InstanceType            : c5a.large
ImageId                 : ami-0abcdef1234567890
```

Determinar o modo de inicialização do sistema operacional para a instância do EC2

O modo de inicialização da AMI orienta o Amazon EC2 sobre o modo de inicialização que deve ser usado para inicializar uma instância. Para verificar se o sistema operacional da instância está configurado para a UEFI, é necessário se conectar à instância usando SSH (instâncias do Linux) ou RDP (instâncias do Windows).

Use as instruções para o sistema operacional da sua instância.

Linux

Para determinar o modo de inicialização do sistema operacional da instância

1. Conecte-se à instância do Linux usando SSH.
2. Para exibir o modo de inicialização do sistema operacional, tente um dos seguintes procedimentos:

   - Execute o comando a seguir.

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

     Saída esperada de uma instância inicializada no modo de inicialização UEFI

     ```
     BootCurrent: 0001
     Timeout: 0 seconds
     BootOrder: 0000,0001
     Boot0000* UiApp
     Boot0001* UEFI Amazon Elastic Block Store vol-xyz
     ```

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

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

Saída esperada de uma instância inicializada no modo de inicialização UEFI

```
UEFI Boot Detected
```

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

```
Legacy BIOS Boot Detected
```

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

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

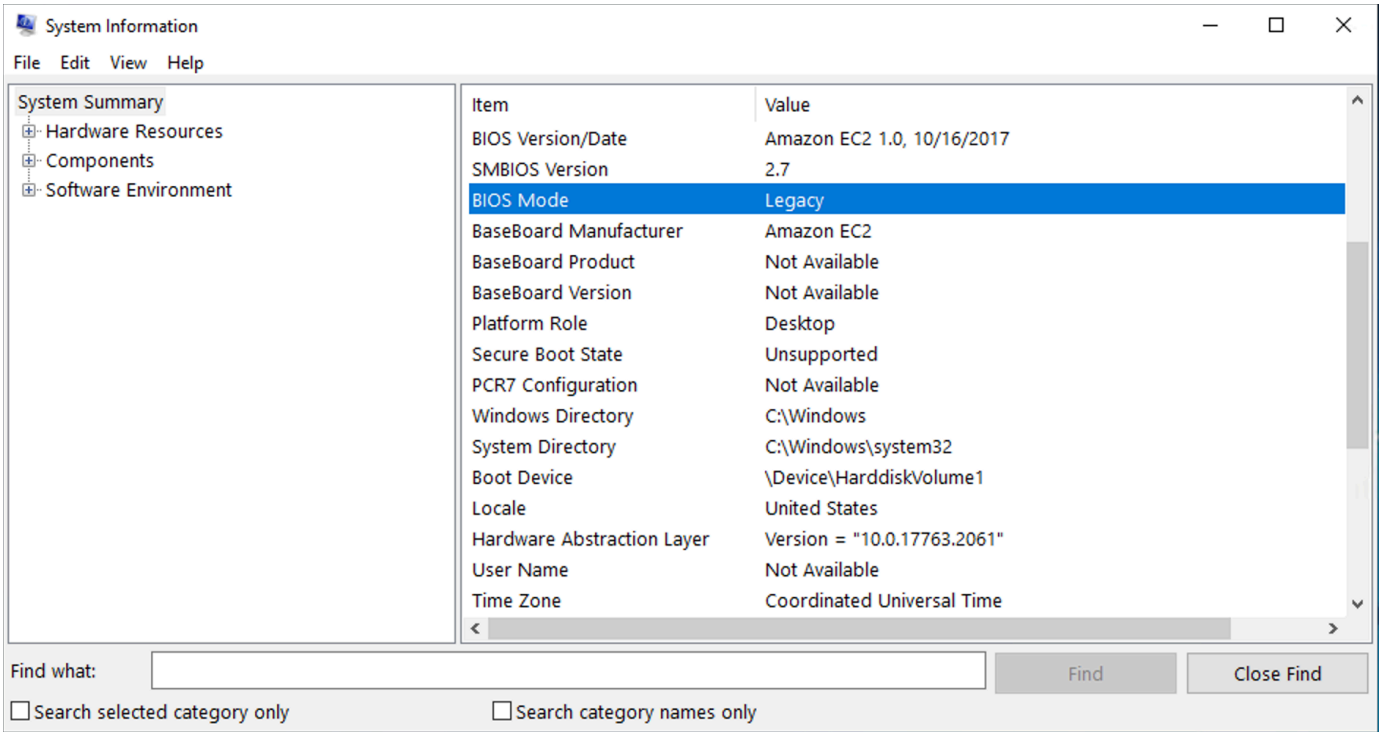
Saída esperada de uma instância inicializada no modo de inicialização UEFI

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

Windows

Para determinar o modo de inicialização do sistema operacional da instância

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



Definir o modo de inicialização de uma AMI do Amazon EC2

Por padrão, a AMI herda o modo de inicialização da instância do EC2 usada para criar a AMI. Por exemplo, se você criar uma AMI de uma instância do EC2 executada em BIOS legado, o modo de inicialização da nova AMI será `legacy-bios`. Se você criar uma AMI de uma instância do EC2 com um modo de inicialização `uefi-preferred`, o modo de inicialização da nova AMI será `uefi-preferred`.

Ao registrar uma AMI, é possível definir o modo de inicialização da AMI como `uefi`, `legacy-bios` ou `uefi-preferred`.

Quando o modo de inicialização da AMI estiver definido como `uefi-preferred`, a instância será inicializada da seguinte forma:

- Para tipos de instância que ofereçam suporte a UEFI e BIOS legado (por exemplo, `m5.large`), a instância será inicializada usando UEFI.
- Para tipos de instância que ofereçam suporte somente a BIOS legado (por exemplo, `m4.large`), a instância será inicializada usando BIOS legado.

Se você definir o modo de inicialização da AMI como `uefi-preferred`, o sistema operacional deverá oferecer suporte à capacidade de inicialização tanto com UEFI quanto com BIOS legado.

Para converter uma instância existente baseada em BIOS legado para UEFI, ou uma instância existente baseada em UEFI para BIOS legado, primeiro é necessário modificar o volume e o sistema operacional da instância para oferecer suporte ao modo de inicialização selecionado. Em seguida, crie um snapshot do volume. Finalmente, crie uma AMI do snapshot.

Considerações

- Definir o parâmetro de modo de inicialização da AMI não configura automaticamente o sistema operacional para o modo de inicialização especificado. Primeiro é necessário fazer as modificações adequadas no volume e no sistema operacional da instância para oferecer suporte à inicialização via modo de inicialização selecionado. Caso contrário, a AMI resultante não poderá ser usada. Por exemplo, caso esteja realizando a conversão de uma instância do Windows baseada em BIOS legado para a UEFI, será possível usar a ferramenta MBR2GPT da Microsoft para converter o disco do sistema de MBR para GPT. As modificações necessárias são específicas do sistema operacional. Para obter mais informações, consulte o manual do sistema operacional.
- Não é possível usar o comando register-image ou o cmdlet Register-EC2Image para criar uma AMI compatível tanto com a NitroTPM quanto com a UEFI Preferred.
- Alguns recursos, como o UEFI Secure Boot, só estão disponíveis em instâncias que inicializadas em UEFI. Quando você usa o parâmetro do modo de inicialização `uefi-preferred` da AMI com um tipo de instância que não oferece suporte a UEFI, a instância é iniciada como BIOS legado e o recurso dependente de UEFI é desativado. Se você confia na disponibilidade de um recurso dependente de UEFI, defina o parâmetro do modo de inicialização da AMI como `uefi`.

AWS CLI

Para definir o modo de inicialização de uma AMI

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

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

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

```
aws ec2 describe-instances \
    --instance-ids i-1234567890abcdef0 \
    --query Reservations[].Instances[].BlockDeviceMappings
```

O seguinte é um exemplo de saída.

```
[
    [
        {
            "DeviceName": "/dev/xvda",
            "Ebs": {
                "AttachTime": "2024-07-11T01:05:51+00:00",
                "DeleteOnTermination": true,
                "Status": "attached",
                "VolumeId": "vol-1234567890abcdef0"
            }
        }
    ]
]
```

3. Para criar um snapshot do volume, use o comando create-snapshot. Use o ID do volume da etapa anterior.

```
aws ec2 create-snapshot \
    --volume-id vol-01234567890abcdef \
    --description "my snapshot"
```

O seguinte é um exemplo de saída.

```
{
    "Description": "my snapshot",
    "Encrypted": false,
    "OwnerId": "123456789012",
```

```
    "Progress": "",
    "SnapshotId": "snap-0abcdef1234567890",
    "StartTime": "",
    "State": "pending",
    "VolumeId": "vol-01234567890abcdef",
    "VolumeSize": 30,
    "Tags": []
}
```

4. Aguarde até que o estado do snapshot seja `completed` antes de avançar para a próxima etapa. Para obter o estado do snapshot, use o comando describe-snapshots com o ID do snapshot da etapa anterior.

```
aws ec2 describe-snapshots \
    --snapshot-ids snap-0abcdef1234567890 \
    --query Snapshots[].State \
    --output text
```

O seguinte é um exemplo de saída.

```
completed
```

5. Para criar uma nova AMI, use o comando register-image. Use o valor de `SnapshotId` da saída de CreateSnapshot.

   - Para definir o modo de inicialização como UEFI, adicione o parâmetro `--boot-mode` com o valor `uefi`.

```
aws ec2 register-image \
   --description "my image" \
   --name "my-image" \
   --block-device-mappings "DeviceName=/dev/
sda1,Ebs={SnapshotId=snap-0abcdef1234567890,DeleteOnTermination=true}" \
   --root-device-name /dev/sda1 \
   --virtualization-type hvm \
   --ena-support \
   --boot-mode uefi
```

   - Para definir o modo de inicialização como `uefi-preferred`, defina o valor de `--boot-mode` como `uefi-preferred`

```
aws ec2 register-image \
   --description "my description" \
   --name "my-image" \
   --block-device-mappings "DeviceName=/dev/
sda1,Ebs={SnapshotId=snap-0abcdef1234567890,DeleteOnTermination=true}" \
   --root-device-name /dev/sda1 \
   --virtualization-type hvm \
   --ena-support \
   --boot-mode uefi-preferred
```

6. (Opcional) Para verificar se a AMI recém-criada tem o modo de inicialização que você especificou, use o comando describe-images.

```
aws ec2 describe-images \
    --image-id ami-1234567890abcdef0 \
    --query Images[].BootMode \
    --output text
```

O seguinte é um exemplo de saída.

```
uefi
```

PowerShell

Para definir o modo de inicialização de uma AMI

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

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

2. Para localizar o ID do volume da instância, use o cmdlet Get-EC2Instance.

```
(Get-EC2Instance `
```

```
    -InstanceId i-1234567890abcdef0).Instances.BlockDeviceMappings.Ebs
```

O seguinte é um exemplo de saída.

```
AssociatedResource  :
AttachTime          : 7/11/2024 1:05:51 AM
DeleteOnTermination : True
Operator            :
Status              : attached
VolumeId            : vol-01234567890abcdef
```

3. Para criar um snapshot do volume, use o cmdlet New-EC2Snapshot. Use o ID do volume da etapa anterior.

```
New-EC2Snapshot `
    -VolumeId vol-01234567890abcdef `
    -Description "my snapshot"
```

O seguinte é um exemplo de saída.

```
AvailabilityZone          :
Description               : my snapshot
Encrypted                 : False
FullSnapshotSizeInBytes   : 0
KmsKeyId                  :
OwnerId                   : 123456789012
RestoreExpiryTime         :
SnapshotId                : snap-0abcdef1234567890
SseType                   :
StartTime                 : 4/25/2025 6:08:59 PM
State                     : pending
StateMessage              :
VolumeId                  : vol-01234567890abcdef
VolumeSize                : 30
```

4. Aguarde até que o estado do snapshot seja `completed` antes de avançar para a próxima etapa. Para obter o estado do snapshot, use o cmdlet Get-EC2Snapshot com o ID do snapshot da etapa anterior.

```
(Get-EC2Snapshot `
    -SnapshotId snap-0abcdef1234567890).State.Value
```

O seguinte é um exemplo de saída.

```
completed
```

5. Para criar uma nova AMI, use o cmdlet Register-EC2Image. Use o valor de `SnapshotId` da saída de New-EC2Snapshot.

   - Para definir o modo de inicialização como UEFI, adicione o parâmetro `-BootMode` com o valor `uefi`.

   ```
   $block = @{SnapshotId=snap-0abcdef1234567890}
   Register-EC2Image `
      -Description "my image" `
      -Name "my-image" `
      -BlockDeviceMapping @{DeviceName="/dev/xvda";Ebs=$block} `
      -RootDeviceName /dev/xvda `
      -EnaSupport $true `
      -BootMode uefi
   ```

   - Para definir o modo de inicialização como `uefi-preferred`, defina o valor de `-BootMode` como `uefi-preferred`

   ```
   $block = @{SnapshotId=snap-0abcdef1234567890}
   Register-EC2Image `
      -Description "my image" `
      -Name "my-image" `
      -BlockDeviceMapping @{DeviceName="/dev/xvda";Ebs=$block} `
      -RootDeviceName /dev/xvda `
      -EnaSupport $true `
      -BootMode uefi-preferred
   ```

6. (Opcional) Para verificar se a AMI recém-criada tem o modo de inicialização que você especificou, use o cmdlet Get-EC2Image.

   ```
   (Get-EC2Image `
       -ImageId ami-1234567890abcdef0).BootMode.Value
   ```

   O seguinte é um exemplo de saída.

   ```
   uefi
   ```

Variáveis da UEFI para instâncias do Amazon EC2

Quando você inicia uma instância em que o modo de inicialização é definido como UEFI, um armazenamento de chave-valor para variáveis é criado. O armazenamento pode ser usado pela UEFI e pelo sistema operacional da instância para armazenar variáveis UEFI.

As variáveis UEFI são usadas pelo carregador de inicialização e pelo sistema operacional para configurar o startup antecipado do sistema. Eles permitem que o sistema operacional gerencie determinadas configurações do processo de inicialização, como a ordem de inicialização, ou gerencie as chaves para o UEFI Secure Boot.

> **Warning**
>
> Qualquer pessoa que possa se conectar à instância (e possivelmente a qualquer software em execução na instância) ou qualquer pessoa com permissão para usar a API GetInstanceUefiData na instância pode ler as variáveis. Você nunca deve armazenar dados sigilosos, como senhas ou informações de identificação pessoal, no armazenamento de variáveis UEFI.

Persistência de variáveis UEFI

- Para instâncias que foram iniciadas até 10 de maio de 2022, as variáveis UEFI são apagadas ao reinicializar ou parar.
- Para instâncias iniciadas a partir e 11 de maio de 2022, as variáveis UEFI marcadas como não voláteis persistem na reinicialização e na parada/início.
- As instâncias bare metal não preservam variáveis não voláteis da UEFI nas operações de parada/início da instância.

UEFI Secure Boot para instâncias do Amazon EC2

O UEFI Secure Boot baseia-se no longo processo de inicialização segura do Amazon EC2, e fornece mais proteção abrangente que ajuda os clientes a proteger o software de ameaças que persistem durante as reinicializações. Ele garante que a instância inicialize apenas o software assinado com chaves criptográficas. As chaves são armazenadas no banco de dados de chaves do armazenamento de variáveis não voláteis UEFI. O UEFI Secure Boot impede a modificação não autorizada do fluxo de inicialização da instância.

Conteúdo

- Como o UEFI Secure Boot funciona com instâncias do Amazon EC2
- Requisitos para o UEFI Secure Boot no Amazon EC2
- Verificar se uma instância do Amazon EC2 está habilitada para o UEFI Secure Boot
- Criar uma AMI do Linux com chaves personalizadas do UEFI Secure Boot
- Crie o blob binário da AWS para o UEFI Secure Boot

Como o UEFI Secure Boot funciona com instâncias do Amazon EC2

O UEFI Secure Boot é um recurso especificado na UEFI que fornece verificação sobre o estado da cadeia de inicialização. Ele é projetado para garantir que apenas binários UEFI verificados criptograficamente sejam executados após a autoinicialização do firmware. Esses binários incluem drivers de UEFI e o carregador de inicialização principal, bem como componentes carregados em cadeia.

O UEFI Secure Boot especifica quatro bancos de dados principais que são usados em uma cadeia de confiança. Os bancos de dados são armazenados no armazenamento de variáveis UEFI.

A cadeia de confiança é a seguinte:

Banco de dados de chave de plataforma (PK

O banco de dados de PK é a raiz de confiança. Ele contém uma única chave PK pública usada na cadeia de confiança para atualizar o banco de dados de chaves de troca de chave (KEK).

Para alterar o banco de dados de PK, você deve ter a chave PK privada para assinar uma solicitação de atualização. Isso inclui excluir o banco de dados de PK escrevendo uma chave PK vazia.

Banco de dados de chaves de troca de chave (KEK

O banco de dados de KEK é uma lista de chaves KEK públicas que são usadas na cadeia de confiança para atualizar os bancos de dados de assinaturas (db) e de lista de negação (dbx).

Para alterar o banco de dados de KEK público, você deve ter a chave PK privada para assinar uma solicitação de atualização.

Banco de dados de assinaturas (db

O banco de dados db é uma lista de chaves públicas e hashes que são usados na cadeia de confiança para validar todos os binários de inicialização UEFI.

Para alterar o banco de dados db, você deve ter a chave PK privada ou qualquer uma das chaves KEK privadas para assinar uma solicitação de atualização.

Banco de dados de lista de negação de assinatura (dbx

O banco de dados dbx é uma lista de chaves públicas e hashes binários que não são confiáveis e são usados na cadeia de confiança como um arquivo de revogação.

O banco de dados dbx sempre tem precedência sobre todos os outros bancos de dados de chaves.

Para alterar o banco de dados dbx, você deve ter a chave PK privada ou qualquer uma das chaves KEK privadas para assinar uma solicitação de atualização.

O Fórum UEFI mantém um dbx disponível publicamente para muitos binários e certificados conhecidamente ruins em https://uefi.org/revocationlistfile.

Important

O UEFI Secure Boot impõe a validação da assinatura em qualquer binário UEFI. Para permitir a execução de um binário UEFI no UEFI Secure Boot, você o assina com qualquer uma das chaves db privadas descritas acima.

Por padrão, o UEFI Secure Boot é desabilitado e o sistema está no `SetupMode`. Quando o sistema estiver no `SetupMode`, todas as variáveis principais podem ser atualizadas sem uma assinatura criptográfica. Quando a PK está definida, o UEFI Secure Boot é habilitado e o SetupMode é encerrado.

Requisitos para o UEFI Secure Boot no Amazon EC2

Quando você executar uma instância do Amazon EC2com uma AMI e um tipo de instância compatíveis, essa instância validará automaticamente os binários de inicialização da UEFI em relação ao banco de dados do UEFI Secure Boot. Não é exigida nenhuma configuração adicional. Você também pode configurar o UEFI Secure Boot em uma instância após o início.

Note

O UEFI Secure Boot protege sua instância e seu sistema operacional contra modificações no fluxo de inicialização. Se você criar uma nova AMI a partir de uma AMI de origem com

a Inicialização Segura UEFI habilitada e modificar determinados parâmetros durante o processo de cópia, como alterar os `UefiData` na AMI, poderá desabilitar a Inicialização Segura UEFI.

Conteúdo

- AMIs compatíveis
- Tipos de instâncias compatíveis

AMIs compatíveis

AMIs do Linux

Para iniciar uma instância Linux, a AMI Linux deve ter o UEFI Secure Boot habilitado.

O Amazon Linux oferece suporte ao UEFI Secure Boot a partir do AL2023 versão 2023.1. No entanto, o UEFI Secure Boot não está habilitado nas AMIs padrão. Para obter mais informações, consulte UEFI Secure Boot no Guia do usuário do AL2023. As versões mais antigas das AMIs do Amazon Linux não estão habilitadas para o UEFI Secure Boot. Para usar uma AMI compatível, é necessário executar várias etapas de configuração em sua própria AMI do Linux. Para obter mais informações, consulte Criar uma AMI do Linux com chaves personalizadas do UEFI Secure Boot.

AMIs Windows

Para iniciar uma instância Windows, a AMI Windows deve ter o UEFI Secure Boot habilitado. Para encontrar uma AMI do AWS Windows pré-configurada para UEFI Secure Boot com chaves da Microsoft, consulte Encontrar AMIs do Windows Server configuradas com NitroTPM e UEFI Secure Boot na Referência de AMIs do AWS Windows.

Atualmente, não oferecemos suporte à importação do Windows com o UEFI Secure Boot o comando import-image.

Tipos de instâncias compatíveis

Todos os tipos de instâncias virtualizadas que são compatíveis com a UEFI também são compatíveis com o UEFI Secure Boot. Para ver os tipos de instância compatíveis com o UEFI Secure Boot, consulte Requisitos para o modo de inicialização da UEFI.

> **Note**
>
> Os tipos de instância bare metal não oferecem suporte ao UEFI Secure Boot.

Verificar se uma instância do Amazon EC2 está habilitada para o UEFI Secure Boot

É possível usar os procedimentos a seguir para determinar se um Amazon EC2 está habilitado para o UEFI Secure Boot.

Instâncias do Linux

É possível usar o utilitário `mokutil` para verificar se uma instância do Linux está habilitada para o UEFI Secure Boot. Se o `mokutil` não estiver instalado em sua instância, você precisará instalá-lo. Para obter as instruções de instalação do Amazon Linux 2, consulte Find and install software packages on an Amazon Linux 2 instance. Para outras distribuições do Linux, consulte a documentação específica.

Verificar se uma instância do Linux está habilitada para o UEFI Secure Boot

Conecte-se à instância e execute o comando a seguir como `root` na janela de terminal.

```
mokutil --sb-state
```

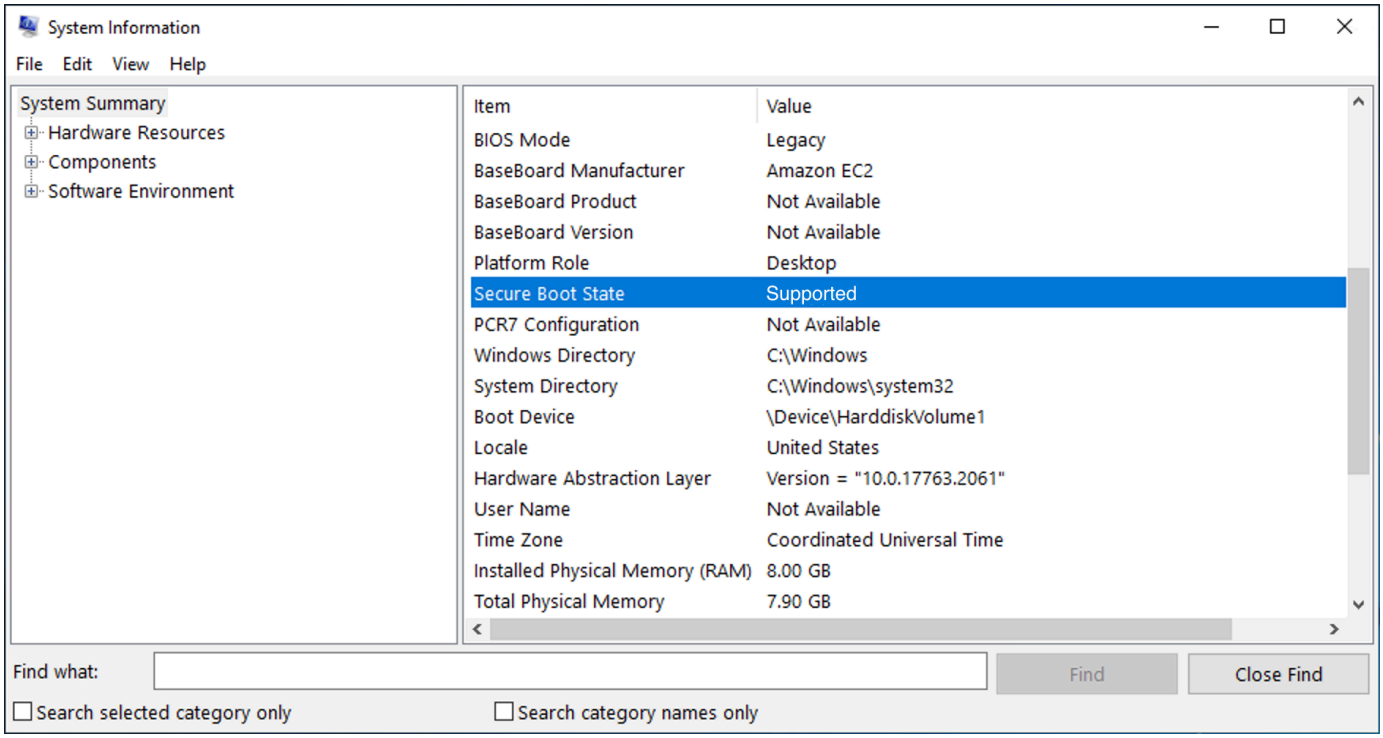
O seguinte é um exemplo de saída.

- Se o UEFI Secure Boot estiver habilitado, a saída conterá `SecureBoot enabled`.
- Se o UEFI Secure Boot não estiver habilitado, a saída conterá `SecureBoot disabled` ou `Failed to read SecureBoot`.

Instâncias do Windows

Para verificar se uma instância do Windows está habilitada para o UEFI Secure Boot

1. Conecte-se à sua instância.
2. Abra a ferramenta msinfo32.
3. Verifique o campo Secure Boot State (Estado do Secure Boot). Se o UEFI Secure Boot estiver habilitado, o valor será Compatível, conforme mostrado na imagem a seguir.



Você também pode usar o cmdlet `Confirm-SecureBootUEFI` do Windows PowerShell para verificar o status da Secure Boot. Para obter mais informações sobre o cmdlet, consulte Confirm-SecureBootUEFI na documentação da Microsoft.

Criar uma AMI do Linux com chaves personalizadas do UEFI Secure Boot

Estas instruções mostram como criar uma AMI do Linux com o UEFI Secure Boot e chaves privadas personalizadas. O Amazon Linux oferece suporte ao UEFI Secure Boot a partir do AL2023 versão 2023.1. Para obter mais informações, consulte UEFI Secure Boot on AL2023 no Guia do usuário do Amazon Linux 2023.

> **Important**
>
> O procedimento a seguir destina-se somente a usuários avançados. Você deve ter conhecimento suficiente de SSL e do fluxo de inicialização da distribuição do Linux para usar esses procedimentos.

Pré-requisitos

- As seguintes ferramentas serão usadas:

- OpenSSL: https://www.openssl.org/
- efivar: https://github.com/rhboot/efivar
- efitools: https://git.kernel.org/pub/scm/linux/kernel/git/jejb/efitools.git/
- Comando get-instance-uefi-data

- Sua instância do Linux deve ter sido iniciada com uma AMI do Linux com suporte para o modo de inicialização UEFI e ter dados não voláteis presentes.

Instâncias recém-criadas sem chaves do UEFI Secure Boot são criadas em `SetupMode`, o que permite que você inscreva suas próprias chaves. Algumas AMIs vêm pré-configuradas com o UEFI Secure Boot, e você não pode alterar as chaves existentes. Se você desejar alterar as chaves, deve criar uma nova AMI com base na AMI original.

Você tem duas maneiras de propagar as chaves no armazenamento de variáveis, descritas na Opção A e na Opção B a seguir. A opção A descreve como fazer isso de dentro da instância, imitando o fluxo de hardware real. A opção B descreve como criar um blob binário, que será então passado como um arquivo codificado em base64 quando você criar a AMI. Para ambas as opções, você deve primeiro criar os três pares de chaves, que são usados para a cadeia de confiança.

Para criar uma AMI do Linux compatível com o UEFI Secure Boot, primeiro crie os três pares de chaves e, em seguida, conclua a Opção A ou a Opção B, mas não ambas:

- Tarefa 1: criar pares de chaves
- Tarefa 2: opção A: adicionar chaves ao armazenamento de variáveis de dentro da instância
- Tarefa 2: opção B: criar um blob binário contendo um armazenamento de variáveis pré-preenchido

Tarefa 1: criar pares de chaves

O UEFI Secure Boot é baseado nos três seguintes bancos de dados de chaves, que são usados em uma cadeia de confiança: a chave de plataforma (PK), a chave de troca de chaves (KEK) e o banco de dados de assinatura (db).[1]

Você cria cada chave na instância. Para preparar as chaves públicas em um formato válido para o padrão UEFI Secure Boot, você cria um certificado para cada chave. `DER` define o formato SSL (codificação binária de um formato). Em seguida, você converte cada certificado em uma lista de assinaturas UEFI, que é o formato binário entendido pelo UEFI Secure Boot. E, finalmente, você assina cada certificado com a chave relevante.

Tarefas

- Preparar para criar os pares de chaves
- Par de chaves 1: criar a chave da plataforma (PK)
- Par de chaves 2: criar a chave de troca de chaves (KEK)
- Par de chaves 3: criar o banco de dados de assinaturas (db)
- Assine a imagem de inicialização (kernel) com a chave privada

Preparar para criar os pares de chaves

Antes de criar os pares de chaves, crie um identificador exclusivo globalmente (GUID) para ser usado na geração de chaves.

1. Conecte-se à instância.
2. Execute o comando a seguir em um prompt de shell.

```
uuidgen --random > GUID.txt
```

Par de chaves 1: criar a chave da plataforma (PK)

A PK é a raiz da confiança para instâncias UEFI Secure Boot. A PK privada é usado para atualizar a KEK, que por sua vez pode ser usada para adicionar chaves autorizadas ao banco de dados de assinaturas (db).

O padrão X.509 é usado para criar o par de chaves. Para obter informações sobre o padrão, consulte X.509 na Wikipédia.

Para criar o PK

1. Crie a chave. Você deve nomear a variável PK.

```
openssl req -newkey rsa:4096 -nodes -keyout PK.key -new -x509 -sha256 -days 3650 -
subj "/CN=Platform key/" -out PK.crt
```

   Os seguintes parâmetros são especificados:

   - `-keyout PK.key`: o arquivo da chave privada.
   - `-days 3650`: o número de dias em que o certificado é válido.

- `-out PK.crt`: o certificado usado para criar a variável UEFI.
- `CN=`*`Platform key`*: o nome comum (CN) para a chave. É possível inserir o nome da sua própria organização em vez de *`Chave da plataforma`*.

2. Crie o certificado.

```
openssl x509 -outform DER -in PK.crt -out PK.cer
```

3. Converta o certificado em uma lista de assinaturas UEFI.

```
cert-to-efi-sig-list -g "$(< GUID.txt)" PK.crt PK.esl
```

4. Assine a lista de assinaturas UEFI com a PK privada (autoassinada).

```
sign-efi-sig-list -g "$(< GUID.txt)" -k PK.key -c PK.crt PK PK.esl PK.auth
```

Par de chaves 2: criar a chave de troca de chaves (KEK)

A KEK privada é usada para adicionar chaves ao db, que é a lista de assinaturas autorizadas a inicializar no sistema.

Para criar a KEK

1. Crie a chave.

```
openssl req -newkey rsa:4096 -nodes -keyout KEK.key -new -x509 -sha256 -days 3650 -
subj "/CN=Key Exchange Key/" -out KEK.crt
```

2. Crie o certificado.

```
openssl x509 -outform DER -in KEK.crt -out KEK.cer
```

3. Converta o certificado em uma lista de assinaturas UEFI.

```
cert-to-efi-sig-list -g "$(< GUID.txt)" KEK.crt KEK.esl
```

4. Assine a lista de assinaturas com a PK privada.

```
sign-efi-sig-list -g "$(< GUID.txt)" -k PK.key -c PK.crt KEK KEK.esl KEK.auth
```

Par de chaves 3: criar o banco de dados de assinaturas (db)

A lista db contém chaves autorizadas que estão autorizadas a ser inicializadas no sistema. Para modificar a lista, é necessária a KEK privada. As imagens de inicialização serão assinadas com a chave privada criada nesta etapa.

Para criar o db

1. Crie a chave.

```
openssl req -newkey rsa:4096 -nodes -keyout db.key -new -x509 -sha256 -days 3650 -
subj "/CN=Signature Database key/" -out db.crt
```

2. Crie o certificado.

```
openssl x509 -outform DER -in db.crt -out db.cer
```

3. Converta o certificado em uma lista de assinaturas UEFI.

```
cert-to-efi-sig-list -g "$(< GUID.txt)" db.crt db.esl
```

4. Assine a lista de assinaturas com a KEK privada.

```
sign-efi-sig-list -g "$(< GUID.txt)" -k KEK.key -c KEK.crt db db.esl db.auth
```

Assine a imagem de inicialização (kernel) com a chave privada

Para o Ubuntu 22.04, as imagens a seguir exigem assinaturas.

```
/boot/efi/EFI/ubuntu/shimx64.efi
/boot/efi/EFI/ubuntu/mmx64.efi
/boot/efi/EFI/ubuntu/grubx64.efi
/boot/vmlinuz
```

Para assinar uma imagem

Utilize uma sintaxe semelhante à seguinte.

```
sbsign --key db.key --cert db.crt --output /boot/vmlinuz /boot/vmlinuz
```

> **Note**
>
> Você deve assinar todos os novos kernels. `/boot/vmlinuz` geralmente será um link simbólico para o último kernel instalado.

Consulte a documentação da sua distribuição para saber sobre sua cadeia de inicialização e as imagens necessárias.

[1] Nossos agradecimentos à comunidade ArchWiki por todo o trabalho que eles fizeram. Os comandos para criar a PK, criar a KEK, criar o DB e assinar a imagem são de Criação de chaves, de autoria da Equipe de Manutenção do ArchWiki e/ou dos colaboradores do ArchWiki.

Tarefa 2: opção A: adicionar chaves ao armazenamento de variáveis de dentro da instância

Depois de criar os três pares de chaves, é possível se conectar à sua instância e adicionar as chaves ao armazenamento de variáveis de dentro da instância, concluindo as etapas a seguir. Como alternativa, conclua as etapas em the section called “Tarefa 2: opção B: criar um blob binário contendo um armazenamento de variáveis pré-preenchido”.

Etapas da Opção A:

- Etapa 1: iniciar uma instância que ofereça suporte ao UEFI Secure Boot
- Etapa 2: configurar uma instância para oferecer suporte ao UEFI Secure Boot
- Etapa 3: criar uma AMI da instância

Etapa 1: iniciar uma instância que ofereça suporte ao UEFI Secure Boot

Quando você iniciar uma instância com os pré-requisitos a seguir, a instância estará pronta para ser configurada para oferecer suporte ao UEFI Secure Boot. Você só pode habilitar o suporte ao UEFI Secure Boot em uma instância na inicialização; não será possível habilitá-lo mais tarde.

Pré-requisitos

- AMI: a AMI do Linux deve oferecer suporte ao modo de inicialização UEFI. Para verificar se a AMI oferece suporte ao modo de inicialização UEFI, o parâmetro do modo de inicialização da AMI deve ser UEFI. Para obter mais informações, consulte Determinar o parâmetro do modo de inicialização de uma AMI do Amazon EC2.

Observe que fornece a AWS só fornece AMIs do Linux configuradas para compatibilidade com UEFI para tipos de instância baseados no Graviton. A AWS atualmente não fornece AMIs do Linux x86_64 que sejam compatíveis com o modo de inicialização UEFI. É possível configurar a AMI para compatibilidade com o modo de inicialização UEFI para todas as arquiteturas. Para configurar sua própria AMI para compatibilidade com o modo de inicialização UEFI, é necessário realizar várias etapas de configuração em sua própria AMI. Para obter mais informações, consulte Definir o modo de inicialização de uma AMI do Amazon EC2.

- Tipo de instância: todos os tipos de instâncias virtualizadas com suporte a UEFI também oferecem suporte a UEFI Secure Boot. Os tipos de instância bare metal não oferecem suporte ao UEFI Secure Boot. Para ver os tipos de instância compatíveis com o UEFI Secure Boot, consulte Requisitos para o modo de inicialização da UEFI.
- Inicie sua instância após o lançamento do UEFI Secure Boot. Somente instâncias iniciadas após 10 de maio de 2022 (quando o UEFI Secure Boot foi lançado) podem oferecer suporte ao UEFI Secure Boot.

Depois de iniciar sua instância, é possível verificar se ela está pronta para ser configurada para oferecer suporte à UEFI Secure Boot (em outras palavras, é possível prosseguir para a Etapa 2) verificando se os dados da UEFI estão presentes. A presença de dados de UEFI indica que dados não voláteis são persistidos.

Para verificar se sua instância está pronta para a Etapa 2

Use o comando get-instance-uefi-data e especifique o ID da instância.

```
aws ec2 get-instance-uefi-data --instance-id i-1234567890abcdef0
```

A instância estará pronta para a Etapa 2 se os dados da UEFI estiverem presentes na saída. Se a saída estiver vazia, a instância não poderá ser configurada para oferecer suporte ao UEFI Secure Boot. Isso pode acontecer se sua instância tiver sido iniciada antes que o suporte ao UEFI Secure Boot fique disponível. Inicie uma nova instância e tente novamente.

Etapa 2: configurar uma instância para oferecer suporte ao UEFI Secure Boot

Registre os pares de chaves no armazenamento de variáveis UEFI na instância

> **Warning**
>
> Você deve assinar suas imagens de inicialização depois de registrar as chaves, caso contrário, não poderá inicializar sua instância.

Depois que você criar as listas de assinaturas UEFI assinadas (`PK`, `KEK`, e `db`), elas devem ser registradas no firmware do UEFI.

A gravação na variável `PK` só será possível se:

- Ainda não houver PK registrada, o que será indicado se a variável `SetupMode` for `1`. Verifique isso usando o comando a seguir. A saída for `1` ou `0`.

  ```
  efivar -d -n 8be4df61-93ca-11d2-aa0d-00e098032b8c-SetupMode
  ```

- A nova PK for assinada pela chave privada da PK existente.

Para registrar as chaves no seu armazenamento de variáveis UEFI

Os comandos a seguir devem ser executados na instância.

Se SetupMode estiver habilitado (o valor será 1), as chaves podem ser registradas executando os seguintes comandos na instância:

```
[ec2-user ~]$ efi-updatevar -f db.auth db
```

```
[ec2-user ~]$ efi-updatevar -f KEK.auth KEK
```

```
[ec2-user ~]$ efi-updatevar -f PK.auth PK
```

Para verificar se o UEFI Secure Boot está habilitado

Para verificar se o UEFI Secure Boot está habilitado, siga as etapas em Verificar se uma instância do Amazon EC2 está habilitada para o UEFI Secure Boot.

Agora é possível exportar seu armazenamento de variáveis UEFI com o comando get-instance-uefi-data da CLI, ou prosseguir para a próxima etapa e assinar suas imagens de inicialização para reinicializar em uma instância habilitada para o UEFI Secure Boot.

Etapa 3: criar uma AMI da instância

Para criar uma AMI a partir da instância, é possível usar o console ou a API `CreateImage`, a CLI ou SDKs. Para obter instruções sobre o console, consulte Criação de uma AMI baseada no Amazon EBS. Para obter instruções sobre a API, consulte CreateImage.

> **Note**
>
> A API `CreateImage` copia automaticamente o armazenamento de variáveis UEFI da instância para a AMI. O console usa a API `CreateImage`. Depois de executar instâncias usando essa AMI, as instâncias terão o mesmo armazenamento de variáveis UEFI.

Tarefa 2: opção B: criar um blob binário contendo um armazenamento de variáveis pré-preenchido

Depois de criar os três pares de chaves, é possível criar um blob binário contendo um armazenamento de variáveis pré-preenchido contendo as chaves do UEFI Secure Boot. Como alternativa, conclua as etapas em the section called “Tarefa 2: opção A: adicionar chaves ao armazenamento de variáveis de dentro da instância”.

> **Warning**
>
> Você deverá assinar suas imagens de inicialização antes de registrar as chaves, caso contrário, não poderá inicializar sua instância.

Etapas da Opção B:

- Etapa 1: criar um novo armazenamento de variáveis ou atualizar um existente
- Etapa 2: carregar o blob binário na criação da AMI

Etapa 1: criar um novo armazenamento de variáveis ou atualizar um existente

É possível criar o armazenamento de variáveis offline, sem uma instância em execução, usando a ferramenta python-uefivars. A ferramenta pode criar um novo armazenamento de variáveis a partir

de suas chaves. O script atualmente oferece suporte ao formato EDK2, ao formato AWS e a uma representação JSON que é mais fácil de editar com ferramentas de nível superior.

Para criar o armazenamento de variáveis offline sem uma instância em execução

1. Baixe a ferramenta no link a seguir.

   ```
   https://github.com/awslabs/python-uefivars
   ```

2. Crie um novo armazenamento de variáveis a partir de suas chaves executando o comando a seguir. Isso criará um blob binário codificado em base64 em *your_binary_blob*.bin. A ferramenta também suporta a atualização de um blob binário através do parâmetro `-I`.

   ```
   ./uefivars.py -i none -o aws -O your_binary_blob.bin -P PK.esl -K KEK.esl --db
    db.esl --dbx dbx.esl
   ```

Etapa 2: carregar o blob binário na criação da AMI

Use register-image para passar seus dados de armazenamento de variáveis UEFI. Para o parâmetro `--uefi-data`, especifique seu blob binário e para o parâmetro `--boot-mode`, especifique `uefi`.

```
aws ec2 register-image \
    --name uefi_sb_tpm_register_image_test \
    --uefi-data $(cat your_binary_blob.bin) \
    --block-device-mappings "DeviceName=/dev/sda1,Ebs=
 {SnapshotId=snap-0123456789example,DeleteOnTermination=true}" \
    --architecture x86_64 \
    --root-device-name /dev/sda1 \
    --virtualization-type hvm \
    --ena-support \
    --boot-mode uefi
```

Crie o blob binário da AWS para o UEFI Secure Boot

É possível usar as seguintes etapas para personalizar as variáveis do UEFI Secure Boot durante a criação da AMI. A KEK usado nessas etapas está atual desde de setembro de 2021. Se a Microsoft atualizar a KEK, você deverá usar a KEK mais recente.

Para criar o blob binário da AWS

1. Crie uma lista de assinaturas PK vazia.

```
touch empty_key.crt
cert-to-efi-sig-list empty_key.crt PK.esl
```

2. Baixe os certificados de KEK.

```
https://go.microsoft.com/fwlink/?LinkId=321185
```

3. Empacote os certificados de KEK em uma lista de assinaturas UEFI (`siglist`).

```
sbsiglist --owner 77fa9abd-0359-4d32-bd60-28f4e78f784b --type x509 --output
 MS_Win_KEK.esl MicCorKEKCA2011_2011-06-24.crt
```

4. Baixe os certificados de db da Microsoft.

```
https://www.microsoft.com/pkiops/certs/MicWinProPCA2011_2011-10-19.crt
https://www.microsoft.com/pkiops/certs/MicCorUEFCA2011_2011-06-27.crt
```

5. Gere a lista de assinaturas db.

```
sbsiglist --owner 77fa9abd-0359-4d32-bd60-28f4e78f784b --type x509 --output
 MS_Win_db.esl MicWinProPCA2011_2011-10-19.crt
sbsiglist --owner 77fa9abd-0359-4d32-bd60-28f4e78f784b --type x509 --output
 MS_UEFI_db.esl MicCorUEFCA2011_2011-06-27.crt
cat MS_Win_db.esl MS_UEFI_db.esl > MS_db.esl
```

6. O Unified Extensible Firmware Interface Forum não fornece mais os arquivos DBX. Eles agora são fornecidos pela Microsoft no GitHub. Baixe a atualização mais recente do DBX do repositório de atualizações do Microsoft Secure Boot em https://github.com/microsoft/secureboot_objects.
7. Descompacte o binário de atualização assinado.

   Crie `SplitDbxContent.ps1` com o conteúdo do script abaixo. Como alternativa, você pode instalar o script da Galeria do PowerShell usando `Install-Script -Name SplitDbxContent`.

```
<#PSScriptInfo
```

```
.VERSION 1.0

.GUID ec45a3fc-5e87-4d90-b55e-bdea083f732d

.AUTHOR Microsoft Secure Boot Team

.COMPANYNAME Microsoft

.COPYRIGHT Microsoft

.TAGS Windows Security

.LICENSEURI

.PROJECTURI

.ICONURI

.EXTERNALMODULEDEPENDENCIES

.REQUIREDSCRIPTS

.EXTERNALSCRIPTDEPENDENCIES

.RELEASENOTES
Version 1.0: Original published version.

#>

<#
.DESCRIPTION
 Splits a DBX update package into the new DBX variable contents and the signature
 authorizing the change.
 To apply an update using the output files of this script, try:
 Set-SecureBootUefi -Name dbx -ContentFilePath .\content.bin -SignedFilePath .
\signature.p7 -Time 2010-03-06T19:17:21Z -AppendWrite'
.EXAMPLE
.\SplitDbxAuthInfo.ps1 DbxUpdate_x64.bin
#>


# Get file from script input
$file  = Get-Content -Encoding Byte $args[0]
```

```
# Identify file signature
$chop = $file[40..($file.Length - 1)]
if (($chop[0] -ne 0x30) -or ($chop[1] -ne 0x82 )) {
    Write-Error "Cannot find signature"
    exit 1
}

# Signature is known to be ASN size plus header of 4 bytes
$sig_length = ($chop[2] * 256) + $chop[3] + 4
$sig = $chop[0..($sig_length - 1)]

if ($sig_length -gt ($file.Length + 40)) {
    Write-Error "Signature longer than file size!"
    exit 1
}

# Content is everything else
$content = $file[0..39] + $chop[$sig_length..($chop.Length - 1)]

# Write signature and content to files
Set-Content -Encoding Byte signature.p7 $sig
Set-Content -Encoding Byte content.bin $content
```

Use o script para descompactar os arquivos DBX assinados.

```
PS C:\Windows\system32> SplitDbxContent.ps1 .\dbx.bin
```

Isso produz dois arquivos: `signature.p7` e `content.bin`. Use `content.bin` na próxima etapa.

8. Construa um armazenamento de variáveis UEFI usando o script `uefivars.py`.

```
./uefivars.py -i none -o aws -O uefiblob-microsoft-keys-empty-pk.bin -P ~/PK.esl -K
 ~/MS_Win_KEK.esl --db ~/MS_db.esl  --dbx ~/content.bin
```

9. Verifique o blob binário e o armazenamento de variáveis UEFI.

```
./uefivars.py -i aws -I uefiblob-microsoft-keys-empty-pk.bin -o json | less
```

10. É possível atualizar o blob passando-o para a mesma ferramenta novamente.

```
./uefivars.py -i aws -I uefiblob-microsoft-keys-empty-pk.bin -o aws -O uefiblob-
microsoft-keys-empty-pk.bin -P ~/PK.esl -K ~/MS_Win_KEK.esl --db ~/MS_db.esl  --dbx
 ~/content.bin
```

Saída esperada

```
Replacing PK
Replacing KEK
Replacing db
Replacing dbx
```

Usar criptografia com AMIs com EBS

As AMIs com snapshots do Amazon EBS podem se beneficiar da criptografia do Amazon EBS. Os snapshots de volumes raiz e de dados podem ser criptografados e anexados a uma AMI. É possível executar instâncias e copiar imagens com suporte total à criptografia do EBS. Os parâmetros de criptografia para essas operações são compatíveis em todas as regiões em que o AWS KMS está disponível.

As instâncias do EC2 com volumes do EBS criptografados são executadas em AMIs da mesma forma que outras instâncias. Além disso, ao executar uma instância a partir de uma AMI baseada em snapshots não criptografados do EBS, será possível criptografar alguns ou todos os volumes durante a execução.

Como os volumes do EBS, os snapshots em AMIs podem ser criptografados pelo padrão do AWS KMS key ou por um chave gerenciada pelo cliente que você especificar. Em todos os casos, é necessário ter permissão para usar a Chave do KMS selecionada.

As AMIs com snapshots criptografados podem ser compartilhadas em todas as contas da AWS. Para obter mais informações, consulte Saiba mais sobre o uso da AMI compartilhada no Amazon EC2.

Tópicos de criptografia em AMIs com EBS

- Cenários de execução de instância
- Cenários de cópia de imagem

Cenários de execução de instância

As instâncias do Amazon EC2 são iniciadas nas AMIs usando a ação `RunInstances` com parâmetros fornecidos pelo mapeamento de dispositivos de blocos, seja por meio do Console de gerenciamento da AWS ou diretamente usando a CLI ou a API do Amazon EC2. Para ter mais informações, consulte Mapeamento de dispositivos de blocos para volumes em instâncias do Amazon EC2. Para exemplos de mapeamento de dispositivos de blocos da AWS CLI, consulte Executar, listar e encerrar instâncias do EC2.

Por padrão, sem parâmetros de criptografia explícitos, uma ação `RunInstances` mantém o estado de criptografia existente dos snapshots de origem de uma AMI enquanto restaura os volumes do EBS a partir deles. Se a opção de criptografar por padrão estiver habilitada, todos os volumes criados com base na AMI (seja de snapshots criptografados ou não criptografados) serão criptografados. Se a opção de criptografar por padrão não estiver habilitada, a instância manterá o estado de criptografia da AMI.

Também é possível executar uma instância e aplicar simultaneamente um estado de criptografia aos volumes resultantes fornecendo parâmetros de criptografia. Consequentemente, os seguintes comportamentos são observados:

Executar sem parâmetros de criptografia

- Um snapshot não criptografado é restaurado para um volume não criptografado, a menos que a criptografia por padrão esteja habilitada, e, nesse caso, todos os volumes recém-criados serão criptografados.
- Um snapshot criptografado que você possui é restaurado para um volume que é criptografado para a mesma Chave do KMS.
- Um snapshot criptografado do qual você não é proprietário (por exemplo, a AMI é compartilhada com você) é restaurado para um volume que é criptografado pela chave do KMS padrão da sua conta da AWS.

Os comportamentos padrão podem ser substituídos fornecendo parâmetros de criptografia. Os parâmetros disponíveis são `Encrypted` e `KmsKeyId`. Configurar somente o parâmetro `Encrypted` resulta no seguinte:

A instância executa comportamentos com **`Encrypted`** definido, mas sem **`KmsKeyId`** especificado

- Um snapshot não criptografado é restaurado em um volume do EBS que é criptografado pela chave do KMS padrão da sua conta da AWS.

- Um snapshot criptografado que você possui é restaurado para um volume do EBS criptografado pela mesma Chave do KMS. (Em outras palavras, o parâmetro `Encrypted` não tem efeito.)
- Um snapshot criptografado do qual você não é proprietário (por exemplo, a AMI é compartilhada com você) é restaurado para um volume que é criptografado pela chave do KMS padrão da sua conta da AWS. (Em outras palavras, o parâmetro `Encrypted` não tem efeito.)

A configuração dos parâmetros `Encrypted` e `KmsKeyId` permite especificar uma Chave do KMS não padrão para uma operação de criptografia. Os seguintes comportamentos resultam em:

A instância com **`Encrypted`** e **`KmsKeyId`** definidos

- Um snapshot não criptografado é restaurado para um volume do EBS criptografado pela Chave do KMS especificada.
- Um snapshot criptografado é restaurado para um volume do EBS criptografado, não para a Chave do KMS original, mas para a Chave do KMS especificada.

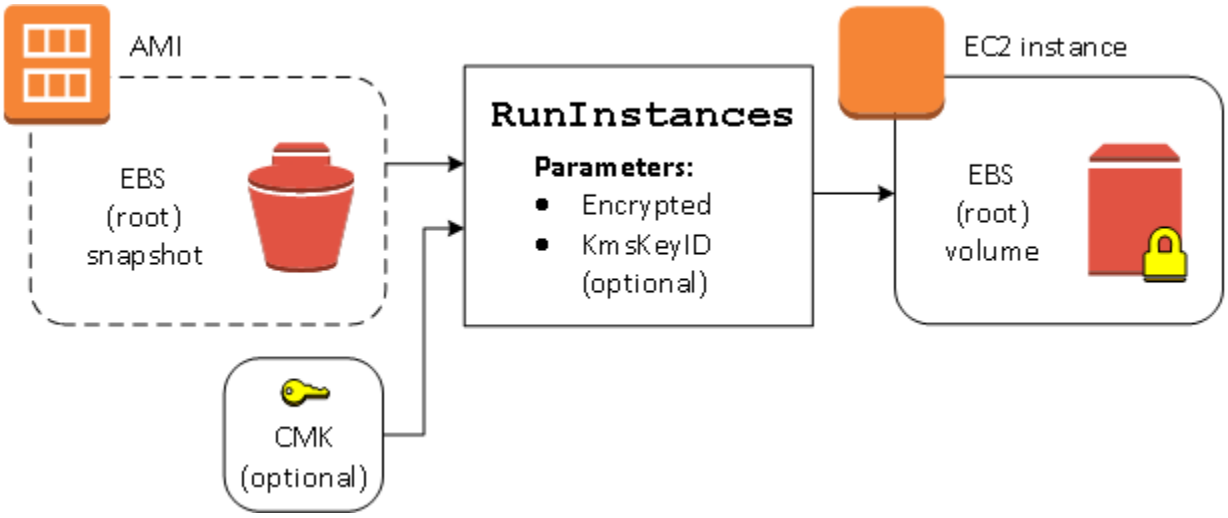
Enviar um `KmsKeyId` sem também configurar o parâmetro `Encrypted` resulta em um erro.

As seções a seguir fornecem exemplos da execução de instâncias de AMIs usando parâmetros de criptografia não padrão. Em cada um desses cenários, os parâmetros fornecidos à ação `RunInstances` resultam em uma alteração do estado de criptografia durante a restauração de um volume a partir de um snapshot.

Para obter informações sobre como usar o console para executar uma instância a partir de uma AMI, consulte Iniciar uma instância do Amazon EC2.

Criptografar um volume durante a execução

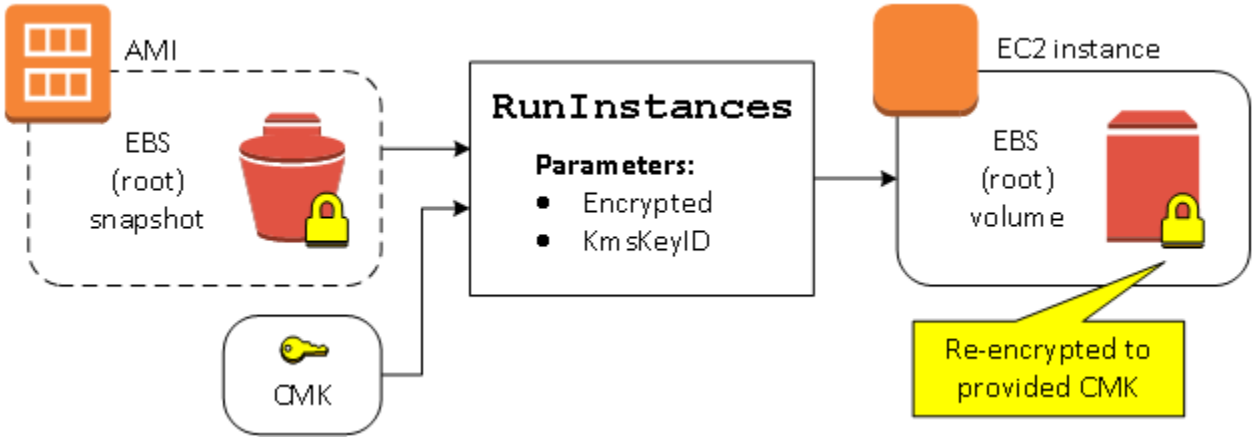
Neste exemplo, uma AMI baseada em um snapshot não criptografado é usada para executar uma instância do EC2 com um volume não criptografado do EBS.



Somente o parâmetro `Encrypted` resulta no volume que será criptografado para essa instância. É opcional fornecer um parâmetro `KmsKeyId`. Se nenhum ID de Chave do KMS for especificado, a Chave do KMS padrão da conta da AWS será usada para criptografar o volume. Para criptografar o volume em uma Chave do KMS diferente que pertença a você, forneça o parâmetro `KmsKeyId`.

Criptografar novamente um volume durante a execução

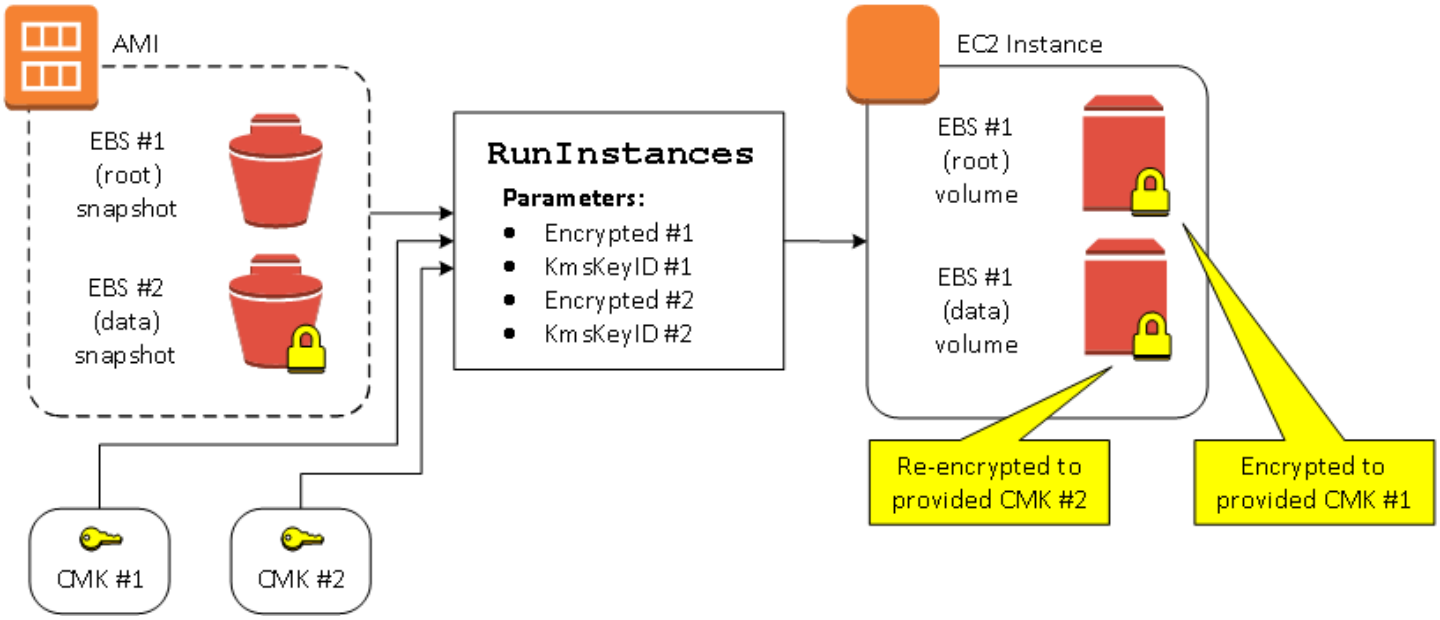
Neste exemplo, uma AMI baseada em um snapshot criptografado é usada para executar uma instância do EC2 com um volume do EBS criptografado por uma nova Chave do KMS.



Se você possuir a AMI e não fornecer nenhum parâmetro de criptografia, a instância resultante terá um volume criptografado pela mesma chave do KMS do snapshot. Se a AMI for compartilhada e não pertencer a você, e nenhum parâmetro de criptografia for fornecido, o volume será criptografado pela Chave do KMS padrão. Com os parâmetros de criptografia fornecidos conforme mostrado, o volume será criptografado pela Chave do KMS especificada.

Alterar o estado de criptografia de vários volumes durante a execução

Neste exemplo mais complexo, uma AMI baseada em vários snapshots (cada um com seu próprio estado de criptografia) é usada para executar uma instância do EC2 com um volume recém-criptografado e um volume criptografado novamente.



Neste cenário, a ação `RunInstances` é fornecida com parâmetros de criptografia para cada um dos snapshots de origem. Quando todos os parâmetros possíveis de criptografia forem especificados, a instância resultante será a mesma, independentemente de você possuir a AMI.

Cenários de cópia de imagem

As AMIs do Amazon EC2 são copiadas usando a ação `CopyImage`, seja pelo Console de gerenciamento da AWS ou diretamente usando a CLI ou a API do Amazon EC2.

Por padrão, sem parâmetros de criptografia explícitos, uma ação `CopyImage` mantém o estado de criptografia existente dos snapshots de origem de uma AMI durante a cópia. Também é possível copiar uma AMI e aplicar simultaneamente um novo estado de criptografia aos snapshots associados do EBS fornecendo parâmetros de criptografia. Consequentemente, os seguintes comportamentos são observados:

Copiar sem parâmetros de criptografia

- Um snapshot não criptografado é copiado para outro snapshot não criptografado, a menos que a criptografia por padrão esteja habilitada, e, nesse caso, todos os snapshots recém-criados serão criptografados.

- Um snapshot criptografado de sua propriedade é copiado para um snapshot criptografado com a mesma Chave do KMS.
- Um snapshot criptografado do qual você não é proprietário (por exemplo, a AMI é compartilhada com você) é copiado para um snapshot que é criptografado pela chave do KMS padrão da sua conta da AWS.

Todos esses comportamentos padrão podem ser substituídos fornecendo parâmetros de criptografia. Os parâmetros disponíveis são `Encrypted` e `KmsKeyId`. Configurar somente o parâmetro `Encrypted` resulta no seguinte:

Comportamentos de cópia de imagem com **`Encrypted`** definido, mas nenhum **`KmsKeyId`** especificado

- Um snapshot não criptografado é copiado para um snapshot criptografado pela chave do KMS padrão da conta da AWS.
- Um snapshot criptografado é copiado para outro snapshot criptografado pela mesma Chave do KMS. (Em outras palavras, o parâmetro `Encrypted` não tem efeito.)
- Um snapshot criptografado do qual você não é proprietário (por exemplo, a AMI é compartilhada com você) é copiado para um volume que é criptografado pela chave do KMS padrão da sua conta da AWS. (Em outras palavras, o parâmetro `Encrypted` não tem efeito.)

A configuração dos parâmetros `Encrypted` e `KmsKeyId` permite especificar uma Chave do KMS gerenciada pelo cliente para uma operação de criptografia. Os seguintes comportamentos resultam em:

Comportamentos de cópia de imagem com **`Encrypted`** e **`KmsKeyId`** definidos

- Um snapshot não criptografado é copiado para um snapshot criptografado pela Chave do KMS especificada.
- Um snapshot criptografado é copiado para outro snapshot criptografado, não para a Chave do KMS original, mas para a Chave do KMS especificada.

Enviar um `KmsKeyId` sem também configurar o parâmetro `Encrypted` resulta em um erro.

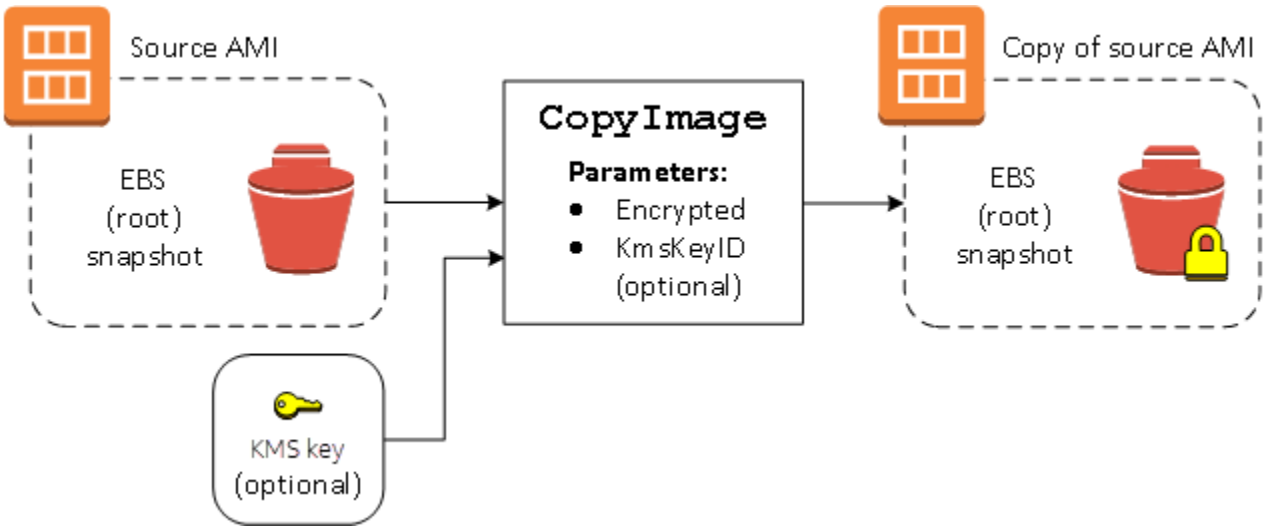
A seção a seguir fornece um exemplo de como copiar uma AMI usando parâmetros de criptografia não padrão, resultando em uma alteração do estado de criptografia.

Para obter instruções detalhadas usando o console, consulte Copiar uma AMI do Amazon EC2.

Criptografar uma imagem não criptografada durante a cópia

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

> **Note**
>
> Habilitar a criptografia por padrão tem o mesmo efeito que configurar o parâmetro `Encrypted` como `true` para todos os snapshots na AMI.



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

> **Note**
>
> Também é possível copiar uma imagem com vários snapshots e configurar o estado de criptografia de cada uma individualmente.

Saiba mais sobre o uso da AMI compartilhada no Amazon EC2

Uma AMI compartilhada é uma AMI que um desenvolvedor criou e disponibilizou para que outros desenvolvedores usem. Uma das maneiras mais fáceis de começar a usar o Amazon EC2 é usar AMIs compartilhadas com os componentes necessários e adicionar o conteúdo personalizado. Também é possível 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 considerasse implantar em seu próprio data center e execute a investigação aplicável. Recomendamos que você obtenha uma AMI de uma fonte confiável, como um provedor verificado.

Provedor verificado

No console do Amazon EC2, AMIs públicas de propriedade da Amazon ou de um parceiro verificado da Amazon são marcadas como Provedor verificado.

Você também pode usar o comando describe-images da AWS CLI para identificar as AMIs públicas provenientes de um provedor verificado. As imagens públicas de propriedade da Amazon ou de um parceiro verificado têm um proprietário com alias, que são `amazon`, `aws-backup-vault` ou `aws-marketplace`. Na saída da CLI, esses valores aparecem para `ImageOwnerAlias`. Outros usuários não podem dar um alias às AMIs deles. Isso permite que você encontre AMIs da Amazon ou de parceiros verificados facilmente.

Para se tornar um fornecedor verificado, você deve se registrar como vendedor no AWS Marketplace. Após o registro, você pode listar sua AMI no AWS Marketplace. Para obter mais informações, consulte Conceitos básicos como vendedor e Produtos baseados em AMIs no Guia do vendedor do AWS Marketplace.

Tópicos da AMI compartilhada

- Encontre AMIs compartilhadas para usar em instâncias do Amazon EC2
- Preparar-se para usar AMIs compartilhadas para Linux
- Controlar a descoberta e o uso de AMIs no Amazon EC2 com AMIs permitidas.
- Disponibilizar publicamente sua AMI para uso no Amazon EC2
- Saiba mais sobre o bloqueio de acesso público para AMIs

- Compartilhar uma AMI com organizações e unidades organizacionais
- Compartilhar uma AMI com contas específicas da AWS
- Cancelar o compartilhamento de uma AMI com sua Conta da AWS
- Recomendações para criar AMIs compartilhadas no Linux

Se você estiver procurando informações sobre outros tópicos

- Para obter informações sobre como criar uma AMI, consulte the section called “Criação de uma AMI baseada no Amazon S3” ou the section called “Criar uma AMI”.
- Para obter informações sobre como criar, fornecer e manter suas aplicações no AWS Marketplace, consulte a Documentação do AWS Marketplace.

Encontre AMIs compartilhadas para usar em instâncias do Amazon EC2

É possível usar o console do Amazon EC2 ou a linha de comandos para encontrar AMIs compartilhadas públicas ou privadas para usar com suas instâncias do Amazon EC2.

As AMIs são um recurso regional. Ao pesquisar uma AMI compartilhada (pública ou privada), é necessário procurá-la na mesma região de onde ela é 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 do Amazon EC2.

Console

O console fornece um campo de filtro de AMI. Você também pode definir o escopo das pesquisas usando os filtros fornecidos no campo Pesquisar.

Para encontrar uma compartilhada ou AMI

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 uma das seguintes opções:
   - Imagens privadas: lista todas as AMIs compartilhadas com você.
   - Imagens públicas: lista todas as AMIs públicas.
4. (Opcional) Para exibir apenas as imagens públicas da Amazon, escolha o campo Pesquisar e, nas opções de menu exibidas, escolha Alias do proprietário, = e amazon.

5. (Opcional) Adicione filtros para limitar o escopo da pesquisa às AMIs que atendam aos seus requisitos.

Para encontrar uma AMI pública de um provedor verificado

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha AMI Catalog (Catálogo de AMIs).
3. Escolha Community AMIs (AMIs da comunidade).
4. No painel Refinar resultados, selecione Provedor verificado. O rótulo Provedor verificado indica se as AMIs são da Amazon ou de um parceiro verificado.

AWS CLI

Use o comando describe-images para listar as AMIs. É possível direcionar o escopo da lista para os tipos de AMI que lhe interessam, conforme exibido nos exemplos a seguir.

Para 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
```

Para listar AMIs com permissões de execução explícitas

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
```

Para listar AMIs pertencentes a provedores verificados

O comando a seguir lista as AMIs pertencentes a provedores verificados. As AMIs públicas pertencentes a fornecedores verificados (da Amazon ou de parceiros verificados) têm um proprietário com alias, que é exibido como `amazon`, `aws-backup-vault` ou `aws-marketplace` no campo da conta. Isso ajuda você a encontrar facilmente AMIs de fornecedores verificados. Outros usuários não podem dar um alias às AMIs deles.

```
aws ec2 describe-images \
```

```
    --owners amazon aws-marketplace \
    --query 'Images[*].[ImageId]' \
    --output text
```

Para listar AMIs pertencentes a uma conta

O comando a seguir lista as AMIs de propriedade da Conta da AWS especificada.

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

Para definir o 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"
```

PowerShell

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

Para listar todas as AMIs públicas

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

```
Get-EC2Image -ExecutableUser all
```

Para listar AMIs com permissões de execução explícitas

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.

```
Get-EC2Image -ExecutableUser self
```

Para listar AMIs pertencentes a provedores verificados

O comando a seguir lista as AMIs pertencentes a provedores verificados. As AMIs públicas pertencentes a fornecedores verificados (da Amazon ou de parceiros verificados) têm um

proprietário com alias, que é exibido como `amazon`, `aws-backup-vault` ou `aws-marketplace` no campo da conta. Isso ajuda você a encontrar facilmente AMIs de fornecedores verificados. Outros usuários não podem dar um alias às AMIs deles.

```
Get-EC2Image -Owner amazon aws-marketplace
```

Para listar AMIs pertencentes a uma conta

O comando a seguir lista as AMIs de propriedade da Conta da AWS especificada.

```
Get-EC2Image -Owner 123456789012
```

Para definir o escopo das AMIs usando um filtro

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

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

Preparar-se para usar AMIs compartilhadas para Linux

Para que você use uma AMI compartilhada para Linux, execute as etapas a seguir para confirmar que não há credenciais pré-instaladas que permitam acesso indesejado à sua instância por terceiros e que não há nenhum registro remoto pré-configurado que poderia transmitir dados confidenciais para 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 acidentalmente 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, é possível desativar a capacidade de fazer login na instância como usuário raiz:

```
PermitRootLogin No
```

Reinicie o serviço sshd.

3. Verifique se há outros usuários que possam fazer login na sua instância. Usuários com privilégios de superusuário são particularmente perigosos. Remova ou bloqueie senha de todas as contas desconhecidas.
4. Verifique se há portas abertas que você não está usando e escuta de serviços de rede em execução para as conexões de entrada.
5. Para evitar o registro em log remoto pré-configurado, exclua o arquivo de configuração existente e reinicie o serviço `rsyslog`. Por exemplo:

```
[ec2-user ~]$ sudo rm /etc/rsyslog.conf
[ec2-user ~]$ sudo service rsyslog restart
```

6. Verifique se todos os trabalhos cron são legítimos.

Se você descobrir uma AMI pública que sente que apresenta um risco de segurança, entre em contato com a equipe de segurança da AWS. Para obter informações, consulte o Centro de segurança da AWS.

Controlar a descoberta e o uso de AMIs no Amazon EC2 com AMIs permitidas.

Para controlar a descoberta e o uso de imagens de máquina da Amazon (AMIs) pelos usuários da sua Conta da AWS, é possível usar o atributo de AMIs permitidas. Você especifica os critérios que as AMIs devem atender para ficarem visíveis e disponíveis em sua conta. Quando os critérios são habilitados, os usuários que iniciam instâncias só verão e terão acesso às AMIs que estejam em conformidade com os critérios especificados. Por exemplo, é possível especificar uma lista de provedores de AMIs confiáveis como critério, e somente as AMIs desses provedores estarão visíveis e disponíveis para uso.

Antes de ativar as configurações de AMIs permitidas, é possível ativar o modo de auditoria para visualizar quais AMIs estarão ou não visíveis e disponíveis para uso. Isso permite que você refine os critérios conforme necessário para garantir que somente as AMIs pretendidas estejam visíveis e disponíveis para os usuários em sua conta. Além disso, use o comando describe-instance-image-metadata para encontrar as instâncias que foram iniciadas com AMIs que não atendiam aos critérios especificados. Essas informações podem orientar sua decisão de atualizar suas configurações de inicialização para usar AMIs em conformidade (por exemplo, especificar uma AMI diferente em um modelo de inicialização) ou ajustar seus critérios para permitir essas AMIs.

Você especifica as configurações de AMIs permitidas no nível da conta, diretamente na conta ou usando uma política declarativa. Essas configurações devem ser definidas em cada Região da AWS onde você deseja controlar o uso de AMIs. O uso de uma política declarativa permite que você aplique as configurações em várias regiões simultaneamente, bem como em várias contas simultaneamente. Quando uma política declarativa está em uso, você não pode modificar as configurações diretamente em uma conta. Este tópico descreve como ajustar as configurações diretamente em uma conta. Para obter informações sobre o uso de políticas declarativas, consulte Políticas declarativas no Guia do usuário do AWS Organizations.

> **Note**
>
> O atributo AMIs permitidas controla somente a descoberta e o uso de AMIs públicas ou AMIs compartilhadas com sua conta. Ele não restringe as AMIs pertencentes à sua conta. Independentemente dos critérios definidos, as AMIs criadas pela sua conta sempre poderão ser descobertas e usadas pelos usuários da sua conta.

Principais benefícios das AMIs permitidas

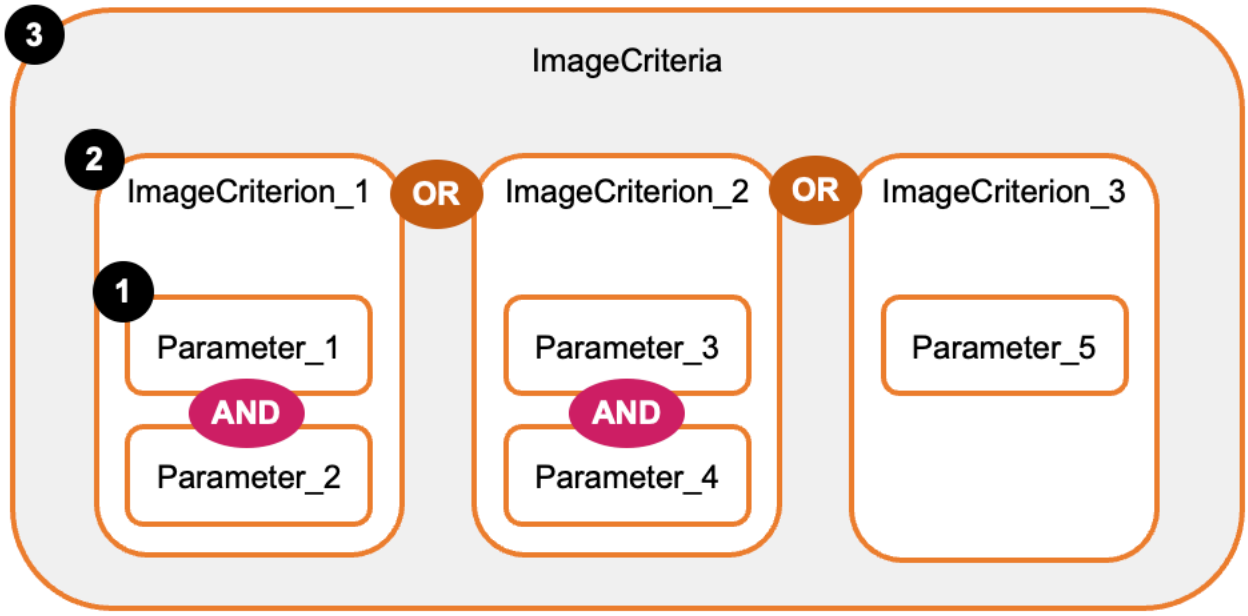
- Conformidade e segurança: os usuários só podem descobrir e usar AMIs que atendam aos critérios especificados, reduzindo o risco de uso de AMIs fora de conformidade.
- Gerenciamento eficiente: ao reduzir o número de AMIs permitidas, o gerenciamento das demais se torna mais fácil e eficiente.
- Implementação centralizada em nível de conta: defina as configurações de AMIs permitidas no nível da conta, diretamente na conta ou por meio de uma política declarativa. Isso fornece uma maneira centralizada e eficiente de controlar o uso de AMIs em toda a conta.

Conteúdo

- Como funcionam as AMIs permitidas
- Práticas recomendadas para a implementação de AMIs permitidas
- Permissões obrigatórias do IAM
- Gerenciar as configurações de AMIs permitidas

Como funcionam as AMIs permitidas

Para controlar quais AMIs podem ser detectadas e usadas em sua conta, defina um conjunto de critérios de avaliação de AMIs. Os critérios são compostos de um ou mais `ImageCriterion`, como mostra o diagrama a seguir. Uma explicação se segue ao diagrama.



A configuração tem três níveis:

- 1 – valores dos parâmetros
  - Parâmetros com vários valores:
    - `ImageProviders`
    - `ImageNames`
    - `MarketplaceProductCodes`

      Uma AMI pode atender a qualquer valor dentro de um parâmetro para ser permitida.

      Exemplo: `ImageProviders` = `amazon` OU conta `111122223333` OU conta `444455556666` (a lógica de avaliação de valores dos parâmetros não é mostrada no diagrama.)

  - Parâmetros de valor único:
    - `CreationDateCondition`
    - `DeprecationTimeCondition`
- 2: `ImageCriterion`
  - Agrupa vários parâmetros com a lógica E.
  - Uma AMI deve atender a todos os parâmetros dentro de um `ImageCriterion` para ser permitida.
  - Exemplo: `ImageProviders` = `amazon` E `CreationDateCondition` = 300 dias ou menos
- 3: `ImageCriteria`
  - Agrupa vários `ImageCriterion` com a lógica OU.
  - Uma AMI pode atender a qualquer `ImageCriterion` para ser permitida.
  - Forma a configuração completa em relação à qual as AMIs são avaliadas.

Tópicos

- Parâmetros de AMIs permitidas
- Configuração de AMIs permitidas
- Como os critérios são avaliados
- Limites
- Operações de AMIs permitidas

Parâmetros de AMIs permitidas

Os seguintes parâmetros podem ser configurados para criar `ImageCriterion`:

`ImageProviders`

Os provedores de AMIs cujas AMIs são permitidas.

Os valores válidos são aliases definidos pela AWS, e IDs de Conta da AWS, da seguinte forma:

- `amazon`: um alias que identifica as AMIs criadas pela Amazon ou por provedores verificados
- `aws-marketplace`: um alias que identifica AMIs criadas por provedores verificados no AWS Marketplace

- `aws-backup-vault`: um alias que identifica AMIs de backup que residem em contas do cofre de backup da AWS logicamente isoladas. Se você usar o atributo de cofre logicamente isolado de backup da AWS, certifique-se de que esse alias esteja incluído como provedor de AMI.
- IDs de Conta da AWS: um ou mais IDs de Conta da AWS de 12 dígitos
- `none`: indica que somente as AMIs criadas pela sua conta podem ser descobertas e usadas. AMIs públicas ou compartilhadas não podem ser descobertas e usadas. Quando especificado, nenhum outro critério pode ser especificado.

`ImageNames`

Os nomes das AMIs permitidas, usando correspondências exatas ou curingas (`?` ou `*`).

`MarketplaceProductCodes`

Os códigos de produto do AWS Marketplace para as AMIs permitidas.

`CreationDateCondition`

A idade máxima das AMIs permitidas.

`DeprecationTimeCondition`

O período máximo desde a obsolescência para as AMIs permitidas.

Para ver os valores e as restrições válidas para cada critério, consulte ImageCriterionRequest na Amazon EC2 API Reference.

Configuração de AMIs permitidas

A configuração básica das AMIs permitidas é a configuração de `ImageCriteria` que define os critérios para as AMIs permitidas. A seguinte estrutura JSON mostra os parâmetros que podem ser especificados:

```
{
    "State": "enabled" | "disabled" | "audit-mode",
    "ImageCriteria" : [
        {
            "ImageProviders": ["string",...],
            "MarketplaceProductCodes": ["string",...],
            "ImageNames":["string",...],
            "CreationDateCondition" : {
                "MaximumDaysSinceCreated": integer
```

```
            },
            "DeprecationTimeCondition" : {
                "MaximumDaysSinceDeprecated": integer
            }
         },
         ...
}
```

Exemplo de ImageCriteria

O exemplo de `ImageCriteria` a seguir configura quatro `ImageCriterion`. Uma AMI será permitida se atender a um desses `ImageCriterion`. Para obter informações sobre como os critérios são avaliados, consulte Como os critérios são avaliados.

```
{
    "ImageCriteria": [
        // ImageCriterion 1: Allow AWS Marketplace AMIs with product code
 "abcdefg1234567890"
        {
            "MarketplaceProductCodes": [
                "abcdefg1234567890"
            ]
        },
        // ImageCriterion 2: Allow AMIs from providers whose accounts are
        // "123456789012" OR "123456789013" AND AMI age is less than 300 days
        {
            "ImageProviders": [
                "123456789012",
                "123456789013"
            ],
            "CreationDateCondition": {
                "MaximumDaysSinceCreated": 300
            }
        },
        // ImageCriterion 3: Allow AMIs from provider whose account is "123456789014"
        // AND with names following the pattern "golden-ami-*"
        {
            "ImageProviders": [
                "123456789014"
            ],
            "ImageNames": [
                "golden-ami-*"
            ]
```

```
        },
        // ImageCriterion 4: Allow AMIs from Amazon or verified providers
        // AND which aren't deprecated
        {
            "ImageProviders": [
                "amazon"
            ],
            "DeprecationTimeCondition": {
                "MaximumDaysSinceDeprecated": 0
            }
        }
    ]
}
```

Como os critérios são avaliados

A seguinte tabela explica as regras de avaliação que determinam se uma AMI é permitida, mostrando como o operador AND ou OR é aplicado em cada nível:

Nível de avaliação	Operador	Requisito para ser uma AMI permitida
Valores de parâmetros para `ImageProviders` , `ImageNames` e `MarketplaceProductCodes`	OR	A AMI deve atender a pelo menos um valor de cada lista de parâmetros
`ImageCriterion`	AND	A AMI deve atender a todos os parâmetros de cada `ImageCriterion`
`ImageCriteria`	OR	A AMI deve atender a um dos `ImageCriterion`

Usando as regras de avaliação anteriores, vamos ver como aplicá-las ao Exemplo de ImageCriteria:

- `ImageCriterion` 1: permite AMIs que tenham o código de produto de AWS Marketplace `abcdefg1234567890`

  OR

- `ImageCriterion` 2: permite AMIs que atendam a estes dois critérios:
  - Pertencente à conta `123456789012` `OR` `123456789013`
    - `AND`
  - Criada nos últimos 300 dias

  `OR`
- `ImageCriterion` 3: permite AMIs que atendam a estes dois critérios:
  - Pertencente à conta `123456789014`
    - `AND`
  - Nomeada com o padrão `golden-ami-*`

  `OR`
- `ImageCriterion` 4: permite AMIs que atendam a estes dois critérios:
  - Publicada pela Amazon ou por fornecedores verificados (especificado pelo alias `amazon`)
    - `AND`
  - Não obsoletas (o número máximo de dias desde a obsolescência é `0`)

Limites

O `ImageCriteria` podem incluir até:

- 10 `ImageCriterion`

Cada `ImageCriterion` pode incluir até:

- 200 valores para `ImageProviders`
- 50 valores para `ImageNames`
- 50 valores para `MarketplaceProductCodes`

Exemplo de limites

Usando o Exemplo de ImageCriteria anterior:

- Existem 4 `ImageCriterion`. Podem ser adicionados até 6 à solicitação para atingir o limite de 10.

- No primeiro `ImageCriterion`, há 1 valor para `MarketplaceProductCodes`. Podem ser adicionados até 49 a esse `ImageCriterion` para atingir o limite de 50.
- No segundo `ImageCriterion`, há 2 valores para `ImageProviders`. Podem ser adicionados até 198 a esse `ImageCriterion` para atingir o limite de 200.
- No terceiro `ImageCriterion`, há 1 valor para `ImageNames`. Podem ser adicionados até 49 a esse `ImageCriterion` para atingir o limite de 50.

Operações de AMIs permitidas

O atributo AMIs permitidas tem três estados operacionais para gerenciamento dos critérios de imagem: habilitado, desabilitado e modo de auditoria. Esses modos permitem que você habilite ou desabilite os critérios de imagem, ou os revise conforme necessário.

Habilitado

Quando as AMIs permitidas estão habilitadas:

- Os `ImageCriteria` são aplicados.
- Somente as AMIs permitidas podem ser descobertas no console do EC2 e por APIs que usam imagens (por exemplo, que descrevem, copiam, armazenam ou executam outras ações que usam imagens).
- As instâncias só podem ser iniciadas usando AMIs permitidas.

Desabilitado

Quando as AMIs permitidas estão desabilitadas:

- As `ImageCriteria` não são aplicadas.
- Nenhuma restrição é imposta à descoberta ou ao uso da AMI.

Modo de auditoria

No modo de auditoria:

- Os `ImageCriteria` são aplicados, mas nenhuma restrição é imposta à descoberta ou ao uso da AMI.

- No console do EC2, para cada AMI, o campo Imagem permitida exibe Sim ou Não para indicar se a AMI será detectável e estará disponível para os usuários na conta quando AMIs permitidas estiver habilitado.
- Na linha de comando, a resposta para a operação `describe-image` inclui `"ImageAllowed": true` ou `"ImageAllowed": false` para indicar se a AMI será detectável e estará disponível para os usuários na conta quando AMIs permitidas estiver habilitado.
- No console do EC2, o Catálogo de AMIs exibirá Não permitido ao lado de AMIs que não serão detectáveis ou estarão disponíveis para os usuários na conta quando AMIs permitidas estiver habilitado.

Práticas recomendadas para a implementação de AMIs permitidas

Ao implementar AMIs permitidas, considere estas práticas recomendadas para garantir uma transição tranquila e minimizar possíveis interrupções em seu ambiente da AWS.

1. Habilitar o modo de auditoria

   Comece ativando AMIs permitidas no modo de auditoria. Esse estado permite que você veja quais são as AMIs que seriam afetadas por seus critérios sem realmente restringir o acesso, fornecendo um período de avaliação sem riscos.

2. Definir critérios de AMIs permitidas

   Estabeleça cuidadosamente quais provedores de AMI estão alinhados com as políticas de segurança, os requisitos de conformidade e as necessidades operacionais da sua organização.

   > **Note**
   >
   > Ao usar serviços gerenciados da AWS, como Amazon ECS ou o Amazon EKS ou as instâncias gerenciadas do AWS Lambda, recomendamos especificar o alias da `amazon` para permitir as AMIs criadas pela AWS. Esses serviços dependem das AMIs publicadas pela Amazon para iniciar instâncias.
   > Tenha cuidado ao definir restrições de `CreationDateCondition` para as AMIs. Definir condições de data excessivamente restritivas (por exemplo, as AMIs devem ter menos de 5 dias) pode causar falhas na inicialização da instância se as AMIs da AWS ou de outros provedores não forem atualizadas dentro do prazo especificado.

Recomendamos emparelhar `ImageNames` com `ImageProviders` para ter mais controle e especificidade. O uso de `ImageNames` sozinho pode não identificar exclusivamente uma AMI.

3. Verificar o impacto nos processos de negócios esperados

   É possível usar o console ou a CLI para identificar instâncias que foram iniciadas com AMIs e que não atendem aos critérios especificados. Essas informações podem orientar sua decisão de atualizar suas configurações de inicialização para usar AMIs em conformidade (por exemplo, especificar uma AMI diferente em um modelo de inicialização) ou ajustar seus critérios para permitir essas AMIs.

   Console: use a regra ec2-instance-launched-with-allowed-ami do AWS Config para verificar se as instâncias em execução ou paradas foram iniciadas com AMIs que atendem aos seus critérios de AMIs permitidas. A regra é NON_COMPLIANT quando uma AMI não atende aos critérios de AMIs permitidas e COMPLIANT quando atende. A regra apenas funciona quando a configuração de AMIs permitidas está definida como habilitada ou modo de auditoria.

   CLI: execute o comando describe-instance-image-metadata e filtre a resposta para identificar quaisquer instâncias que foram iniciadas com AMIs que não atendem aos critérios especificados.

   Para obter instruções sobre o console e a CLI, consulte Encontrar instâncias inicializadas de AMIs que não são permitidas.

4. Habilitar AMIs permitidas

   Depois de confirmar que os critérios não afetarão de forma adversa os processos de negócios esperados, habilite AMIs permitidas.

5. Monitorar as execuções de instâncias

   Continue monitorando as execuções de instâncias a partir de AMIs em ssuas aplicações e nos serviços da AWS gerenciados que você usa, como o Amazon EMR, Amazon ECR, Amazon EKS e AWS Elastic Beanstalk. Verifique se há problemas inesperados e faça os ajustes necessários nos critérios de AMIs permitidas.

6. Testar novas AMIs

   Para testar AMIs de terceiros que não estejam em conformidade com suas configurações atuais de AMIs permitidas, a AWS recomenda as abordagens a seguir:

- Use uma Conta da AWS separada: crie uma conta sem acesso aos recursos essenciais para os seus negócios. Garanta que a configuração de AMIs permitidas não esteja habilitada nessa conta ou que as AMIs que você deseja testar sejam explicitamente permitidas, para que você possa testá-las.
- Teste em outra Região da AWS: use uma região em que as AMIs de terceiros estejam disponíveis, mas em que você ainda não tenha habilitado as configurações de AMIs permitidas.

Essas abordagens ajudam a garantir que seus recursos essenciais para os negócios permaneçam seguros durante o teste de novas AMIs.

Permissões obrigatórias do IAM

Para usar o atributo de AMIs permitidas, você precisa das seguintes permissões do IAM:

- `GetAllowedImagesSettings`
- `EnableAllowedImagesSettings`
- `DisableAllowedImagesSettings`
- `ReplaceImageCriteriaInAllowedImagesSettings`

Gerenciar as configurações de AMIs permitidas

É possível gerenciar as configurações de AMIs permitidas. Essas configurações são por região, por conta.

Tarefas

- Habilitar AMIs permitidas
- Definir os critérios de AMIs permitidas
- Desabilitar AMIs permitidas
- Obter os critérios de AMIs permitidas
- Localizar AMIs que são permitidas
- Encontrar instâncias inicializadas de AMIs que não são permitidas

Habilitar AMIs permitidas

É possível habilitar AMIs permitidas e especificar critérios para AMIs permitidas. Recomendamos que você comece no modo de auditoria, que mostra quais AMIs seriam afetadas pelos critérios sem realmente restringir o acesso.

Console

Para habilitar AMIs permitidas

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Painel.
3. Em Atributos da conta (canto superior direito), escolha AMIs permitidas.
4. Na guia AMIs permitidas, escolha Gerenciar.
5. Em Configurações de AMIs permitidas, escolha Modo de auditoria ou Habilitado. Recomendamos que você comece no modo de auditoria, teste os critérios e retorne a essa etapa para habilitar as AMIs permitidas.
6. (Opcional) Em Critérios de AMI, verifique os critérios no formato JSON.
7. Selecione Atualizar.

AWS CLI

Para habilitar AMIs permitidas

Use o comando enable-allowed-images-settings.

```
aws ec2 enable-allowed-images-settings --allowed-images-settings-state enabled
```

Para habilitar o modo de auditoria em vez disso, especifique `audit-mode` em vez de `enabled`.

```
aws ec2 enable-allowed-images-settings --allowed-images-settings-state audit-mode
```

PowerShell

Para habilitar AMIs permitidas

Use o cmdlet Enable-EC2AllowedImagesSetting.

```
Enable-EC2AllowedImagesSetting -AllowedImagesSettingsState enabled
```

Para habilitar o modo de auditoria em vez disso, especifique `audit-mode` em vez de `enabled`.

```
Enable-EC2AllowedImagesSetting -AllowedImagesSettingsState audit-mode
```

Definir os critérios de AMIs permitidas

Depois de habilitar as AMIs permitidas, será possível definir ou substituir os critérios de AMIs permitidas.

Para obter a configuração correta e valores válidos, consulte Configuração de AMIs permitidas e Parâmetros de AMIs permitidas.

Console

Para definir os critérios de AMIs permitidas

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Painel.
3. Em Atributos da conta (canto superior direito), escolha AMIs permitidas.
4. Na guia AMIs permitidas, escolha Gerenciar.
5. Em Critérios de AMI, verifique os critérios no formato JSON.
6. Selecione Atualizar.

AWS CLI

Para definir os critérios de AMIs permitidas

Use o comando replace-image-criteria-in-allowed-images-settings e especifique o arquivo JSON que contém os critérios para AMIs permitidas.

```
aws ec2 replace-image-criteria-in-allowed-images-settings --cli-input-json
 file://file_name.json
```

PowerShell

Para definir os critérios de AMIs permitidas

Use o cmdlet Set-EC2ImageCriteriaInAllowedImagesSetting e especifique o arquivo JSON que contém os critérios para AMIs permitidas.

```
$imageCriteria = Get-Content -Path .\file_name.json | ConvertFrom-Json
Set-EC2ImageCriteriaInAllowedImagesSetting -ImageCriterion $imageCriteria
```

Desabilitar AMIs permitidas

É possível desabilitar as AMIs permitidas da seguinte maneira.

Console

Para desabilitar AMIs permitidas

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Painel.
3. Em Atributos da conta (canto superior direito), escolha AMIs permitidas.
4. Na guia AMIs permitidas, escolha Gerenciar.
5. Em Configurações de AMIs permitidas, escolha Desabilitado.
6. Selecione Atualizar.

AWS CLI

Para desabilitar AMIs permitidas

Use o comando disable-allowed-images-settings.

```
aws ec2 disable-allowed-images-settings
```

PowerShell

Para desabilitar AMIs permitidas

Use o cmdlet Disable-EC2AllowedImagesSetting.

```
Disable-EC2AllowedImagesSetting
```

Obter os critérios de AMIs permitidas

É possível obter o estado atual da configuração de AMIs permitidas e os critérios de AMIs permitidas.

Console

Para obter o estado e os critérios das AMIs permitidas

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Painel.
3. Em Atributos da conta (canto superior direito), escolha AMIs permitidas.
4. Na guia AMIs permitidas, as Configurações de AMIs permitidas estarão definidas como Habilitado, Desabilitado ou Modo de auditoria.
5. Se o estado das AMIs permitidas for Habilitado ou Modo de auditoria, os Critérios da AMI exibirão os critérios da AMI no formato JSON.

AWS CLI

Para obter o estado e os critérios das AMIs permitidas

Use o comando get-allowed-images-settings.

```
aws ec2 get-allowed-images-settings
```

Na exemplo de saída a seguir, o estado é `audit-mode` e os critérios de imagem são definidos na conta.

```
{
    "State": "audit-mode",
    "ImageCriteria": [
        {
            "MarketplaceProductCodes": [
                "abcdefg1234567890"
            ]
        },
        {
            "ImageProviders": [
                "123456789012",
                "123456789013"
            ],
            "CreationDateCondition": {
                "MaximumDaysSinceCreated": 300
            }
        },
```

```
        {
            "ImageProviders": [
                "123456789014"
            ],
            "ImageNames": [
                "golden-ami-*"
            ]
        },
        {
            "ImageProviders": [
                "amazon"
            ],
            "DeprecationTimeCondition": {
                "MaximumDaysSinceDeprecated": 0
            }
        }
    ],
    "ManagedBy": "account"
}
```

PowerShell

Para obter o estado e os critérios das AMIs permitidas

Use o cmdlet Get-EC2AllowedImagesSetting.

```
Get-EC2AllowedImagesSetting | Select-Object `
    State, `
    ManagedBy, `
    @{Name='ImageProviders'; Expression={($_.ImageCriteria.ImageProviders)}}, `
    @{Name='MarketplaceProductCodes';
 Expression={($_.ImageCriteria.MarketplaceProductCodes)}}, `
    @{Name='ImageNames'; Expression={($_.ImageCriteria.ImageNames)}}, `
    @{Name='MaximumDaysSinceCreated';
 Expression={($_.ImageCriteria.CreationDateCondition.MaximumDaysSinceCreated)}}, `
    @{Name='MaximumDaysSinceDeprecated';
 Expression={($_.ImageCriteria.DeprecationTimeCondition.MaximumDaysSinceDeprecated)}}
```

Na exemplo de saída a seguir, o estado é `audit-mode` e os critérios de imagem são definidos na conta.

```
State      : audit-mode
ManagedBy  : account
```

```
ImageProviders            : {123456789012, 123456789013, 123456789014, amazon}
MarketplaceProductCodes   : {abcdefg1234567890}
ImageNames                : {golden-ami-*}
MaximumDaysSinceCreated   : 300
MaximumDaysSinceDeprecated: 0
```

Localizar AMIs que são permitidas

É possível encontrar as AMIs que são permitidas ou não são permitidas pelos critérios atuais de AMIs permitidas.

> **Note**
>
> As AMIs permitidas precisam estar no modo de auditoria.

Console

Para identificar se uma AMI atende aos critérios de AMIs permitidas

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione AMIs.
3. Selecione a AMI.
4. Na guia Detalhes (se você marcou a caixa de seleção) ou na área de resumo (se você selecionou o ID da AMI), encontre o campo Imagem permitida.
   - Sim: a AMI atende aos critérios de AMIs permitidas. Essa AMI estará disponível para os usuários em sua conta depois que você habilitar as AMIs permitidas.
   - Não: a AMI não atende aos critérios de AMIs permitidas.
5. No painel de navegação, escolha AMI Catalog (Catálogo de AMIs).

   Uma AMI marcada como Não permitida indica uma AMI que não atende aos critérios de AMIs permitidas. Essa AMI não estará visível ou disponível para os usuários em sua conta quando as AMIs permitidas estiverem habilitadas.

AWS CLI

Para identificar se uma AMI atende aos critérios de AMIs permitidas

Use o comando describe-images.

```
aws ec2 describe-images \
    --image-id ami-0abcdef1234567890 \
    --query Images[].ImageAllowed \
    --output text
```

O seguinte é um exemplo de saída.

```
True
```

Para encontrar AMIs que atendam aos critérios de AMIs permitidas

Use o comando describe-images.

```
aws ec2 describe-images \
    --filters "Name=image-allowed,Values=true" \
    --max-items 10 \
    --query Images[].ImageId
```

O seguinte é um exemplo de saída.

```
ami-000eaaa8be2fd162a
ami-000f82db25e50de8e
ami-000fc21eb34c7a9a6
ami-0010b876f1287d7be
ami-0010b929226fe8eba
ami-0010957836340aead
ami-00112c992a47ba871
ami-00111759e194abcc1
ami-001112565ffcafa5e
ami-0011e45aaee9fba88
```

PowerShell

Para identificar se uma AMI atende aos critérios de AMIs permitidas

Use o cmdlet Get-EC2Image.

```
(Get-EC2Image -ImageId ami-0abcdef1234567890).ImageAllowed
```

O seguinte é um exemplo de saída.

```
True
```

Para encontrar AMIs que atendam aos critérios de AMIs permitidas

Use o cmdlet Get-EC2Image.

```
Get-EC2Image `
    -Filter @{Name="image-allows";Values="true"} `
    -MaxResult 10 | `
    Select ImageId
```

O seguinte é um exemplo de saída.

```
ami-000eaaa8be2fd162a
ami-000f82db25e50de8e
ami-000fc21eb34c7a9a6
ami-0010b876f1287d7be
ami-0010b929226fe8eba
ami-0010957836340aead
ami-00112c992a47ba871
ami-00111759e194abcc1
ami-001112565ffcafa5e
ami-0011e45aaee9fba88
```

Encontrar instâncias inicializadas de AMIs que não são permitidas

É possível identificar as instâncias que foram iniciadas com uma AMI que não atende aos critérios de AMIs permitidas.

Console

Para verificar se uma instância foi iniciada usando uma AMI que não é permitida

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 Detalhes, em Detalhes da instância, encontre Imagem permitida.

- Sim: a AMI atende aos critérios de AMIs permitidas.
- Não: a AMI não atende aos critérios de AMIs permitidas.

AWS CLI

Para encontrar instâncias inicializadas usando AMIs que não são permitidas

Use o comando describe-instance-image-metadata com o filtro `image-allowed`.

```
aws ec2 describe-instance-image-metadata \
    --filters "Name=image-allowed,Values=false" \
    --query "InstanceImageMetadata[*].[InstanceId,ImageMetadata.ImageId]" \
    --output table
```

O seguinte é um exemplo de saída.

```
-------------------------------------------------
|          DescribeInstanceImageMetadata         |
+----------------------+-------------------------+
|  i-08fd74f3f1595fdbd |  ami-09245d5773578a1d6  |
|  i-0b1bf24fd4f297ab9 |  ami-07cccf2bd80ed467f  |
|  i-026a2eb590b4f7234 |  ami-0c0ec0a3a3a4c34c0  |
|  i-006a6a4e8870c828f |  ami-0a70b9d193ae8a799  |
|  i-0781e91cfeca3179d |  ami-00c257e12d6828491  |
|  i-02b631e2a6ae7c2d9 |  ami-0bfddf4206f1fa7b9  |
+----------------------+-------------------------+
```

PowerShell

Para encontrar instâncias inicializadas usando AMIs que não são permitidas

Use o cmdlet Get-EC2InstanceImageMetadata.

```
Get-EC2InstanceImageMetadata `
    -Filter @{Name="image-allowed";Values="false"} | `
    Select InstanceId, @{Name='ImageId'; Expression={($_.ImageMetadata.ImageId)}}
```

O seguinte é um exemplo de saída.

```
InstanceId          ImageId
```

```
----------          -------
i-08fd74f3f1595fdbd ami-09245d5773578a1d6
i-0b1bf24fd4f297ab9 ami-07cccf2bd80ed467f
i-026a2eb590b4f7234 ami-0c0ec0a3a3a4c34c0
i-006a6a4e8870c828f ami-0a70b9d193ae8a799
i-0781e91cfeca3179d ami-00c257e12d6828491
i-02b631e2a6ae7c2d9 ami-0bfddf4206f1fa7b9
```

AWS Config

É possível adicionar a regra ec2-instance-launched-with-allowed-ami do AWS Config, configurá-la de acordo com seus requisitos e usá-la para avaliar suas instâncias.

Para obter mais informações, consulte Adicionar regras do AWS Config e ec2-instance-launched-with-allowed-ami no Guia do desenvolvedor do AWS Config.

Disponibilizar publicamente sua AMI para uso no Amazon EC2

É possível tornar sua AMI disponível publicamente compartilhando-a com todos os Contas da AWS.

Se você quiser impedir o compartilhamento público de suas AMIs, você pode habilitar o bloqueio de acesso público para AMIs. Isso bloqueia qualquer tentativa de tornar uma AMI pública, ajudando a evitar acesso não autorizado e possível uso indevido dos dados da AMI. Observe que habilitar o bloqueio de acesso público não afeta as AMIs que já estão publicamente disponíveis; elas permanecem publicamente acessíveis. Para obter mais informações, consulte Saiba mais sobre o bloqueio de acesso público para AMIs.

Para permitir que apenas contas específicas usem sua AMI para iniciar instâncias, consulte Compartilhar uma AMI com contas específicas da AWS.

Conteúdo

- Considerações
- Compartilhe uma AMI com todas as AWS contas (compartilhe publicamente)

Considerações

Considere as informações a seguir antes de tornar uma AMI pública.

- Propriedade: para tornar uma AMI pública, sua Conta da AWS deve ser proprietária da AMI.

- Region: as AMIs são um recurso regional. Quando você compartilha uma AMI, ela só está disponível na região de onde foi 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 do Amazon EC2.
- Bloquear o acesso público — Para compartilhar publicamente uma AMI, o bloqueio do acesso público para AMIs deve ser desativado em cada região na qual a AMI será compartilhada publicamente. Depois de compartilhar publicamente a AMI, você pode reativar o bloqueio do acesso público para AMIs para evitar mais compartilhamentos públicos de suas AMIs.
- Algumas AMIs não podem ser tornadas públicas: se sua AMI tiver um dos seguintes componentes, você não poderá torná-la pública (mas poderá compartilhar a AMI com Contas da AWS específicas):
  - Volumes criptografados
  - Snapshots de volumes criptografados
  - Códigos do produto
- Evite a exposição de dados confidenciais: para evitar expor dados confidenciais ao compartilhar uma AMI, leia as considerações de segurança em Recomendações para criar AMIs compartilhadas no Linux e siga as ações recomendadas.
- Uso: quando você compartilha uma AMI, os usuários podem apenas iniciar instâncias pela AMI. Eles não podem excluí-la, compartilhá-la nem modificá-la. Porém, após iniciarem uma instância usando sua AMI, poderão criar uma AMI com base na instância que iniciaram.
- Descontinuação automática: por padrão, a data de descontinuação de todas as AMIs públicas é definida como dois anos após a data de criação da AMI. É possível definir a data de descontinuação para antes de dois anos. Para cancelar a data de descontinuação ou adiá-la para uma data posterior, você deve tornar a AMI privada compartilhando-a somente com Contas da AWS específicas.
- Remoção de AMIs obsoletas: depois que uma AMI pública atinge a data de descontinuação, se novas instâncias não forem iniciadas usando a AMI por seis meses ou mais, a AWS eventualmente remove a propriedade de compartilhamento público para que as AMIs obsoletas não apareçam nas listas de AMI públicas.
- Faturamento: você não é cobrado quando sua AMI é usada por outras Contas da AWS para executar instâncias. As contas que iniciam instâncias usando a AMI são cobradas pelas instâncias que iniciam.

Compartilhe uma AMI com todas as AWS contas (compartilhe publicamente)

Depois de tornar uma AMI pública, ela fica disponível nas AMIs da comunidade no console, que você pode acessar no catálogo da AMI no navegador esquerdo do console do EC2 ou ao iniciar uma instância usando o console. Observe que pode demorar um pouco para a AMI aparecer em AMIs da comunidade depois de você torná-la pública.

Console

Para tornar um AMI pública

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione AMIs.
3. Selecione a AMI na lista e escolha Actions (Ações), Edit AMI permissions (Editar permissões de AMI).
4. Em AMI availability (Disponibilidade da AMI), escolha Public (Pública).
5. Escolha Salvar alterações.

AWS CLI

Cada AMI tem uma propriedade `launchPermission` que controla quais Contas da AWS, além do proprietário, têm permissão para usar essa AMI para executar instâncias. Ao modificar a propriedade `launchPermission` da AMI, é possível 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 você especificar.

É possível 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`. É possível especificar permissões públicas e permissões de execução explícita.

Para tornar um AMI pública

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

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

2. Para verificar as permissões de execução da AMI, use o comando describe-image-attribute.

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

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

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

PowerShell

Cada AMI tem uma propriedade `launchPermission` que controla quais Contas da AWS, além do proprietário, têm permissão para usar essa AMI para executar instâncias. Ao modificar a propriedade `launchPermission` da AMI, é possível 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 você especificar.

É possível 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`. É possível especificar permissões públicas e permissões de execução explícita.

Para tornar um AMI pública

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

```
Edit-EC2ImageAttribute `
    -ImageId ami-0abcdef1234567890 `
    -Attribute launchPermission `
    -OperationType add `
    -UserGroup all
```

2. Para verificar as permissões de execução da AMI, use o seguinte comando Get-EC2ImageAttribute.

```
Get-EC2ImageAttribute `
    -ImageId ami-0abcdef1234567890 `
    -Attribute launchPermission
```

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

```
Edit-EC2ImageAttribute `
    -ImageId ami-0abcdef1234567890 `
    -Attribute launchPermission `
    -OperationType remove `
    -UserGroup all
```

Saiba mais sobre o bloqueio de acesso público para AMIs

Para evitar o compartilhamento público de suas AMIs, habilite o bloqueio de acesso público para AMIs no nível da conta.

Quando o bloqueio de acesso público está habilitado, qualquer tentativa de tornar uma AMI pública é automaticamente bloqueada. Entretanto, se você já tiver AMIs públicas, elas permanecerão disponíveis publicamente.

Para compartilhar AMIs publicamente, é necessário desabilitar o bloqueio de acesso público. Quando você terminar de compartilhar, é uma prática recomendada reabilitar o bloqueio de acesso público para evitar qualquer compartilhamento público não intencional das suas AMIs.

> **Note**
>
> Essa configuração é definida no nível da conta, diretamente na conta ou usando uma política declarativa. Ela deve ser configurada em cada Região da AWS onde você desejar impedir o compartilhamento público de suas AMIs. O uso de uma política declarativa permite que você aplique a configuração em várias regiões simultaneamente, bem como em várias contas simultaneamente. Quando uma política declarativa está em uso, você não pode modificar a configuração diretamente em uma conta. Este tópico descreve como ajustar a configuração diretamente em uma conta. Para obter informações sobre o uso de políticas declarativas, consulte Políticas declarativas no Guia do usuário do AWS Organizations.

É possível restringir as permissões do IAM a um usuário administrador para que apenas essa pessoa possa habilitar ou desabilitar o bloqueio de acesso público para AMIs.

Tópicos

- Configurações padrão
- Gerenciar a configuração do bloqueio de acesso público para AMIs

Configurações padrão

A configuração Bloquear acesso público para AMIs está habilitada ou desabilitada por padrão, dependendo se sua conta for nova ou existente e se você tem AMIs públicas. A tabela abaixo mostra as configurações padrão:

Conta da AWS	Configuração padrão de bloquear acesso público para AMIs
Novas contas	Habilitado
Contas existentes sem AMIs públicas[1]	Habilitado
Contas existentes com um ou mais AMIs públicas	Desabilitado

[1] Se sua conta tinha uma ou mais AMIs públicas em ou após 15 de julho de 2023, a opção Bloquear acesso público para AMIs estará desabilitada por padrão, mesmo que você tenha posteriormente tornado todas as AMIs privadas.

Gerenciar a configuração do bloqueio de acesso público para AMIs

É possível gerenciar a configuração de bloqueio de acesso público para suas AMIs para controlar se elas podem ser compartilhadas publicamente. É possível habilitar, desabilitar ou exibir o estado atual do bloqueio de acesso público para suas AMIs usando o console do Amazon EC2 ou a AWS CLI.

Veja o estado do bloqueio de acesso público para AMIs

Para ver se o compartilhamento público de suas AMIs está bloqueado em sua conta, você pode ver o estado do bloqueio de acesso público para AMIs. Você deve visualizar o estado em cada um Região da AWS no qual deseja ver se o compartilhamento público de suas AMIs está bloqueado.

Permissões obrigatórias

Para obter a configuração atual do bloqueio de acesso público para AMIs, você deve ter a permissão `GetImageBlockPublicAccessState` do IAM.

Console

Para visualizar o estado do bloqueio de acesso público para AMIs na região especificada

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 na qual deseja visualizar o estado de bloqueio de acesso público para AMIs.
3. Se o painel não for exibido, no painel de navegação, escolha EC2 Dashboard (Painel EC2).
4. Em Account attributes (Atributos da conta), escolha Data orotection and security (Proteção e segurança de dados).
5. Em Block public access for AMIs (Bloquear acesso público para AMIs), marque o campo Public access (Acesso público). O valor é New public sharing blocked (Novo compartilhamento público bloqueado) ou New public sharing allowed (Novo compartilhamento público permitido).

AWS CLI

Para obter o estado do bloqueio de acesso público para as AMIs

Use o comando get-image-block-public-access-state. O valor é `block-new-sharing` ou `unblocked`.

Exemplo: para uma região específica

```
aws ec2 get-image-block-public-access-state --region us-east-1
```

O campo `ManagedBy` indica a entidade que definiu a configuração. Neste exemplo, `account` indica que a configuração foi definida diretamente na conta. Um valor de `declarative-`

`policy` significaria que a configuração foi definida por uma política declarativa. Para obter mais informações, consulte Políticas declarativas no Guia do Usuário do AWS Organizations.

```
{
    "ImageBlockPublicAccessState": "block-new-sharing",
    "ManagedBy": "account"
}
```

Exemplo: para todas as regiões em sua conta

```
echo -e "Region   \t Public Access State" ; \
echo -e "-------------- \t ----------------------" ; \
for region in $(
    aws ec2 describe-regions \
        --region us-east-1 \
        --query "Regions[*].[RegionName]" \
        --output text
    );
    do (output=$(
        aws ec2 get-image-block-public-access-state \
            --region $region \
            --output text)
        echo -e "$region \t $output"
    );
done
```

O seguinte é um exemplo de saída.

```
Region           Public Access State
--------------   ----------------------
ap-south-1       block-new-sharing
eu-north-1       unblocked
eu-west-3        block-new-sharing
...
```

PowerShell

Para obter o estado do bloqueio de acesso público para as AMIs

Use o cmdlet Get-EC2ImageBlockPublicAccessState. O valor é `block-new-sharing` ou `unblocked`.

Exemplo: para uma região específica

```
Get-EC2ImageBlockPublicAccessState -Region us-east-1
```

O seguinte é um exemplo de saída.

```
block-new-sharing
```

Exemplo: para todas as regiões em sua conta

```
(Get-EC2Region).RegionName | `
    ForEach-Object {
        [PSCustomObject]@{
            Region   = $_
            PublicAccessState = (Get-EC2ImageBlockPublicAccessState -Region $_)
        }
} | `
Format-Table -AutoSize
```

O seguinte é um exemplo de saída.

```
Region         PublicAccessState
------         -----------------
ap-south-1     block-new-sharing
eu-north-1     block-new-sharing
eu-west-3      block-new-sharing
...
```

Habilite o bloqueio de acesso público para AMIs

Para evitar o compartilhamento público de suas AMIs, habilite o bloqueio de acesso público para AMIs no nível da conta. Você deve habilitar o bloqueio de acesso público para AMIs em cada Região da AWS na qual deseja evitar o compartilhamento público das suas AMIs. Se você já tiver AMIs públicas, elas permanecerão disponíveis publicamente.

Permissões obrigatórias

Para habilitar a configuração atual do bloqueio de acesso público para AMIs, você deve ter a permissão `EnableImageBlockPublicAccess` do IAM.

Considerações

- A configuração dessa opção poderá demorar até 10 minutos. Durante esse período, se você descrever o estado de acesso público, a resposta será `unblocked`. Quando a configuração for concluída, a resposta será `block-new-sharing`.

Console

Para habilitar o bloqueio de acesso público para AMIs na região especificada

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 na qual deseja executar o bloqueio de acesso público para as AMIs.
3. Se o painel não for exibido, no painel de navegação, escolha EC2 Dashboard (Painel EC2).
4. Em Account attributes (Atributos da conta), escolha Data orotection and security (Proteção e segurança de dados).
5. Em Block public access for AMIs (Bloquear acesso público para AMIs), escolha Manage (Gerenciar).
6. Marque a caixa de seleção Bloquear novos compartilhamentos públicos e escolha Atualizar.

AWS CLI

Para habilitar o bloqueio de acesso público para as AMIs

Use o comando enable-image-block-public-access.

Exemplo: para uma região específica

```
aws ec2 enable-image-block-public-access \
--region us-east-1 \
--image-block-public-access-state block-new-sharing
```

O seguinte é um exemplo de saída.

```
{
    "ImageBlockPublicAccessState": "block-new-sharing"
}
```

Exemplo: para todas as regiões em sua conta

```
echo -e "Region   \t Public Access State" ; \
echo -e "-------------- \t ----------------------" ; \
for region in $(
    aws ec2 describe-regions \
        --region us-east-1 \
        --query "Regions[*].[RegionName]" \
        --output text
    );
    do (output=$(
        aws ec2 enable-image-block-public-access \
            --region $region \
            --image-block-public-access-state block-new-sharing \
            --output text)
        echo -e "$region \t $output"
    );
done
```

O seguinte é um exemplo de saída.

```
Region           Public Access State
--------------   ----------------------
ap-south-1       block-new-sharing
eu-north-1       block-new-sharing
eu-west-3        block-new-sharing
...
```

PowerShell

Para habilitar o bloqueio de acesso público para as AMIs

Use o comando Enable-EC2ImageBlockPublicAccess.

Exemplo: para uma região específica

```
Enable-EC2ImageBlockPublicAccess `
    -Region us-east-1 `
    -ImageBlockPublicAccessState block-new-sharing
```

O seguinte é um exemplo de saída.

```
Value
-----
block-new-sharing
```

Exemplo: para todas as regiões em sua conta

```
(Get-EC2Region).RegionName | `
    ForEach-Object {
    [PSCustomObject]@{
        Region            = $_
        PublicAccessState = (
        Enable-EC2ImageBlockPublicAccess `
         -Region $_ `
         -ImageBlockPublicAccessState block-new-sharing)
    }
} | `
Format-Table -AutoSize
```

O seguinte é um exemplo de saída.

```
Region         PublicAccessState
------         -----------------
ap-south-1     block-new-sharing
eu-north-1     block-new-sharing
eu-west-3      block-new-sharing
...
```

Desabilite o bloqueio de acesso público para AMIs

Para permitir que os usuários da sua conta compartilhem publicamente suas AMIs, desative o bloqueio do acesso público no nível da conta. Você deve desabilitar o bloqueio de acesso público para AMIs em cada Região da AWS na qual deseja permitir o compartilhamento público das suas AMIs.

Permissões obrigatórias

Para desabilitar a configuração atual do bloqueio de acesso público para AMIs, você deve ter a permissão `DisableImageBlockPublicAccess` do IAM.

Considerações

- A configuração dessa opção poderá demorar até 10 minutos. Durante esse período, se você descrever o estado de acesso público, a resposta será `block-new-sharing`. Quando a configuração for concluída, a resposta será `unblocked`.

Console

Para desabilitar o bloqueio de acesso público para AMIs na região especificada

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 na qual deseja desabilitar o bloqueio de acesso público para AMIs.
3. Se o painel não for exibido, no painel de navegação, escolha EC2 Dashboard (Painel EC2).
4. Em Account attributes (Atributos da conta), escolha Data orotection and security (Proteção e segurança de dados).
5. Em Block public access for AMIs (Bloquear acesso público para AMIs), escolha Manage (Gerenciar).
6. Desmarque a caixa de seleção Bloquear novos compartilhamentos públicos e escolha Atualizar.
7. Insira **`confirm`** quando solicitado para confirmação e, em seguida, escolha Allow public sharing (Permitir compartilhamento público).

AWS CLI

Para desabilitar o bloqueio de acesso público para as AMIs

Use o comando disable-image-block-public-access.

Exemplo: para uma região específica

```
aws ec2 disable-image-block-public-access --region us-east-1
```

O seguinte é um exemplo de saída.

```
{
   "ImageBlockPublicAccessState": "unblocked"
```

```
}
```

Exemplo: para todas as regiões em sua conta

```
echo -e "Region   \t Public Access State" ; \
echo -e "-------------- \t ----------------------" ; \
for region in $(
    aws ec2 describe-regions \
        --region us-east-1 \
        --query "Regions[*].[RegionName]" \
        --output text
    );
    do (output=$(
        aws ec2 disable-image-block-public-access \
            --region $region \
            --output text)
        echo -e "$region \t $output"
    );
done
```

O seguinte é um exemplo de saída.

```
Region           Public Access State
--------------   ----------------------
ap-south-1       unblocked
eu-north-1       unblocked
eu-west-3        unblocked
...
```

PowerShell

Para desabilitar o bloqueio de acesso público para as AMIs

Use o cmdlet Disable-EC2ImageBlockPublicAccess.

Exemplo: para uma região específica

```
Disable-EC2ImageBlockPublicAccess -Region us-east-1
```

O seguinte é um exemplo de saída.

```
Value
```

```
-----
unblocked
```

Exemplo: para todas as regiões em sua conta

```
(Get-EC2Region).RegionName | `
    ForEach-Object {
    [PSCustomObject]@{
        Region            = $_
        PublicAccessState = (Disable-EC2ImageBlockPublicAccess -Region $_)
    }
} | `
Format-Table -AutoSize
```

O seguinte é um exemplo de saída.

```
Region         PublicAccessState
------         -----------------
ap-south-1     unblocked
eu-north-1     unblocked
eu-west-3      unblocked
...
```

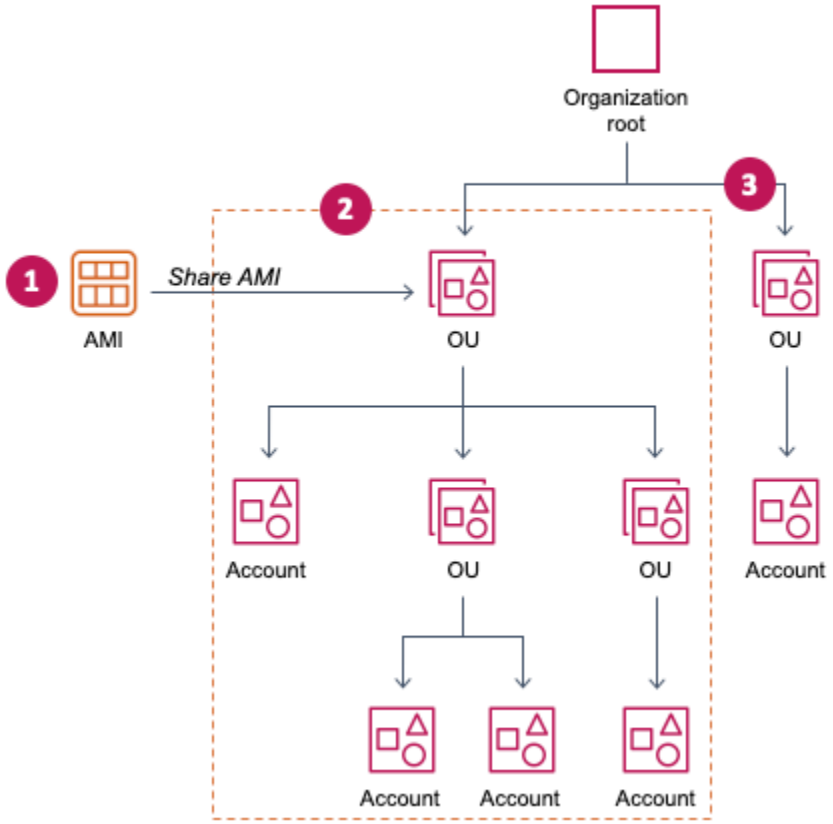
Compartilhar uma AMI com organizações e unidades organizacionais

O AWS Organizations é um serviço de gerenciamento de contas que permite consolidar várias Contas da AWS em uma só organização, que você cria e gerencia centralmente. É possível compartilhar uma AMI com uma organização ou uma unidade organizacional (UO) que você criou, além de compartilhá-la com contas específicas.

Uma organização é uma entidade que você cria para consolidar e gerenciar suas Contas da AWS. É possível organizar as contas em uma estrutura em árvore hierárquica, com uma raiz no alto e unidades organizacionais aninhadas abaixo da raiz. Cada conta pode ser adicionada diretamente na raiz ou ser colocada em uma das UOs na hierarquia. Para obter mais informações, consulte Terminologia e conceitos das organizações da AWS no Guia do usuário do AWS Organizations.

Quando você compartilha uma AMI com uma organização ou uma UO, todas as contas subordinadas ganham acesso à AMI. Por exemplo, no diagrama a seguir, a AMI é compartilhada com uma UO de nível superior (indicada pela seta no número 1). Todas as UOs e contas aninhadas sob essa UO de

nível superior (indicadas pela linha pontilhada no número 2) também têm acesso à AMI. As contas na organização e UO fora da linha pontilhada (indicadas pelo número 3) não têm acesso à AMI porque não são filhas da UO com a qual a AMI é compartilhada.



Tópicos

- Considerações
- Obter o ARN de uma organização ou unidade organizacional
- Permitir que organizações e UOs usem uma chave do KMS
- Gerenciar o compartilhamento de uma AMI com uma organização ou uma UO

Considerações

Considere as informações a seguir ao compartilhar AMIs com organizações ou unidades organizacionais específicas.

- Propriedade: para compartilhar uma AMI, sua Conta da AWS deve ser proprietária da AMI.
- Limites de compartilhamento: o proprietário da AMI pode compartilhar uma AMI com qualquer organização ou UO, incluindo organizações e UOs às quais ele não pertence.

Para saber o número máximo de entidades com as quais uma AMI pode ser compartilhada em uma região, consulte Service Quotas do Amazon EC2.

- Tags: você não pode compartilhar tags definidas pelo usuário (tags que você anexa a uma AMI). Quando você compartilha uma AMI, as tags definidas pelo usuário não estão disponíveis para nenhuma Conta da AWS em uma organização ou UO com a qual a AMI é compartilhada.
- Formato de ARN: ao especificar uma organização ou UO em um comando, verifique se usou o formato de ARN correto. Você receberá um erro se especificar apenas o ID, por exemplo, se você especificar apenas `o-123example` ou `ou-1234-5example`.

  Formatos corretos de ARN:

  - ARN de organização: `arn:aws:organizations::`*`111122223333`*`:organization/`*`organization-id`*
  - ARN de UO: `arn:aws:organizations::`*`111122223333`*`:ou/`*`organization-id`*`/`*`ou-id`*

  Em que:

  - *`111122223333`* é um exemplo do ID de conta de 12 dígitos para a conta gerencial. Se você não souber o número da conta de gerenciamento, poderá descrever a organização ou a unidade organizacional para obter o ARN, que inclui o número da conta de gerenciamento. Para obter mais informações, consulte Obter o ARN de uma organização ou unidade organizacional.
  - *`organization-id`* é o ID da organização, por exemplo, `o-123example`.
  - *`ou-id`* é o ID da unidade organizacional, por exemplo, `ou-1234-5example`.

  Para obter mais informações sobre o formato dos ARNs, consulte Nome do recurso da Amazon (ARN) no Guia do usuário do IAM.
- Criptografia e chaves: é possível compartilhar AMIs que tenham snapshots criptografados e não criptografados.
  - Os snapshots criptografados devem ser criptografados com uma chave gerenciada pelo cliente. Não é possível compartilhar AMIs que tenham snapshots que sejam criptografados com a chave gerenciada pela AWS padrão.
  - Se você compartilhar uma AMI que tenha snapshots criptografados, deverá permitir que as organizações ou UOs usem as chaves gerenciadas pelo cliente que foram usadas para criptografar os snapshots. Para obter mais informações, consulte Permitir que organizações e UOs usem uma chave do KMS.
- Region: as AMIs são um recurso regional. Quando você compartilha uma AMI, ela só está disponível na região de onde foi 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 do Amazon EC2.

- Uso: quando você compartilha uma AMI, os usuários podem apenas iniciar instâncias pela AMI. Eles não podem excluí-la, compartilhá-la nem modificá-la. Porém, após iniciarem uma instância usando sua AMI, poderão criar uma AMI com base na instância que iniciaram.
- Faturamento: você não é cobrado quando sua AMI é usada por outras Contas da AWS para executar instâncias. As contas que iniciam instâncias usando a AMI são cobradas pelas instâncias que iniciam.

Obter o ARN de uma organização ou unidade organizacional

Os ARNs de organizações e de unidades organizacionais contêm o número da conta de gerenciamento de 12 dígitos. Se você não souber o número da conta de gerenciamento, poderá descrever a organização e a unidade organizacional para obter o ARN para cada uma delas. Nos exemplos a seguir, `123456789012` é o ID da conta gerencial.

Permissões obrigatórias

Antes de obter os ARNs, é necessário ter permissão para descrever organizações e unidades organizacionais. O modelo de política a seguir fornece as permissões necessárias.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "organizations:Describe*"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS CLI

Para obter o ARN de uma organização

Use o comando describe-organization. Adicione a opção `--query` para retornar apenas o ARN da organização.

```
aws organizations describe-organization --query 'Organization.Arn'
```

O seguinte é um exemplo de saída.

```
"arn:aws:organizations::123456789012:organization/o-1234567abc"
```

Para obter o ARN de uma unidade organizacional

Use o comando describe-organizational-unit. Use o parâmetro `--query` para retornar apenas o ARN da unidade organizacional.

```
aws organizations describe-organizational-unit \
    --organizational-unit-id ou-a123-b4567890 \
    --query 'OrganizationalUnit.Arn'
```

O seguinte é um exemplo de saída.

```
"arn:aws:organizations::123456789012:ou/o-1234567abc/ou-a123-b4567890"
```

PowerShell

Para obter o ARN de uma organização

Use o cmdlet Get-ORGOrganization.

```
(Get-ORGOrganization).Arn
```

O seguinte é um exemplo de saída.

```
arn:aws:organizations::123456789012:organization/o-1234567abc
```

Para obter o ARN de uma unidade organizacional

Use o cmdlet Get-ORGOrganizationalUnit.

```
(Get-ORGOrganizationalUnit -OrganizationalUnitId "ou-a123-b4567890").Arn
```

O seguinte é um exemplo de saída.

```
arn:aws:organizations::123456789012:ou/o-1234567abc/ou-a123-b4567890
```

Permitir que organizações e UOs usem uma chave do KMS

Se você compartilhar uma AMI que tenha snapshots criptografados, também deverá permitir que as organizações ou unidades organizacionais (UOs) usem as chaves do KMS que foram usadas para criptografar os snapshots.

> **Note**
>
> Os snapshots criptografados devem ser criptografados com uma chave gerenciada pelo cliente. Não é possível compartilhar AMIs que tenham snapshots que sejam criptografados com a chave gerenciada pela AWS padrão.

Para controlar o acesso à chave do KMS, na política de chave, é possível usar as chaves de condição `aws:PrincipalOrgID` e `aws:PrincipalOrgPaths` para conceder permissão somente a determinadas entidades principais para as ações especificadas. Uma entidade principal pode ser um usuário, um perfil do IAM, um usuário federado ou um usuário-raiz da Conta da AWS.

As chaves de condição são usadas da seguinte forma:

- `aws:PrincipalOrgID`: permite qualquer entidade principal pertencente à organização representada pelo ID especificado.
- `aws:PrincipalOrgPaths`: permite qualquer entidade principal pertencente às UOs representadas pelos caminhos especificados.

Para conceder a uma organização (incluindo as UOs e contas que pertençam a ela) permissão para usar uma chave do KMS, adicione a instrução a seguir à política de chave.

```
{
    "Sid": "Allow access for organization root",
    "Effect": "Allow",
    "Principal": "*",
    "Action": [
        "kms:Describe*",
        "kms:List*",
        "kms:Get*",
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:CreateGrant"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:PrincipalOrgID": "o-123example"
        }
    }
}
```

Para dar permissão a UOs específicas (e às contas que pertençam a elas) para usar uma chave do KMS, é possível usar uma política semelhante ao exemplo a seguir.

```
{
        "Sid": "Allow access for specific OUs and their descendants",
        "Effect": "Allow",
        "Principal": "*",
        "Action": [
            "kms:Describe*",
            "kms:List*",
            "kms:Get*",
            "kms:Encrypt",
            "kms:Decrypt",
            "kms:ReEncrypt*",
            "kms:GenerateDataKey*",
            "kms:CreateGrant"
        ],
        "Resource": "*",
        "Condition": {
            "StringEquals": {
                "aws:PrincipalOrgID": "o-123example"
```

```
            },
            "ForAnyValue:StringLike": {
                "aws:PrincipalOrgPaths": [
                    "o-123example/r-ab12/ou-ab12-33333333/*",
                    "o-123example/r-ab12/ou-ab12-22222222/*"
                ]
            }
        }
}
```

Para obter mais exemplos de instruções de condição, consulte aws:PrincipalOrgID e aws:PrincipalOrgPaths no Guia do usuário do IAM.

Para obter mais informações sobre acesso entre contas, consulte Permissão para que usuários de outras contas usem uma chave do KMS no Guia do desenvolvedor do AWS Key Management Service.

Gerenciar o compartilhamento de uma AMI com uma organização ou uma UO

É possível gerenciar o compartilhamento de AMIs com organizações e unidades organizacionais (UO) para controlar se elas podem executar instâncias do Amazon EC2.

Veja as organizações e as UOs com as quais uma AMI é compartilhada

É possível descobrir as organizações e UOs com as quais você compartilhou sua AMI.

Console

Para verificar com quais organizações e UOs você compartilhou sua AMI

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, escolha a guia Permissions (Permissões) e role para baixo até Shared organizations/OUs (Organizações/UOs compartilhadas).

   Para localizar as AMIs que são compartilhadas com você, consulte Encontre AMIs compartilhadas para usar em instâncias do Amazon EC2.

AWS CLI

Para verificar com quais organizações e UOs você compartilhou sua AMI

Use o comando describe-image-attribute com o atributo `launchPermission`.

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

O seguinte é um exemplo de resposta.

```
{
    "ImageId": "ami-0abcdef1234567890",
    "LaunchPermissions": [
        {
            "OrganizationalUnitArn": "arn:aws:organizations::111122223333:ou/
o-123example/ou-1234-5example"
        }
    ]
}
```

PowerShell

Para verificar com quais organizações e UOs você compartilhou sua AMI

Use o cmdlet Get-EC2ImageAttribute.

```
Get-EC2ImageAttribute `
    -ImageId ami-0abcdef1234567890 `
    -Attribute launchPermission
```

Compartilhar uma AMI com uma organização ou uma UO

É possível compartilhar uma AMI com uma organização ou UO

> **Note**
>
> Você não precisa compartilhar os snapshots do Amazon EBS aos quais a AMI faz referência para compartilhar a AMI. Apenas a própria AMI precisa ser compartilhada, e o sistema fornece automaticamente à instância acesso aos snapshots do EBS referenciados para a execução. Mas, você precisa compartilhar todas as chaves do KMS usadas para criptografar os snapshots referenciados pela AMI. Para obter mais informações, consulte Permitir que organizações e UOs usem uma chave do KMS.

Console

Para compartilhar uma AMI com uma organização ou uma UO

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 Actions (Ações), Edit AMI permissions (Editar permissões de AMI).
4. Em AMI availability (Disponibilidade da AMI), escolha Private (Privado).
5. Próximo a Shared organizations/OUs (Organizações/UOs compartilhadas), escolha Add organization/OU ARN (Adicionar ARN de organização/UO).
6. Em Organization/OU ARN (ARN de organização/UO), insira o ARN da organização ou o ARN da UO com o qual você deseja compartilhar a AMI e, em seguida, escolha Share AMI (Compartilhar AMI). Observe que especifique o ARN completo, e não apenas o ID.

   Para compartilhar essa AMI com várias organizações ou UOs, repita essa etapa até adicionar todas as organizações ou UOs necessárias.
7. Após terminar, escolha Save changes (Salvar alterações).
8. (Opcional) Para visualizar as organizações ou UOs com as quais você compartilhou a AMI, selecione a AMI na lista, escolha a guia Permissions (Permissões) e role para baixo até Shared organizations/OUs Organizações/UOs compartilhadas. Para localizar as AMIs que são compartilhadas com você, consulte Encontre AMIs compartilhadas para usar em instâncias do Amazon EC2.

AWS CLI

Para compartilhar uma AMI com uma organização

Use o comando modify-image-attribute para conceder à organização especificada permissões de execução para a AMI especificada.

```
aws ec2 modify-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --launch-permission
 "Add=[{OrganizationArn=arn:aws:organizations::123456789012:organization/
o-123example}]"
```

Para compartilhar uma AMI com uma UO

O comando modify-image-attribute concede permissões de execução para a AMI especificada à UO especificada. Observe que especifique o ARN completo, e não apenas o ID.

```
aws ec2 modify-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --launch-permission
 "Add=[{OrganizationalUnitArn=arn:aws:organizations::123456789012:ou/o-123example/
ou-1234-5example}]"
```

PowerShell

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

Para compartilhar uma AMI com uma organização ou uma UO

O comando a seguir concede permissões de execução para a AMI especificada à organização especificada.

```
Edit-EC2ImageAttribute `
    -ImageId ami-0abcdef1234567890 `
    -Attribute launchPermission `
    -OperationType add `
    -OrganizationArn "arn:aws:organizations::123456789012:organization/o-123example"
```

Para interromper o compartilhamento de uma AMI com uma organização ou uma UO

O comando a seguir remove as permissões de execução para a AMI especificada da organização especificada:

```
Edit-EC2ImageAttribute `
    -ImageId ami-0abcdef1234567890 `
    -Attribute launchPermission `
    -OperationType remove `
    -OrganizationArn "arn:aws:organizations::123456789012:organization/o-123example"
```

Para interromper o compartilhamento de uma AMI com todas as organizações, UOs e Contas da AWS

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.

```
Reset-EC2ImageAttribute `
    -ImageId ami-0abcdef1234567890 `
    -Attribute launchPermission
```

Interromper o compartilhamento de uma AMI com uma organização ou uma UO

É possível interromper o compartilhamento de uma AMI com uma organização ou UO.

> **Note**
>
> Você não pode interromper o compartilhamento de uma AMI com uma conta específica se ela estiver em uma organização ou UO com a qual uma AMI é compartilhada. Se você tentar parar de compartilhar a AMI removendo as permissões de execução da conta, o Amazon EC2 retornará uma mensagem de êxito. Porém, a AMI continua sendo compartilhada com a conta.

Console

Para interromper o compartilhamento de uma AMI com uma organização ou uma UO

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 Actions (Ações), Edit AMI permissions (Editar permissões de AMI).
4. Em Shared organizations/OUs (Organizações/UOs compartilhadas), selecione as organizações ou UOs com as quais você deseja parar de compartilhar a AMI e, em seguida, escolha Remove selected (Remover selecionado).
5. Após terminar, escolha Save changes (Salvar alterações).
6. (Opcional) Para confirmar que você parou de compartilhar a AMI com as organizações ou UOs, selecione a AMI na lista, escolha a guia Permissions (Permissões) e role para baixo até Shared organizations/OUs (Organizações/UOs compartilhadas).

AWS CLI

Para interromper o compartilhamento de uma AMI com uma organização ou uma UO

Use o comando modify-image-attribute. Este exemplo remove da organização especificada as permissões de execução para a AMI especificada.

```
aws ec2 modify-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --launch-permission
 "Remove=[{OrganizationArn=arn:aws:organizations::123456789012:organization/
o-123example}]"
```

Para interromper o compartilhamento de uma AMI com todas as organizações, UOs e Contas da AWS

Use o comando reset-image-attribute. Este exemplo remove todas as permissões de execução explícita e pública da AMI especificada. Observe que o proprietário da AMI sempre tem permissões de execução e, portanto, não é afetado por este comando.

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

PowerShell

Para interromper o compartilhamento de uma AMI com uma organização ou uma UO

Use o cmdlet Edit-EC2ImageAttribute. Este exemplo remove da organização especificada as permissões de execução para a AMI especificada.

```
Edit-EC2ImageAttribute `
    -ImageId ami-0abcdef1234567890 `
    -Attribute launchPermission `
    -OperationType remove `
    -OrganizationArn "arn:aws:organizations::123456789012:organization/o-123example"
```

Para interromper o compartilhamento de uma AMI com todas as organizações, UOs e Contas da AWS

Use o cmdlet Reset-EC2ImageAttribute. Este exemplo 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.

```
Reset-EC2ImageAttribute `
```

```
    -ImageId ami-0abcdef1234567890 `
    -Attribute LaunchPermission
```

Compartilhar uma AMI com contas específicas da AWS

É possível compartilhar uma AMI com Contas da AWS específicas sem torná-la pública. Basta ter os IDs de Conta da AWS.

Um ID de Conta da AWS é um número de 12 dígitos, como `012345678901`, que identifica de forma exclusiva uma Conta da AWS. Para obter mais informações, consulte View Conta da AWS identifiers no AWS Gerenciamento de contas Reference Guide.

Considerações

Considere as informações a seguir ao compartilhar AMIs com Contas da AWS específicas.

- Propriedade: para compartilhar uma AMI, sua Conta da AWS deve ser proprietária da AMI.
- Limites de compartilhamento: para saber o número máximo de entidades com as quais uma AMI pode ser compartilhada em uma região, consulte Service Quotas do Amazon EC2.
- Tags: você não pode compartilhar tags definidas pelo usuário (tags que você anexa a uma AMI). Quando você compartilha uma AMI, suas tags definidas pelo usuário não estão disponíveis para nenhuma Conta da AWS com a qual a AMI é compartilhada.
- Snapshots: não é necessário compartilhar os snapshots do Amazon EBS referenciados por uma AMI para compartilhá-la. É possível compartilhar apenas a própria AMI, e o sistema fornecerá à instância acesso imediato aos snapshots do Amazon EBS referenciados para a inicialização. Porém, você deve compartilhar todas as chaves do KMS usadas para criptografar os snapshots referenciados por uma AMI. Para obter mais informações, consulte Compartilhar um snapshot do Amazon EBS no Guia do usuário do Amazon EBS.
- Criptografia e chaves: é possível compartilhar AMIs que tenham snapshots criptografados e não criptografados.
  - Os snapshots criptografados devem ser criptografados com uma chave do KMS. Não é possível compartilhar AMIs que tenham snapshots que sejam criptografados com a chave gerenciada pela AWS padrão.
  - Se você compartilhar uma AMI que tenha snapshots criptografados, permita que as Contas da AWS usem as chaves do KMS que foram usadas para criptografar os snapshots. Para obter

mais informações, consulte Permitir que organizações e UOs usem uma chave do KMS. Para configurar a política de chave de que você precisa para executar instâncias do Auto Scaling ao usar uma chave gerenciada pelo cliente para criptografia, consulte Política necessária de AWS KMS key para uso com volumes criptografados no Guia do usuário do Amazon EC2 Auto Scaling.

- Region: as AMIs são um recurso regional. Quando você compartilha uma AMI, ela só está disponível naquela região. 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 do Amazon EC2.
- Uso: quando você compartilha uma AMI, os usuários podem apenas iniciar instâncias pela AMI. Eles não podem excluí-la, compartilhá-la nem modificá-la. Porém, após iniciarem uma instância usando a sua AMI, eles podem criar uma AMI a partir da instância deles.
- Cópias de AMIs compartilhadas: se os usuários em outra conta quiserem copiar uma AMI compartilhada, você deverá conceder a eles permissões de leitura para o armazenamento que oferece suporte à AMI. Para obter mais informações, consulte Cópia entre contas.
- Faturamento: você não é cobrado quando sua AMI é usada por outras Contas da AWS para executar instâncias. As contas que iniciam instâncias usando a AMI são cobradas pelas instâncias que iniciam.

Console

Para conceder permissões de execução explícitas

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 Actions (Ações), Edit AMI permissions (Editar permissões de AMI).
4. Selecione Private (Privado).
5. Em Shared accounts (Contas compartilhadas), escolha Add account ID (Adicionar ID de conta).
6. Em Conta da AWS ID (ID da), insira o ID da Conta da AWS com a qual você deseja compartilhar a AMI e, em seguida, escolha Share AMI (Compartilhar AMI).

   Para compartilhar essa AMI com várias contas, repita as Etapas 5 e 6 até adicionar todos os ID de conta necessários.
7. Quando concluir, escolha Salvar alterações.

8. (Opcional) Para visualizar os IDs de Conta da AWS com a qual você compartilhou a AMI, selecione a AMI na lista e escolha a guia Permissions (Permissões). Para localizar as AMIs que são compartilhadas com você, consulte Encontre AMIs compartilhadas para usar em instâncias do Amazon EC2.

AWS CLI

Use o comando modify-image-attribute para compartilhar uma AMI conforme indicado nos exemplos a seguir.

Para conceder permissões de execução explícitas

O exemplo a seguir concede permissões de execução da AMI especificada à Conta da AWS especificada.

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

Para remover as permissões de execução de uma conta

O exemplo a seguir remove permissões de execução da AMI especificada da Conta da AWS especificada.

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

Para remover todas as permissões de execução

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

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

PowerShell

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

Para conceder permissões de execução explícitas

O exemplo a seguir concede permissões de execução da AMI especificada à Conta da AWS especificada.

```
Edit-EC2ImageAttribute `
    -ImageId ami-0abcdef1234567890 `
    -Attribute launchPermission `
    -OperationType add `
    -UserId "123456789012"
```

Para remover as permissões de execução de uma conta

O exemplo a seguir remove permissões de execução da AMI especificada da Conta da AWS especificada.

```
Edit-EC2ImageAttribute `
    -ImageId ami-0abcdef1234567890 `
    -Attribute launchPermission -OperationType remove `
    -UserId "123456789012"
```

Para remover todas as permissões de execução

O exemplo 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.

```
Reset-EC2ImageAttribute `
    -ImageId ami-0abcdef1234567890 `
    -Attribute launchPermission
```

Cancelar o compartilhamento de uma AMI com sua Conta da AWS

Uma imagem de máquina da Amazon (AMI) pode ser compartilhada com Contas da AWS específicas adicionando as contas às permissões de execução da AMI. Se uma AMI tiver sido

compartilhada com sua Conta da AWS e você não quiser mais compartilhá-la com sua conta, poderá remover sua conta das permissões de execução da AMI. É possível fazer isso executando o comando `cancel-image-launch-permission` da AWS CLI. Ao executar esse comando, sua Conta da AWS é removida das permissões de execução para a AMI especificada. Para localizar as AMIs que são compartilhadas com sua Conta da AWS, consulte Encontre AMIs compartilhadas para usar em instâncias do Amazon EC2.

É possível cancelar o compartilhamento de uma AMI com sua conta, p. ex., para reduzir a probabilidade de executar uma instância com uma AMI não utilizada ou obsoleta que tenha sido compartilhada com você. Quando você cancela o compartilhamento de uma AMI com sua conta, ela não aparece mais em nenhuma lista de AMI no console do EC2 ou na saída do comando describe-images.

Tópicos

- Limitações
- Cancelar o compartilhamento de uma AMI com sua conta

Limitações

- É possível remover sua conta das permissões de execução de uma AMI que seja compartilhada apenas com a sua Conta da AWS. Você não pode usar `cancel-image-launch-permission` para remover sua conta das permissões de execução de uma AMI compartilhada com uma organização ou unidade organizacional (UO) ou para remover o acesso a AMIs públicas.
- Você não pode remover permanentemente sua conta das permissões de execução de uma AMI. O proprietário de uma AMI pode compartilhar uma AMI com sua conta novamente.
- As AMIs são um recurso regional. Ao executar `cancel-image-launch-permission`, você deve especificar a região na qual a AMI está localizada. Especifique uma região no comando ou use a variável de ambiente AWS_DEFAULT_REGION.
- Somente a AWS CLI e os SDKs são compatíveis com a remoção de sua conta das permissões de execução de uma AMI. No momento, o console do EC2 não é compatível com essa ação.

Cancelar o compartilhamento de uma AMI com sua conta

> **Note**
>
> Após cancelar o compartilhamento de uma AMI com sua conta, você não poderá desfazer essa ação. Para recuperar o acesso à AMI, o proprietário da AMI deverá compartilhá-la com sua conta.

AWS CLI

Para cancelar o compartilhamento de uma AMI com sua conta

Use o comando cancel-image-launch-permission.

```
aws ec2 cancel-image-launch-permission \
    --image-id ami-0abcdef1234567890 \
    --region us-east-1
```

PowerShell

Para cancelar o compartilhamento de uma AMI com sua conta

Use o cmdlet Stop-EC2ImageLaunchPermission.

```
Stop-EC2ImageLaunchPermission `
    -ImageId ami-0abcdef1234567890 `
    -Region us-east-1
```

Recomendações para criar AMIs compartilhadas no Linux

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

> **Important**
>
> Nenhuma lista de diretrizes de segurança consegue ser exaustiva. Crie suas AMIs compartilhadas cuidadosamente e tire um tempo para considerar onde é possível expor dados confidenciais.

Tópicos

- Desabilitar logins remotos com senha para o usuário raiz
- Desabilitar o acesso à raiz local
- Remover pares de chave do host SSH
- Instalação de credenciais de chave pública
- Desabilitação de verificações de DNS para SSHD (opcional)
- Remover dados confidenciais

Se você estiver criando AMIs para o AWS Marketplace, consulte Práticas recomendadas para a criação de AMIs no Guia do vendedor do AWS Marketplace para obter diretrizes, políticas e práticas recomendadas.

Desabilitar logins remotos com senha para o usuário 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 o usuário raiz

1. Abra o arquivo `/etc/ssh/sshd_config` com um editor de texto e localize a seguinte linha:

   ```
   #PermitRootLogin yes
   ```

2. Altere a linha para:

   ```
   PermitRootLogin without-password
   ```

   O local desse arquivo de configuração pode diferir para sua distribuição ou se você não estiver executando OpenSSH. Se esse for o caso, consulte a documentação apropriada.

Desabilitar o acesso à raiz local

Quando você trabalha com AMIs compartilhadas, a prática recomendada é desabilitar logins diretos na raiz. Para isso, faça login na sua instância em execução e emita o seguinte comando:

```
[ec2-user ~]$ sudo passwd -l root
```

> **Note**
>
> Esse comando não afeta o uso de `sudo`.

Remover pares de chave do host SSH

Se você pretende compartilhar uma AMI derivada de uma AMI pública, remova os pares de chaves do host SSH existentes localizadas em `/etc/ssh`. Isso força o SSH a gerar novos pares de chaves SSH exclusivos quando alguém executar uma instância usando sua AMI, melhorando a segurança e reduzindo a probabilidade de ataques "man-in-the-middle".

Elimine todos os arquivos de chave a seguir presentes no seu sistema.

- ssh_host_dsa_key
- ssh_host_dsa_key.pub
- ssh_host_key
- ssh_host_key.pub
- ssh_host_rsa_key
- ssh_host_rsa_key.pub
- ssh_host_ecdsa_key
- ssh_host_ecdsa_key.pub
- ssh_host_ed25519_key
- ssh_host_ed25519_key.pub

É possível 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 de 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, é necessário 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`, é possível adicionar o código a seguir a um script de inicialização do sistema (como `/etc/rc.local`) para puxar a chave pública especificada na execução para o usuário raiz.

Note

No exemplo a seguir, o endereço IP do http://169.254.169.254/ é um endereço local de link e é válido apenas a partir da instância.

IMDSv2

```
if [ ! -d /root/.ssh ] ; then
        mkdir -p /root/.ssh
        chmod 700 /root/.ssh
fi
# Fetch public key using HTTP
TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-
token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-
data/public-keys/0/openssh-key > /tmp/my-key
if [ $? -eq 0 ] ; then
        cat /tmp/my-key >> /root/.ssh/authorized_keys
        chmod 700 /root/.ssh/authorized_keys
        rm /tmp/my-key
fi
```

IMDSv1

```
if [ ! -d /root/.ssh ] ; then
        mkdir -p /root/.ssh
        chmod 700 /root/.ssh
fi
# Fetch public key using HTTP
curl http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key > /tmp/my-key
if [ $? -eq 0 ] ; then
        cat /tmp/my-key >> /root/.ssh/authorized_keys
        chmod 700 /root/.ssh/authorized_keys
        rm /tmp/my-key
fi
```

Isso pode se aplicar a qualquer usuário; não precisa ficar restrito ao `root`.

> **Note**
>
> Reempacotar uma instância baseada nessa AMI inclui a chave com a qual ela foi executada. Para evitar a inclusão de chaves, é necessário desmarcar (ou excluir) o arquivo `authorized_keys` ou excluir esse arquivo do reempacotamento.

Desabilitação de verificações de DNS para 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.

Remover dados confidenciais

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 os armazenam na `/root/.ssh` do usuário raiz e `/home/`*`user_name`*`/.ssh/` para os usuário regulares. Para obter mais informações, consulte ec2-bundle-vol.

- Sempre exclua o histórico do shell antes de empacotar. Se você tentar fazer mais de um upload de bundle na mesma AMI, o histórico do shell conterá sua chave de acesso. O exemplo a seguir deve ser o último comando executado antes de empacotar na 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.

- O empacotamento de 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).

Monitorar eventos da AMI usando o Amazon EventBridge

Quando o estado de uma imagem de máquina da Amazon (AMI) muda, o Amazon EC2 gera um evento que é enviado para o Amazon EventBridge (anteriormente conhecido como Amazon CloudWatch Events). Os eventos são enviados para o barramento de eventos do EventBridge padrão no formato JSON. É possível usar o Amazon EventBridge para detectar e reagir a esses eventos. Você faz isso criando regras no EventBridge que acionem uma ação em resposta a um evento. Por exemplo, é possível criar uma regra do EventBridge que detecte quando o processo de criação da AMI foi concluído e, em seguida, invoque um tópico do Amazon SNS para enviar uma notificação por email para você.

O Amazon EC2 gera um evento `EC2 AMI State Change` quando uma AMI entra em qualquer um dos seguintes estados:

- `available`
- `failed`
- `deregistered`

- `disabled`

Os eventos são gerados com base no melhor esforço.

A tabela abaixo mostra as operações da AMI e os estados que podem ser atribuídos a ela. Na tabela, Sim indica os estados que podem ser atribuídos à AMI ao executar a operação correspondente.

Operações da AMI	available	failed	deregistered	disabled
CopyImage	Sim	Sim		
CreateImage	Sim	Sim		
CreateRestoreImageTask	Sim	Sim		
DeregisterImage			Sim	
DisableImage				Sim
EnableImage	Sim			
RegisterImage	Sim	Sim		

EC2 AMI State ChangeEventos do

- Detalhes do evento
- availableEventos do
- failedEventos do
- deregisteredEventos do
- disabledEventos do

Detalhes do evento

Você pode usar os seguintes campos no evento para criar regras que acionem uma ação:

`"source": "aws.ec2"`

Identifica que o evento é do Amazon EC2.

`"detail-type": "EC2 AMI State Change"`

Identifica o nome do evento.

`"detail": { "ImageId": "ami-0abcdef1234567890", "State": "available", }`

Fornece o ID e o estado da AMI (`available`, `failed`, `deregistered` ou `disabled`).

Para obter mais informações, consulte os seguintes tópicos no Guia do usuário do Amazon EventBridge:

- Eventos do Amazon EventBridge
- Padrões de eventos do Amazon EventBridge
- Regras do Amazon EventBridge

Para obter um tutorial sobre como criar uma função do Lambda e uma regra do EventBridge que execute a função do Lambda, consulte Tutorial: Log the state of an Amazon EC2 instance using EventBridge no Guia do desenvolvedor do AWS Lambda.

availableEventos do

Veja a seguir um exemplo de um evento que o Amazon EC2 gera quando a AMI entra no estado `available` após uma operação de `CreateImage`, `CopyImage`, `RegisterImage`, `CreateRestoreImageTask` ou `EnableImage` com êxito.

`"State": "available"` indica que a operação teve êxito.

```
{
    "version": "0",
    "id": "example-9f07-51db-246b-d8b8441bcdf0",
    "detail-type": "EC2 AMI State Change",
    "source": "aws.ec2",
    "account": "012345678901",
    "time": "yyyy-mm-ddThh:mm:ssZ",
    "region": "us-east-1",
    "resources": ["arn:aws:ec2:us-east-1::image/ami-0abcdef1234567890"],
    "detail": {
        "RequestId": "example-9dcc-40a6-aa77-7ce457d5442b",
```

```
        "ImageId": "ami-0abcdef1234567890",
        "State": "available",
        "ErrorMessage": ""
    }
}
```

failedEventos do

Veja a seguir um exemplo de um evento que o Amazon EC2 gera quando a AMI entra no estado `failed` após uma operação de `CreateImage`, `CopyImage`, `RegisterImage` ou `CreateRestoreImageTask` com êxito.

Os campos a seguir fornecem informações pertinentes:

- `"State": "failed"`: indica que a operação falhou.
- `"ErrorMessage": ""`: Fornece o motivo da operação com falha.

```
{
    "version": "0",
    "id": "example-9f07-51db-246b-d8b8441bcdf0",
    "detail-type": "EC2 AMI State Change",
    "source": "aws.ec2",
    "account": "012345678901",
    "time": "yyyy-mm-ddThh:mm:ssZ",
    "region": "us-east-1",
    "resources": ["arn:aws:ec2:us-east-1::image/ami-0abcdef1234567890"],
    "detail": {
        "RequestId": "example-9dcc-40a6-aa77-7ce457d5442b",
        "ImageId": "ami-0abcdef1234567890",
        "State": "failed",
        "ErrorMessage": "Description of failure"
    }
}
```

deregisteredEventos do

Veja a seguir um exemplo de um evento que o Amazon EC2 gera quando a AMI entra no estado `deregistered` após uma operação de `DeregisterImage` com êxito. Se a operação falhar, nenhum evento será gerado. Qualquer falha será conhecida imediatamente, pois `DeregisterImage` é uma operação síncrona.

`"State": "deregistered"` indica que a operação `DeregisterImage` teve êxito.

```
{
    "version": "0",
    "id": "example-9f07-51db-246b-d8b8441bcdf0",
    "detail-type": "EC2 AMI State Change",
    "source": "aws.ec2",
    "account": "012345678901",
    "time": "yyyy-mm-ddThh:mm:ssZ",
    "region": "us-east-1",
    "resources": ["arn:aws:ec2:us-east-1::image/ami-0abcdef1234567890"],
    "detail": {
        "RequestId": "example-9dcc-40a6-aa77-7ce457d5442b",
        "ImageId": "ami-0abcdef1234567890",
        "State": "deregistered",
        "ErrorMessage": ""
    }
}
```

disabledEventos do

Veja a seguir um exemplo de um evento que o Amazon EC2 gera quando a AMI entra no estado `disabled` após uma operação de `DisableImage` com êxito. Se a operação falhar, nenhum evento será gerado. Qualquer falha será conhecida imediatamente, pois `DisableImage` é uma operação síncrona.

`"State": "disabled"` indica que a operação `DisableImage` teve êxito.

```
{
    "version": "0",
    "id": "example-9f07-51db-246b-d8b8441bcdf0",
    "detail-type": "EC2 AMI State Change",
    "source": "aws.ec2",
    "account": "012345678901",
    "time": "yyyy-mm-ddThh:mm:ssZ",
    "region": "us-east-1",
    "resources": ["arn:aws:ec2:us-east-1::image/ami-0abcdef1234567890"],
    "detail": {
        "RequestId": "example-9dcc-40a6-aa77-7ce457d5442b",
        "ImageId": "ami-0abcdef1234567890",
        "State": "disabled",
        "ErrorMessage": ""
```

```
    }
}
```

Noções básicas sobre as informações de faturamento da AMI

Há muitas Imagens de máquina da Amazon (AMIs) para escolher ao executar suas instâncias e elas oferecem suporte a uma variedade de plataformas e recursos do sistema operacional. Para entender como a AMI escolhida ao executar sua instância afeta os resultados da sua fatura da AWS, é possível pesquisar a plataforma do sistema operacional associada e as informações de faturamento. Faça isso antes de executar qualquer on-demand ou Instâncias spot, ou comprar uma Instância reservada.

Aqui estão dois exemplos de como pesquisar sua AMI com antecedência pode ajudá-lo a escolher a AMI que melhor se adapte às suas necessidades:

- Para Instâncias spot, é possível usar os detalhes da plataforma da AMI para confirmar se há suporte à AMI para Instâncias spot.
- Ao comprar uma Instância reservada, é possível certificar-se de selecionar a plataforma do sistema operacional (Plataforma) que mapeia para os detalhes da Plataforma AMI.

Para obter mais informações sobre a definição de instâncias, consulte Definição de preço do Amazon EC2.

Tópicos

- Campos de informações de faturamento da AMI
- Localizando detalhes de faturamento e uso da AMI
- Verificar cobranças da AMI em sua fatura

Campos de informações de faturamento da AMI

Os campos a seguir fornecem informações de faturamento associadas a uma AMI:

Detalhes da plataforma

> Os detalhes da plataforma associada ao código de faturamento da AMI. Por exemplo, `.Red Hat Enterprise Linux`

Operação de uso

A operação da instância do Amazon EC2 e o código de faturamento associado à AMI. Por exemplo, `.RunInstances:0010` A Usage operation (Operação de uso) corresponde à coluna lineitem/Operation (lineitem/Operação) no seu Relatório de custos e uso (CUR) da AWS e na API de tabela de preços da AWS.

É possível visualizar esses campos na página Instâncias ou AMIs no console do Amazon EC2 ou na resposta retornada pelo comando describe-images ou Get-EC2Image.

Dados de amostra: operação de uso por plataforma

A tabela a seguir lista os detalhes da plataforma e os valores de operação de uso que podem ser exibidos na página Instâncias ou AMIs no console do Amazon EC2 ou na resposta retornada pelo comando describe-images ou Get-EC2Image.

Detalhes da plataforma	Operação de uso [2]
Linux/UNIX	RunInstances
Red Hat BYOL Linux	RunInstances:00g0 [3]
Red Hat Enterprise Linux	RunInstances:0010
Red Hat Enterprise Linux with HA	RunInstances:1010
Red Hat Enterprise Linux with SQL Server Standard and HA	RunInstances:1014
Red Hat Enterprise Linux with SQL Server Enterprise and HA	RunInstances:1110
Red Hat Enterprise Linux with SQL Server Standard	RunInstances:0014
Red Hat Enterprise Linux with SQL Server Web	RunInstances:0210

Detalhes da plataforma	Operação de uso [2]
Red Hat Enterprise Linux with SQL Server Enterprise	RunInstances:0110
SQL Server Enterprise	RunInstances:0100
SQL Server Standard	RunInstances:0004
SQL Server Web	RunInstances:0200
SUSE Linux	RunInstances:000g
Ubuntu Pro	RunInstances:0g00
Windows	RunInstances:0002
Windows BYOL	RunInstances:0800
Windows with SQL Server Enterprise [1]	RunInstances:0102
Windows with SQL Server Standard [1]	RunInstances:0006
Windows with SQL Server Web [1]	RunInstances:0202

[1] Se duas licenças de software estiverem associadas a uma AMI, o campo Detalhes da plataforma mostrará ambas.

[2] Se você estiver executando instâncias spot, o item lineitem/Operation no Relatório de Custos e Uso da AWS poderá ser diferente do valor da Operação de uso listado aqui. Por exemplo, se `lineitem/Operation` exibir `RunInstances:0010:SV006`, significa que o Amazon EC2 está executando a instância spot do Red Hat Enterprise Linux por hora no Leste dos EUA (Norte da Virgínia) na Zona 6.

[3] Isso aparece como RunInstances (Linux/UNIX) em seus relatórios de uso.

Localizando detalhes de faturamento e uso da AMI

As propriedades a seguir podem ajudar a verificar as cobranças da AMI em sua fatura:

- Detalhes da plataforma
- Operação de uso
- ID DA AMI

Console

Para encontrar as informações de cobrança de AMI para uma AMI

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione AMIs.
3. Selecione a AMI.
4. Na guia Detalhes, vá para Detalhes da plataforma e Operação de uso.

Para encontrar as informações de cobrança de AMI para uma instância

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância.
4. Na guia Detalhes, expanda Detalhes da instância e vá para Detalhes da plataforma e Operação de uso.

AWS CLI

Para encontrar as informações de cobrança de AMI para uma AMI

Use o comando describe-images.

```
aws ec2 describe-images \
    --image-ids ami-0abcdef1234567890 \
    --query "Images[].
{PlatformDetails:PlatformDetails,UsageOperation:UsageOperation}"
```

Veja a seguir um exemplo de saída de uma AMI do Linux.

```
[
    {
        "PlatformDetails": "Linux/UNIX",
        "UsageOperation": "RunInstances"
    }
]
```

Para encontrar as informações de cobrança de AMI para uma instância

Use o comando describe-instances.

```
aws ec2 describe-instances \
    --instance-ids i-1234567890abcdef0 \
    --query "Reservations[].Instances[].
{PlatformDetails:PlatformDetails,UsageOperation:UsageOperation}"
```

Este é um exemplo de saída de uma instância do Windows.

```
[
    {
        "PlatformDetails": "Windows",
        "UsageOperation": "RunInstances:0002"
    }
]
```

PowerShell

Para encontrar as informações de cobrança de AMI para uma AMI

Use o cmdlet Get-EC2Image.

```
Get-EC2Image `
    -ImageId ami-0abcdef1234567890 | `
    Format-List PlatformDetails, UsageOperation
```

Veja a seguir um exemplo de saída de uma AMI do Linux.

```
PlatformDetails : Linux/UNIX
UsageOperation  : RunInstances
```

Para encontrar as informações de cobrança de AMI para uma instância

Use o cmdlet Get-EC2Instance.

```
(Get-EC2Instance `
    -InstanceId i-1234567890abcdef0).Instances | `
    Format-List PlatformDetails, UsageOperation
```

Este é um exemplo de saída de uma instância do Windows.

```
PlatformDetails : Windows
UsageOperation  : RunInstances:0002
```

Verificar cobranças da AMI em sua fatura

Para garantir que você não incorra em custos não planejados, verifique se as informações de faturamento de uma instância no Relatório de custos e uso (CUR) da AWS correspondem às informações de faturamento associadas à AMI que você usou para executar a instância.

Para confirmar as informações de faturamento, localize o ID da instância no CUR e verifique o valor correspondente na coluna `lineitem/Operation`. O valor deve corresponder ao valor da Usage operation (Operação de uso) associada à AMI.

Por exemplo, a AMI `ami-0123456789EXAMPLE` tem as seguintes informações de faturamento:

- Detalhes da plataforma = `Red Hat Enterprise Linux`
- Operação de uso = `RunInstances:0010`

Se você executou uma instância usando essa AMI, poderá localizar o ID da instância no CUR e verificar o valor correspondente na coluna `lineitem/Operation`. Neste exemplo, o valor deve ser `RunInstances:0010`.

Cotas da AMI no Amazon EC2

As cotas a seguir se aplicam à criação e ao compartilhamento de AMIs. Estas cotas são aplicáveis por Região da AWS.

Nome da cota	Descrição	Cota padrão por região
AMIs	O número máximo de AMIs públicas e privadas permitido por região. Isso inclui AMIs disponíveis, pendentes e desabilitadas e AMIs na Lixeira.	50.000
AMIs públicas	O número máximo de AMIs públicas, inclusive AMIs públicas na Lixeira, permitido por região.	5
Compartilhamento de AMIs	O número máximo de entidades (organizações, unidades organizacionais [UOs] e contas) com as quais uma AMI pode ser compartil hada em uma região. Se você compartilhar uma AMI com uma organização ou UO, o número de contas na organização ou na UO não contará para a cota.	1.000

Se exceder suas cotas e quiser criar ou compartilhar mais AMIs, você poderá fazer o seguinte:

- Se você exceder sua cota de AMIs total ou de AMIs públicas, considere cancelar o registro de imagens não usadas.
- Se você exceder sua cota de AMIs públicas, considere tornar uma ou mais AMIs públicas privadas.
- Se você exceder sua cota de compartilhamento de AMIs, considere compartilhar suas AMIs com uma organização ou UO em vez de contas separadas.
- Solicite um aumento de cota para AMIs.

Solicitar um aumento de cota para AMIs

Se precisar exceder a cota padrão de AMIs, solicite um aumento de cota.

Para solicitar um aumento de cota para AMIs

1. Abra o console Service Quotas em https://console.aws.amazon.com/servicequotas/.
2. No painel de navegação, selecione serviços da AWS.
3. Escolha Amazon Elastic Compute Cloud (Amazon EC2) na lista ou digite o nome do serviço na caixa de pesquisa.
4. Escolha a cota da AMI para solicitar um aumento. As cotas da AMI que você pode selecionar são:
   - AMIs
   - AMIs públicas
   - Compartilhamento de AMI
5. Selecione Solicitar aumento de cota.
6. Em Change quota value (Alterar valor da cota), insira o novo valor da cota e escolha Request (Solicitar).

Para exibir quaisquer solicitações pendentes ou resolvidas recentemente, escolha Dashboard (Painel) no painel de navegação. Para solicitações pendentes, escolha o status da solicitação para abrir o recibo da solicitação. O status inicial de uma solicitação é Pending (Pendente). Depois que o status for alterado para Quota requested (Cota solicitada), você verá o número do caso em Support Center case number (Número do caso no Support Center). Escolha o número do caso para abrir o tíquete de sua solicitação.

Depois que a solicitação é resolvida, o Applied quota value (Valor da cota aplicada) para a cota é definido como o novo valor.

Para obter mais informações, consulte o Manual do usuário do Service Quotas.

Instâncias do Amazon EC2

Uma instância do Amazon EC2 é um servidor virtual no ambiente da Nuvem AWS. Você tem controle total sobre sua instância, desde o momento em que a inicia pela primeira vez (chamado de executar uma instância) até excluí-la (chamado de encerramento de uma instância). É possível escolher entre uma variedade de sistemas operacionais ao executar a instância. É possível se conectar à instância e personalizá-la para atender às suas necessidades. Por exemplo, você pode configurar e instalar atualizações do sistema operacional e instalar aplicações na sua instância.

O Amazon EC2 fornece uma ampla variedade de tipos de instância. É possível escolher um tipo de instância que forneça os recursos de computação, a memória, o armazenamento e a performance de rede de que você precisa para executar suas aplicações.

Com o Amazon EC2, você paga somente pelo que for usado. O faturamento da sua instância começa quando você a executa e ela passa para o estado de execução. O faturamento é interrompido quando você interrompe a instância e é retomado quando você a inicia. Quando você encerra sua instância, o faturamento é interrompido quando ela passa para o estado de desligamento.

O Amazon EC2 fornece recursos que você pode usar para otimizar a performance e o custo das instâncias. Por exemplo, você pode usar o Amazon EC2 Fleet ou o Amazon EC2 Auto Scaling para aumentar ou reduzir a escala verticalmente da capacidade à medida que a utilização da instância muda. É possível reduzir os custos das instâncias usando instâncias spot ou o Savings Plans.

Uma instância gerenciada é gerenciada por um provedor de serviços, como o Modo Automático do Amazon EKS. Você não pode modificar diretamente as configurações de uma instância gerenciada. As instâncias gerenciadas são identificadas por um valor true no campo Gerenciada. Para obter mais informações, consulte Instâncias gerenciadas do Amazon EC2.

Recursos e tarefas

- Tipos de instância do Amazon EC2
- Instâncias gerenciadas do Amazon EC2
- Use a virtualização aninhada para executar hipervisores em instâncias do Amazon EC2
- Opções de faturamento e compra do Amazon EC2
- Armazenar os parâmetros de execução de instâncias nos modelos de execução do Amazon EC2
- Iniciar uma instância do Amazon EC2

- Conexão com a instância do EC2
- Alterações do estado de instâncias do Amazon EC2
- Recuperação automática de instâncias
- Usar metadados da instância para gerenciar a instância do EC2
- Detectar se um host é uma instância do EC2
- Documentos de identidade da instância para instâncias do Amazon EC2
- Conformidade com STIG para a instância do EC2
- Relógio de precisão e sincronização de horas em sua instância do EC2
- EC2 Capacity Manager
- Gerenciar drivers de dispositivo para a instância do Amazon EC2
- Configurar a instância do Windows do Amazon EC2
- Atualizar uma instância do Windows do EC2 para uma versão mais recente do Windows Server
- Tutorial: conectar uma instância do Amazon EC2 a um banco de dados do Amazon RDS

Tipos de instância do Amazon EC2

Quando executa uma instância, o tipo de instância que você especifica determina o hardware do computador host usado para sua instância. Cada tipo de instância oferece recursos de computação, memória e armazenamento diferentes, além de ser agrupado em famílias de instâncias de acordo com esses recursos. Selecione um tipo de instância com base nos requisitos da aplicação ou do software que você pretende executar na instância. Para obter mais informações sobre recursos e casos de uso, consulte Tipos de instâncias do Amazon EC2.

O Amazon EC2 dedica alguns recursos do computador host, como CPU, memória e armazenamento de instâncias, a uma instância específica. O Amazon EC2 compartilha outros recursos do computador host, como a rede e o subsistema de disco, entre instâncias. Se cada instância em um computador host tentar usar o máximo desses recursos compartilhados quanto for possível, cada uma receberá uma parte igual daquele recurso. No entanto, quando um recurso for pouco utilizado, uma instância poderá consumir uma parte maior desse recurso enquanto ele estiver disponível.

Cada tipo de instância fornece uma performance mínima superior ou inferior com base em um recurso compartilhado. Por exemplo, tipos de instância com performance alta de E/S têm uma alocação maior dos recursos compartilhados. A alocação de uma parte maior dos recursos

compartilhados também reduz a variação da performance de E/S. Para a maioria das aplicações, a performance moderada de E/S é mais do que suficiente. No entanto, para aplicações que exigem uma performance de E/S maior ou mais consistente, considere um tipo de instância com performance mais alta de E/S.

Tópicos

- Tipos de instâncias disponíveis
- Especificações de hardware
- Tipo de hipervisor
- Tipos de virtualização de AMI
- Processadores
- Localizar um tipo de instância do Amazon EC2
- Obtenha recomendações do localizador de tipo de instância do EC2
- Obter as recomendações de instâncias do EC2 no Compute Optimizer
- Alterações no tipo de instância do Amazon EC2
- Instâncias expansíveis
- Aceleração de performance com instâncias de GPU
- Instâncias Mac do Amazon EC2
- Tipos de instância otimizados para o Amazon EBS
- Opções de CPU para instâncias do Amazon EC2
- AMD SEV-SNP para instâncias do Amazon EC2
- Controle do estado do processador para instâncias Linux do Amazon EC2

Tipos de instâncias disponíveis

O Amazon EC2 fornece uma ampla seleção de tipos de instância otimizadas para de adequarem a diferentes casos de uso. Os tipos de instância incluem combinações variadas de capacidade de CPU, memória, armazenamento e redes e oferecem a flexibilidade de escolher a combinação de recursos adequada para suas aplicações. Cada tipo de instância inclui um ou mais tamanhos de instância, permitindo que você escale seus recursos de acordo com os requisitos de sua workload de destino.

Convenções de nomenclatura para o tipo de instância

Os nomes são baseados na família da instância, na geração, na família do processador, nas funcionalidades e no tamanho. Para obter mais informações, consulte Naming conventions no Guia de tipos de instância do Amazon EC2.

Localizar um tipo de instância do

Para determinar quais tipos de instância atendem aos seus requisitos, por exemplo, regiões, recursos de computação ou recursos de armazenamento compatíveis, consulte Localizar um tipo de instância do Amazon EC2 e Amazon EC2 instance type specifications no Guia de tipos de instância do Amazon EC2.

Especificações de hardware

Para obter especificações detalhadas sobre o tipo de instância, consulte Specifications no Guia de tipos de instância do Amazon EC2. Para obter informações sobre os preços, consulte Preço sob demanda do Amazon EC2.

Para determinar que tipo de instância atende melhor às suas necessidades, recomendamos executar uma instância e usar seu própria aplicação de referência. Como você paga pelo segundo da instância, é conveniente e econômico testar vários tipos de instância antes de tomar uma decisão. Se suas necessidades mudarem, mesmo depois de tomar uma decisão, será possível alterar o tipo de instância mais tarde. Para obter mais informações, consulte Alterações no tipo de instância do Amazon EC2.

Tipo de hipervisor

O Amazon EC2 é compatível com os seguintes hipervisores: Xen e Nitro.

Instâncias baseadas em Nitro

- Uso geral: M5 | M5a | M5ad | M5d | M5dn | M5n | M5zn | M6a | M6g | M6gd | M6i | M6id | M6idn | M6in | M7a | M7g | M7gd | M7i | M7i-flex | M8a | M8azn | M8g | M8gb | M8gd | M8gn | M8i | M8id | M8i-flex | T3 | T3a | T4g
- Otimizadas para computação: C5 | C5a | C5ad | C5d | C5n | C6a | C6g | C6gd | C6gn | C6i | C6id | C6in | C7a | C7g | C7gd | C7gn | C7i | C7i-flex | C8a | C8g | C8gb | C8gd | C8gn | C8i | C8id | C8i-flex
- Otimizadas para memória: R5 | R5a | R5ad | R5b | R5d | R5dn | R5n | R6a | R6g | R6gd | R6i | R6id | R6idn | R6in | R7a | R7g | R7gd | R7i | R7iz | R8a | R8g | R8gb | R8gd | R8gn | R8i | R8id | R8i-flex

| U-3tb1 | U-6tb1 | U-9tb1 | U-12tb1 | U-18tb1 | U-24tb1 | U7i-6tb | U7i-8tb | U7i-12tb | U7in-16tb | U7in-24tb | U7in-32tb | U7inh-32tb | X2gd | X2idn | X2iedn | X2iezn | X8g | X8aedz | X8i | z1d

- Otimizadas para armazenamento: D3 | D3en | I3en | I4g | I4i | I7i | I7ie | I8g | I8ge | Im4gn | Is4gen
- Computação acelerada: DL1 | DL2q | F2 | G4ad | G4dn | G5 | G5g | G6 | G6e | G6f | Gr6 | Gr6f | G7e | Inf1 | Inf2 | P4d | P4de | P5 | P5e | P5en | P6-B200 | P6-B300 | P6e-GB200 | Trn1 | Trn1n | Trn2 | Trn2u | VT1
- Computação de alta performance: Hpc6a | Hpc6id | Hpc7a | Hpc7g | Hpc8a
- Geração anterior: A1 | P3dn

Para obter mais informações sobre as versões compatíveis do hipervisor Nitro, consulte Network feature support no Guia de tipos de instâncias do Amazon EC2.

Instâncias baseadas en Xen

- Uso geral: M1 | M2 | M3 | M4 | T1 | T2
- Otimizadas para computação: C1 | C3 | C4
- Otimizadas para memória: R3 | R4 | X1 | X1e
- Otimizadas para armazenamento: D2 | H1 | I2 | I3
- Computação acelerada: F1 | G3 | P2 | P3

Tipos de virtualização de AMI

O tipo de virtualização da sua instância é determinado pela AMI usada para executá-la. Os tipos de instância da geração atual oferecem suporte apenas a HVM. Alguns tipos de instância de geração anterior são compatíveis com paravirtual (PV) e algumas regiões da AWS são compatíveis com as instâncias PV. Para obter mais informações, consulte Tipos de virtualização.

Para a melhor performance, recomendamos usar uma AMI HVM. Além disso, as AMIs HVM são necessárias para aproveitar as maiores capacidades de rede. A virtualização da HVM usa tecnologia assistida por hardware fornecida pela plataforma AWS. Com a virtualização da HVM, a VM guest é executada como se estivesse em uma plataforma de hardware nativa, exceto pelo fato de que ela ainda usa drivers de rede e armazenamento PV para melhorar a performance.

Processadores

As instâncias do EC2 são compatíveis com uma variedade de processadores.

Processadores

- Processadores Intel
- Processadores AMD
- AWSProcessadores Graviton
- AWS Trainium
- AWS Inferentia

Processadores Intel

As instâncias do Amazon EC2 executadas nos processadores Intel podem incluir os recursos de processador a seguir. Nem todas as instâncias executadas nos processadores Intel são compatíveis com esses recursos de processador. Para obter informações sobre quais recursos estão disponíveis para cada tipo de instância, consulte Tipos de instância do Amazon EC2.

- Intel AES New Instructions (AES-NI) — O conjunto de instruções de criptografia Intel AES-NI aprimora o algoritmo Advanced Encryption Standard (AES) original para oferecer proteção de dados mais rápida e maior segurança. Todas as instâncias do EC2 da geração atual oferecem suporte a esse recurso de processador.
- Intel Advanced Vector Extensions (Intel AVX, Intel AVX2 e AVX-512): o Intel AVX e o Intel AVX2 são extensões de conjunto de instruções de 256 bits e o Intel AVX-512 é uma extensão de conjunto de instruções de 512 bits projetadas para aplicações com uso intensivo de Floating Point (FP – Ponto flutuante). As instruções Intel AVX melhoram a performance de aplicações, como de processamento de imagem, áudio e vídeo, simulações científicas, analytics financeira e modelagem e análise 3D. Esses recursos só estão disponíveis em instâncias executadas com AMIs de HVM.
- Tecnologia Intel Turbo Boost — Os processadores com Tecnologia Intel Turbo Boost executam núcleos automaticamente com mais rapidez do que a frequência operacional básica.
- Intel Deep Learning Boost (Intel DL Boost) — Acelera os casos de uso de deep learning profundo da IA. Os processadores Intel Xeon Scalable da segunda geração ampliam o Intel AVX-512 com uma nova Vector Neural Network Instruction (VNNI/INT8), que aumenta significativamente a performance de inferência de deep learning em comparação com a geração anterior dos processadores Intel Xeon Scalable (com FP32), para reconhecimento/segmentação de imagens, detecção de objetos, reconhecimento de fala, tradução de idiomas, sistemas de recomendação, aprendizado por reforço e outros. A VNNI pode não ser compatível com todas as distribuições Linux.

As seguintes instâncias oferecem suporte a VNNI: `M5n`, `R5n`, `M5dn`, `M5zn`, `R5b`, `R5dn`, `D3`, `D3en` e `C6i`. As instâncias `C5` e `C5d` só oferecem suporte a VNNI para as instâncias `12xlarge`, `24xlarge` e `metal`.

As convenções de nomenclatura do setor para CPUs de 64 bits podem gerar confusão. 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 que executa o Ubuntu ou o Windows exibe a arquitetura de CPU como AMD64, ainda que as instâncias estejam sendo executadas em hardware Intel.

Processadores AMD

As instâncias do Amazon EC2 executadas nos processadores AMD EPYC podem ajudar a otimizar o custo e a performance de suas workloads. Essas instâncias podem ser compatíveis com os recursos de processador a seguir. Nem todas as instâncias executadas nos processadores AMD são compatíveis com esses recursos de processador. Para obter informações sobre quais recursos estão disponíveis para cada tipo de instância, consulte Tipos de instância do Amazon EC2.

- Secure Memory Encryption (SME) da AMD
- Transparent Single Key Memory Encryption (TSME) da AMD
- Advanced Vector Extensions (AVX) da AMD
- Secure Encrypted Virtualization-Secure Nested Paging (SEV-SNP) da AMD
- Vector Neural Network Instructions (VNNI)
- BFloat 16

AWSProcessadores Graviton

O AWS Graviton é uma família de processadores projetada para oferecer a melhor relação entre preço e performance para as workloads executadas em instâncias do Amazon EC2.

Para obter mais informações, consulte Getting started with Graviton.

AWS Trainium

As instâncias desenvolvidas pelo AWS Trainium têm propósito específico para o treinamento de aprendizado profundo com alta performance e baixo custo. É possível usar essas instâncias para treinar modelos de processamento de linguagem natural, de visão computacional e de recomendação usados em um amplo conjunto de aplicações, como reconhecimento de fala, recomendações, detecção de fraudes e classificação de imagens e vídeos. Use os fluxos de trabalho existentes em estruturas de ML conhecidas, como PyTorch e TensorFlow.

AWS Inferentia

As instâncias desenvolvidas pelo AWS Inferentia são projetadas para acelerar o machine learning. Essas instâncias fornecem inferência de machine learning de alta performance e baixa latência. Essas instâncias são otimizadas para implantar modelos de aprendizagem profunda (DL) para aplicações, como processamento de linguagem natural, detecção e classificação de objetos, personalização e filtragem de conteúdo e reconhecimento de fala.

É possível começar de diversas maneiras:

- Use o SageMaker AI, um serviço totalmente gerenciado que é a maneira mais fácil de começar a usar modelos de machine learning. Para obter informações, consulte Noções básicas do SageMaker AI no Guia do desenvolvedor do Amazon SageMaker AI.
- Inicie uma instância Inf1 ou Inf2 usando a AMI de aprendizado profundo. Para obter mais informações, consulte AWS Inferentia com DLAMI no Guia do desenvolvedor do AMIs de deep learning da AWS.
- Execute uma instância Inf1 ou Inf2 usando sua própria AMI e instale o AWS Neuron SDK, que permite compilar, executar e criar perfis de modelos de aprendizado profundo para o AWS Inferentia.
- Inicie uma instância de contêiner usando uma instância Inf1 ou Inf2 e uma AMI otimizada para o Amazon ECS. Para obter mais informações, consulte AMIs do Amazon Linux 2 (Inferentia) no Amazon Elastic Container Service Developer Guide.
- Crie um cluster do Amazon EKS com nós executando instâncias Inf1. Para obter mais informações, consulte Inferentia support (Suporte para Inferentia) no Amazon EKS User Guide (Manual do usuário do Amazon EKS).

Localizar um tipo de instância do Amazon EC2

Para poder executar uma instância, é necessário selecionar um tipo de instância para usar. O tipo de instância escolhido pode depender dos recursos necessários para sua workload, como recursos de computação, memória ou armazenamento. Pode ser benéfico identificar vários tipos de instância possivelmente adequadas à sua workload e avaliar a performance deles em um ambiente de teste. Não há substituto para medir a performance de sua aplicação sob carga.

Você pode obter sugestões e orientações para os tipos de instância do EC2 usando o localizador de tipos de instância do EC2. Para obter mais informações, consulte the section called “Localizador de tipo de instância do EC2”.

Se já tiver instâncias do EC2 em execução, será possível usar o AWS Compute Optimizer para obter recomendações sobre os tipos de instâncias que deve usar para melhorar a performance, economizar dinheiro ou ambos. Para obter mais informações, consulte the section called “Recomendações do Compute Optimizer”.

Tarefas

- Localizar um tipo de instância usando o console
- Descrever um tipo de instância usando a AWS CLI
- Encontrar um tipo de instância usando a AWS CLI
- Encontrar um tipo de instância usando as Ferramentas para PowerShell

Localizar um tipo de instância usando o console

É possível encontrar um tipo de instância que atenda às suas necessidades usando o console do Amazon EC2.

Como encontrar um tipo de instância usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Na barra de navegação, selecione a região na qual executar as instâncias. Selecione qualquer região que estiver disponível para você, independentemente do seu local.
3. No painel de navegação, selecione Instance Types (Tipos de instância).
4. (Opcional) Selecione o ícone de preferências (engrenagem) para escolher quais atributos de tipos de instância exibir, como a Definição de preço do Linux sob demanda e selecione Confirmar. Como alternativa, selecione o nome de um tipo de instância para abrir a respectiva

página de detalhes e exibir todos os atributos disponíveis por meio do console. O console não exibe todos os atributos disponíveis por meio da API ou da linha de comando.

5. Use os atributos de tipo de instância para filtrar a lista de tipos de instância exibidos apenas para os tipos de instância que atendem às suas necessidades. Por exemplo, é possível filtrar com base nos seguintes atributos:

   - Availability zones (Zonas de disponibilidade): o nome da zona de disponibilidade, zona local ou zona Wavelength. Para obter mais informações, consulte the section called “A VPC abrange as zonas de disponibilidade e a zona Wavelength.”.
   - vCPUs (vCPUs) ou Cores (Núcleos): o número de vCPUs ou núcleos.
   - Memory (GiB) (Memória [GiB]): o tamanho da memória em GiB.
   - Network performance (Performance de rede): o desempenho da rede, em Gigabits.
   - Local instance storage (Armazenamento de instâncias locais): indica se o tipo de instância tem armazenamento de instância local (`true` | `false`).

6. (Opcional) Para ver um comparativo lado a lado, marque a caixa de seleção para vários tipos de instâncias. A comparação é exibida na parte inferior da tela.
7. (Opcional) Para salvar a lista de tipos de instância em um arquivo de valores separados por vírgula (.csv) para análise adicional, escolha Actions (Ações), Download list CSV (Baixar lista em CSV). O arquivo inclui todos os tipos de instância que correspondem aos filtros definidos.
8. (Opcional) Para executar instâncias usando um tipo de instância que satisfaça suas necessidades, marque a caixa de seleção para o tipo de instância e escolha Actions (Ações), Launch instance (Executar instância). Para obter mais informações, consulte Executar uma instância do EC2 usando o assistente de inicialização de instâncias no console.

Descrever um tipo de instância usando a AWS CLI

Você pode usar o comando describe-instance-types para descrever um tipo de instância específico.

Descrever por completo um tipo de instância

O comando a seguir exibe todos os detalhes disponíveis do tipo da instância especificado. A saída é longa, portanto ela é omitida aqui.

```
aws ec2 describe-instance-types \
    --instance-types t2.micro \
    --region us-east-2
```

Elas descrevem um tipo de instância e filtram a saída

O comando a seguir exibe os detalhes da rede para o tipo de instância especificado.

```
aws ec2 describe-instance-types \
    --instance-types t2.micro \
    --region us-east-2 \
    --query "InstanceTypes[].NetworkInfo"
```

O seguinte é um exemplo de saída.

```
[
    {
        "NetworkPerformance": "Low to Moderate",
        "MaximumNetworkInterfaces": 2,
        "MaximumNetworkCards": 1,
        "DefaultNetworkCardIndex": 0,
        "NetworkCards": [
            {
                "NetworkCardIndex": 0,
                "NetworkPerformance": "Low to Moderate",
                "MaximumNetworkInterfaces": 2,
                "BaselineBandwidthInGbps": 0.064,
                "PeakBandwidthInGbps": 1.024
            }
        ],
        "Ipv4AddressesPerInterface": 2,
        "Ipv6AddressesPerInterface": 2,
        "Ipv6Supported": true,
        "EnaSupport": "unsupported",
        "EfaSupported": false,
        "EncryptionInTransitSupported": false,
        "EnaSrdSupported": false
    }
]
```

O comando a seguir exibe a memória disponível para o tipo de instância especificado.

```
aws ec2 describe-instance-types \
    --instance-types t2.micro \
    --region us-east-2 \
    --query "InstanceTypes[].MemoryInfo"
```

O seguinte é um exemplo de saída.

```
[
    {
        "SizeInMiB": 1024
    }
]
```

Encontrar um tipo de instância usando a AWS CLI

Você pode usar os comandos describe-instance-types e describe-instance-type-offerings para encontrar os tipos de instância que atendem às suas necessidades.

Exemplos

- Exemplo 1: encontrar um tipo de instância por zona de disponibilidade
- Exemplo 2: encontrar um tipo de instância por tamanho de memória disponível
- Exemplo 3: encontrar um tipo de instância por armazenamento de instância disponível
- Exemplo 4: encontrar um tipo de instância compatível com hibernação

Exemplo 1: encontrar um tipo de instância por zona de disponibilidade

O exemplo a seguir exibe somente os tipos de instância oferecidos na zona de disponibilidade especificada.

```
aws ec2 describe-instance-type-offerings \
    --location-type "availability-zone" \
    --filters "Name=location,Values=us-east-2a" \
    --region us-east-2 \
    --query "InstanceTypeOfferings[*].[InstanceType]" --output text | sort
```

A saída é uma lista de tipos de instâncias ordenadas alfabeticamente. Veja a seguir apenas o início da saída da chamada.

```
a1.2xlarge
a1.4xlarge
a1.large
a1.medium
a1.metal
a1.xlarge
c4.2xlarge
```

```
   ...
```

Exemplo 2: encontrar um tipo de instância por tamanho de memória disponível

O exemplo a seguir exibe somente os tipos de instância da geração atual com 64 GiB (65.536 MiB) de memória.

```
aws ec2 describe-instance-types \
    --filters "Name=current-generation,Values=true" "Name=memory-info.size-in-
mib,Values=65536" \
    --region us-east-2 \
    --query "InstanceTypes[*].[InstanceType]" --output text | sort
```

A saída é uma lista de tipos de instâncias ordenadas alfabeticamente. Veja a seguir apenas o início da saída da chamada.

```
c5a.8xlarge
c5ad.8xlarge
c6a.8xlarge
c6g.8xlarge
c6gd.8xlarge
c6gn.8xlarge
c6i.8xlarge
c6id.8xlarge
c6in.8xlarge
   ...
```

Exemplo 3: encontrar um tipo de instância por armazenamento de instância disponível

O exemplo a seguir exibe o tamanho total do armazenamento de instâncias para todas as instâncias R7 com volumes de armazenamento de instâncias.

```
aws ec2 describe-instance-types \
    --filters "Name=instance-type,Values=r7*" "Name=instance-storage-
supported,Values=true" \
    --region us-east-2 \
    --query "InstanceTypes[].[InstanceType, InstanceStorageInfo.TotalSizeInGB]" \
    --output table
```

O seguinte é um exemplo de saída.

```
---------------------------
```

```
|  DescribeInstanceTypes  |
+-----------------+--------+
|  r7gd.xlarge    |  237   |
|  r7gd.8xlarge   |  1900  |
|  r7gd.16xlarge  |  3800  |
|  r7gd.medium    |  59    |
|  r7gd.4xlarge   |  950   |
|  r7gd.2xlarge   |  474   |
|  r7gd.metal     |  3800  |
|  r7gd.large     |  118   |
|  r7gd.12xlarge  |  2850  |
+-----------------+--------+
```

Exemplo 4: encontrar um tipo de instância compatível com hibernação

O exemplo a seguir exibe os tipos de instância compatíveis com hibernação.

```
aws ec2 describe-instance-types \
    --filters "Name=hibernation-supported,Values=true" \
    --region us-east-2 \
    --query "InstanceTypes[*].[InstanceType]" \
    --output text | sort
```

A saída é uma lista de tipos de instâncias ordenadas alfabeticamente. Veja a seguir apenas o início da saída da chamada.

```
c4.2xlarge
c4.4xlarge
c4.8xlarge
c4.large
c4.xlarge
c5.12xlarge
c5.18xlarge
c5.2xlarge
c5.4xlarge
c5.9xlarge
...
```

Encontrar um tipo de instância usando as Ferramentas para PowerShell

É possível usar os cmdlets Get-EC2InstanceType e Get-EC2InstanceTypeOffering para encontrar os tipos de instância que atendem às suas necessidades.

Exemplos

- Encontrar um tipo de instância por zona de disponibilidade
- Encontrar um tipo de instância por tamanho de memória disponível
- Encontrar um tipo de instância por armazenamento de instância disponível
- Encontrar um tipo de instância compatível com hibernação

Encontrar um tipo de instância por zona de disponibilidade

O exemplo a seguir exibe somente os tipos de instância oferecidos na zona de disponibilidade especificada.

```
(Get-EC2InstanceTypeOffering `
    -LocationType "availability-zone" `
    -Region us-east-2 `
    -Filter @{Name="location"; Values="us-east-2a"}).InstanceType | Sort-Object `
```

Encontrar um tipo de instância por tamanho de memória disponível

O exemplo a seguir exibe somente os tipos de instância da geração atual com 64 GiB (65.536 MiB) de memória.

```
(Get-EC2InstanceType `
    -Filter @{Name="current-generation"; Values="true"},
            @{Name="memory-info.size-in-mib"; Values="65536"}).InstanceType | Sort-
Object
```

Encontrar um tipo de instância por armazenamento de instância disponível

O exemplo a seguir exibe o tamanho total do armazenamento de instâncias para todas as instâncias R7 com volumes de armazenamento de instâncias.

```
Get-EC2InstanceType `
    -Filter @{Name="instance-type"; Values="r7*"},
            @{Name="instance-storage-supported"; Values="true"} | `
     Select InstanceType, @{Name="TotalSizeInGB";
 Expression={($_.InstanceStorageInfo.TotalSizeInGB)}}
```

O seguinte é um exemplo de saída.

```
InstanceType  TotalSizeInGB
------------  -------------
r7gd.8xlarge           1900
r7gd.16xlarge          3800
r7gd.xlarge             237
r7gd.4xlarge            950
r7gd.medium              59
r7gd.2xlarge            474
r7gd.large              118
r7gd.metal             3800
r7gd.12xlarge          2850
```

Encontrar um tipo de instância compatível com hibernação

O exemplo a seguir exibe os tipos de instância compatíveis com hibernação.

```
(Get-EC2InstanceType `
    -Filter @{Name="hibernation-supported"; Values="true"}).InstanceType | Sort-Object
```

Obtenha recomendações do localizador de tipo de instância do EC2

O assistente de seleção de tipo de instância do EC2 considera o caso de uso, o tipo de workload, a preferência do fabricante da CPU e como você prioriza preço e desempenho, bem como os parâmetros adicionais que você pode especificar. Em seguida, ele usa esses dados para fornecer sugestões e orientações sobre os tipos de instância do Amazon EC2 mais adequados às suas novas workloads.

Com tantos tipos de instância disponíveis, encontrar os tipos de instância mais adequados para sua workload pode ser demorado e complexo. Ao usar o assistente de seleção de tipo de instância do EC2, é possível se manter atualizado com os tipos de instância mais recentes e obter a melhor relação entre preço e desempenho para as workloads.

Você pode obter sugestões e orientações para tipos de instância do EC2 usando o console do Amazon EC2. Você também pode ir diretamente ao Amazon Q para obter conselhos sobre tipos de instância. Para obter mais informações, consulte o Guia do usuário do Amazon Q Developer.

Se você estiver procurando recomendações de tipo de instância para uma workload existente, use o AWS Compute Optimizer. Para ter mais informações, consulte Obter as recomendações de instâncias do EC2 no Compute Optimizer.

Usar o assistente de seleção de tipo de instância do EC2

No console do Amazon EC2, é possível obter sugestões de tipos de instância do assistente de seleção de tipo de instância do EC2 no assistente de inicialização de instâncias ao criar um modelo de execução ou na página Tipos de instância.

Use as instruções apresentadas a seguir para obter sugestões e orientações para os tipos de instância do EC2 usando o assistente de seleção de tipo de instância do EC2 no console do Amazon EC2. Para visualizar uma animação dessas etapas, consulte Veja uma animação: como receber sugestões de tipos de instância usando o assistente de seleção de tipo de instância do EC2.

Para obter sugestões de tipos de instância usando o assistente de seleção de tipo de instância do EC2

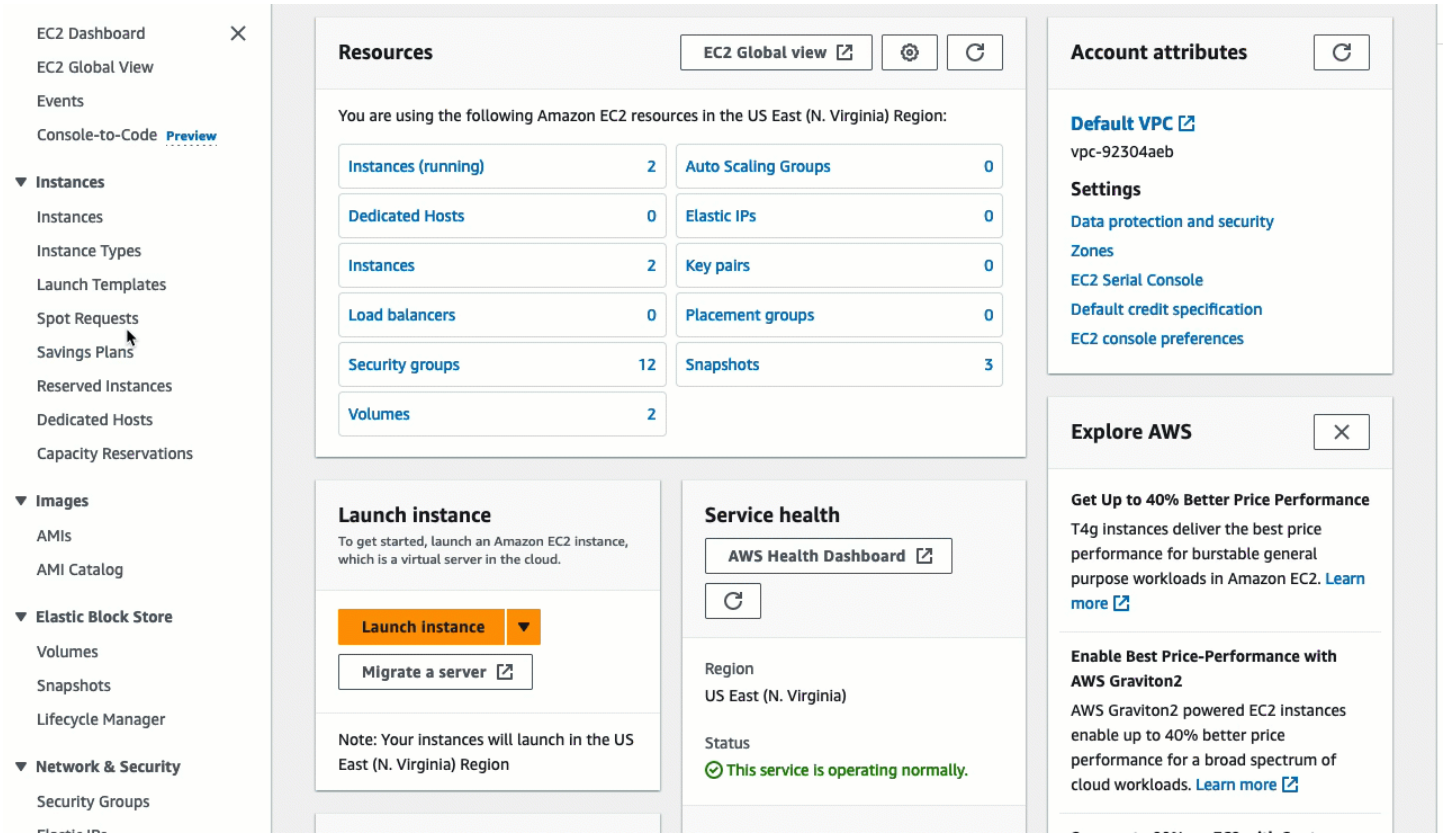
1. Inicie o processo usando qualquer um dos seguintes:
   - Siga o procedimento para iniciar uma instância. Ao lado de Tipo de instância, escolha o link Obter conselho.
   - Siga o procedimento para criar um modelo de execução. Ao lado de Tipo de instância, escolha o link Obter conselho.
   - No painel de navegação, escolha Tipos de instância e, em seguida, escolha o botão Assistente de seleção de tipo de instância.
2. Na tela Obter conselhos sobre a seleção do tipo de instância, faça o seguinte:
   a. Especifique os requisitos de tipo de instância ao selecionar opções para Tipo de workload, Caso de uso, Prioridade e Fabricantes de CPU.
   b. (Opcional) Para especificar requisitos mais detalhados para a workload, faça o seguinte:
      i. Expanda Parâmetros avançados.
      ii. Para adicionar um parâmetro, selecione um parâmetro, escolha Adicionar e especifique um valor para o parâmetro. Repita para cada parâmetro adicional que você deseja adicionar. Para não indicar um valor mínimo ou máximo, deixe o campo vazio.
      iii. Para remover um parâmetro após adicioná-lo, escolha o símbolo X ao lado do parâmetro.
   c. Escolha Obter conselho sobre tipo de instância.

      O Amazon EC2 fornece sugestões de famílias de instâncias que atendem aos requisitos especificados.

3. Para visualizar os detalhes de cada tipo de instância nas famílias de instâncias sugeridas, escolha Exibir detalhes recomendados da família de instâncias.
4. Selecione um tipo de instância que atenda aos seus requisitos e escolha Ações e Executar instância ou Ações e Criar modelo de execução.

   Como alternativa, se você iniciou o processo no assistente de inicialização de instâncias ou na página do modelo de execução e prefere retornar para o fluxo original, faça uma anotação do tipo de instância que deseja usar. Em seguida, no assistente de inicialização de instâncias ou no modelo de execução, em Tipo de instância, escolha o tipo de instância e conclua o procedimento para iniciar uma instância ou criar um modelo de execução.

Veja uma animação: como receber sugestões de tipos de instância usando o assistente de seleção de tipo de instância do EC2



Obter as recomendações de instâncias do EC2 no Compute Optimizer

O AWS Compute Optimizer fornece recomendações do Amazon EC2 para ajudar a melhorar a performance, a economizar dinheiro ou as duas coisas. Você pode usar essas recomendações para decidir se deseja mudar para um novo tipo de instância.

Para fazer recomendações, o Compute Optimizer analisa as especificações de instância existentes e as métricas de utilização. Os dados compilados são usados para recomendar quais tipos de instância do Amazon EC2 são melhores para lidar com a workload existente. As recomendações são retornadas com a definição de preço de instância por hora. Para obter mais informações, consulte Amazon EC2 instance metrics no Guia do usuário do AWS Compute Optimizer.

Conteúdo

- Requisitos
- Classificações de descobertas
- Exibir recomendações
- Considerações para avaliação das recomendações

Requisitos

Para obter recomendações do Compute Optimizer, primeiro é necessário optar pelo Compute Optimizer. Para obter mais informações, consulte Conceitos básicos do AWS Compute Optimizer no Manual do usuário do AWS Compute Optimizer.

O Compute Optimizer gera recomendações para alguns tipos de instâncias, mas não para todos os tipos. Se você estiver usando um tipo de instância não compatível, o Compute Optimizer não vai gerar recomendações. Para ver a lista de tipos de instância compatíveis, consulte Amazon EC2 instance requirements no Guia do usuário do AWS Compute Optimizer.

Classificações de descobertas

O Compute Optimizer classifica suas descobertas para instâncias do EC2 da seguinte forma:

- Under-provisioned (Subprovisionada) – uma instância do EC2 será considerada subprovisionada quando pelo menos uma especificação, como CPU, memória ou rede, não atender aos requisitos de performance de sua workload. Instâncias do EC2 subprovisionadas podem gerar performance ruim da aplicação.
- Over-provisioned (Superprovisionada) – uma instância do EC2 será considerada superprovisionada quando pelo menos uma especificação, como CPU, memória ou rede, puder ser reduzida sem deixar de atender aos requisitos de performance de sua workload e quando nenhuma especificação estiver subprovisionada. Instâncias do EC2 superprovisionadas podem gerar custos desnecessários de infraestrutura.

- Optimized (Otimizada) – uma instância do EC2 será considerada otimizada quando todas as especificações, como CPU, memória e rede, atenderem aos requisitos de performance de sua workload e a instância não estiver superprovisionada. Uma instância do EC2 otimizada executa suas workloads com performance e custo de infraestrutura ideais. Para instâncias otimizadas, o Compute Optimizer às vezes pode recomendar um tipo de instância de nova geração.
- None (Nenhum) – não há recomendações para essa instância. Isso pode ocorrer se você tiver optado pelo Compute Optimizer há menos de 12 horas, quando a instância estiver sendo executada há menos de 30 horas ou quando o tipo de instância não for compatível com o Compute Optimizer.

Exibir recomendações

Depois de optar pelo Compute Optimizer, você poderá visualizar as descobertas que o Compute Optimizer gera para as instâncias do EC2 no console do Amazon EC2. Depois, será possível acessar o console do Compute Optimizer para visualizar as recomendações. Caso tenha realizado a opção recentemente, as descobertas poderão não ser refletidas no console do EC2 durante até 12 horas.

Para visualizar recomendações para uma instância 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. Escolha o ID da instância para abrir a página de detalhes da instância.
4. Na página de detalhes da instância, na seção de resumo superior, localize AWS Compute Optimizer finding. Se houver uma descoberta, exibiremos a classificação da descoberta e um link para ver os detalhes. Caso contrário, exibiremos Nenhuma recomendação disponível para essa instância.
5. Se houver uma descoberta, escolha Visualizar detalhes. Isso abre a página Recomendações para instâncias do EC2 no console do Compute Optimizer. O tipo de instância atual é rotulado como Atual. Há também até três recomendações de tipo de instância, rotuladas como Opção 1, Opção 2 e Opção 3. Essa página também mostra dados de métricas recentes do CloudWatch para a instância.

Para visualizar as recomendações para todas as instâncias em todas as regiões

Você pode visualizar recomendações para todas as instâncias do Amazon EC2 em todas as regiões usando o console do Compute Optimizer. Para obter mais informações, consulte Viewing EC2 instances recommendations e Viewing EC2 instance details no Guia do usuário do AWS Compute Optimizer.

Considerações para avaliação das recomendações

Ao receber uma recomendação, você deve decidir se deve agir de acordo com ela. Antes de alterar um tipo de instância, considere o seguinte:

- As recomendações não preveem seu uso. As recomendações são baseadas em seu histórico de uso durante os últimos 14 dias. Escolha um tipo de instância que tenha a expectativa de atender às suas necessidades futuras de recursos.
- Concentre-se nas métricas gráficas para determinar se o uso real é menor do que a capacidade da instância. Também é possível visualizar dados de métricas (média, pico, percentil) no CloudWatch para aprofundar a avaliação de suas recomendações de instâncias do EC2. Por exemplo, observe como as métricas de porcentagem da CPU mudam durante o dia e se há picos que precisem ser acomodados. Para obter mais informações, consulte Visualizar métricas disponíveis no Guia do usuário do Amazon CloudWatch.
- O Compute Optimizer pode fornecer recomendações para instâncias expansíveis, que são as instâncias T3, T3a e T2. Se você ultrapassa periodicamente a linha de base, verifique se poderá continuar a fazer isso com base nas vCPUs do novo tipo de instância. Para ter mais informações, consulte Principais conceitos para instâncias de desempenho expansível.
- Se você comprou uma Instância reservada, sua instância sob demanda poderá ser cobrada como uma Instância reservada. Antes de alterar o tipo de instância atual, avalie o impacto sobre o uso e a cobertura da Instância reservada.
- Considere conversões para instâncias da geração mais recente, sempre que possível.
- Ao migrar para uma família de instâncias diferente, verifique se o tipo de instância atual e o novo tipo de instância são compatíveis, por exemplo, em termos de virtualização, arquitetura ou tipo de rede. Para ter mais informações, consulte Compatibilidade para alterar o tipo de instância.
- Por fim, considere a classificação de risco de performance fornecida para cada recomendação. O risco de performance indica o esforço necessário para validar se o tipo de instância recomendado atende aos requisitos de performance da sua workload. Também recomendamos testes rigorosos de carga e performance antes e depois de fazer quaisquer alterações.

Alterações no tipo de instância do Amazon EC2

À medida que suas necessidades mudarem, é possível descobrir que a instância está sobreutilizada (o tipo de instância é muito pequeno) ou subutilizada (o tipo de instância é muito grande). Se esse for o caso, será possível redimensionar a sua instância alterando o seu tipo de instância. Por exemplo, se a instância `t2.micro` for muito pequena para sua workload, é possível alterar o tamanho a para um tipo de instância T2 maior, como um `t2.large`. Ou é possível alterá-lo para outro tipo de instância, como `m5.large`. Também é possível migrar de um tipo de instância de uma geração anterior para um tipo de instância da geração atual para aproveitar alguns recursos, por exemplo, suporte para IPv6.

Se você quiser uma recomendação para um tipo de instância que esteja mais apto a lidar com sua workload existente, é possível usar o AWS Compute Optimizer. Para obter mais informações, consulte Obter as recomendações de instâncias do EC2 no Compute Optimizer.

Ao alterar o tipo de instância, você começará a pagar a taxa do novo tipo de instância. Para obter as taxas sob demanda para todos os tipos de instância, consulte Preço sob demanda do Amazon EC2.

Para adicionar armazenamento extra à sua instância sem alterar o tipo de instância, adicione um volume do EBS à instância. Para obter mais informações, consulte Associar um volume do Amazon EBS a uma instância no Guia do usuário do Amazon EBS.

Quais as instruções a serem seguidas?

Existem instruções diferentes para alterar o tipo de instância. As instruções a serem usadas dependem do volume raiz da instância e se o tipo de instância é compatível com a configuração atual da instância. Para obter informações sobre como a compatibilidade é determinada, consulte Compatibilidade para alterar o tipo de instância.

Use a tabela a seguir para determinar quais instruções seguir.

Volume raiz	Compatibilidade	Siga estas instruções
EBS	Compatível	Alterar o tipo de instância
EBS	Não compatível	Migrar para um novo tipo de instância
Armazenamento de instâncias	Não aplicável	Migrar para um novo tipo de instância

Compatibilidade para alterar o tipo de instância

Você só pode alterar o tipo de instância se a configuração atual da instância for compatível com tipo de instância desejado. Se o tipo de instância que você deseja não for compatível com a configuração atual da instância, é necessário iniciar uma nova instância com uma configuração que seja compatível com o tipo de instância e, em seguida, migrar sua aplicação para a nova instância.

A compatibilidade é determinada da seguinte maneira:

Tipo de virtualização

As AMIs do Linux usam um dos dois tipos de virtualização: paravirtual (PV) ou máquina virtual de hardware (HVM). Se uma instância foi iniciada em uma AMI PV, você não poderá alterar para um tipo de instância que seja somente HVM. Para obter mais informações, consulte Tipos de virtualização. Para conferir o tipo de virtualização da instância, confira o valor do campo Virtualization (Virtualização) no painel de detalhes da tela Instances (Instâncias) no console do Amazon EC2.

Arquitetura

As AMIs são específicas da arquitetura do processador, portanto, é necessário selecionar um tipo de instância com a mesma arquitetura de processador que o tipo da instância atual. Por exemplo:

- Se o tipo de instância atual tiver um processador baseado na arquitetura Arm, você estará limitado aos tipos de instância que oferecem suporte a um processador baseado na arquitetura Arm, como o C6g e M6g.
- Os seguintes tipos de instância são os únicos tipos de instância que oferecem suporte a AMIs de 32 bits: `t2.nano`, `t2.micro`, `t2.small`, `t2.medium`, `c3.large`, `t1.micro`, `m1.small`, `m1.medium` e `c1.medium`. Se estiver alterando o tipo de instância de uma instância de 32 bits, você estará limitado a esses tipos de instância.

Adaptadores de rede

Se você alternar de um driver de um adaptador de rede para outro, as configurações do adaptador de rede serão redefinidas quando o sistema operacional criar o novo adaptador. Para redefinir as configurações, talvez seja necessário ter acesso a uma conta local com permissões de administrador. Veja a seguir exemplos de mudança de um adaptador de rede para outro:

- AWS PV (instâncias T2) para Intel 82599 VF (instâncias M4)
- Intel 82599 VF (maioria das instâncias M4) para ENA (instâncias M5)
- ENA (instâncias M5) para ENA de alta largura de banda (instâncias M5n)

Redes avançadas

Tipos de instância que oferecem suporte a redes avançadas exigem que os drivers necessários estejam instalados. Por exemplo, as instâncias baseadas em Nitro precisam de AMIs baseadas no EBS com os drivers do Adaptador de Rede Elástica (ENA) instalados. Para alterar de um tipo de instância sem suporte para redes avançadas para um tipo com suporte para redes avançadas, é necessário instalar os drivers ENA ou os drivers ixgbevf na instância, conforme apropriado.

> **Note**
>
> Quando você redimensiona uma instância com o ENA Express habilitado, o novo tipo de instância também deve ser compatível com o ENA Express. Para obter uma lista dos tipos de instâncias compatíveis com o ENA Express, consulte Tipos de instâncias compatíveis com o ENA Express.
> Para alterar de um tipo de instância compatível com o ENA Express para um tipo de instância não compatível com o ENA Express, certifique-se de que o ENA Express não esteja habilitado antes de você redimensionar a instância.

NVMe

Os volumes do EBS são expostos como dispositivos de blocos NVMe em Instâncias baseadas em Nitro. Se você alterar de um tipo de instância sem suporte para NVMe para um tipo de instância com suporte para NVMe, deverá primeiro instalar os drivers NVMe na sua instância. Além disso, os nomes dos dispositivos para os dispositivos especificados no mapeamento de dispositivos de blocos são renomeados usando nomes de dispositivos NVMe (`/dev/nvme[0-26]n1`).

[Instâncias do Linux] Portanto, para a montagem de sistemas de arquivos no momento da inicialização usando `/etc/fstab`, você deve utilizar um UUID, ou um rótulo, em vez de nomes de dispositivos.

Limite de volume

O número máximo de volumes do Amazon EBS que é possível anexar a uma instância depende do tipo e do tamanho da instância. Para obter mais informações, consulte Limites de volume do Amazon EBS para instâncias do Amazon EC2.

Só é possível mudar para um tipo ou tamanho de instância que ofereça suporte ao mesmo número ou a um número maior de volumes do que os anexados à instância

no momento. Se você mudar para um tipo ou tamanho de instância que não ofereça suporte ao número de volumes anexados no momento, a solicitação falhará. Por exemplo, se você mudar de uma instância `m7i.4xlarge` com 32 volumes anexados para uma instância `m6i.4xlarge` compatível com um máximo de 27 volumes, a solicitação falhará.

NitroTPM

Se você tiver inicializado a instância usando uma AMI com NitroTPM habilitado e com um tipo de instância compatível com o NitroTPM, a instância será inicializada com o NitroTPM habilitado. Você só pode mudar para um tipo de instância que também seja compatível com o NitroTPM.

Alterar o tipo de instância para a instância do Amazon EC2

Use as instruções a seguir para alterar o tipo de instância de uma instância baseada no Amazon EBS caso o tipo de instância de que precisa seja compatível com a configuração atual da instância. Para obter mais informações, consulte the section called “Compatibilidade”.

Considerações

- Você deve interromper a instância antes de poder alterar o tipo da instância. Planeje tempo de inatividade enquanto a instância estiver parada. Interromper a instância e alterar o tipo de instância pode levar alguns minutos, e o tempo necessário para iniciar a instância pode variar dependendo dos scripts de startup da aplicação. Para obter mais informações, consulte Início e interrupção de instâncias do Amazon EC2.
- Quando você interrompe e inicia uma instância, nós movemos a instância para um novo hardware. Se sua instância tiver um endereço IPv4 público que não seja um IP elástico, nós liberamos o endereço e damos à instância um novo endereço IPv4 público. Para obter mais informações sobre o comportamento do endereço IP em todo o ciclo de vida de uma instância, consulte Diferenças entre os estados de instâncias.
- Você não pode alterar o tipo de instância de uma instância spot.
- [Instâncias do Windows] Recomendamos atualizar o pacote de driver PV da AWS antes de alterar o tipo de instância. Para obter mais informações, consulte the section called “Atualizar drivers de PV”.
- Se a 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 de substituição. Para evitar isso, é possível suspender os processos de escalabilidade para o grupo enquanto estiver alterando o tipo de instância. Para obter mais informações, consulte

Suspensão e retomada de um processo para um grupo do Auto Scaling no Guia do usuário do Amazon EC2 Auto Scaling.

- Quando você altera o tipo de instância de uma instância com volumes de armazenamento de instâncias NVMe, a instância atualizada pode ter volumes adicionais de armazenamento, pois todos os volumes de armazenamento de instâncias NVMe estão disponíveis mesmo que não estejam especificados na AMI ou no mapeamento de dispositivos de blocos de instâncias. Caso contrário, a instância atualizada tem o mesmo número de volumes de armazenamento de instância que você especificou ao iniciar a instância original.
- O número máximo de volumes do Amazon EBS que é possível anexar a uma instância depende do tipo e do tamanho da instância. Não é possível mudar para um tipo ou tamanho de instância que não ofereça suporte ao número de volumes que já estão conectados à sua instância. Para obter mais informações, consulte Limites de volume do Amazon EBS para instâncias do Amazon EC2.
- [Instâncias do Linux] é possível usar o runbook `AWSSupport-MigrateXenToNitroLinux` para migrar instâncias do Linux compatíveis de um tipo de instância do Xen para um tipo de instância do Nitro. Para obter mais informações, consulte AWSSupport-MigrateXenToNitroLinux runbook na Referência do runbook do AWS Systems Manager Automation.
- [Instâncias do Windows] Para obter orientações adicionais sobre a migração de instâncias do Windows compatíveis de um tipo de instância do Xen para um tipo de instância do Nitro, consulte Migrate to latest generation instance types.

Para alterar o tipo de instância de uma instância baseada no Amazon EBS

1. (Opcional) Se o tipo de instância requer drivers que não estejam instalados na instância atual, é necessário se conectar à sua instância e instalar os drivers primeiro. Para obter mais informações, consulte Compatibilidade para alterar o tipo de instância.
2. [Instâncias do Windows] Se você configurou a instância do Windows para usar o endereçamento IP estático e alterar de um tipo de instância que não é compatível com as redes aperfeiçoadas para um tipo de instância que é compatível com as redes aperfeiçoadas, você poderá receber um aviso sobre um possível conflito de endereço IP ao reconfigurar o endereçamento IP estático. Para evitar isso, habilite o DHCP na interface de rede da instância antes de alterar o tipo de instância. Na sua instância, abra a Network and Sharing Center (Central de rede e compartilhamento), vá para Internet Protocol Version 4 (TCP/IPv4) Properties (Propriedades do protocolo IP versão 4 (TCP/IPv4)) para a interface de rede e escolha Obtain an IP address

automatically (Obter um endereço IP automaticamente). Altere o tipo de instância e reconfigure o endereçamento IP estático na interface de rede.

3. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
4. No painel de navegação, escolha Instances (Instâncias).
5. Selecione a instância e escolha Estado da instância e Parar instância. Quando a confirmação for solicitada, escolha Parar. Pode demorar alguns minutos para que a instância pare.
6. Com a instância ainda selecionada, escolha Actions (Ações), Instance settings (Configurações de instância), Change instance type (Alterar tipo de instância). Essa ação ficará esmaecida se o estado da instância não for `stopped`.
7. Em Change Instance Type (Alterar tipo de instância), faça o seguinte:

   a. Em Instance type (Tipo de instância), selecione o tipo de instância desejado.

      Se o tipo de instância não estiver na lista, ele não é compatível com a configuração da sua instância. Em vez disso, use as seguintes instruções: Migrar para um novo tipo de instância executando uma nova instância do EC2.

   b. (Opcional) Se o tipo de instância selecionado oferecer suporte à otimização para EBS, selecione EBS-optimized (Otimizado para EBS) ou desmarque a opção EBS-optimized (Otimizado para EBS) 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 desfazer a seleção.

   c. (Opcional) Configure as opções de vCPU no novo tipo de instância.

      Ao alterar o tipo de instância de uma instância existente, o Amazon EC2 aplica as configurações de opções de CPU da instância existente à nova instância, se possível. Se o novo tipo de instância não for compatível com essas configurações, as opções de CPU serão redefinidas como Nenhum. Essa opção usa o número padrão de vCPUs para o novo tipo de instância.

      Se o tipo de instância selecionado for compatível com a configuração de vCPU, selecione Especificar opções de CPU no painel Detalhes avançados para configurar vCPUs para seu novo tipo de instância.

   d. Escolha Alterar para aceitar as novas configurações.
8. Para iniciar a instância, selecione a instância e escolha Instance state (Estado da instância) e Start instance (Iniciar instância). Pode demorar alguns minutos para que a instância entre no

estado `running`. Se a instância não iniciar, consulte Solucionar problemas de alteração de tipo de instância.

9. [Instâncias do Windows] Se a instância executar o Windows Server 2016 ou o Windows Server 2019 com EC2Launch v1, conecte-se à sua instância do Windows e execute o script do PowerShell para EC2Launch, apresentado a seguir, a fim de configurar a instância depois que o tipo de instância for alterado.

> **Important**
>
> A senha do administrador será redefinida quando você habilitar o script de inicialização do EC2 da instância. É possível modificar o arquivo de configuração para desabilitar a redefinição da senha do administrador especificando-a nas configurações das tarefas de inicialização. Para obter as etapas para desabilitar a redefinição de senha, consulte Configure initialization tasks (EC2Launch) ou Change settings (EC2Launch v2).

```
PS C:\> C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeInstance.ps1 -
Schedule
```

Migrar para um novo tipo de instância executando uma nova instância do EC2

Você poderá alterar o tipo de instância de uma instância do EC2 somente se for uma instância baseada no EBS com uma configuração que seja compatível com o novo tipo de instância desejado. Caso contrário, se a configuração ou sua instância não for compatível com o novo tipo de instância, ou se for uma instância baseada em armazenamento de instância, você deverá executar uma instância de substituição que seja compatível com o tipo de instância desejado. Para obter informações sobre como a compatibilidade é determinada, consulte Compatibilidade para alterar o tipo de instância.

Visão geral do processo de migração

- Faça backup dos dados na instância original.
- Execute uma nova instância com uma configuração que seja compatível com o novo tipo de instância desejado e anexe todos os volumes do EBS que estavam anexados à instância original.
- Instale sua aplicação na nova instância.
- Restaure todos os dados.

- Se a instância original tiver um endereço IP elástico, você deve associá-la à nova instância para garantir que os usuários possam continuar a usar a aplicação sem interrupção.

Para migrar uma instância para uma nova instância

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Faça backup dos dados de que ainda precisa da seguinte forma:
   - Conecte-se à instância e copie os dados nos volumes do armazenamento de instância para o armazenamento persistente.
   - Crie snapshots dos volumes do EBS para que você possa criar novos volumes com os mesmos dados, ou desanexe os volumes da instância para que possa anexá-los à nova instância.
3. No painel de navegação, escolha Instâncias.
4. Selecione Iniciar instâncias. Quando configurar as instâncias, faça o seguinte:
   a. Selecione uma AMI que seja compatível com o tipo de instância desejado. Por exemplo, você deve selecionar uma AMI que seja compatível com o tipo de processador do novo tipo de instância. Além disso, os tipos de instância da geração atual requerem uma AMI de HVM.
   b. Selecione o novo tipo de instância desejado. Se o tipo de instância desejado não estiver disponível, ele não é compatível com a configuração da AMI selecionada.
   c. Se quiser permitir que algum tráfego alcance a nova instância, selecione a mesma VPC e o grupo de segurança usados com a instância original.
   d. Quando terminar de configurar sua nova instância, execute as etapas para selecionar um par de chaves e inicie sua instância. Pode demorar alguns minutos para que a instância entre no estado `running`.
5. Se você fez backup dos dados em um snapshot do EBS, crie um volume do snapshot e, em seguida, anexe o volume à nova instância.

   Para mover um volume do EBS da instância original para a nova instância, desanexe o volume da instância original e, em seguida, anexe o volume à nova instância.
6. Instale sua aplicação e o software necessário na nova instância.
7. Restaure todos os dados dos quais você fez backup dos volumes de armazenamento de instâncias da instância original.

8. Se a instância original tiver um endereço IP elástico, atribua-o à nova instância da seguinte maneira:

   a. No painel de navegação, escolha IPs elásticos.

   b. Selecione o endereço IP elástico que está associado à instância original e escolha Actions (Ações) e Disassociate Elastic IP address (Desassociar endereço IP elástico). Quando a confirmação for solicitada, escolha Disassociate (Desassociar).

   c. Com o endereço IP elástico ainda selecionado, escolha Actions (Ações) e Associate Elastic IP address (Associar endereço IP elástico).

   d. Em Resource type (Tipo de recurso), escolha Instance (Instância).

   e. Em Instância, escolha a nova instância.

   f. (Opcional) Em Private IP address (Endereço IP privado), especifique um endereço IP privado ao qual associar o endereço IP elástico.

   g. Escolha Associate.

9. (Opcional) É possível encerrar a instância original se ela não for mais necessária. Selecione a instância e confirme que está prestes a terminar a instância original e não a nova instância (por exemplo, confira o nome ou a hora do lançamento) e depois escolha Instance state (Estado da instância), Terminate instance (Terminar instância).

Solucionar problemas de alteração de tipo de instância

Use as informações a seguir para ajudar a diagnosticar e corrigir os problemas que podem ocorrer com a alteração do tipo de instância.

A instância não inicia após a alteração do tipo de instância

Causa possível: requisitos de novo tipo de instância não atendidos

Se a sua instância não inicializar, é possível que um dos requisitos de novo tipo de instância não tenha sido atendido. Para obter mais informações, consulte Por que minha instância do Linux não está inicializando depois que mudei seu tipo?

Causa possível: a AMI não oferece suporte para o tipo de instância

Se você usar o console do EC2 para alterar o tipo de instância, somente os tipos de instância com suporte pela AMI selecionada estarão disponíveis. Porém, se você usar a AWS CLI para iniciar uma instância, é possível especificar uma AMI e um tipo de instância incompatíveis. Se

a AMI e o tipo de instância forem incompatíveis, a instância não poderá ser iniciada. Para obter mais informações, consulte Compatibilidade para alterar o tipo de instância.

Causa possível: a instância está no grupo de posicionamento de cluster

Se sua instância estiver em um grupo de posicionamento de cluster e, após a alteração do tipo de instância, a instância não iniciar, tente o seguinte:

1. Interrompa todas as instâncias no grupo de posicionamento de cluster.
2. Altere o tipo de instância da instância afetada.
3. Inicie todas as instâncias no grupo de posicionamento de cluster.

Aplicação ou site não acessíveis na Internet após a alteração do tipo de instância

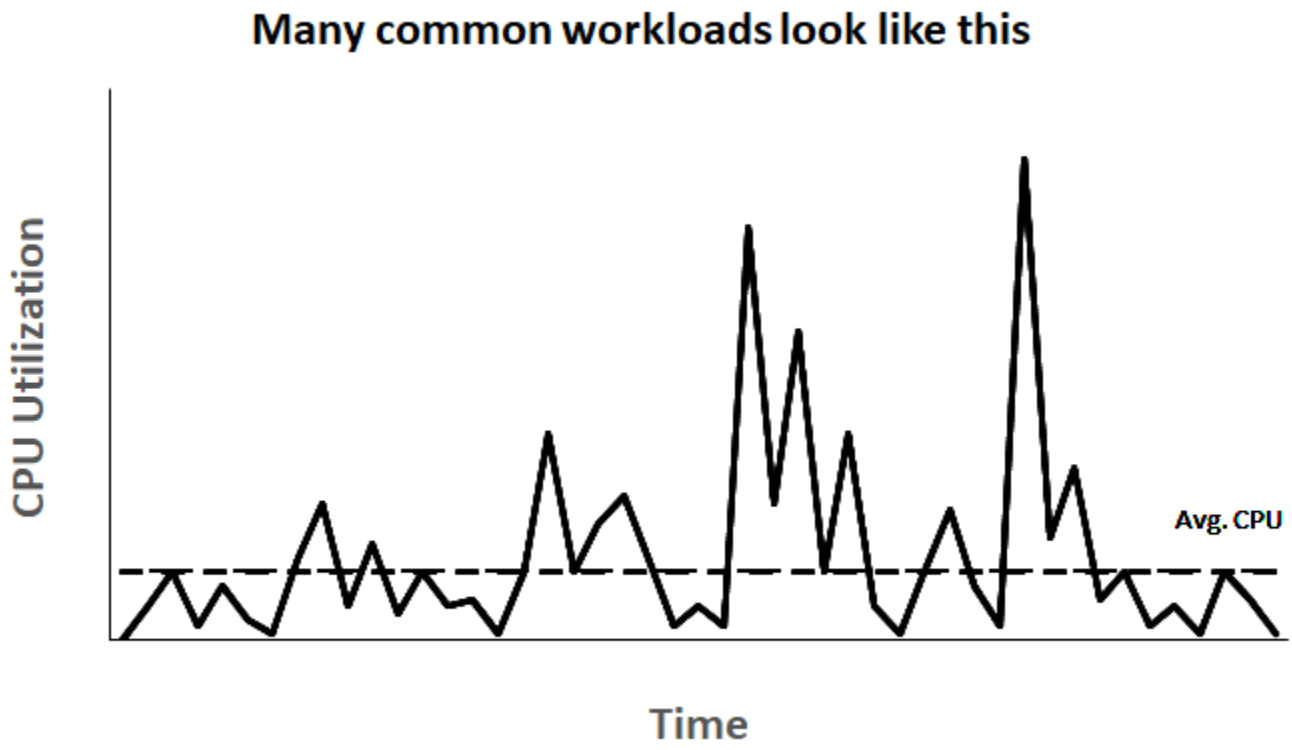
Causa possível: o endereço IPv4 público foi liberado

Quando altera o tipo de instância, primeiro é necessário interromper a instância. Quando você interrompe uma instância, liberamos o endereço IPv4 público e fornecemos a sua instância um novo endereço IPv4 público.

Para reter o endereço IPv4 público entre as interrupções e inicializações da instância, recomendamos que você use um endereço de IP elástico, sem nenhum custo extra, desde que sua instância esteja em execução. Para obter mais informações, consulte Endereços IP elásticos.

Instâncias expansíveis

Muitas workloads de uso geral não estão, em média, ocupadas e não exigem alto nível de performance da CPU sustentada. O gráfico a seguir ilustra a utilização da CPU para muitas workloads comuns executadas por clientes na Nuvem AWS hoje.



Essas workloads de utilização de CPU de baixa a moderada causam desperdício de ciclos de CPU e, consequentemente, você paga por mais do que usa. Para superar isso, é possível aproveitar as instâncias de uso geral expansíveis com baixo custo, que são as instâncias T.

A família de instâncias T fornece performance de CPU de linha de base com capacidade de expansão acima da linha de base a qualquer momento, pelo tempo que for necessário. A CPU de linha de base é definida para atender às necessidades da maioria das workloads de uso geral, inclusive microsserviços de grande escala, servidores Web, bancos de dados pequenos e médios, registro em log de dados, repositórios de código, desktops virtuais, ambientes de desenvolvimento e teste e aplicações essenciais aos negócios. As instâncias T oferecem um equilíbrio de recursos de computação, memória e rede e fornecem a maneira mais econômica de executar um amplo espectro de aplicações de uso geral que têm uso de CPU de baixo a moderado. Podem economizar até 15% em custos, quando comparadas às instâncias M, e podem gerar ainda mais economia com tamanhos de instância menores e mais econômicas, oferecendo até 2 vCPUs e 0,5 GiB de memória. Os tamanhos de instância T menores, como nano, micro, pequeno e médio, são adequados para workloads que precisam de uma pequena quantidade de memória e não esperam alto uso da CPU.

> **Note**
>
> Este tópico descreve a CPU intermitente. Para obter mais informações sobre performance de rede intermitente, consulte Largura de banda de rede de instâncias do Amazon EC2.

Tipos de instância do EC2 expansíveis

As instâncias do EC2 expansíveis consistem em tipos de instância T4g, T3a e T3 e nos tipos de instância T2 da geração anterior.

Os tipos de instância T4g são a geração mais recente de instâncias expansíveis. Fornecem o melhor preço por performance e o menor custo entre todos os tipos de instância do EC2. Os tipos de instância T4g são alimentados por processadores AWS Graviton2 baseados em Arm com amplo suporte ao ecossistema de fornecedores de sistemas operacionais, fornecedores de software independentes e serviços e aplicações da AWS.

A tabela a seguir resume as principais diferenças entre os tipos de instância expansível.

Type	Descrição	Família de processadores
Última geração		
T4g	Tipo de instância do EC2 de menor custo com relação preço/performance até 40% mais alta e custos 20% menores em relação às T3	AWSProcessadores Graviton2 com núcleos Arm Neoverse N1
T3a	Instâncias baseadas em x86 de menor custo com custos 10% mais baixos em relação às instâncias T3	Processadores AMD EPYC de 1.ª geração
T3	Melhor relação preço/per formance de pico para workloads x86 com preço/per formance até 30% mais baixos	Intel Xeon escalável (processa dores Skylake, Cascade Lake)

Type	Descrição	Família de processadores
	em relação às instâncias T2 da geração anterior	
Geração anterior		
T2	Instâncias expansíveis da geração anterior	Processadores Intel Xeon

Para obter informações sobre o preço de instâncias e outras especificações, consulte Preços do Amazon EC2 e Tipos de instância do Amazon EC2. Para obter mais informações sobre performance de rede intermitente, consulte Largura de banda de rede de instâncias do Amazon EC2.

Caso tenha criado sua Conta da AWS antes de 15 julho de 2025 e ela tenha menos de 12 meses, é possível usar uma instância `t2.micro` gratuitamente (ou uma instância `t3.micro` em regiões onde o tipo `t2.micro` estiver indisponível) com determinados limites de uso. Caso tenha criado sua Conta da AWS em 15 de julho de 2025 ou após essa data, será possível usar os tipos de instância `t3.micro`, `t3.small`, `t4g.micro` e `t4g.small` por seis meses ou até que seus créditos acabem. Para obter mais informações, consulte Nível gratuito da AWS.

Opções de compra compatíveis com instâncias T

- On-Demand Instances
- Reserved Instances
- Instâncias dedicadas (apenas T3)
- Hosts dedicados (apenas T3, apenas no modo `standard`)
- Instâncias spot

Para obter mais informações, consulte Opções de faturamento e compra do Amazon EC2.

Tópicos

- Práticas recomendadas
- Principais conceitos para instâncias de desempenho expansível
- Modo ilimitado de instâncias expansíveis
- Modo padrão de instâncias expansíveis

- Configurar instâncias de desempenho expansível
- Monitore créditos de CPU para instâncias com capacidade de expansão

Práticas recomendadas

Siga estas melhores práticas para obter o benefício máximo com as instâncias expansíveis.

- Verifique se o tamanho da instância escolhido ultrapassa os requisitos mínimos de memória do sistema operacional e das aplicações. Os sistemas operacionais com interfaces gráficas de usuário que consomem memória e recursos de CPU significativos (por exemplo, o Windows) podem exigir um tamanho de instância `t3.micro`, ou maior, para muitos casos de uso. À medida que os requisitos de memória e de CPU de sua workload aumentam, você tem a flexibilidade nas instâncias T para escalar para tamanhos de instâncias maiores do mesmo tipo ou selecionar outro tipo de instância.
- Habilite o AWS Compute Optimizer para sua conta e verifique as recomendações do Compute Optimizer para sua workload. O Compute Optimizer pode ajudar a avaliar se as instâncias devem ser ampliadas para melhorar a performance ou reduzidas para economizar custos. O Compute Optimizer também pode recomendar um tipo de instância diferente com base no cenário. Para obter mais informações, consulte Visualizar recomendações de instância do EC2 no Guia do usuário do AWS Compute Optimizer.

Principais conceitos para instâncias de desempenho expansível

Os tipos de instância do Amazon EC2 tradicionais fornecem recursos fixos de CPU, enquanto as instâncias expansíveis fornecem um nível de linha de base de uso de CPU com capacidade para expandir o uso de CPU acima desse nível da linha de base. Isso garante que você pague somente pela CPU de linha de base, além dos usos adicionais de CPU de expansão, resultando em custos de computação mais baixos. O uso de linha de base e a capacidade de expansão são governados por créditos de CPU. As instâncias expansíveis são os únicos tipos de instância que usam créditos para uso de CPU.

Cada instância expansível ganha créditos continuamente quando permanece abaixo da linha de base da CPU e gasta créditos continuamente quando expande acima da linha de base. A quantidade de créditos obtidos ou gastos depende do uso da CPU da instância:

- Se a utilização da CPU for maior do que linha de base, os créditos gastos serão maiores do que os créditos obtidos.

- Se a utilização da CPU for igual à linha de base, os créditos obtidos serão iguais aos créditos gastos.
- Se a utilização da CPU for maior do que linha de base, os créditos gastos serão maiores do que os créditos obtidos.

Quando os créditos obtidos são maiores do que os créditos gastos, a diferença é chamada de créditos acumulados, que podem ser usados posteriormente para expandir acima da utilização da CPU de linha de base. Da mesma forma, quando os créditos gastos são maiores do que créditos obtidos, o comportamento da instância depende do modo de configuração de crédito (modo padrão ou modo ilimitado).

No modo padrão, quando os créditos gastos são maiores do que os créditos obtidos, a instância usa os créditos acumulados para expandir acima da utilização da CPU de linha de base. Se não houver mais créditos acumulados, a instância se reduzirá gradualmente à utilização da CPU de linha de base e não poderá expandir acima da linha de base até acumular mais créditos.

No modo ilimitado, se a instância expandir acima da utilização da CPU de linha de base, a instância usará primeiro os créditos acumulados para expandir. Se não houver mais créditos acumulados, a instância gastará créditos excedentes para expandir. Quando sua utilização de CPU ficar abaixo da linha de base, ela usará os créditos de CPU que ela ganhar para pagar os créditos excedentes gastos anteriormente. A capacidade de ganhar créditos de CPU para pagar créditos excedentes permite que o Amazon EC2 mantenha a média de utilização de CPU de uma instância em um período de 24 horas. Se o uso médio da CPU durante um período de 24 horas exceder a lista de referência, a instância será cobrada pelo uso adicional em uma taxa adicional fixa por hora de vCPU.

Conteúdo

- Principais conceitos e definições
- Ganhe créditos de CPU
- Taxa de ganhos de créditos de CPU
- Limite de acúmulo de créditos de CPU
- Duração dos créditos de CPU acumulados
- Utilização da linha de base

Principais conceitos e definições

Os principais conceitos e definições a seguir são aplicáveis a instâncias expansíveis.

Utilização da CPU

Utilização de CPU é o percentual de unidades de processamento EC2 alocadas que estão em uso na instância no momento. Essa métrica mede a porcentagem de ciclos de CPU alocados que estão sendo utilizados em uma instância. A métrica CPU Utilization do CloudWatch mostra o uso da CPU por instância e não o uso da CPU por núcleo. A especificação de CPU de linha de base de uma instância também se baseia no uso da CPU por instância. Para medir a utilização da CPU usando o Console de gerenciamento da AWS ou a AWS CLI, consulte Obter estatísticas para uma instância específica.

Crédito da CPU

Uma unidade de VCPU-time.

Exemplos:

1 crédito de CPU = 1 vCPU * 100% de utilização * 1 minuto.

1 crédito de CPU = 1 vCPU * 50% de utilização * 2 minutos

1 crédito de CPU = 2 vCPUs * 25% de utilização * 2 minutos

Utilização da linha de base

A utilização da lista de base é o nível no qual a CPU pode ser utilizada para um saldo de crédito líquido igual a zero, quando o número de créditos de CPU obtidos correspondem ao número de créditos de CPU usados. A utilização da linha de base também é conhecida como a linha de base. A utilização de linha de base é expressa como uma porcentagem da utilização da vCPU, que é calculada da seguinte forma: % da utilização de referência = (número de créditos ganhos/número de vCPUs)/60 minutos.

Para a utilização de linha de base de cada tipo de instância expansível, consulte a tabela de crédito.

Créditos ganhos

Créditos obtidos continuamente por uma instância quando ela está em execução.

Número de créditos ganhos por hora = % de utilização da linha de base * número de vCPUs * 60 minutos

Exemplo:

Um t3.nano com 2 vCPUs e utilização de linha de base de 5% ganha 6 créditos por hora, calculados da seguinte forma:

2 vCPUs * 5% da linha de base * 60 minutos = 6 créditos por hora

Créditos gastos ou usados

Créditos usados continuamente por uma instância quando ela está em execução.

Créditos de CPU gastos por minuto = Número de vCPUs * utilização da CPU * 1 minuto

Créditos acumulados

Créditos de CPU que não são gastos quando uma instância usa menos créditos do que o necessário para a utilização da linha de base. Em outras palavras, créditos acumulados = (Créditos obtidos - Créditos usados) abaixo da linha de base.

Exemplo:

Se um t3.nano estiver sendo executado com 2% de utilização da CPU, que está abaixo de sua linha de base de 5% por uma hora, os créditos acumulados serão calculados da seguinte forma:

Créditos de CPU acumulados = (Créditos obtidos por hora - Créditos usados por hora) = 6 - 2 vCPUs * 2% de utilização da CPU * 60 minutos = 6 - 2,4 = 3,6 créditos acumulados por hora

Limite de acúmulo de créditos

Depende do tamanho da instância, mas em geral é igual ao número máximo de créditos obtidos em 24 horas.

Exemplo:

Para t3.nano, o limite de crédito acumulado = 24 * 6 = 144 créditos

Créditos de execução

Aplicável somente a instâncias T2 configuradas para o modo padrão. Os créditos de inicialização são um número limitado de créditos de CPU alocados para uma nova instância T2, de modo que, quando iniciada no modo padrão, possa expandir acima da linha de base.

Créditos excedentes

Créditos que são gastos por uma instância após esgotar o saldo de crédito acumulado. Os créditos excedentes são projetados para instâncias expansíveis para sustentar alta performance por um longo período e são usados somente no modo ilimitado. O saldo de créditos excedentes

é usado para determinar quantos créditos foram usados pela instância para expandir no modo ilimitado.

Modo padrão

Modo de configuração de crédito, que permite que uma instância se expanda acima da linha de base, gastando créditos acumulados no saldo de crédito.

Modo ilimitado

Modo de configuração de crédito, que permite que uma instância se expanda acima da linha de base, sustentando alta utilização da CPU por qualquer período, sempre que necessário. O preço por hora da instância cobre automaticamente todos os picos de uso da CPU se a utilização média de CPU da instância for igual ou menor que a linha de base durante um período contínuo de 24 horas ou durante a vida útil da instância, o que for menor. Se a instância for executada com maior utilização de CPU por um período prolongado, ela poderá fazê-lo por uma taxa adicional uniforme por hora de vCPU.

A tabela a seguir resume as principais diferenças de crédito entre os tipos de instância expansível.

Type	Tipo de créditos de CPU compatíveis	Modos de configuração de crédito	Vida útil de créditos de CPU acumulados entre a inicialização e a interrupção da instância
Última geração			
T4g	Créditos obtidos, créditos acumulados, créditos gastos, créditos excedentes (somente no modo ilimitado)	Padrão, ilimitado (padrão)	7 dias (os créditos permanecem por 7 dias após a interrupção de uma instância)
T3a	Créditos obtidos, créditos acumulados, créditos gastos, créditos excedente	Padrão, ilimitado (padrão)	7 dias (os créditos permanecem por 7 dias após a interrupção de uma instância)

Type	Tipo de créditos de CPU compatíveis	Modos de configuração de crédito	Vida útil de créditos de CPU acumulados entre a inicialização e a interrupção da instância
	s (somente no modo ilimitado)		
T3	Créditos obtidos, créditos acumulados, créditos gastos, créditos excedentes (somente no modo ilimitado)	Padrão, ilimitado (padrão)	7 dias (os créditos permanecem por 7 dias após a interrupção de uma instância)
Geração anterior			
T2	Créditos obtidos, créditos acumulados, Créditos gastos, créditos de inicialização (somente no modo padrão), créditos excedentes (somente no modo ilimitado)	Standard (padrão), ilimitado	0 dias (os créditos são perdidos quando uma instância é interrompida)

> **Note**
>
> O modo ilimitado não é compatível com instâncias T3 que são iniciadas em um host dedicado.

Ganhe créditos de CPU

Cada instância expansível ganha continuamente (a uma resolução no nível de milissegundo) uma taxa definida de créditos de CPU por hora, de acordo com o tamanho da instância. O processo de

contabilidade de se os créditos são acumulados ou gastos também ocorre em uma resolução em nível de milissegundo, portanto, você não precisa se preocupar com gastos excessivos de créditos de CPU. Uma expansão curta da CPU usa uma pequena fração de um crédito de CPU.

Se uma instância expansível usar menos recursos de CPU do que o necessário para o uso de linha de base (como, por exemplo, quando está inativa), os créditos de CPU não gastos serão acumulados no saldo de créditos de CPU. Se uma instância expansível precisar de expansão acima do nível do uso da linha de base, ela gastará os créditos acumulados. Quanto mais créditos a instância expansível acumular, mais tempo de expansão ela poderá ter acima da linha de base quando mais uso de CPU for necessário.

A tabela a seguir lista os tipos de instância expansível, a taxa na qual os créditos de CPU são ganhos por hora, o número máximo de créditos de CPU ganhos que uma instância pode acumular, o número de vCPUs por instância e o uso da linha de base como uma porcentagem do total de um núcleo (usando uma única vCPU).

Tipo de instância	Créditos de CPU ganhos por hora	Máximo de créditos obtidos que podem ser acumulados*	vCPUs***	Utilização da linha de base por vCPU
T2				
t2.nano	3	72	1	5%
t2.micro	6	144	1	10%
t2.small	12	288	1	20%
t2.medium	24	576	2	20%**
t2.large	36	864	2	30%**
t2.xlarge	54	1296	4	22,5%**
t2.2xlarge	81.6	1958.4	8	17%**
T3				
t3.nano	6	144	2	5%**

Tipo de instância	Créditos de CPU ganhos por hora	Máximo de créditos obtidos que podem ser acumulados*	vCPUs***	Utilização da linha de base por vCPU
t3.micro	12	288	2	10%**
t3.small	24	576	2	20%**
t3.medium	24	576	2	20%**
t3.large	36	864	2	30%**
t3.xlarge	96	2304	4	40%**
t3.2xlarge	192	4608	8	40%**
T3a				
t3a.nano	6	144	2	5%**
t3a.micro	12	288	2	10%**
t3a.small	24	576	2	20%**
t3a.medium	24	576	2	20%**
t3a.large	36	864	2	30%**
t3a.xlarge	96	2304	4	40%**
t3a.2xlarge	192	4608	8	40%**
T4g				
t4g.nano	6	144	2	5%**
t4g.micro	12	288	2	10%**
t4g.small	24	576	2	20%**

Tipo de instância	Créditos de CPU ganhos por hora	Máximo de créditos obtidos que podem ser acumulados*	vCPUs***	Utilização da linha de base por vCPU
t4g.medium	24	576	2	20%**
t4g.large	36	864	2	30%**
t4g.xlarge	96	2304	4	40%**
t4g.2xlarge	192	4608	8	40%**

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

**A porcentagem de utilização da linha de base na tabela é por vCPU. Em CloudWatch, a utilização da CPU é exibida por vCPU. Por exemplo, a utilização de CPU para uma instância `t3.large` que opera no nível de linha de base é mostrada como 30% nas métricas de CPU do CloudWatch. Para obter informações sobre como calcular a utilização da linha de base, consulte Utilização da linha de base.

*** Cada vCPU é uma thread de um núcleo Intel Xeon ou de um núcleo AMD EPYC, exceto para instâncias T2 e T4g.

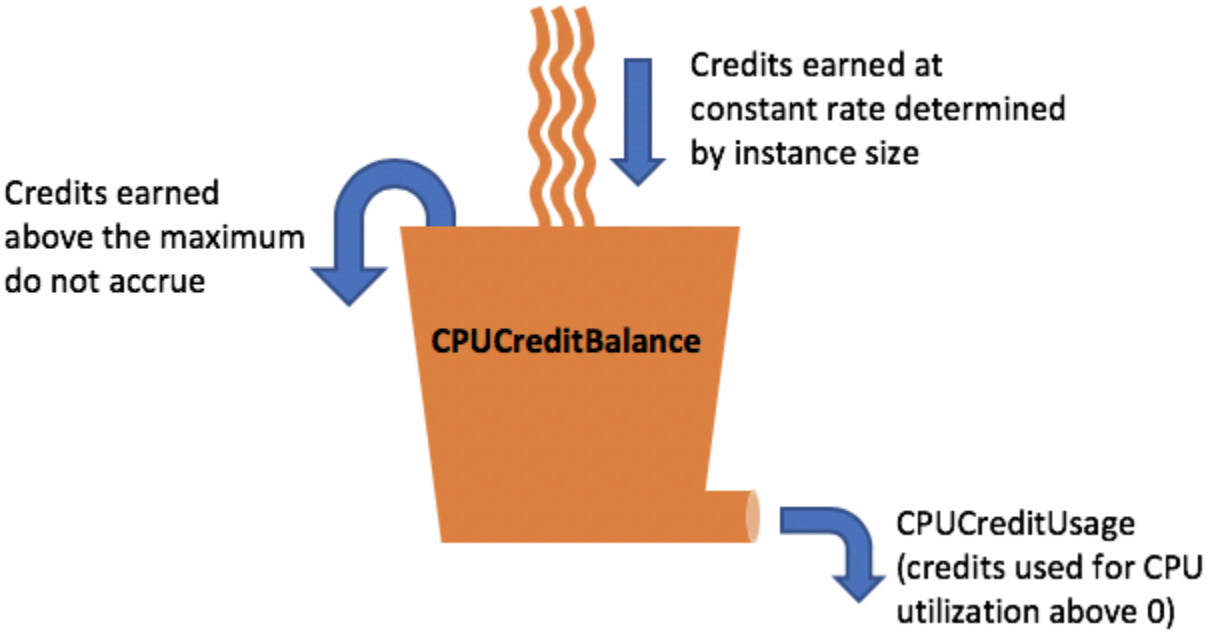
Taxa de ganhos de créditos de CPU

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

Limite de acúmulo de créditos de CPU

Embora os créditos obtidos nunca expirem em uma instância em execução, há um limite para o número de créditos obtidos que uma instância pode acumular. O limite é determinado pelo limite de saldo de créditos de CPU. Após o limite ser atingido, todos os créditos novos que foram ganhos

serão rejeitados, como indicado na imagem a seguir. O bucket 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 de Por exemplo, uma instância `t3.micro` pode acumular no máximo 288 créditos no saldo de créditos de CPU. A tabela anterior lista o número máximo de créditos ganhos que cada instância pode acumular.

As instâncias T2 padrão também ganham créditos de execução. Os créditos de execução não são contabilizados para o limite de sado 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.

As instâncias T4g, T3a e T3 não ganham créditos de inicialização. Essas instâncias são executadas como `unlimited` por padrão e, portanto, podem apresentar expansão imediatamente desde o início, sem nenhum crédito de execução. Instâncias T3 iniciadas em um lançamento de host dedicado como `standard` por padrão; o modo `unlimited` não é compatível com instâncias T3 em um host dedicado.

Duração dos créditos de CPU acumulados

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

Para T2, o saldo de créditos de CPU não persiste entre interrupções e inicializações da instância. Se você interromper uma instância T2, a instância perderá todos os créditos acumulados.

Para T4g, T3a e T3, o saldo de créditos de CPU persiste durante sete dias após uma instância ser interrompida, e os créditos são perdidos após esse período. Se você iniciar a instância dentro de sete dias, nenhum crédito será perdido.

Para obter mais informações, consulte `CPUCreditBalance` na Tabela de métricas do CloudWatch.

Utilização da linha de base

A utilização da lista de base é o nível no qual a CPU pode ser utilizada para um saldo de crédito líquido igual a zero, quando o número de créditos de CPU obtidos correspondem ao número de créditos de CPU usados. A utilização da linha de base também é conhecida como a linha de base.

A utilização da linha de base é expressa como uma porcentagem da utilização da vCPU, que é calculada da seguinte forma:

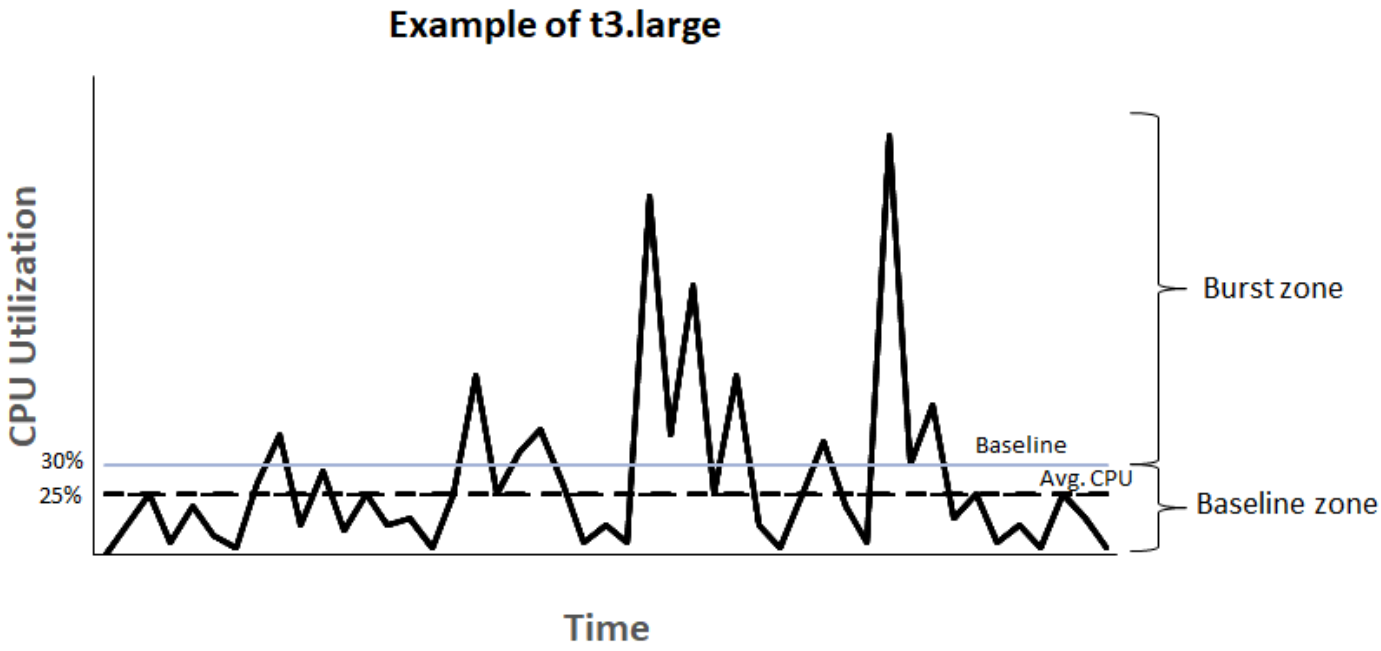
```
(number of credits earned/number of vCPUs)/60 minutes = % baseline utilization
```

Por exemplo, uma instância `t3.nano`, com 2 vCPUs, ganha 6 créditos por hora, resultando em uma utilização de linha de base de 5%, que é calculada da seguinte forma:

```
(6 credits earned/2 vCPUs)/60 minutes = 5% baseline utilization
```

Uma instância `t3.large`, com 2 vCPUs, ganha 36 créditos por hora, resultando em uma utilização básica de 30% (`(36/2)/60`).

O gráfico a seguir fornece um exemplo de `t3.large` com utilização média da CPU abaixo da linha de base.



Modo ilimitado de instâncias expansíveis

Uma instância expansível configurada como `unlimited` pode sustentar alta utilização de CPU por qualquer período, sempre que necessário. O preço por hora da instância cobre automaticamente todos os picos de uso da CPU se a utilização média de CPU da instância for igual ou menor que a linha de base durante um período contínuo de 24 horas ou durante a vida útil da instância, o que for menor.

Na grande maioria das workloads de uso geral, as instâncias configuradas como `unlimited` fornecem uma performance ampla sem encargos adicionais. Se a instância funcionar com maior utilização de CPU por um período prolongado, ela poderá fazer isso por uma taxa adicional uniforme por hora de vCPU. Para obter informações sobre preços, consulte a definição de preço do Amazon EC2 e definição de preço do modo ilimitado T2/T3/T4.

Caso tenha criado sua Conta da AWS antes de 15 de julho de 2025 e use uma instância `t2.micro` ou `t3.micro` da oferta do Nível gratuito da AWS no modo `unlimited`, poderão ser aplicadas cobranças se o consumo médio durante um período contínuo de 24 horas exceder o uso de linha de base da instância.

As instâncias T4g, T3a e T3 são iniciadas como `unlimited` por padrão (a menos que você altere o padrão). Se a média de uso de CPU em um período de 24 horas exceder a linha de base, você incorrerá em cobranças por créditos excedentes. Se você executar Instâncias spot

como `unlimited` e planejar usá-las imediatamente e por um curto período, sem tempo ocioso para acumular créditos de CPU, serão cobrados créditos excedentes. Recomendamos iniciar as instâncias spot no modo padrão para evitar custos mais altos. Para obter mais informações, consulte Os créditos excedentes podem gerar cobranças e Executar instâncias de desempenho expansível.

> **Note**
>
> Instâncias T3 iniciadas em um lançamento de host dedicado como `standard` por padrão; o modo `unlimited` não é compatível com instâncias T3 em um host dedicado.

Conteúdo

- Conceitos de modo ilimitado de instâncias com capacidade de expansão
  - Como funcionam as instâncias expansíveis
  - Quando usar o modo ilimitado versus CPU fixa
  - Os créditos excedentes podem gerar cobranças
  - Quanto custa uma performance intermitente ilimitada?
  - Nenhum crédito de execução para T2 ilimitada
  - Ativar modo ilimitado
  - O que acontece com os créditos quando é feita alternância de ilimitada para padrão
  - Monitorar uso de crédito
- Exemplos de modo ilimitado de instâncias com capacidade de expansão
  - Exemplo 1: explicar o uso de créditos com T3 ilimitada
  - Exemplo 2: explicar o uso de créditos com T2 ilimitada

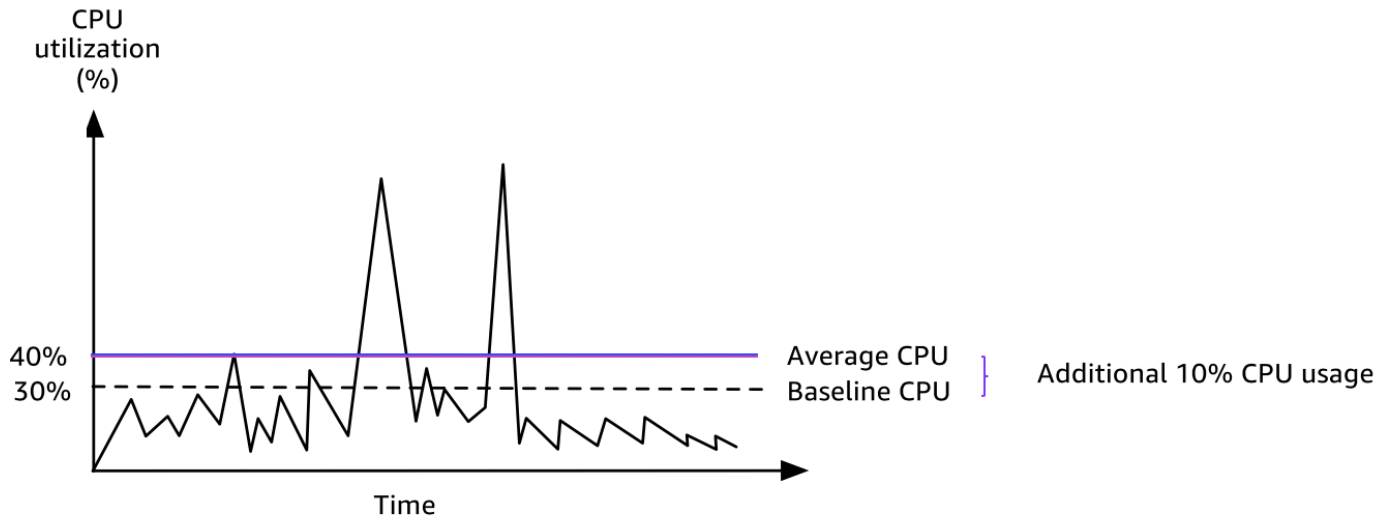
Conceitos de modo ilimitado de instâncias com capacidade de expansão

O modo `unlimited` é uma opção de configuração de crédito para instâncias expansíveis. Ele pode ser habilitado ou desabilitado a qualquer momento para uma instância interrompida ou em execução. É possível definir `unlimited` como a opção de crédito padrão no nível da conta por região da AWS, por família de instâncias expansíveis, para que todas as novas instâncias de performance expansível na conta sejam iniciadas usando a opção de crédito padrão.

Como funcionam as instâncias expansíveis

Se uma instância expansível configurada como `unlimited` esgota seu crédito de CPU, ela pode gastar créditos excedentes para ter expansão 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 lista de referência, a instância será cobrada pelo uso adicional em uma taxa adicional fixa por hora de vCPU.

O gráfico a seguir mostra o uso da CPU de um `t3.large`. A utilização da CPU de linha de base para um `t3.large` é 30%. Se a instância for executada com 30% de utilização da CPU ou menos, em média, durante um período de 24 horas, não haverá cobrança adicional porque o custo já está coberto pelo preço por hora da instância. No entanto, se a instância for executada com 40% de utilização da CPU, em média, durante um período de 24 horas, conforme mostrado no gráfico, a instância será cobrada pelo uso adicional de 10% da CPU em uma taxa adicional fixa por hora de vCPU.



Para obter mais informações sobre a utilização da linha de base por vCPU para cada tipo de instância e quantos créditos cada tipo de instância recebe, consulte a tabela de créditos.

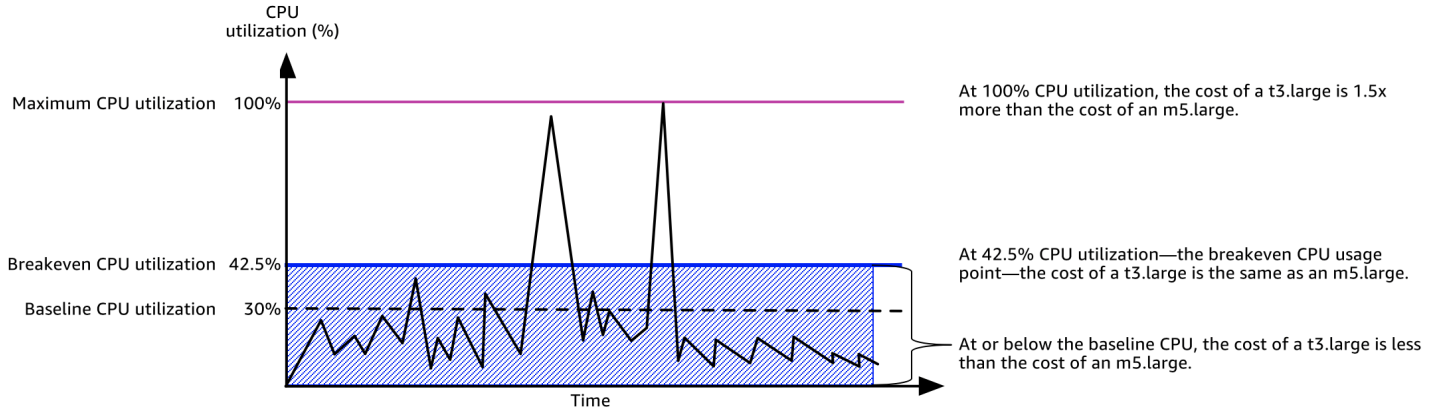
Quando usar o modo ilimitado versus CPU fixa

Ao determinar se use uma instância expansível no modo `unlimited`, como T3, ou uma instância de performance fixa, como M5, você precisa determinar o uso da CPU de equilíbrio. O uso da CPU de

equilíbrio para uma instância expansível é o ponto em que uma instância expansível custa o mesmo que uma instância de performance fixa. O uso da CPU de equilíbrio ajuda a determinar o seguinte:

- Se o uso médio da CPU em um período de 24 horas estiver no uso de CPU de equilíbrio ou abaixo dele, use uma instância expansível no modo `unlimited` para que você possa se beneficiar do preço mais baixo de uma instância expansível enquanto obtém ao mesma performance de uma instância de performance fixa.
- Se o uso médio da CPU durante um período de 24 horas estiver acima do uso de CPU de equilíbrio, a instância expansível custará mais do que a instância de performance fixa de tamanho equivalente. Se uma instância T3 apresentar uma expansão 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 mesma que um `m5.large`. O ponto de uso da CPU de equilíbrio para um `t3.large` é 42,5%. Se o uso médio da CPU estiver em 42,5%, o custo de executar o `t3.large` é o mesmo que um `m5.large`, e é mais caro se o uso médio da CPU estiver acima de 42,5%. Se a workload precisar de menos de 42,5% do uso médio da CPU, será possível se beneficiar do preço mais baixo do `t3.large` ao obter a mesma performance de um `m5.large`.



A tabela a seguir mostra como calcular o limite de uso da CPU de equilíbrio para que você possa determinar quando é mais barato usar uma instância expansível no modo `unlimited` ou uma instância de performance fixa. As colunas na tabela são rotuladas de A a K.

Tipo de instância	vCPUs	Preço*/ hora de T3	Preço*/ hora de M5	Diferença de preço	Utilização da linha de base T3 por vCPU (%)	Cobrança por hora de vCPU de créditos excedentes	Cobrança por minuto de vCPU	Mais minutos de expansão disponíveis por vCPU	% de CPU adicional disponível	% 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$ 0,0835	0,096 USD	0,0125 US	30%	0,05 USD	US$ 0,000833	15	12,5%	42,5%

*O preço é baseado no us-east-1 e no SO Linux.

A tabela fornece as seguintes informações:

- A coluna A mostra o tipo de instância, `t3.large`.
- A coluna B mostra o número de vCPUs para o `t3.large`.
- A coluna C mostra o preço de um `t3.large` por hora.
- A coluna D mostra o preço de um `m5.large` por hora.
- A coluna E mostra a diferença de preço entre o `t3.large` e o `m5.large`.
- A coluna F mostra a utilização da linha de base por vCPU do `t3.large`, que é 30%. Na linha de base, o custo por hora da instância abrange o custo do uso da CPU.
- A coluna G mostra a taxa adicional fixa por hora de vCPU em que uma instância é cobrada, se apresentar uma expansão em 100% da CPU depois de ter esgotado seus créditos ganhos.
- A coluna H mostra a taxa adicional fixa por minuto de vCPU em que uma instância é cobrada, se apresentar uma expansão em 100% da CPU depois de ter esgotado seus créditos ganhos.

- A coluna I mostra o número de minutos adicionais que o `t3.large` pode apresentar uma expansão 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 expansão 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 expansão 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
`t3.large`	42,5%
`t3.xlarge`	52,5 %
`t3.2xlarge`	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 em um período de 24 horas (por exemplo, uma instância `t3.micro` pode ganhar no máximo 288 créditos em um período de 24 horas), ela pode gastar créditos excedentes até esse limite máximo sem gerar uma cobranças imediatamente.

Contudo, se a utilização de CPU permanecer acima da linha de base, a instância não poderá obter créditos suficientes para pagar os créditos excedentes que ela gastou. Os créditos excedentes que não são pagos são cobrados a uma taxa adicional fixa por hora de vCPU. Para obter informações sobre a taxa, consulte a definição de preço do modo ilimitado T2/T3/T4g.

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

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

Os créditos excedentes gastos são monitorados pela métrica CloudWatch do `CPUSurplusCreditBalance`. Os créditos excedentes cobrados são monitorados pela métrica CloudWatch do `CPUSurplusCreditsCharged`. Para obter mais informações, consulte Métricas adicionais do CloudWatch para instâncias expansíveis.

Quanto custa uma performance intermitente ilimitada?

Se você usa créditos excedentes e eles não são pagos pelos créditos ganhos (consulte Os créditos excedentes podem gerar cobranças), você paga uma taxa adicional fixa por hora de vCPU pelos créditos excedentes. A taxa está listada na seção Definição de preços do modo ilimitado T2/T3/T4g, na página Definição de preços sob demanda do Amazon EC2.

Nenhum crédito de execução para T2 ilimitada

As instâncias T2 padrão recebem créditos de execução, mas as instâncias T2 ilimitadas não as recebem. Uma instância T2 ilimitada pode apresentar expansão acima da linha de base a qualquer momento, sem encargos adicionais, desde que sua utilização média de CPU seja igual ou inferior à linha de base em um período contínuo de 24 horas ou durante sua vida útil, o que for menor. Como tal, as instâncias T2 ilimitadas não requerem créditos de execução para atingir alta performance imediatamente após a execução.

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

As instâncias T4g, T3a e T3 nunca recebem créditos de inicialização porque são iniciadas no modo Ilimitado por padrão e, portanto, podem ter picos de utilização imediatamente após a inicialização. A configuração de crédito de modo ilimitado permite que as instâncias T4g, T3a e T3 usem o máximo de CPU necessário para expandir além da linha de base e pelo tempo necessário.

Ativar modo ilimitado

É possível 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 Configurar a especificação de crédito ao iniciar e Gerenciar a especificação de crédito de uma instância de desempenho expansível.

É possível definir `unlimited` como a opção de crédito padrão no nível da conta por região da AWS, por família de instâncias expansíveis, para que todas as novas instâncias de performance com capacidade de expansão na conta sejam executadas usando a opção de crédito padrão. Para obter mais informações, consulte Gerenciar a especificação de crédito padrão para uma conta.

É possível verificar se uma instância expansível está configurada como `unlimited` ou `standard` usando o console do Amazon EC2 ou a AWS CLI. Para obter mais informações, consulte Configurar instâncias de desempenho expansível.

O que acontece com os créditos quando é feita alternância de ilimitada para padrão

`CPUCreditBalance` é uma métrica do CloudWatch que controla o número de créditos que uma instância acumulou. `CPUSurplusCreditBalance` é uma métrica do CloudWatch que monitora o número de créditos excedentes que uma instância gastou.

Ao alterar uma instância configurada como `unlimited` para `standard`, ocorre o seguinte:

- O valor `CPUCreditBalance` permanece inalterado e é transferido.
- O valor `CPUSurplusCreditBalance` é cobrado imediatamente.

Quando uma instância `standard` é alterada para `unlimited`, ocorre o seguinte:

- O valor `CPUCreditBalance` que contém créditos ganhos acumulados é transferido.
- Para instâncias T2 padrão, todos os créditos de execução são removidos do valor `CPUCreditBalance`, e o valor `CPUCreditBalance` que contém os créditos ganhos acumulados é transferido.

Monitorar uso de crédito

Para verificar se a instância está gastando mais créditos do que a linha de base fornece, é possível 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 Monitore créditos de CPU para instâncias com capacidade de expansão.

Exemplos de modo ilimitado de instâncias com capacidade de expansão

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

Exemplos

- Exemplo 1: explicar o uso de créditos com T3 ilimitada
- Exemplo 2: explicar o uso de créditos com T2 ilimitada

Exemplo 1: explicar o uso de créditos com T3 ilimitada

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

A instância `t3.nano` ganha 144 créditos de CPU em um período contínuo de 24 horas, que ela pode resgatar para 144 minutos de uso de vCPU. Quando ela esgotar o saldo de créditos de CPU (representado pela métrica CloudWatch do `CPUCreditBalance`), poderá gastar os créditos de CPU — excedentes, que ela ainda não ganhou—, para ter expansão 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 expansão 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.

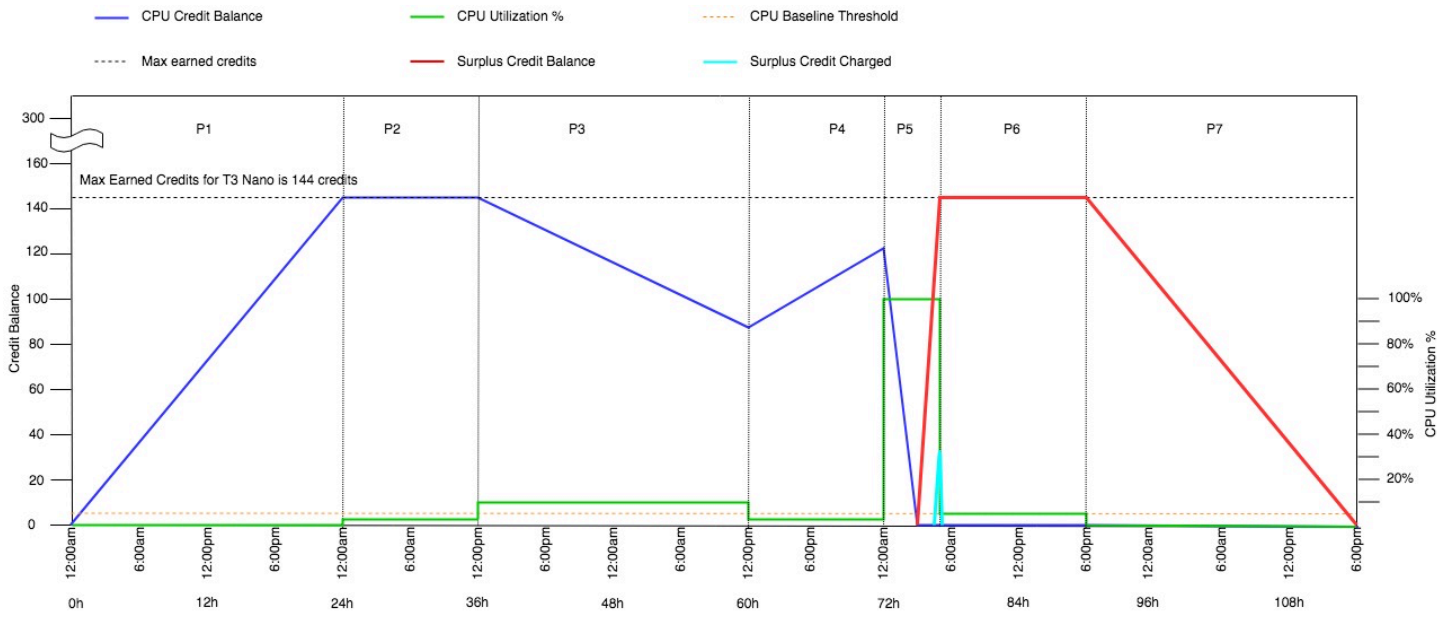
P3 – nas próximas 24 horas, a utilização de CPU é de 7% (acima da linha de base), o que exige um gasto de 57,6 créditos. A instância gasta mais do que ganha, e o valor `CPUCreditBalance` diminui para 86,4 créditos.

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 expansão para 100% de utilização de CPU e gasta um total de 570 créditos para sustentar a expansão. Após aproximadamente uma hora desse período, a instância esgota todo o `CPUCreditBalance` de 122 créditos e começa a gastar os créditos excedentes para sustentar o alto uso de CPU, totalizando 448 créditos excedentes nesse período (570 - 122 = 448). Quando o valor `CPUSurplusCreditBalance` atingir 144 créditos de CPU (o máximo que uma instância `t3.nano` pode ganhar em um período de 24 horas), todos os créditos excedentes gastos após esse período não poderão ser compensados por créditos ganhos. Os créditos excedentes gastos depois desse período totalizam 304 créditos (448 - 144 = 304), resultando em uma pequena cobrança adicional ao fim dessa hora para 304 créditos.

P6 – nas próximas 13 horas, a utilização de CPU é de 5%, (a linha de base). A instância ganha o número de créditos que gastar, sem precisar pagar por excessos do `CPUSurplusCreditBalance`. O valor `CPUSurplusCreditBalance` permanece em 144 créditos.

P7 – nas últimas 24 horas neste exemplo, a instância está inativa, e a utilização de CPU é de 0%. Durante esse período, a instância ganha 144 créditos, que usa para pagar o `CPUSurplusCreditBalance`.



Exemplo 2: explicar o uso de créditos com T2 ilimitada

Neste exemplo, você verá a utilização de CPU de uma instância `t2.nano` executada como `unlimited` e como ela gasta créditos ganhos e excedentes para sustentar a utilização de CPU.

A instância `t2.nano` ganha 72 créditos de CPU em um período contínuo de 24 horas, que ela pode resgatar para 72 minutos de uso de vCPU. Quando ela esgotar o saldo de créditos de CPU (representado pela métrica CloudWatch do `CPUCreditBalance`), poderá gastar os créditos de CPU — excedentes, que ela ainda não ganhou—, para ter expansão 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 expansão usando créditos excedentes, mesmo após esgotar seu `CPUCreditBalance`. É possível supor que, no início de linha de tempo no gráfico, a instância tem um saldo de créditos acumulados igual ao número máximo de créditos que ela pode ganhar em 24 horas. O fluxo de trabalho a seguir faz referência aos pontos numerados no gráfico:

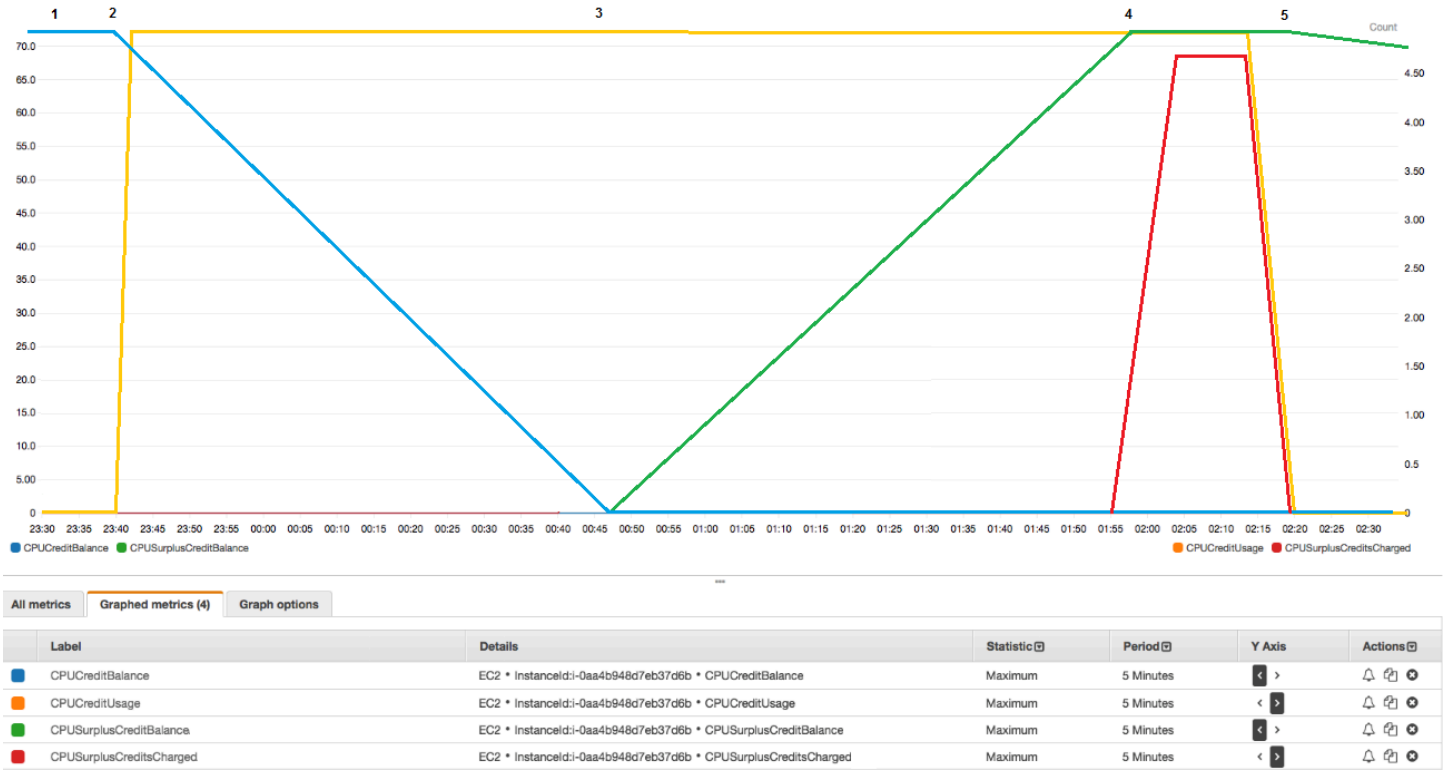
1 – Nos primeiros 10 minutos, `CPUCreditUsage` está em 0 e o valor `CPUCreditBalance` permanece no limite máximo de 72.

2 – Às 23H40, à medida que a utilização da CPU aumenta, a instância gasta os créditos de CPU e o valor `CPUCreditBalance` diminui.

3 – Por volta de 00h47, a instância esgota todo o seu `CPUCreditBalance` e começa a gastar os créditos excedentes para manter o alto uso da CPU.

4 – Os créditos excedentes são gastos até 01h55, quando o valor `CPUSurplusCreditBalance` atinge 72 créditos de CPU. Isso é igual ao limite máximo que uma instância `t2.nano` pode ganhar em um período de 24 horas. Qualquer crédito excedente gasto a partir daí não poderá ser compensado pelos créditos ganhos no período de 24 horas, o que resultará em uma pequena taxa adicional no final da hora.

5 – A instância continua a gastar os créditos excedentes até às 02h20. Nesse momento, a utilização da CPU cai abaixo da linha de base, e a instância começa a ganhar 3 créditos por hora (ou 0,25 crédito a cada 5 minutos), que ela usa para pagar o `CPUSurplusCreditBalance`. Quando o valor `CPUSurplusCreditBalance` reduz para 0, a instância começa a acumular créditos ganhos em seu `CPUCreditBalance` a 0,25 crédito a cada 5 minutos.



Como calcular a fatura (instância do Linux)

Os créditos excedentes custam USD 0,05 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 de USD 0,42 por hora de vCPU x USD 0,05/hora de vCPU = USD 0,021, que é arredondado para USD 0,02. 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

Como calcular a fatura (instância do Windows)

Os créditos excedentes custam USD 0,096 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 de USD 0,42 por hora de vCPU x USD 0,096/hora de vCPU = USD 0,04032, que é arredondado para USD 0,04. Esta é a conta de final do mês desta instância T2 ilimitada:

Amazon Elastic Compute Cloud running Windows		
$0.0081 per On Demand Windows t2.nano Instance Hour	720.000 Hrs	$5.83

Amazon Elastic Compute Cloud T2 CPU Credits		
$0.096 per vCPU-Hour of T2 CPU credits	0.420 vCPU-Hours	$0.04

É possível configurar alertas de pagamento para ser notificado a cada hora sobre quaisquer cobranças acumuladas e tomar providências, se necessário.

Modo padrão de instâncias expansíveis

Uma instância expansível configurada como `standard` é adequada para workloads com uma utilização média de CPU consistentemente abaixo da utilização de CPU de linha de base da instância. Para expansãos acima da linha de base, a instância gasta os créditos acumulados no seu saldo de créditos de CPU. Se a instância estiver ficando sem créditos acumulados, o uso de CPU será gradualmente reduzido para o nível da linha de base, para que a instância não experimente uma queda de performance acentuada quando o saldo de créditos de CPU acumulado se esgotar. Para obter mais informações, consulte Principais conceitos para instâncias de desempenho expansível.

Conteúdo

- Conceitos do modo padrão de instâncias com capacidade de expansão
  - Como funcionam as instâncias expansíveis padrão
  - Créditos de execução
  - Limites de crédito de execução
  - Diferenças entre créditos de execução e créditos ganhos
- Exemplos do modo padrão para instâncias com capacidade de expansão
  - Exemplo 1: explicar o uso de créditos com T3 padrão
  - Exemplo 2: explicar o uso de créditos com T2 padrão
    - Período 1: 1 a 24 horas
    - Período 2: 25 a 36 horas
    - Período 3: 37 a 61 horas
    - Período 4: 62 a 72 horas
    - Período 5: 73 – 75 horas

- Período 6: 76 a 90 horas
- Período 7: 91 a 96 horas

Conceitos do modo padrão de instâncias com capacidade de expansão

O modo `standard` é uma opção de configuração para instâncias expansíveis Ele pode ser habilitado ou desabilitado a qualquer momento para uma instância interrompida ou em execução. É possível definir `standard` como a opção de crédito padrão no nível da conta por região da AWS, por família de instâncias expansíveis, para que todas as novas instâncias de performance expansível na conta sejam iniciadas usando a opção de crédito padrão.

Como funcionam as instâncias expansíveis padrão

Quando uma instância expansível configurada como `standard` estiver em um estado de execução, ela receberá continuamente (a uma resolução no nível de milissegundo) uma taxa definida de créditos ganhos por hora. Para T2 padrão, quando a instância é interrompida, ela perde todos os créditos acumulados, e seu saldo de créditos é redefinido para zero. Quando é reiniciada, ela recebe um novo conjunto de créditos de execução e começa a acumular créditos ganhos. Para instâncias T4g, T3a e T3 padrão, o saldo de crédito de CPU persiste durante sete dias após a instância ser interrompida, e os créditos são perdidos após esse período. Se você iniciar a instância dentro de sete dias, nenhum crédito será perdido.

As instâncias T2 Standard recebem dois tipos de créditos de CPU: créditos ganhos e créditos de inicialização. Quando uma instância T2 padrão estiver em um estado de execução, ela recebe continuamente (a uma resolução no nível de milissegundo) uma taxa definida de créditos ganhos por hora. No começo, ela ainda não ganhou créditos para uma boa experiência de inicialização. Portanto, para oferecer uma boa experiência de startup, ela recebe créditos de execução para começar, que ela gasta primeiro ao acumular créditos ganhos.

As instâncias T4g, T3a e T3 não recebem créditos de inicialização porque oferecem suporte ao modo Ilimitado. A configuração de crédito de modo Ilimitado permite que as instâncias T4g, T3a e T3 usem o máximo de CPU necessário para expandir além da linha de base e pelo tempo necessário.

Créditos de execução

As instâncias T2 Standard recebem 30 créditos de inicialização por vCPU ao serem iniciadas, e as instâncias T1 Standard recebem 15 créditos de inicialização. Por exemplo, uma instância `t2.micro` tem uma vCPU e recebe 30 créditos de execução, enquanto uma instância `t2.xlarge` tem quatro vCPUs e recebe 120 créditos de execução. Os créditos de execução foram criados para oferecer

uma boa experiência de startup, permitindo, assim, que as instâncias apresentem uma expansão 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.

A tabela a seguir lista a alocação de crédito de CPU inicial recebida na execução ou no início, e o número de vCPUs.

Tipo de instância	Créditos de execução	vCPUs
`t1.micro`	15	1
`t2.nano`	30	1
`t2.micro`	30	1
`t2.small`	30	1
`t2.medium`	60	2
`t2.large`	60	2
`t2.xlarge`	120	4
`t2.2xlarge`	240	8

Limites de crédito de execução

Existe um limite para o número de vezes em que instâncias T2 padrão podem receber créditos de execução. O limite padrão é de 100 execuções ou inicializações de todas as instâncias T2 padrão combinadas por conta, por região, por período de 24 horas de acúmulo. Por exemplo, o limite é atingido quando uma instância é interrompida e iniciada 100 vezes em um período de 24 horas, ou

quando 100 instâncias são executadas em um período de 24 horas ou outras combinações que se igualem a 100 inicializações. As novas contas podem ter um limite inferior, que aumenta ao longo do tempo com base no seu uso.

> **Tip**
>
> Para garantir que as workloads sempre obtenham a performance de que precisam, alterne para Modo ilimitado de instâncias expansíveis ou considere o uso de uma instância maior.

Diferenças entre créditos de execução e créditos ganhos

A tabela a seguir lista as diferenças entre créditos de execução e créditos ganhos.

	Créditos de execução	Créditos ganhos
Taxa de ganhos de crédito	As instâncias T2 padrão recebem 30 créditos de execução por vCPU na execução ou inicialização. Se uma instância T2 for alterada de `unlimited` para `standard`, ela não obtém créditos de execução no momento em que é alterada.	Cada instância T2 obtém continuam ente (a uma resolução no nível de milissegundo) uma taxa definida de créditos de CPU por hora, dependend o 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.
Limite de ganho de crédito	O limite para receber créditos de execução é de 100 execuções ou inicializações de todas as instância s 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 descartad os. 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.

	Créditos de execução	Créditos ganhos
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 CloudWatch `CPUCreditBalance`. Para obter mais informações, consulte `CPUCreditBalance` na Tabela de métricas do CloudWatch.

Exemplos do modo padrão para instâncias com capacidade de expansão

Os seguintes exemplos explicam o uso de créditos quando as instâncias estão configuradas como `standard`.

Exemplos

- Exemplo 1: explicar o uso de créditos com T3 padrão
- Exemplo 2: explicar o uso de créditos com T2 padrão

Exemplo 1: explicar o uso de créditos com T3 padrão

Neste exemplo, você verá como uma instância `t3.nano` executada como `standard` ganha, acumula e gasta créditos ganhos. Você verá como o saldo de créditos reflete os créditos ganhos que foram acumulados.

Uma instância `t3.nano` em execução ganha 144 créditos a cada 24 horas. Seu limite de saldo de créditos é de 144 créditos ganhos. Assim que o limite é atingido, os novos créditos ganhos são descartados. Para obter mais informações sobre o número de créditos que podem ser ganhos e acumulados, consulte a Tabela de créditos.

É possível iniciar uma instância T3 padrão e usá-la imediatamente. Ou, é possível iniciar uma instância padrão T3 e deixá-la inativa por alguns dias antes de executar aplicações. O fato de uma instância ser usada ou permanecer inativa determina se os créditos são acumulados ou gastos. Se uma instância permanecer inativa por 24 horas a partir do momento em que é executada, o saldo de créditos atingirá seu limite, que é o número máximo de créditos ganhos que podem ser acumulados.

Esse exemplo descreve uma instância em permanece inativa por 24 horas após sua execução e mostra sete períodos em um período de 96 horas, mostrando a taxa na qual os créditos são ganhos, acumulados, gastos e descartados, e o valor do saldo no final de cada período.

O fluxo de trabalho a seguir faz referência aos pontos numerados no gráfico:

P1 – às 0 horas no gráfico, a instância é executada como `standard` e começa a ganhar créditos imediatamente. A instância permanece inativa desde a sua execução (o uso da CPU é de 0%), e nenhum crédito é gasto. Todos os créditos não gastos são acumulados no saldo de crédito. Nas primeiras 24 horas, `CPUCreditUsage` é de 0, e o valor `CPUCreditBalance` atinge seu máximo de 144.

P2 – nas próximas 12 horas, a utilização de CPU é de 2,5%, que é abaixo da linha de base de 5%. A instância ganha mais créditos do que gasta, mas o valor `CPUCreditBalance` não pode exceder seu máximo de 144 créditos. Todos os créditos ganhos que excedem o limite são descartados.

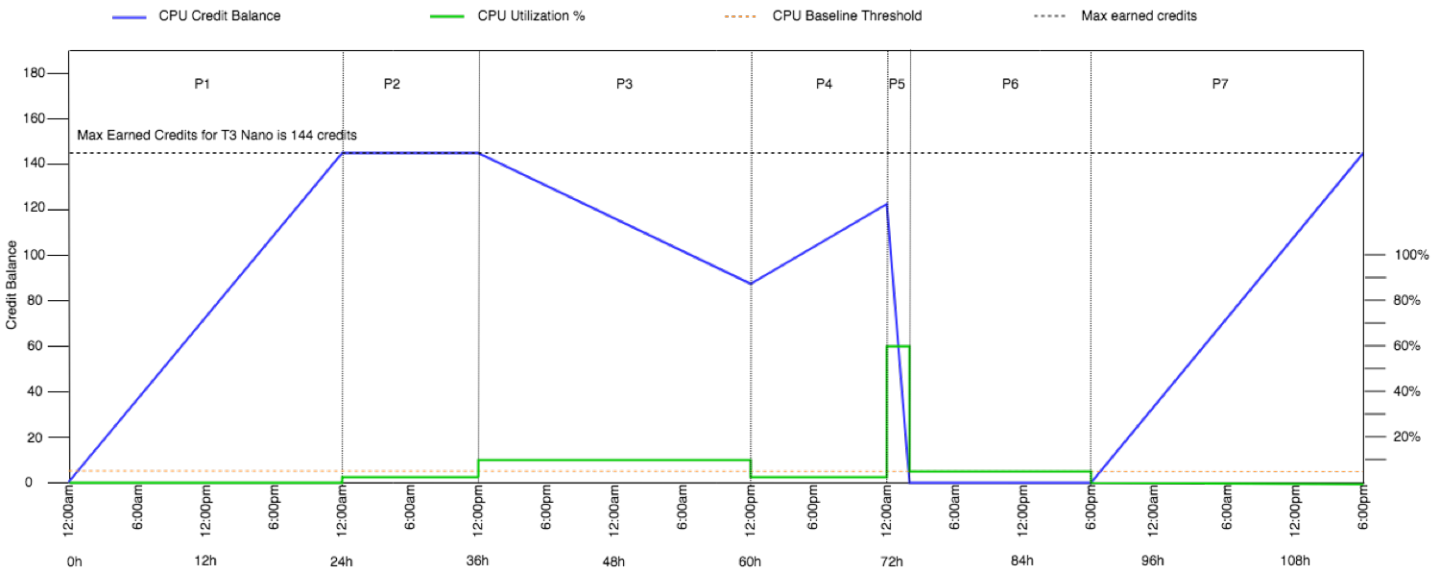
P3 – nas próximas 24 horas, a utilização de CPU é de 7% (acima da linha de base), o que exige um gasto de 57,6 créditos. A instância gasta mais do que ganha, e o valor `CPUCreditBalance` diminui para 86,4 créditos.

P4 – nas próximas 12 horas, a utilização de CPU diminui para 2,5% (abaixo da linha de base), o que exige um gasto de 36 créditos. Ao mesmo tempo, a instância ganha 72 créditos. A instância ganha mais créditos do que gasta, e o valor `CPUCreditBalance` aumenta para 122 créditos.

P5: nas próximas duas horas, a instância terá expansão para 60% de utilização de CPU e esgotará todo o valor `CPUCreditBalance` de 122 créditos. Ao fim desse período, com o `CPUCreditBalance` em zero, a utilização de CPU é forçada a diminuir para o nível de utilização de linha de base de 5%. Na linha de base, a instância ganha o mesmo número de créditos que são gastos.

P6 – nas próximas 14 horas, a utilização de CPU é de 5%, (a linha de base). A instância ganha o mesmo número de créditos que são gastos. O valor de `CPUCreditBalance` permanece em 0.

P7 – nas últimas 24 horas neste exemplo, a instância está inativa, e a utilização de CPU é de 0%. Durante esse período, a instância ganha 144 créditos, que acumula em seu `CPUCreditBalance`.



Exemplo 2: explicar o uso de créditos com T2 padrão

Neste exemplo, você verá como uma instância `t2.nano` executada como `standard` ganha, acumula e gasta créditos ganhos e de execução. Você verá como o saldo de crédito reflete não somente os créditos ganhos acumulados, como também os créditos de execução acumulados.

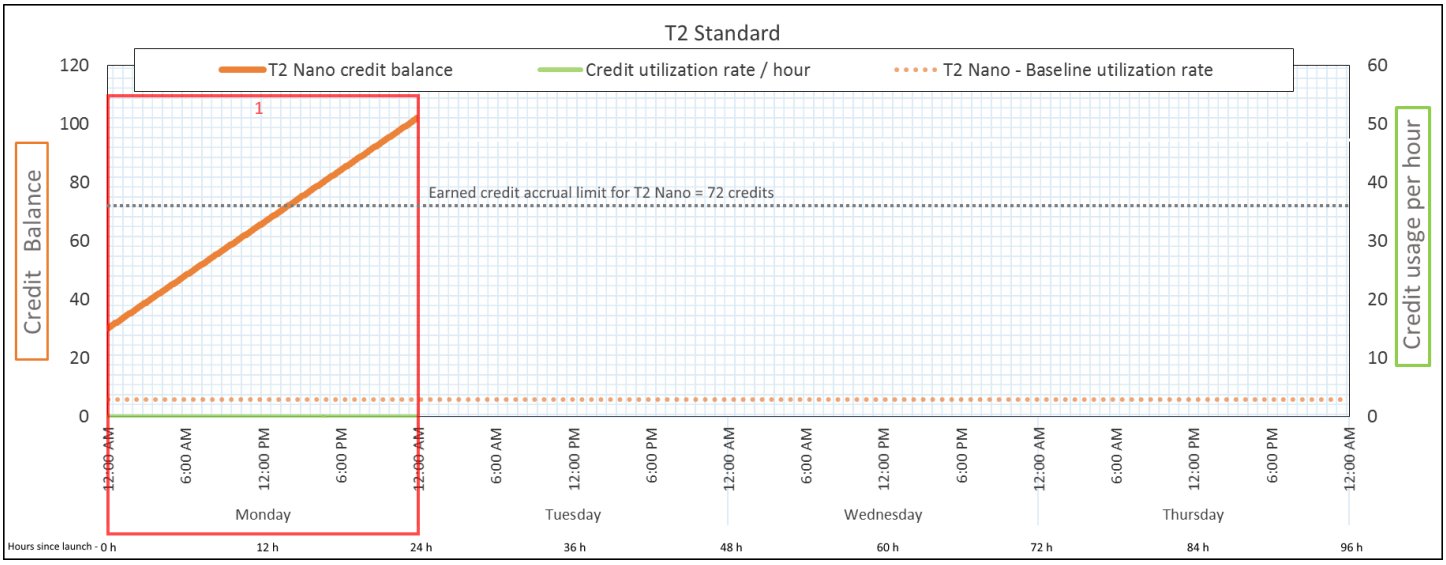
A instância `t2.nano` obtém 30 créditos de execução quando é executada e ganha 72 créditos a cada 24 horas. Seu limite de saldo é de 72 créditos ganhados. Os créditos de execução não são considerados no limite. Assim que o limite é atingido, os novos créditos ganhos são descartados. Para obter mais informações sobre o número de créditos que podem ser ganhos e acumulados, consulte a Tabela de créditos. Para obter mais informações sobre limites, consulte Limites de crédito de execução.

É possível iniciar uma instância T2 padrão e usá-la imediatamente. Ou, é possível iniciar uma instância padrão T2 e deixá-la inativa por alguns dias antes de executar aplicações. O fato de uma instância ser usada ou permanecer inativa determina se os créditos são acumulados ou gastos. Se uma instância permanecer inativa por 24 horas após sua execução, o saldo de crédito será exibido como ultrapassado do limite, pois reflete os créditos ganhos e de execução acumulados. No entanto, após o uso da CPU, os créditos de execução são gastos primeiro. Depois disso, o limite sempre reflete o número máximo de créditos ganhos que podem ser acumulados.

Esse exemplo descreve uma instância em permanece inativa por 24 horas após sua execução e mostra sete períodos em um período de 96 horas, mostrando a taxa na qual os créditos são ganhos, acumulados, gastos e descartados, e o valor do saldo no final de cada período.

Período 1: 1 a 24 horas

Na hora 0 do gráfico, a instância T2 é executada como `standard` e obtém imediatamente 30 créditos de execução. Ela ganha créditos durante o estado de execução. A instância permanece inativa desde a sua execução (o uso da CPU é de 0%), e nenhum crédito é gasto. Todos os créditos não gastos são acumulados no saldo de crédito. Aproximadamente 14 horas após a execução, o saldo de crédito é 72 (30 créditos de execução + 42 créditos ganhos), que é equivalente ao que a instância pode ganhar em 24 horas. Após 24 horas da execução, o saldo ultrapassa 72 créditos, pois os créditos de execução não gastos são acumulados (o saldo é de 102 créditos: 30 créditos de execução + 72 créditos ganhos).



Taxa de gasto de crédito	0 crédito por 24 horas (0% de uso da CPU)
Taxa de ganhos de crédito	72 créditos por 24 horas
Taxa de descarte de crédito	0 crédito por 24 horas
Saldo de crédito	102 créditos (30 créditos de execução + 72 créditos ganhos)

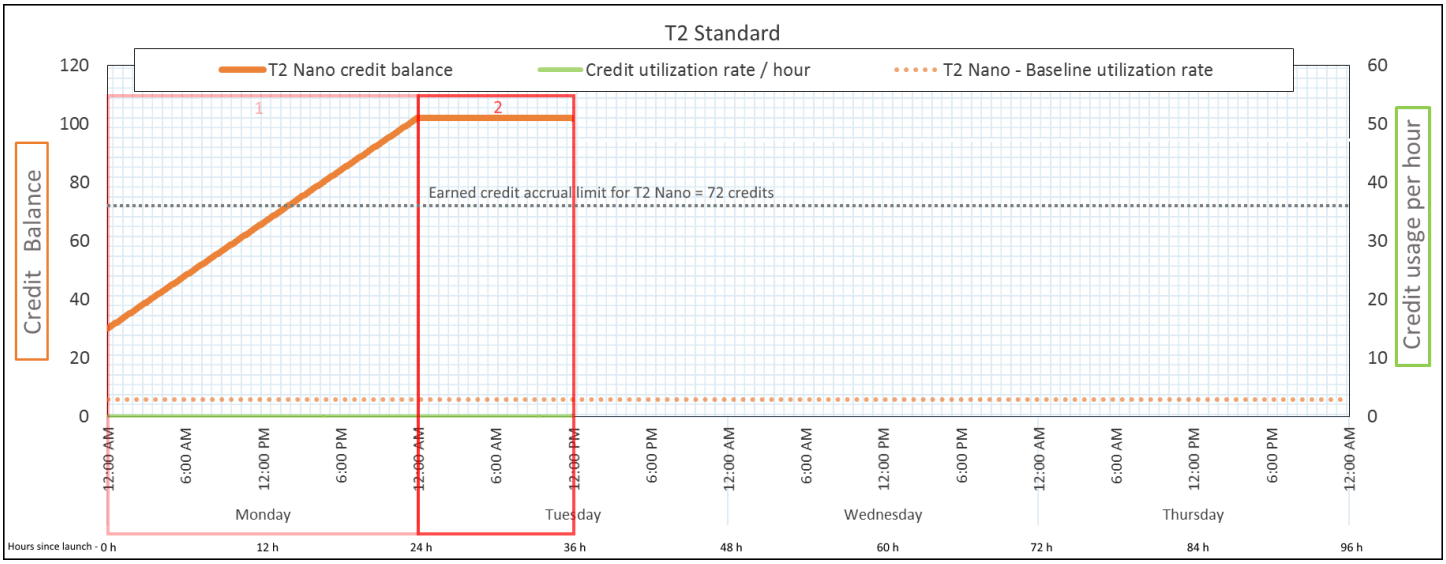
Conclusão

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.



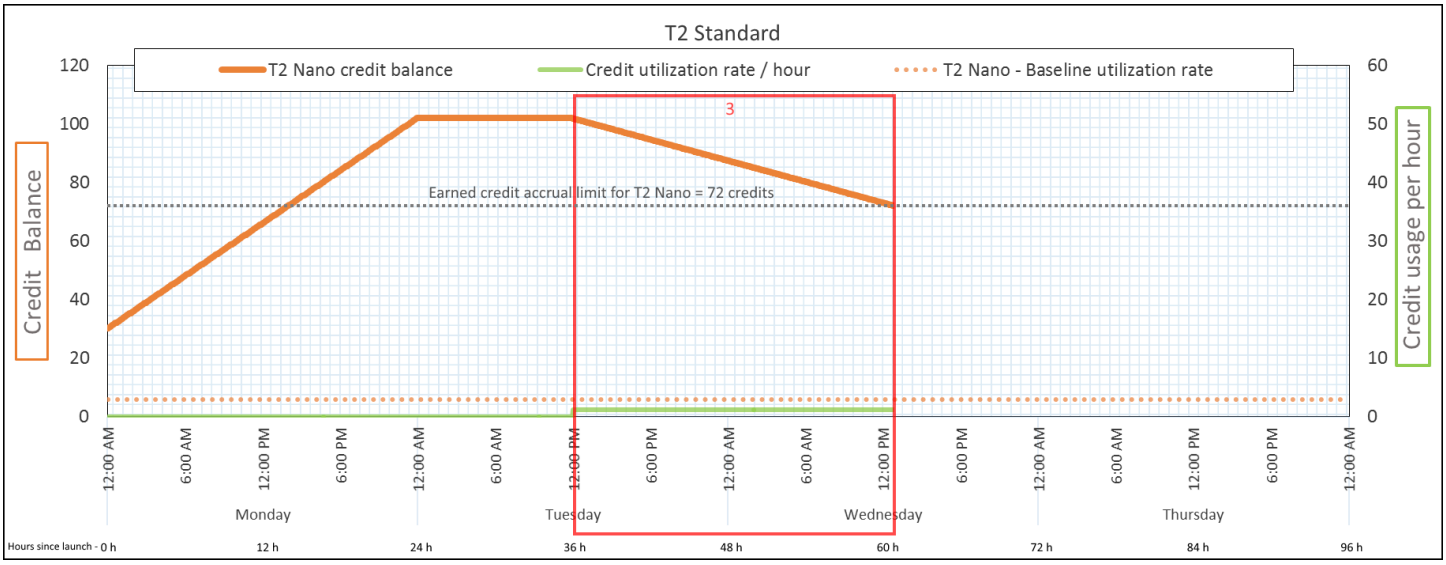
Taxa de gasto de crédito	0 crédito por 24 horas (0% de uso da CPU)
Taxa de ganhos de crédito	72 créditos por 24 horas (3 créditos por hora)
Taxa de descarte de crédito	72 créditos por 24 horas (100% de taxa de ganhos de crédito)
Saldo de crédito	102 créditos (30 créditos de execução + 72 créditos ganhos) – 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 sado de créditos de Se incluir créditos de execução acumulados, o saldo parecerá estar acima do limite.

Período 3: 37 a 61 horas

Nas próximas 25 horas, a instância usa 2% da CPU. Isso requer 30 créditos. No mesmo período, ela ganha 75 créditos, mas o saldo diminuir. O saldo diminui porque os créditos de execução acumulados são gastos primeiro, enquanto os créditos recém-ganhos são descartados, pois o saldo já está no limite de 72 créditos ganhos.



Taxa de gasto de crédito	28,8 créditos por 24 horas (1,2 créditos por hora, 2% de utilização da CPU, 40% de taxa de ganhos de crédito) – 30 créditos— em 25 horas
Taxa de ganhos de crédito	72 créditos por 24 horas
Taxa de descarte de crédito	72 créditos por 24 horas (100% de taxa de ganhos de crédito)
Saldo de crédito	72 créditos (30 créditos de execução foram gastados; 72 créditos ganhos continuam não gastos)

Conclusão

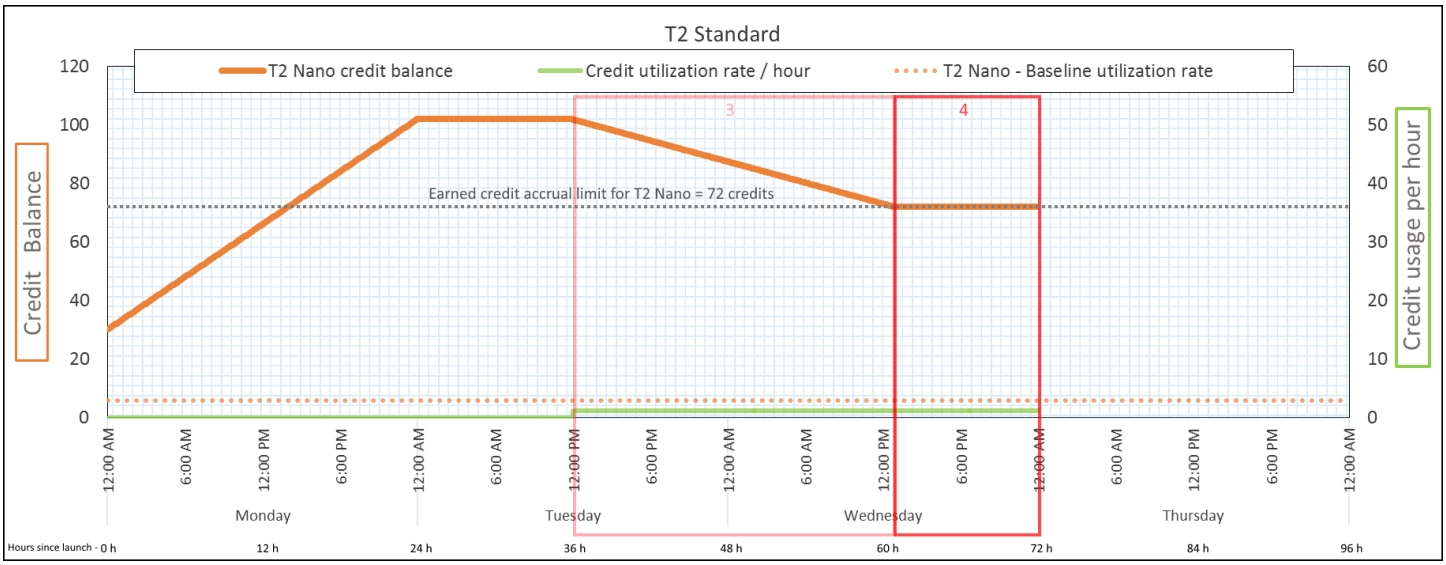
A instância gasta créditos de execução primeiro, antes dos crédito ganhos. Os créditos de execução não são contabilizados para o limite de créditos. Após o gasto dos créditos de execução, o saldo

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.



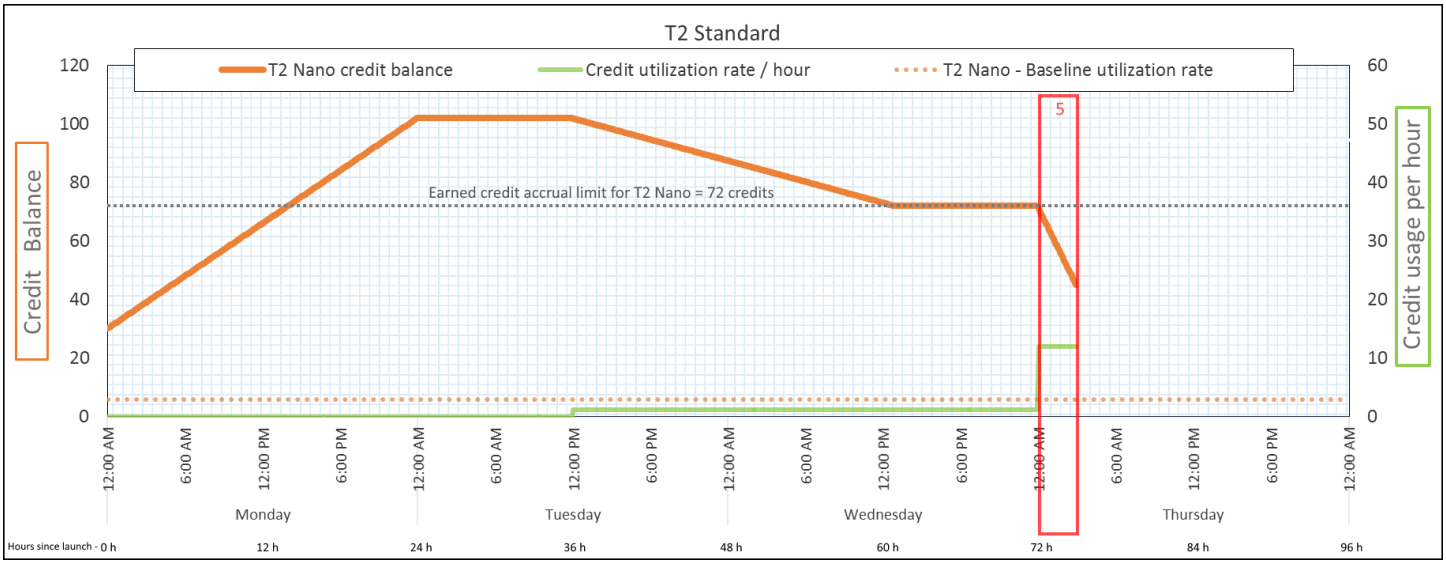
Taxa de gasto de crédito	28,8 créditos por 24 horas (1,2 créditos por hora, 2% de utilização da CPU, 40% de taxa de ganhos de crédito) – 13,2 —créditos em 11 horas
Taxa de ganhos de crédito	72 créditos por 24 horas
Taxa de descarte de crédito	43.2 créditos por 24 horas (60% de taxa de ganhos de crédito)
Saldo de crédito	72 créditos (0 créditos de execução, 72 créditos ganhos) – o —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 – 75 horas

Nas próximas três horas, o uso da CPU pela instância sobe para 20%. Isso requer 36 créditos. A instância ganha nove créditos nas mesmas três horas, resultando em uma diminuição do saldo líquido de 27 créditos. No final das três horas, o saldo é de 45 créditos ganhos.



Taxa de gasto de crédito	288 créditos por 24 horas (12 créditos por hora, 20% de utilização da CPU, 400% de taxa de ganhos de crédito) – 36— créditos em 3 horas
Taxa de ganhos de crédito	72 créditos por 24 horas (9 créditos em 3 horas)
Taxa de descarte de crédito	0 crédito por 24 horas
Saldo de crédito	45 créditos (saldo anterior (72) - créditos gastos (36) + créditos ganhos (9)) – o —saldo diminui a uma taxa de 216 créditos por 24 horas (taxa de gastos de 288/24 + taxa de

	ganhos de 72/24 = taxa de diminuição do saldo de 216/24)

Conclusão

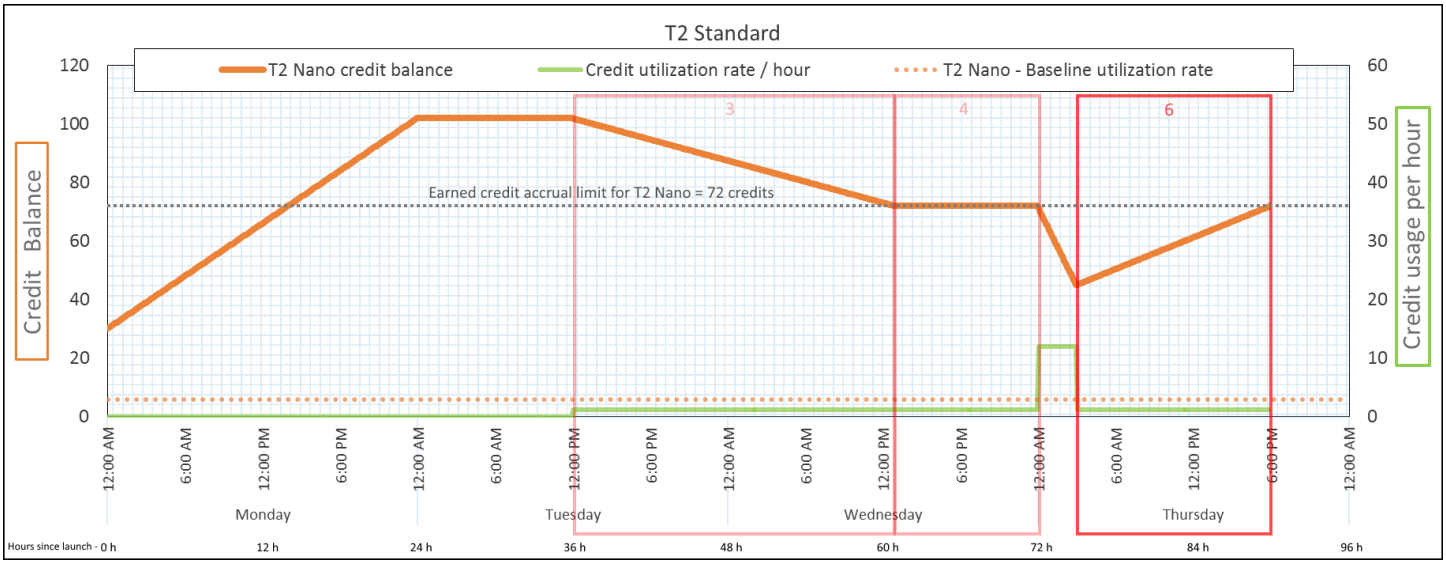
Se uma instância gastar mais créditos do que ganhar, seu balanço diminuirá.

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)

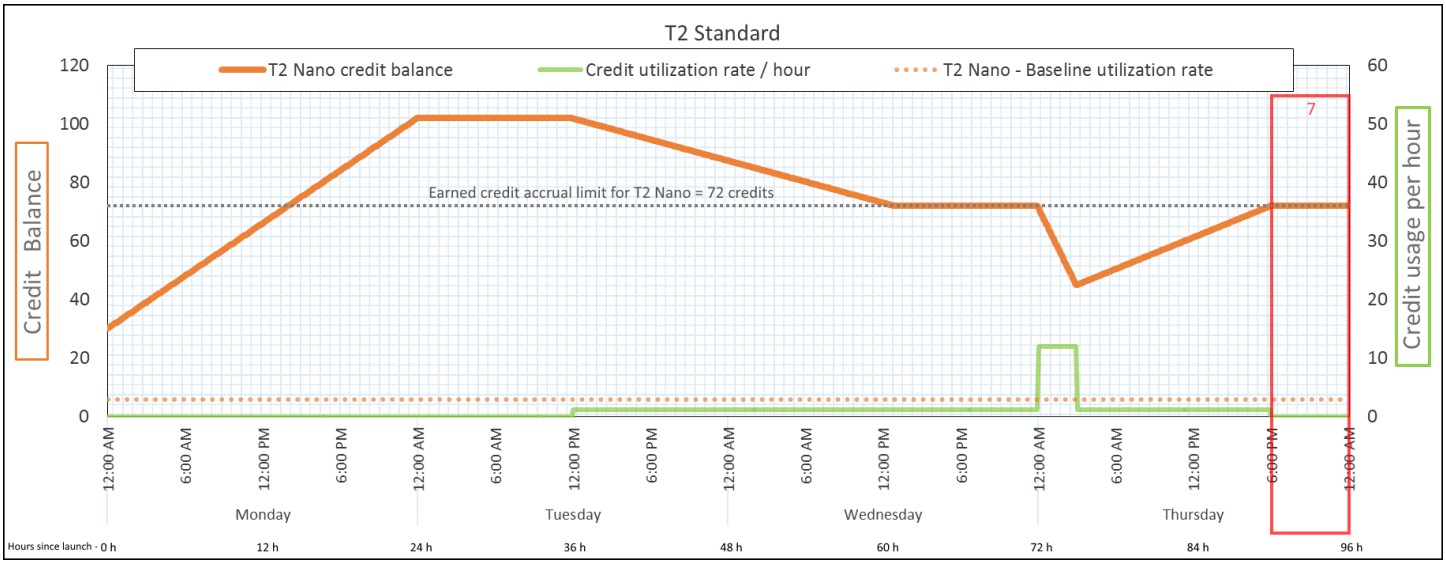
Conclusão

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.

Configurar instâncias de desempenho expansível

As etapas para a execução, monitoramento e modificação de instâncias de desempenho expansível (instâncias T) são semelhantes. A principal diferença é a especificação de crédito padrão na execução.

Cada família de instâncias T vem com a seguinte especificação de crédito padrão:

- As instâncias T4g, T3a e T3 são iniciadas como `unlimited`
- Instâncias T3 em um host dedicado são iniciadas como `standard`
- As instâncias T2 são executadas como `standard`

É possível alterar a especificação de crédito padrão para a conta.

Tarefas

- Configurar a especificação de crédito ao iniciar
- Configurar um grupo do Auto Scaling para definir a especificação de crédito como unlimited
- Gerenciar a especificação de crédito de uma instância de desempenho expansível
- Gerenciar a especificação de crédito padrão para uma conta

Configurar a especificação de crédito ao iniciar

É possível iniciar suas instâncias T com uma especificação de crédito de `unlimited` ou `standard`.

Os procedimentos a seguir descrevem como usar o console do EC2 ou a AWS CLI. Para obter informações sobre o uso de um grupo do Auto Scaling, consulte Configurar um grupo do Auto Scaling para definir a especificação de crédito como unlimited.

Console

Para configurar a especificação de crédito de uma instância ao iniciar

1. Siga o procedimento para iniciar uma instância.
2. Em Instance type (Tipo de instância), selecione um tipo de instância T.
3. Expanda Advanced details (Detalhes avançados). Em Especificação de crédito, selecione uma especificação de crédito.
4. No painel Resumo, analise a configuração da instância e selecione Iniciar instância.

AWS CLI

Para definir a especificação de crédito de uma instância ao iniciar

Use o comando run-instances com a opção `--credit-specification`.

```
--credit-specification CpuCredits=unlimited
```

PowerShell

Para definir a especificação de crédito de uma instância ao iniciar

Use o cmdlet New-EC2Instance com o parâmetro `-CreditSpecification_CpuCredit`.

```
-CreditSpecification_CpuCredit unlimited
```

Configurar um grupo do Auto Scaling para definir a especificação de crédito como unlimited

Quando as instâncias T são executadas ou iniciadas, elas precisam de créditos de CPU para uma boa experiência de bootstrapping. Se você usar um grupo do Auto Scaling para executar suas instâncias, recomendamos configurar suas instâncias como `unlimited`. Caso faça isso, as

instâncias usam créditos excedentes quando são automaticamente iniciadas ou reiniciadas pelo grupo do Auto Scaling. O uso de créditos excedentes impede restrições de performance.

Criar um modelo de execução

Use 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`.

Console

Para criar um modelo de execução que defina a especificação de crédito

1. Siga o procedimento Criar um modelo de execução usando configurações avançadas no Guia do usuário do Amazon EC2 Auto Scaling.
2. Em Launch template contents (Conteúdo do modelo de execução), para Instance type (Tipo de instância), escolha um tamanho de instância.
3. Para iniciar instâncias como `unlimited` em um grupo do Auto Scaling, em Advanced details (Detalhes avançados), para Credit specification (Especificação de crédito), escolha Unlimited (Ilimitado).
4. Ao terminar de definir os parâmetros do modelo de execução, escolha Create launch template (Criar modelo de execução).

AWS CLI

Para criar um modelo de execução que defina a especificação de crédito

Use o comando create-launch-template.

```
aws ec2 create-launch-template \
    --launch-template-name my-launch-template \
    --version-description FirstVersion \
    --launch-template-data CreditSpecification={CpuCredits=unlimited}
```

PowerShell

Para criar um modelo de execução que defina a especificação de crédito

Use o cmdlet New-EC2LaunchTemplate. Defina a especificação de crédito para os dados do modelo de execução conforme descrito a seguir.

```
$creditSpec = New-Object Amazon.EC2.Model.CreditSpecificationRequest
$creditSpec.CpuCredits = "unlimited"
$launchTemplateData = New-Object Amazon.EC2.Model.RequestLaunchTemplateData
$launchTemplateData.CreditSpecification = $creditSpec
```

Associar um grupo de Auto Scaling a um modelo de execução

Para associar o modelo de execução a um grupo do Auto Scaling, crie o grupo do Auto Scaling usando o modelo de execução ou adicione o modelo de execução a um grupo do Auto Scaling existente.

Console

Para criar um grupo do Auto Scaling usando um modelo de inicialização

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Na barra de navegação na parte superior da tela, selecione a mesma região usada ao criar o modelo de execução.
3. No painel de navegação, escolha Auto Scaling Groups, Criar grupo do Auto Scaling.
4. Escolha Launch Template (Modelo de execução), selecione seu modelo de execução e, seguida, Next Step (Próxima etapa).
5. Preencha os campos para o grupo do Auto Scaling. Quando você terminar de revisar as definições de configuração na Review page (Página de revisão), selecione Create Auto Scaling group (Criar grupo do Auto Scaling). Para obter mais informações, consulte Criação de um grupo do Auto Scaling usando um modelo de execução no Guia do usuário do Amazon EC2 Auto Scaling.

Para adicionar um modelo de inicialização a um grupo do Auto Scaling existente

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).

AWS CLI

Para criar um grupo do Auto Scaling usando um modelo de inicialização

Use o comando create-auto-scaling-group e especifique o parâmetro `--launch-template`.

Para adicionar um modelo de inicialização a um grupo do Auto Scaling existente

Use o comando update-auto-scaling-group e especifique o parâmetro `--launch-template`.

PowerShell

Para criar um grupo do Auto Scaling usando um modelo de inicialização

Use o cmdlet New-ASAutoScalingGroup e especifique o parâmetro `-LaunchTemplate_LaunchTemplateId` ou `-LaunchTemplate_LaunchTemplateName`.

Para adicionar um modelo de inicialização a um grupo do Auto Scaling existente

Use o cmdlet Update-ASAutoScalingGroup e especifique o parâmetro `-LaunchTemplate_LaunchTemplateId` ou `-LaunchTemplate_LaunchTemplateName`.

Gerenciar a especificação de crédito de uma instância de desempenho expansível

É possível alterar a qualquer momento entre `unlimited` e `standard` a especificação de crédito de uma instância T interrompida ou em execução.

Observe que, no modo `unlimited`, uma instância pode gastar créditos excedentes, o que pode gerar uma cobrança adicional. Para obter mais informações, consulte Os créditos excedentes podem gerar cobranças.

Console

Para gerenciar a especificação de crédito de uma instância

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação à esquerda, selecione Instâncias.

3. (Opcional) Selecione uma instância. Na guia Detalhes, vá para Especificação de crédito. O valor é `unlimited` ou `standard`.
4. (Opcional) Para modificar a especificação de crédito para várias instâncias ao mesmo tempo, selecione todas elas.
5. Escolha Actions (Ações), Instance settings (Configurações de instância), Change credit specification (Alterar especificação de crédito). Essa opção só será ativada se você tiver selecionado uma instância T.
6. Para o Modo ilimitado, marque ou desmarque a caixa de seleção ao lado de cada ID de instância.

AWS CLI

Para obter a especificação de crédito de uma instância

Use o comando describe-instance-credit-specifications. Se você não especificar um ID de instância, todas as instâncias com a especificação de crédito `unlimited` serão retornadas. A saída também incluiria 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.

```
aws ec2 describe-instance-credit-specifications \
    --instance-id i-1234567890abcdef0 \
    --query InstanceCreditSpecifications[].CpuCredits \
    --output text
```

O seguinte é um exemplo de saída.

```
unlimited
```

Para definir a especificação de crédito de uma instância

Use o comando modify-instance-credit-specification.

```
aws ec2 modify-instance-credit-specification \
    --region us-east-1 \
    --instance-credit-specification
 "InstanceId=i-1234567890abcdef0,CpuCredits=unlimited"
```

PowerShell

Para obter a especificação de crédito de uma instância

Use o cmdlet Get-EC2CreditSpecification.

```
(Get-EC2CreditSpecification `
    -InstanceId i-1234567890abcdef0).CpuCredits
```

O seguinte é um exemplo de saída.

```
unlimited
```

Para definir a especificação de crédito de uma instância

Use o cmdlet Edit-EC2InstanceCreditSpecification.

```
Edit-EC2InstanceCreditSpecification `
    -Region us-east-1 `
    -InstanceCreditSpecification @({InstanceId="i-1234567890abcdef0"
 CpuCredits="unlimited"})
```

Gerenciar a especificação de crédito padrão para uma conta

Cada família de instâncias T vem com uma especificação de crédito padrão. É possível alterar a especificação de crédito padrão por família de instâncias T no nível da conta por região da AWS. Os valores válidos para a especificação de crédito padrão são `unlimited` e `standard`.

Se você usar o assistente de inicialização de instância no console do EC2 para iniciar instâncias, o valor selecionado para a especificação de crédito substituirá a especificação de crédito padrão no nível da conta. Se você usar a AWS CLI para executar instâncias, todas as novas instâncias T na conta serão executadas usando a opção de crédito padrão. A especificação de crédito para instâncias existentes em execução ou interrompidas não é afetada.

Consideração

A especificação de crédito padrão para uma família de instâncias pode ser modificada apenas uma vez em um período contínuo de 5 minutos e até quatro vezes em um período contínuo de 24 horas.

Console

Para gerenciar a especificação de crédito padrão

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Para alterar a Região da AWS, use o seletor de regiões no canto superior direito da página.
3. No painel de navegação, escolha EC2 Dashboard (Painel do EC2).
4. Em Account attributes (Atributos da conta), escolha Default credit specification (Especificação de crédito padrão).
5. Escolha Gerenciar.
6. Para cada família de instâncias, escolha Unlimited (Ilimitado) ou Standard (Padrão) e, em seguida, escolha Update (Atualizar).

AWS CLI

Para obter a especificação de crédito padrão

Use o comando get-default-credit-specification.

```
aws ec2 get-default-credit-specification \
    --region us-east-1 \
    --instance-family t2 \
    --query InstanceFamilyCreditSpecifications[].CpuCredits \
    --output text
```

O seguinte é um exemplo de saída.

```
standard
```

Para definir a especificação de crédito padrão

Use o comando modify-default-credit-specification. O exemplo a seguir define o valor como `unlimited`.

```
aws ec2 modify-default-credit-specification \
    --region us-east-1 \
    --instance-family t2 \
    --cpu-credits unlimited
```

PowerShell

Para obter a especificação de crédito padrão

Use o cmdlet Get-EC2DefaultCreditSpecification.

```
(Get-EC2DefaultCreditSpecification `
    -Region us-east-1 `
    -InstanceFamily t2).CpuCredits
```

O seguinte é um exemplo de saída.

```
standard
```

Para definir a especificação de crédito padrão

Use o cmdlet Edit-EC2DefaultCreditSpecification. O exemplo a seguir define o valor como `unlimited`.

```
Edit-EC2DefaultCreditSpecification `
    -Region us-east-1 `
    -InstanceFamily t2 `
    -CpuCredit unlimited
```

Monitore créditos de CPU para instâncias com capacidade de expansão

O EC2 envia métricas para o Amazon CloudWatch. É possível ver as métricas de crédito da CPU nas métricas do Amazon EC2 por instância do console do CloudWatch ou usando a AWS CLI para listar as métricas de cada instância. Para obter mais informações, consulte As métricas do CloudWatch que estão disponíveis para as instâncias.

Conteúdo

- Métricas adicionais do CloudWatch para instâncias expansíveis
- Calcular o uso de crédito da CPU

Métricas adicionais do CloudWatch para instâncias expansíveis

As instâncias expansíveis têm estas métricas adicionais do CloudWatch, que são atualizadas a cada cinco minutos:

- `CPUCreditUsage` – O número de créditos de CPU gastos durante o período de medição.
- `CPUCreditBalance` – o número de créditos de CPU que uma instância acumulou. Esse saldo é esgotado quando a CPU apresenta expansões e os créditos de CPU são gastos com mais rapidez do que são ganhos.
- `CPUSurplusCreditBalance` – O número de créditos de CPU excedentes gastos para sustentar a utilização de CPU quando o valor de `CPUCreditBalance` for zero.
- `CPUSurplusCreditsCharged` – o número de créditos de CPU excedentes que ultrapassam o número máximo de créditos de CPU que podem ser ganhos em um período de 24 horas, resultando em uma cobrança adicional.

Essas duas últimas métricas aplicam-se somente a instâncias configuradas como `unlimited`.

A tabela a seguir descreve as métricas do CloudWatch para instâncias expansíveis. Para obter mais informações, consulte As métricas do CloudWatch que estão disponíveis para as instâncias.

Métrica	Descrição
`CPUCreditUsage`	O número de créditos de CPU gastos pela instância por utilização de CPU. Um crédito de CPU equivale a um vCPU em execução em 100% de utilização por um minuto ou a uma combinação equivalente de vCPUs, utilização e tempo (por exemplo, um vCPU em execução a 50% de utilização por dois minutos ou dois vCPUs em execução a 25% de utilização por dois minutos). As métricas de crédito de CPU estão disponíveis a uma frequência de apenas 5 minutos. Se você especificar um período de mais cinco minutos, use a estatística `Sum` em vez da estatística `Average`. Unidades: créditos (minutos de vCPU)
`CPUCreditBalance`	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.

Métrica	Descrição
	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. Os créditos do `CPUCreditBalance` são disponibilizados para que a instância gaste e apresente expansão com uma utilização de CPU acima da linha de base. Quando uma instância está em execução, os créditos do `CPUCreditBalance` não expiram. Quando uma instância T4g, T3a ou T3 é interrompida, o valor de `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. As métricas de crédito de CPU estão disponíveis a uma frequência de apenas 5 minutos. Unidades: créditos (minutos de vCPU)
`CPUSurplusCreditBalance`	O número de créditos excedentes gastos por uma instância `unlimited` quando seu valor `CPUCreditBalance` é zero. 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. Unidades: créditos (minutos de vCPU)

Métrica	Descrição
`CPUSurplusCreditsCharged`	O número de créditos excedentes gastos que não são pagos pelos créditos de CPU ganhos e que, portanto, incorrem em uma cobrança adicional. Os créditos excedentes gastos são cobrados quando uma das seguintes situações ocorre: • 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 `unlimited` para `standard`. Unidades: créditos (minutos de vCPU)

Calcular o uso de crédito da CPU

O uso de créditos de CPU de instâncias é calculado por meio das métricas de instância do CloudWatch descritas na tabela anterior.

O Amazon EC2 envia as métricas ao CloudWatch a cada cinco minutos. Uma referência ao valor anterior de uma métrica em qualquer momento implica o valor anterior da métrica, enviado cinco minutos atrás.

Calcular uso de créditos de CPU de instâncias padrão

- O saldo de crédito de CPU aumentará se a utilização de CPU ficar abaixo da linha de base, quando os créditos gastos forem inferiores aos créditos ganhos no intervalo anterior de cinco minutos.
- O saldo de crédito de CPU diminuirá se a utilização de CPU ficar acima da linha de base, quando os créditos gastos forem superiores aos créditos ganhos no intervalo anterior de cinco minutos.

Matematicamente, isso é capturado pela equação a seguir:

Example

```
CPUCreditBalance = prior CPUCreditBalance + [Credits earned per hour * (5/60) -
 CPUCreditUsage]
```

O tamanho da instância determina o número de créditos que a instância pode ganhar por hora e o número de créditos ganhos que ela pode acumular no saldo de créditos. Para obter informações sobre o número de créditos ganhos por hora e o limite de saldo de créditos para cada tamanho de instância, consulte a Tabela de créditos.

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, é possível calcular o valor `CPUCreditBalance`:

Example

```
CPUCreditBalance = 2 + [0.5 - 1] = 1.5
```

Cálculo de uso de créditos de CPU de instâncias ilimitadas

Quando uma instância expansível precisa ter uma expansão 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 expansão de CPU enquanto

precisar. Quando a utilização de CPU ficar abaixo da linha de base, os créditos excedentes sempre serão pagos antes que a instância acumule créditos ganhos.

Usamos o termo `Adjusted balance` nas equações a seguir para refletir a atividade que ocorre nesse intervalo de cinco minutos. Usamos esse valor para atingir os valores das métricas do `CPUCreditBalance` de `CPUSurplusCreditBalance` e CloudWatch.

Example

```
Adjusted balance = [prior CPUCreditBalance - prior CPUSurplusCreditBalance] + [Credits
 earned per hour * (5/60) - CPUCreditUsage]
```

O valor `0` em `Adjusted balance` indica que a instância gastou todos os créditos ganhos para expansão 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 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 expansão. 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 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.

Aceleração de performance com instâncias de GPU

As instâncias baseadas em GPU concedem acesso a GPUs NVIDIA com milhares de núcleos de computação. É possível essas instâncias para acelerar aplicações científicas, de engenharia e renderização utilizando as estruturas de computação paralela CUDA ou Open Computing Language (OpenCL). Também é possível usá-las para aplicações gráficas, incluindo transmissão de jogos, transmissão de aplicações 3-D e outras workloads gráficas.

Antes de ativar ou otimizar uma instância baseada em GPU, é necessário instalar os drivers apropriados, da seguinte forma:

- Para instalar drivers da NVIDIA em uma instância com uma GPU da NVIDIA conectada, como uma instância P3 ou G4dn, consulte Drivers NVIDIA.
- Para instalar drivers da AMD em uma instância com uma GPU da AMD conectada, como uma instância G4ad, consulte Drivers AMD.

Conteúdo

- Ativação das aplicações virtuais NVIDIA GRID em instâncias baseadas em GPU do Amazon EC2
- Otimização das configurações de GPU em instâncias do Amazon EC2
- Configuração de monitores Dual 4K em instâncias G4ad do Linux
- Começar a usar instâncias aceleradas por GPU

Ativação das aplicações virtuais NVIDIA GRID em instâncias baseadas em GPU do Amazon EC2

Para ativar as aplicações virtuais GRID em instâncias baseadas em GPU que usam GPUs da NVIDIA (a estação de trabalho virtual NVIDIA GRID está habilitada por padrão), você deve definir o tipo de produto para o driver. O procedimento a ser usado dependerá do sistema operacional da instância.

Instâncias do Linux

Para ativar aplicações virtuais GRID nas instâncias do Linux

1. Crie o arquivo `/etc/nvidia/gridd.conf` a partir do arquivo de modelo fornecido.

   ```
   [ec2-user ~]$ sudo cp /etc/nvidia/gridd.conf.template /etc/nvidia/gridd.conf
   ```

2. Abra o arquivo `/etc/nvidia/gridd.conf` no editor de texto favorito.
3. Localize a linha `FeatureType` e defina-a como igual a `0`. Em seguida, adicione uma linha com `IgnoreSP=TRUE`.

   ```
   FeatureType=0 IgnoreSP=TRUE
   ```

4. Salve o arquivo e saia.
5. Reinicialize a instância para obter a nova configuração.

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

Instâncias do Windows

Para ativar aplicações virtuais GRID nas instâncias do Windows

1. Execute regedit.exe para abrir o editor do registro.
2. Navegue até `HKEY_LOCAL_MACHINE\SOFTWARE\NVIDIA Corporation\Global\GridLicensing`.
3. Abra o menu de contexto (clique com o botão direito do mouse) no painel direito e escolha New, DWORD.
4. Em Nome, digite FeatureType e `Enter`.

5. Abra o menu de contexto (clique com o botão direito do mouse) em FeatureType e escolha Modify.
6. Para Dados de valor, insira `0` para NVIDIA Grid Virtual Applications e escolha OK.
7. Abra o menu de contexto (clique com o botão direito do mouse) no painel direito e escolha New, DWORD.
8. Em Name, digite IgnoreSP e pressione `Enter`.
9. Abra o menu de contexto (clique com o botão direito do mouse) em IgnoreSP e escolha Modify.
10. Em Value data, digite 1 e escolha OK.
11. Feche o editor de Registro.

Otimização das configurações de GPU em instâncias do Amazon EC2

Há várias otimizações de configuração de GPU que é possível executar para obter a melhor performance nas instâncias GPU NIVIDIA. Com alguns desses tipos de instância, o driver NVIDIA usa um recurso de autoboost, que varia as velocidades de clock da GPU. Ao desativar o recurso de autoboost e definir as velocidades de clock de GPU como a frequência máxima, você pode atingir a performance máxima de forma consistente com suas instâncias de GPU.

Otimização das configurações de GPU no Linux

1. Defina as configurações de GPU para serem persistentes. Esse comando pode levar vários minutos para ser executado.

   ```
   [ec2-user ~]$ sudo nvidia-persistenced
   ```

2. [Somente para instâncias G3 e P2] Desabilite o recurso de autoboost para todas as GPUs na instância.

   ```
   [ec2-user ~]$ sudo nvidia-smi --auto-boost-default=0
   ```

3. Defina todas as velocidades de relógio de GPU como a frequência máxima. Use a memória e as velocidades de relógio de placa gráfica especificadas nos seguintes comandos.

   Algumas versões do driver NVIDIA não suportam a configuração da velocidade de clock da aplicação e exibem o erro `"Setting applications clocks is not supported for GPU..."`, que é possível ignorar.

   - Instâncias G3:

```
[ec2-user ~]$ sudo nvidia-smi -ac 2505,1177
```

- Instâncias G4dn:

```
[ec2-user ~]$ sudo nvidia-smi -ac 5001,1590
```

- Instâncias G5:

```
[ec2-user ~]$ sudo nvidia-smi -ac 6250,1710
```

- Instâncias G6, G6f, Gr6 e Gr6f:

```
[ec2-user ~]$ sudo nvidia-smi -ac 6251,2040
```

- Instâncias G6e:

```
[ec2-user ~]$ sudo nvidia-smi -ac 9001,2520
```

- Instâncias G7e:

```
[ec2-user ~]$ sudo nvidia-smi -ac 12481,2430
```

- Instâncias P2:

```
[ec2-user ~]$ sudo nvidia-smi -ac 2505,875
```

- Instâncias P3 e P3dn:

```
[ec2-user ~]$ sudo nvidia-smi -ac 877,1530
```

- Instâncias P4d:

```
[ec2-user ~]$ sudo nvidia-smi -ac 1215,1410
```

- Instâncias P4de:

```
[ec2-user ~]$ sudo nvidia-smi -ac 1593,1410
```

- Instâncias P5:

```
[ec2-user ~]$ sudo nvidia-smi -ac 2619,1980
```

- Instâncias P5e e P5en:

```
[ec2-user ~]$ sudo nvidia-smi -ac 3201,1980
```

- Instâncias P6-B200:

```
[ec2-user ~]$ sudo nvidia-smi -ac 3996,1965
```

- Instâncias P6-B300:

```
[ec2-user ~]$ sudo nvidia-smi -ac 3996,2032
```

Otimização das configurações de GPU no Windows

1. Abra uma janela do PowerShell e navegue para a pasta de instalação NVIDIA.

```
PS C:\> cd "C:\Windows\System32\DriverStore\FileRepository\nvgridsw_aws.inf_*\"
```

2. [Somente para instâncias G3 e P2] Desabilite o recurso de autoboost para todas as GPUs na instância.

```
PS C:\> .\nvidia-smi --auto-boost-default=0
```

3. Defina todas as velocidades de relógio de GPU como a frequência máxima. Use a memória e as velocidades de relógio de placa gráfica especificadas nos seguintes comandos.

   Algumas versões do driver NVIDIA não suportam a configuração da velocidade de clock da aplicação e exibem o erro `"Setting applications clocks is not supported for GPU..."`, que é possível ignorar.

   - Instâncias G3:

```
PS C:\> .\nvidia-smi -ac "2505,1177"
```

   - Instâncias G4dn:

```
PS C:\> .\nvidia-smi -ac "5001,1590"
```

- Instâncias G5:

```
PS C:\> .\nvidia-smi -ac "6250,1710"
```

- Instâncias G6, G6f, Gr6 e Gr6f:

```
PS C:\> .\nvidia-smi -ac "6251,2040"
```

- Instâncias G6e:

```
PS C:\> .\nvidia-smi -ac "9001,2520"
```

- Instâncias P2:

```
PS C:\> .\nvidia-smi -ac "2505,875"
```

- Instâncias P3 e P3dn:

```
PS C:\> .\nvidia-smi -ac "877,1530"
```

Configuração de monitores Dual 4K em instâncias G4ad do Linux

Depois de executar uma instância G4ad, você pode configurar monitores Dual 4K.

Para instalar os drivers AMD e configurar telas duplas

1. Conecte-se à sua instância Linux para obter o endereço de barramento PCI da GPU a ser direcionado ao Dual 4K (2x4k):

   ```
   lspci -vv | grep -i amd
   ```

   Você terá um resultado semelhante ao seguinte:

   ```
   00:1e.0 Display controller: Advanced Micro Devices, Inc. [*AMD*/ATI] Device 7362 (rev
    c3)
   Subsystem: Advanced Micro Devices, Inc. [AMD/ATI] Device 0a34
   ```

2. O endereço de barramento PCI é 00:1e.0 na saída acima. Crie um arquivo denominado `/etc/modprobe.d/amdgpu.conf` e adicione o seguinte:

```
options amdgpu virtual_display=0000:00:1e.0,2
```

3. Para instalar drivers da AMD no Linux, consulte Drivers AMD para a instância do EC2. Se você já tiver o driver da GPU AMD instalado, precisará reconstruir os módulos do kernel amdgpu via dkms.

4. Utilize o arquivo xorg.conf abaixo para definir a topologia de tela dupla (2x4K) e salve o arquivo no `/etc/X11/xorg.conf`:

```
~$ cat /etc/X11/xorg.conf
Section "ServerLayout"
    Identifier     "Layout0"
    Screen          0 "Screen0"
    Screen        1 "Screen1"
    InputDevice     "Keyboard0" "CoreKeyboard"
    InputDevice     "Mouse0" "CorePointer"
    Option          "Xinerama" "1"
EndSection
Section "Files"
    ModulePath "/opt/amdgpu/lib64/xorg/modules/drivers"
    ModulePath "/opt/amdgpu/lib/xorg/modules"
    ModulePath "/opt/amdgpu-pro/lib/xorg/modules/extensions"
    ModulePath "/opt/amdgpu-pro/lib64/xorg/modules/extensions"
    ModulePath "/usr/lib64/xorg/modules"
    ModulePath "/usr/lib/xorg/modules"
EndSection
Section "InputDevice"
    # generated from default
    Identifier     "Mouse0"
    Driver         "mouse"
    Option         "Protocol" "auto"
    Option         "Device" "/dev/psaux"
    Option         "Emulate3Buttons" "no"
    Option         "ZAxisMapping" "4 5"
EndSection
Section "InputDevice"
    # generated from default
    Identifier     "Keyboard0"
    Driver         "kbd"
EndSection
```

```
Section "Monitor"
    Identifier     "Virtual"
    VendorName     "Unknown"
    ModelName      "Unknown"
    Option         "Primary" "true"
EndSection

Section "Monitor"
    Identifier     "Virtual-1"
    VendorName     "Unknown"
    ModelName      "Unknown"
    Option         "RightOf" "Virtual"
EndSection

Section "Device"
    Identifier     "Device0"
    Driver         "amdgpu"
    VendorName     "AMD"
    BoardName      "Radeon MxGPU V520"
    BusID          "PCI:0:30:0"
EndSection

Section "Device"
    Identifier     "Device1"
    Driver         "amdgpu"
    VendorName     "AMD"
    BoardName      "Radeon MxGPU V520"
    BusID          "PCI:0:30:0"
EndSection

Section "Extensions"
    Option         "DPMS" "Disable"
EndSection

Section "Screen"
    Identifier     "Screen0"
    Device         "Device0"
    Monitor        "Virtual"
    DefaultDepth   24
    Option         "AllowEmptyInitialConfiguration" "True"
    SubSection "Display"
        Virtual    3840 2160
        Depth      32
```

```
    EndSubSection
EndSection

Section "Screen"
    Identifier     "Screen1"
    Device         "Device1"
    Monitor        "Virtual"
    DefaultDepth   24
    Option         "AllowEmptyInitialConfiguration" "True"
    SubSection "Display"
        Virtual    3840 2160
        Depth      32
    EndSubSection
EndSection
```

5. Configure o DCV seguindo as instruções de configuração de um desktop interativo.
6. Quando a configuração do DCV terminar, reinicialize.
7. Verifique se o driver está funcional:

```
dmesg | grep amdgpu
```

   A resposta deve ser parecida com o seguinte:

```
Initialized amdgpu
```

8. Você verá na saída de `DISPLAY=:0 xrandr -q` que existem dois monitores virtuais conectados:

```
~$ DISPLAY=:0 xrandr -q
Screen 0: minimum 320 x 200, current 3840 x 1080, maximum 16384 x 16384
Virtual connected primary 1920x1080+0+0 (normal left inverted right x axis y axis)
 0mm x 0mm
 4096x3112  60.00
 3656x2664  59.99
 4096x2160  60.00
 3840x2160  60.00
 1920x1200  59.95
 1920x1080  60.00
 1600x1200  59.95
 1680x1050  60.00
 1400x1050  60.00
 1280x1024  59.95
```

```
 1440x900 59.99
 1280x960 59.99
 1280x854 59.95
 1280x800 59.96
 1280x720 59.97
 1152x768 59.95
 1024x768 60.00 59.95
 800x600  60.32 59.96 56.25
 848x480  60.00 59.94
 720x480  59.94
 640x480  59.94 59.94
Virtual-1 connected 1920x1080+1920+0 (normal left inverted right x axis y axis) 0mm x
 0mm
 4096x3112  60.00
 3656x2664  59.99
 4096x2160  60.00
 3840x2160  60.00
 1920x1200  59.95
 1920x1080  60.00
 1600x1200  59.95
 1680x1050  60.00
 1400x1050  60.00
 1280x1024  59.95
 1440x900 59.99
 1280x960 59.99
 1280x854 59.95
 1280x800 59.96
 1280x720 59.97
 1152x768 59.95
 1024x768 60.00 59.95
 800x600  60.32 59.96 56.25
 848x480  60.00 59.94
 720x480  59.94
640x480  59.94 59.94
```

9. Quando você se conectar ao DCV, altere a resolução para 2x4K, confirmando que o suporte de monitor duplo está registrado pelo DCV.

Configuração de uma área de trabalho interativa para o Linux

Após confirmar que a instância do Linux tem o driver de GPU da AMD instalado e que o driver AMDgpu está em uso, será possível instalar um gerenciador de área de trabalho interativa. Recomendamos o ambiente de desktop MATE para obter a melhor compatibilidade e performance.

Pré-requisito

Abra um editor de texto e salve o seguinte como um arquivo chamado `xorg.conf`. Você precisará desse arquivo em sua instância.

```
Section "ServerLayout"
Identifier     "Layout0"
Screen          0 "Screen0"
InputDevice     "Keyboard0" "CoreKeyboard"
InputDevice     "Mouse0" "CorePointer"
EndSection
Section "Files"
ModulePath "/opt/amdgpu/lib64/xorg/modules/drivers"
ModulePath "/opt/amdgpu/lib/xorg/modules"
ModulePath "/opt/amdgpu-pro/lib/xorg/modules/extensions"
ModulePath "/opt/amdgpu-pro/lib64/xorg/modules/extensions"
ModulePath "/usr/lib64/xorg/modules"
ModulePath "/usr/lib/xorg/modules"
EndSection
Section "InputDevice"
# generated from default
Identifier     "Mouse0"
Driver         "mouse"
Option         "Protocol" "auto"
Option         "Device" "/dev/psaux"
Option         "Emulate3Buttons" "no"
Option         "ZAxisMapping" "4 5"
EndSection
Section "InputDevice"
# generated from default
Identifier     "Keyboard0"
Driver         "kbd"
EndSection
Section "Monitor"
Identifier     "Monitor0"
VendorName     "Unknown"
ModelName      "Unknown"
```

```
EndSection
Section "Device"
Identifier     "Device0"
Driver         "amdgpu"
VendorName     "AMD"
BoardName      "Radeon MxGPU V520"
BusID          "PCI:0:30:0"
EndSection
Section "Extensions"
Option         "DPMS" "Disable"
EndSection
Section "Screen"
Identifier     "Screen0"
Device         "Device0"
Monitor        "Monitor0"
DefaultDepth   24
Option         "AllowEmptyInitialConfiguration" "True"
SubSection "Display"
    Virtual    3840 2160
    Depth      32
EndSubSection
EndSection
```

Para configurar um desktop interativo no Amazon Linux 2

1. Instale o repositório EPEL.

   ```
   [ec2-user ~]$ sudo amazon-linux-extras install epel -y
   ```

2. Instale o desktop MATE.

   ```
   [ec2-user ~]$ sudo amazon-linux-extras install mate-desktop1.x -y
   [ec2-user ~]$ sudo yum groupinstall "MATE Desktop" -y
   [ec2-user ~]$ sudo systemctl disable firewalld
   ```

3. Copie o arquivo `xorg.conf` para `/etc/X11/xorg.conf`.

4. Reinicialize a instância.

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

5. (Opcional) Instale o servidor Amazon DCV para usar o Amazon DCV como um protocolo de exibição de alta performance. Depois, conecte-se a uma sessão do Amazon DCV usando o cliente preferencial.

Para configurar um desktop interativo no Ubuntu

1. Instale o desktop MATE.

```
$ sudo apt install xorg-dev ubuntu-mate-desktop -y
$ sudo apt purge ifupdown -y
```

2. Copie o arquivo `xorg.conf` para `/etc/X11/xorg.conf`.
3. Reinicialize a instância.

```
$ sudo reboot
```

4. Instale o codificador AMF para a versão apropriada do Ubuntu.

```
$ sudo apt install ./amdgpu-pro-20.20-*/amf-amdgpu-pro_20.20-*_amd64.deb
```

5. (Opcional) Instale o servidor Amazon DCV para usar o Amazon DCV como um protocolo de exibição de alta performance. Depois, conecte-se a uma sessão do Amazon DCV usando o cliente preferencial.
6. Após a instalação do DCV, dê permissões de vídeo ao usuário DCV:

```
$ sudo usermod -aG video dcv
```

Para configurar um desktop interativo no CentOS

1. Instale o repositório EPEL.

```
$ sudo yum update -y
$ sudo yum install epel-release -y
```

2. Instale o desktop MATE.

```
$ sudo yum groupinstall "MATE Desktop" -y
$ sudo systemctl disable firewalld
```

3. Copie o arquivo `xorg.conf` para `/etc/X11/xorg.conf`.
4. Reinicialize a instância.

```
$ sudo reboot
```

5. (Opcional) Instale o servidor Amazon DCV para usar o Amazon DCV como um protocolo de exibição de alta performance. Depois, conecte-se a uma sessão do Amazon DCV usando o cliente preferencial.

Começar a usar instâncias aceleradas por GPU

A última geração de tipos de instância acelerada por GPU de quinta geração, como os mostrados na lista a seguir, oferecem os recursos de maior performance para aplicações de aprendizado profundo e computação de alta performance (HPC). Selecione o link do tipo de instância para saber mais sobre seus recursos.

- Família P6
- Família P
- Família P

Para obter uma lista completa das especificações de tipo de instância para tipos de instâncias aceleradas, consulte Computação acelerada na referência de Tipos de instância do Amazon EC2.

Configuração de software

A maneira mais fácil de começar a usar a última geração de tipos de instâncias aceleradas de GPU de quinta geração é lançar uma instância de uma AMI do AWS Deep Learning pré-configurada com todo o software necessário. Para conecer os AMIs de deep learning da AWS mais recentes para uso com tipos de instância acelerada por GPU, consulte DLAMI compatível com P6, no Guia do desenvolvedor do AMIs de deep learning da AWS.

Se você precisar criar uma AMI personalizada para inicializar instâncias que hospedam aplicações de aprendizado profundo ou HPC, recomendamos instalar as seguintes versões mínimas de software em cima da imagem base.

Tipo de instância	Driver NVIDIA	CUDA	NVIDIA GDRCopy	Instaladora EFA	NCCL	EFA K8s [1]
G7e	575	12.9	2,5	1.45.0	2.28.3	0.5.10
P5	530	12.1	2.3	1.24.1	2.18.3	0.4.4
P5.4xlarge	530	12.1	2.3	1,43.1 [2]	2.18.3	0.4.4
P5e	550	12.1	2.3	1.24.1	2.18.3	0.5.5
P5en	550	12.1	2.3	1.24.1	2.18.3	0.5.6
P6-B200	570	12.8	2,5	1.41.0	2.26.2-1	0.5.10
P6e-GB200	570	12.8	2,5	1.41.0	2.26.2-1	0.5.10
P6-B300	580	13.0	2,5	1.44.0	2.28.3	0.5.10

[1] A coluna EFA K8s contém a versão mínima recomendada para o `aws-efa-k8s-device-plugin`.

[2] Há um problema de compatibilidade que afeta as instâncias `P5.4xlarge` em que a comunicação entre GPUs usa o Elastic Fabric Adapter (EFA) e a NVIDIA Collective Communications Library (NCCL). Para mitigar o problema, defina a variável de ambiente `FI_HMEM_DISABLE_P2P` como `1` e certifique-se de instalar o EFA versão 1.43.1 ou mais recente.

> **Note**
>
> Se você usar a versão 1.41.0 do instalador EFA, o `aws-ofi-nccl plugin` vem com ela. Para versões anteriores do instalador do EFA, use o `aws-ofi-nccl plugin` versão `1.7.2-aws` ou posterior.

Também recomendamos que você configure a instância para não usar estados C mais profundos. Para obter mais informações, consulte High performance and low latency by limiting deeper C-states no Amazon Linux 2 User Guide. As mais recentes AMIs de GPU básica de aprendizado profundo da AWS estão pré-configuradas para não usar estados C mais profundos.

Sobre como configurar redes e Elastic Fabric Adapter (EFA), consulte Maximize a largura de banda da rede em instâncias do Amazon EC2 com várias placas de rede.

Instâncias Mac do Amazon EC2

As instâncias Mac do EC2 são ideais para desenvolver, criar, testar e assinar aplicações para plataformas Apple, como iPhone, iPad, Mac, Vision Pro, Apple Watch, Apple TV e Safari. É possível se conectar à instância do Mac usando SSH ou Apple Remote Desktop (ARD).

> **Note**
>
> A unidade de faturamento é o host dedicado. As instâncias em execução nesse host não têm custo adicional.

As instâncias Mac do Amazon EC2 oferecem suporte nativo ao sistema operacional macOS.

- As instâncias x86 Mac do EC2 (`mac1.metal`) são montadas em hardware Mac mini 2018 com processadores Intel Core i7 de oitava geração (Coffee Lake) de 3,2 GHz, 6 núcleos físicos e 12 núcleos lógicos, e 32 GiB de memória.
- As instâncias M1 Mac do EC2 (`mac2.metal`) são montadas em hardware Mac mini 2020 com processador M1 em chip Apple, 8 núcleos de CPU, 8 núcleos de GPU, 16 GiB de memória e o Apple Neural Engine de 16 núcleos.
- As instâncias M1 Ultra Mac do EC2 (`mac2-m1ultra.metal`) são montadas em hardware Mac Studio 2022 com processador M1 Ultra em chip Apple, 20 núcleos de CPU, 64 núcleos de GPU, 128 GiB de memória e o Apple Neural Engine de 32 núcleos.
- As instâncias M2 Mac do EC2 (`mac2-m2.metal`) são montadas em hardware Mac mini 2023 com processador M2 em chip Apple, 8 núcleos de CPU, 10 núcleos de GPU, 24 GiB de memória e o Apple Neural Engine de 16 núcleos.
- As instâncias Mac M2 Pro do EC2 (`mac2-m2pro.metal`) são montadas em hardware Mac mini 2023, com processador M2 Pro em chip Apple, 12 núcleos de CPU, 19 núcleos de GPU, 32 GiB de memória e o Apple Neural Engine de 16 núcleos.
- As instâncias Mac M4 do EC2 (`mac-m4.metal`) são montadas em hardware Mac mini 2024, com processador M4 em chip Apple, 10 núcleos de CPU, 10 núcleos de GPU, 24 GiB de memória e o Apple Neural Engine de 16 núcleos.

- As instâncias Mac M4 Pro do EC2 (`mac-m4pro.metal`) são montadas em hardware Mac mini 2024, com processador M4 Pro em chip Apple, 14 núcleos de CPU, 20 núcleos de GPU, 48 GiB de memória e o Apple Neural Engine de 16 núcleos.

Os hosts dedicados do Amazon EC2 Mac são compatíveis com a recuperação automática do host dedicado e com a manutenção do host com base na reinicialização.

Conteúdo

- Considerações
- Prontidão da instância
- AMIs do macOS do EC2
- EC2 MacOS Init
- Amazon EC2 System Monitor para macOS
- Recursos relacionados
- Iniciar uma instância do Mac usando o Console de gerenciamento da AWS ou a AWS CLI
- Conectar-se à instância do Mac usando SSH ou uma GUI
- Atualizar o sistema operacional e o software em instâncias Mac do Amazon EC2
- Aumente o tamanho de um volume do EBS na instância do Mac
- Parar ou terminar a instância do Mac no Amazon EC2
- Configurar a proteção da integridade do sistema para instâncias Mac do Amazon EC2
- Encontrar versões do macOS compatíveis para seu host dedicado Mac do Amazon EC2
- Assinar notificações de AMI do macOS
- Recuperar IDs de AMI do macOS usando a API do AWS Systems Manager Parameter Store
- Notas de lançamento das AMIs do Amazon EC2 para o macOS

Considerações

As seguintes considerações se aplicam às instâncias do Mac:

- As instâncias Mac só estão disponíveis como instâncias bare metal em hosts dedicados, com um período mínimo de alocação de 24 horas antes que seja possível liberar o host dedicado. É possível executar uma instância Mac por Host dedicado. É possível compartilhar o Host dedicado

com as contas da AWS ou com unidades organizacionais na sua organização de AWS ou toda a organização da AWS.

- Instâncias Mac estão disponíveis em diferentes Regiões da AWS. Para obter uma lista da disponibilidade de instâncias Mac em cada uma das Regiões da AWS, consulte Tipos de instância do Amazon EC2 por região.
- As instâncias Mac estão disponíveis apenas como Instâncias on-demand. Elas não estão disponíveis como Instâncias spot ou Instâncias reservadas. É possível economizar dinheiro em instâncias Mac comprando um Savings Plan.
- A compatibilidade de diferentes tipos de instância Mac com Amazon Machine Images (AMIs) específicas do macOS varia. Para obter mais informações, consulte Notas de lançamento das AMIs do Amazon EC2 para o macOS.
- Há suporte para o hotplug do EBS.
- AWS não gerencia nem oferece suporte ao SSD interno no hardware Apple. Recomendamos enfaticamente usar os volumes do Amazon EBS em vez disso. Os volumes do EBS oferecem benefícios semelhantes de elasticidade, disponibilidade e durabilidade em instâncias Mac em comparação com qualquer outra instância do EC2.
- Recomendamos usar um volume do Amazon EBS com 10.000 IOPS e throughput de 400 MiB/s com instâncias Mac para uma performance ideal. Para obter mais informações, consulte Tipos de volumes do Amazon EBS no Guia do usuário do Amazon EC2.
- Agora as instâncias Mac são compatíveis com o Amazon EC2 Auto Scaling.
- Em instâncias Mac x86, as atualizações automáticas de software estão desabilitadas. Recomendamos que você aplique as atualizações e as teste na sua instância antes de colocá-la em produção. Para obter mais informações, consulte Atualizar o sistema operacional e o software em instâncias Mac do Amazon EC2.
- Quando você interrompe ou encerra uma instância do Mac, um fluxo de trabalho de depuração é executado no Host dedicado. Para obter mais informações, consulte Parar ou terminar a instância do Mac no Amazon EC2.
- **Important**

  Os atributos do Apple Intelligence não estão disponíveis com a inicialização do hardware Mac a partir de um volume externo. Como as instâncias de Mac do EC2 são inicializadas a partir de volumes externos do EBS por padrão, elas não oferecem suporte aos recursos do Apple Intelligence.

- > **Warning**
  >
  > Não use o FileVault. Se você habilitar o FileVault, o host não inicializará porque as partições estão bloqueadas. Se houvere necessidade de criptografia de dados, use a criptografia do Amazon EBS para evitar problemas de inicialização e impacto na performance. Com a criptografia do Amazon EBS, as operações de criptografia ocorrem nos servidores host, garantindo a segurança dos dados em repouso e dos dados em trânsito e seu armazenamento do EBS anexado. Para obter mais informações, consulte Criptografia do Amazon EBS no Guia do usuário do Amazon EBS.

Prontidão da instância

Depois de iniciar uma instância Mac, você precisará esperar até que a instância esteja pronta para se conectar a ela. Para uma AMI vendida pela AWS com uma instância Mac x86 ou uma instância Apple com chip Mac, o tempo de inicialização pode variar de 6 a 20 minutos aproximadamente. Dependendo dos tamanhos de volume escolhidos do Amazon EBS, da inclusão de scripts adicionais nos dados do usuário ou do software adicional carregado em uma AMI personalizada do macOS, o tempo de inicialização pode aumentar.

É possível usar um pequeno script de shell, como o abaixo, para pesquisar a API describe-instance-status para saber quando a instância está pronta para conexão. No comando a seguir, substitua o ID da instância do exemplo pelo ID da sua própria instância.

```
for i in $(seq 1 200); do aws ec2 describe-instance-status --instance-
ids=i-1234567890abcdef0 \
    --query='InstanceStatuses[0].InstanceStatus.Status'; sleep 5; done;
```

AMIs do macOS do EC2

O macOS Amazon EC2 foi projetado para fornecer um ambiente estável, seguro e de alta performance para workloads de desenvolvedores executadas em instâncias Mac do Amazon EC2. As AMIs do macOS do EC2 também incluem vários pacotes que permitem a fácil integração com o AWS, incluindo ferramentas de configuração de execução bibliotecas e ferramentas populares do AWS .

Para obter mais informações sobre as AMIs do EC2 para o macOS, consulte Notas de lançamento das AMIs do Amazon EC2 para o macOS.

A AWS fornece AMIs do EC2 para o macOS atualizadas regularmente, as quais incluem atualizações para pacotes de propriedade da AWS e a versão mais recente do macOS totalmente testada. Além disso, o AWS fornece AMIs atualizadas com as atualizações mais recentes da versão secundária ou da versão principal assim que elas puderem ser totalmente testadas e aprovadas. Se você não precisar preservar dados ou personalizações das instâncias Mac, poderá obter as atualizações mais recentes ao executar uma nova instância usando a AMI atual e encerrando a instância anterior. Caso contrário, é possível escolher quais atualizações se aplicam às instâncias Mac.

Para obter informações sobre como se tornar assinante de notificações da AMI para o macOS, consulte Assinar notificações de AMI do macOS.

EC2 MacOS Init

O EC2 macOS Init é usado para inicializar instâncias Mac do EC2 na inicialização. Ele usa grupos prioritários para executar grupos lógicos de tarefas ao mesmo tempo.

O arquivo plist launchd é `/Library/LaunchDaemons/com.amazon.ec2.macos-init.plist`. Os arquivos do EC2 macOS Init estão localizados no `/usr/local/aws/ec2-macos-init`.

Para obter mais informações, consulte https://github.com/aws/ec2-macos-init.

Amazon EC2 System Monitor para macOS

O Amazon EC2 System Monitor para macOS fornece métricas de utilização de CPU para o Amazon CloudWatch. Ele envia essas métricas para o CloudWatch por meio de um dispositivo serial personalizado em períodos de 1 minuto. É possível ativar ou desativar este agente da seguinte forma. Ele é habilitado por padrão.

```
sudo setup-ec2monitoring [enable | disable]
```

> **Note**
>
> No momento, não há suporte para o Amazon EC2 System Monitor para macOS por parte de instâncias Mac que usam processadores Apple Silicon.

Recursos relacionados

Para obter mais informações sobre preços consulte Pricing.

Para obter mais informações sobre instâncias Mac, consulte Instâncias Mac do Amazon EC2.

Para obter mais informações sobre especificações de hardware e performance de rede de instâncias Mac, consulte Instâncias de uso geral.

Iniciar uma instância do Mac usando o Console de gerenciamento da AWS ou a AWS CLI

As instâncias Mac do EC2 exigem um host dedicado. Primeiro, você precisa alocar um host para sua conta e depois iniciar a instância no host.

É possível iniciar uma instância usando o Console de gerenciamento da AWS ou a AWS CLI.

Executar uma instância Mac usando o console

Para executar uma instância Mac em um Host dedicado

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Aloque o host dedicado da seguinte forma:
    a. No painel de navegação, selecione Hosts dedicados.
    b. Escolha Allocate (Alocar) Host dedicado e, em seguida, faça o seguinte:
        i. Em Família de instâncias, escolha uma família de instâncias Mac. Se a família de instâncias não aparecer na lista, significa que ela não é compatível com a região selecionada no momento.
        ii. Em Tipo de instância, escolha o tipo de instância com base na família de instâncias escolhida.
        iii. Em Availability Zone (Zona de disponibilidade), selecione a zona de disponibilidade do Host dedicado.
        iv. Em Quantity (Quantidade), mantenha 1.
        v. Escolha Allocate.
3. Inicie a instância no host da seguinte forma:
    a. Selecione o Host dedicado que você criou e, em seguida, faça o seguinte:
        i. Escolha Actions (Ações), Launch instances onto host (Iniciar instâncias no host).

ii. Em Application and OS Images (Amazon Machine Image) (Imagens de aplicações e sistemas operacionais [imagem de máquina da Amazon]), selecione uma AMI do macOS.

iii. Em Tipo de instância, selecione um tipo de instância Mac.

iv. Em Detalhes avançados, verifique se Locação , Host de locação por e ID do host de locação estão pré-configurados de acordo com o host dedicado que você criou. Atualize Tenancy affinity (Afinidade da locação) conforme necessário.

v. Conclua o assistente, especificando os volumes, grupos de segurança e pares de chaves do EBS conforme necessário.

vi. No painel Resumo painel, escolha Iniciar instância.

b. Uma página de confirmação informa que sua instância está sendo executada. Escolha View all instances (Visualizar todas as instâncias) para fechar a página de confirmação e voltar ao console. O estado inicial de uma instância é `pending`. A instância está pronta quando seu estado muda para `running` e passa verificações de status.

Executar uma instância Mac usando o AWS CLI

Alocar o host dedicado

Use o comando allocate-hosts a seguir para alocar um host dedicado à instância Mac, substituindo o `instance-type` por um tipo de instância mac válida e a `region` e `availability-zone` pelas apropriadas para o seu ambiente.

```
aws ec2 allocate-hosts --region us-east-1 --instance-type mac1.metal --availability-
zone us-east-1b --auto-placement "on" --quantity 1
```

Iniciar a instância no host

Use o comando run-instances a seguir para iniciar uma instância Mac, novamente substituindo o `instance-type` por um tipo de instância Mac válido e `region` e `availability-zone` pelas usadas anteriormente.

```
aws ec2 run-instances --region us-east-1 --instance-type mac1.metal --placement
 Tenancy=host --image-id ami_id --key-name my-key-pair
```

O estado inicial de uma instância é `pending`. A instância está pronta quando seu estado muda para `running` e passa verificações de status. Use o comando describe-instance-status para exibir informações de status para a instância.

```
aws ec2 describe-instance-status --instance-ids i-017f8354e2dc69c4f
```

Veja a seguir um exemplo de saída para uma instância que está sendo executada e passou por verificações de status.

```
{
    "InstanceStatuses": [
        {
            "AvailabilityZone": "us-east-1b",
            "InstanceId": "i-017f8354e2dc69c4f",
            "InstanceState": {
                "Code": 16,
                "Name": "running"
            },
            "InstanceStatus": {
                "Details": [
                    {
                        "Name": "reachability",
                        "Status": "passed"
                    }
                ],
                "Status": "ok"
            },
            "SystemStatus": {
                "Details": [
                    {
                        "Name": "reachability",
                        "Status": "passed"
                    }
                ],
                "Status": "ok"
            }
        }
    ]
}
```

Conectar-se à instância do Mac usando SSH ou uma GUI

É possível se conectar à instância do Mac usando SSH ou uma interface gráfica do usuário (GUI).

Vários usuários podem acessar o sistema operacional simultaneamente. Normalmente, existe uma relação 1:1 entre usuário e sessão gráfica (GUI), devido ao serviço de compartilhamento de tela integrado na porta 5900. O uso do SSH no macOS permite várias sessões até o limite de “Sessões máximas” no arquivo `sshd_config`.

Conectar-se à instância usando SSH

Por padrão, as instâncias Mac do Amazon EC2 não permitem SSH de raiz remota. A conta ec2-user está configurada para fazer login remotamente usando SSH. Além disso, a conta ec2-user tem privilégios de sudo. Depois de se conectar à instância, é possível adicionar outros usuários.

Para oferecer suporte à conexão com a instância usando SSH, execute a instância usando um par de chaves e um grupo de segurança que permita acesso SSH e verifique se a instância tem conectividade com a Internet. Você fornece o arquivo `.pem` para o par de chaves quando se conecta à instância.

Use o procedimento a seguir para se conectar à instância MAC usando um cliente SSH. Se você receber um erro ao tentar se conectar à instância, consulte Solucionar problemas de conexão com a instância do Linux do Amazon EC2.

Para se conectar à sua instância usando SSH

1. Verifique se o computador local tem um cliente SSH instalado digitando ssh na linha de comando. Se o computador não reconhecer o comando, procure um cliente SSH para seu sistema operacional e instale-o.
2. Obtenha o nome público do DNS da sua instância. Usando o console do Amazon EC2, é possível encontrar o nome público do DNS nas guias Detalhes e Rede. Usando o AWS CLI, é possível encontrar o nome público do DNS usando o comando describe-instances.
3. Localize o arquivo `.pem` do par de chaves que você especificou quando executou a instância.
4. Conecte-se à instância usando o comando ssh, especificando o nome público do DNS da instância e do arquivo `.pem`.

```
ssh -i /path/key-pair-name.pem ec2-user@instance-public-dns-name
```

A autenticação com senha é desabilitada para evitar ataques de força bruta em senhas. Antes de fazer alterações na configuração SSH, abra `/usr/local/aws/ec2-macos-init/init.toml` e defina `secureSSHDConfig` como `false`.

Conecte-se à interface gráfica do usuário (GUI)

Use o procedimento a seguir para se conectar à instância usando o VNC, o Apple Remote Desktop (ARD) ou a aplicação Apple Screen Sharing (incluído no macOS).

> **Note**
>
> O macOS 10.14 e posterior só permite o controle se o compartilhamento de tela estiver ativado por meio das Preferências do sistema.

Para se conectar à instância usando o cliente ARD ou o cliente VNC

1. Verifique se o computador local tem um cliente ARD ou um cliente VNC que suporte uma instalação do ARD. No macOS, é possível usar a aplicação de compartilhamento de tela integrado. Caso contrário, procure um cliente VNC para o sistema operacional e instale-o.
2. No computador local, conecte-se à instância usando SSH.
3. Defina uma senha para a conta ec2-user usando o comando passwd da seguinte forma.

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

4. Instale e inicie o compartilhamento de tela do macOS usando o comando a seguir.

   ```
   [ec2-user ~]$ sudo launchctl enable system/com.apple.screensharing
   sudo launchctl load -w /System/Library/LaunchDaemons/com.apple.screensharing.plist
   ```

5. Desconecte-se da sua instância digitando exit e pressionando Enter.
6. No computador, conecte-se à instância usando o comando ssh. Além das opções mostradas na seção anterior, use a opção -L para habilitar o encaminhamento de porta e encaminhar todo o tráfego na porta local 5900 para o servidor ARD na instância.

   ```
   ssh -L 5900:localhost:5900 -i /path/key-pair-name.pem ec2-user@instance-public-dns-name
   ```

7. No computador local, use o cliente ARD ou o cliente VNC com suporte a ARD para se conectar a `localhost:5900`. Por exemplo, use a aplicação de compartilhamento de tela no macOS da seguinte forma:

   a. Abra o Finder e selecione Ir.

   b. Selecione Conectar ao servidor.

   c. No campo Endereço do servidor, insira `vnc://localhost:5900`.

   d. Faça login conforme solicitado, usando **`ec2-user`** como o nome de usuário e a senha que você criou para a conta ec2-user.

Modificar a resolução de tela do macOS em instâncias Mac

Depois de se conectar à instância Mac do EC2 usando ARD ou um cliente VNC compatível com ARD instalado, é possível modificar a resolução de tela do ambiente do macOS usando qualquer uma das ferramentas ou utilitários do macOS disponíveis publicamente, como o displayplacer.

Para modificar a resolução da tela usando o displayplacer

1. Instale o displayplacer.

```
[ec2-user ~]$ brew tap jakehilborn/jakehilborn && brew install displayplacer
```

2. Mostre as informações atuais da tela e possíveis resoluções de tela.

```
[ec2-user ~]$ displayplacer list
```

3. Aplique a resolução de tela desejada.

```
[ec2-user ~]$ displayplacer "id:<screenID> res:<width>x<height> origin:(0,0)
 degree:0"
```

   Por exemplo:

```
RES="2560x1600"
displayplacer "id:69784AF1-CD7D-B79B-E5D4-60D937407F68 res:${RES} scaling:off
 origin:(0,0) degree:0"
```

Atualizar o sistema operacional e o software em instâncias Mac do Amazon EC2

O tópico a seguir explica como atualizar o sistema operacional e o software em instâncias Mac em chip Apple (Mac2, Mac2-m1ultra, Mac2-m2, Mac2-m2pro, Mac-m4, e Mac-m4pro) e em instâncias Mac x86 (Mac1).

Warning

A instalação das versões beta ou de pré-visualização do macOS está disponível somente em instâncias Mac com chip Apple. O Amazon EC2 não qualifica as versões beta ou prévia do macOS e não garante que as instâncias permaneçam funcionais após uma atualização para uma versão de pré-produção do macOS.
A tentativa de instalação das versões beta ou prévia do macOS em instâncias do Mac x86 do Amazon EC2 levará à degradação do host dedicado do Mac do Amazon EC2 quando você interromper ou encerrar suas instâncias e impedirá que você inicie ou execute uma nova instância nesse host.

Note

Se você realizar uma atualização local do macOS antes que a AWS lance uma AMI oficial, a atualização se aplicará somente ao host selecionado. Se você tiver outros hosts ou lançar novos hosts, deverá executar o mesmo processo de atualização nesses hosts também. Cada versão do macOS requer uma versão mínima de firmware no hardware Mac Apple. A atualização local atualiza somente o firmware no host selecionado e não é transferida para outros hosts novos ou existentes. Para verificar quais versões do macOS são compatíveis com seu host dedicado Mac do Amazon EC2, consulte Encontrar versões compatíveis do macOS para seu host dedicado Mac do Amazon EC2.

Atualizar software em instâncias Mac com chip Apple

Pré-requisitos

Devido a uma atualização na configuração do driver de rede, a versão 1.0.2 do driver ENA não é compatível com o macOS 13.3 e versões posteriores. Se você quiser instalar qualquer versão macOS beta, prévia ou de produção 13.3 ou posterior e não tiver instalado o driver ENA mais recente, use o procedimento a seguir para instalar uma nova versão do driver.

Para instalar uma nova versão do driver ENA

1. Em uma janela do terminal, conecte-se à instância Mac com chip Apple usando SSH.
2. Atualize o Homebrew e Baixe a aplicação ENA no arquivo `Applications` usando o comando a seguir.

```
[ec2-user ~]$ brew update
```

```
[ec2-user ~]$ brew install amazon-ena-ethernet-dext
```

3. Desconecte-se da sua instância digitando exit e pressionando return.
4. Use o cliente VNC para ativar a aplicação ENA.
   a. Configure o cliente VNC usando Conecte-se à interface gráfica do usuário (GUI).
   b. Depois de se conectar à sua instância usando a aplicação de compartilhamento de tela, acesse a pasta Aplicações e abra a aplicação ENA.
   c. Selecione Ativar
   d. Para confirmar que o driver foi ativado corretamente, execute o comando a seguir na janela do terminal. A saída do comando mostra que o driver antigo está no estado de encerramento e o novo driver está no estado ativado.

```
systemextensionsctl list;
```

   e. Depois de reiniciar a instância, somente o novo driver estará presente.

Realizar a atualização do software

Nas instâncias Mac com chip Apple, você deve concluir várias etapas para realizar uma atualização do sistema operacional no local. Isso inclui delegar a propriedade do volume raiz do Amazon EBS ao usuário administrativo do volume raiz do EBS. Você pode optar por fazer isso automaticamente usando uma API do Amazon EC2 ou manualmente executando os comandos na sua instância.

Automated volume ownership delegation (Recommended)

Considerações

- A tarefa de delegação da propriedade do volume pode demorar entre 30 e 90 minutos para ser concluída. Nesse período, a instância permanece inacessível.

- As seguintes versões do macOS são compatíveis:
  - Mac2 | Mac2-m1ultra: macOS Ventura (versão 13.0 ou posterior)
  - Mac2-m2 | Mac2-m2pro: macOS Ventura (versão 13.2 ou posterior)
  - Mac-M4 | Mac-M4Pro: macOS Sequoia (versão 15.6 ou posterior)
- As instâncias devem ter somente um volume inicializável, e cada volume associado pode ter somente um usuário administrador adicional.

Etapa 1: definir uma senha e ativar o token seguro para o usuário administrativo do volume raiz do EBS

É necessário definir uma senha e ativar o token seguro para o usuário administrativo (`ec2-user`) do volume raiz do Amazon EBS.

> **Note**
>
> A senha e o token seguro são definidos na primeira vez que você se conecta a uma instância Mac com chip Apple usando a GUI. Se você já se conectou à instância usando a GUI, não é necessário executar essas etapas.

1. Conecte-se à instância usando SSH.
2. Defina a senha do usuário `ec2-user`.

```
$ sudo /usr/bin/dscl . -passwd /Users/ec2-user
```

3. Ative o token seguro para o usuário `ec2-user`. Em `-oldPassword`, especifique a mesma senha da etapa anterior. Em `-newPassword`, especifique uma senha diferente. O comando a seguir pressupõe que suas senhas salvas antigas e novas estejam salvas em arquivos `.txt`.

```
$ sysadminctl -oldPassword `cat old_password.txt` -newPassword `cat
 new_password.txt`
```

4. Verifique se o token seguro está habilitado.

```
$ sysadminctl -secureTokenStatus ec2-user
```

Etapa 2: delegar a propriedade do volume raiz do Amazon EBS ao usuário administrativo do volume raiz do EBS

Para delegar a propriedade, é necessário criar uma tarefa de delegação de propriedade do volume.

1. Use o comando create-delegate-mac-volume-ownership-task para criar a tarefa. Em `--instance-id`, especifique o ID da instância. Em `--mac-credentials`, especifique as seguintes credenciais:

   - Usuário administrativo do disco interno
     - Nome de usuário: somente o usuário administrativo padrão (`aws-managed-user`) é aceito e é usado por padrão. Não é possível especificar um usuário administrativo diferente.
     - Senha: se você não alterou a senha padrão para `aws-managed-user`, especifique a senha padrão, que está em branco. Caso contrário, especifique sua senha.
   - Usuário administrativo do volume raiz do Amazon EBS
     - Nome de usuário: se você não alterou o usuário administrativo padrão, especifique `ec2-user`. Caso contrário, especifique o nome de usuário do seu usuário administrativo.
     - Senha: especifique a senha que você definiu para o usuário administrador do volume raiz na Etapa 1 acima.

   ```
   aws ec2 create-delegate-mac-volume-ownership-task \
   --instance-id i-1234567890abcdef0 \
   --mac-credentials file://mac-credentials.json
   ```

   O conteúdo a seguir faz parte do arquivo `mac-credentials.json` mencionado nos exemplos anteriores.

   ```
   {
     "internalDiskPassword":"internal-disk-admin_password",
     "rootVolumeUsername":"root-volume-admin_username",
     "rootVolumepassword":"root-volume-admin_password"
   }
   ```

2. Aguarde até que a tarefa de delegação da propriedade do volume seja concluída e que a instância volte a um estado íntegro. Use o comando describe-mac-modification-tasks. Em `--`

`mac-modification-task-id`, especifique o ID da tarefa de delegação da propriedade do volume da etapa anterior.

```
aws ec2 describe-mac-modification-tasks \
--mac-modification-task-id task-id
```

3. Depois que a tarefa de delegação da propriedade do volume for concluída, prossiga para a Etapa 3.

Etapa 3: atualizar o software

Depois de delegar a propriedade do volume raiz do Amazon EBS, siga as etapas descritas em Atualizar o software em instâncias x86 do Mac (abaixo) para atualizar o software.

Manual volume ownership delegation

Ao executar esse procedimento, você cria duas senhas. Uma senha é para o usuário administrativo do volume raiz do Amazon EBS (`ec2-user`) e a outra é para o usuário administrativo do disco interno (`aws-managed-user`). Lembre-se dessas senhas, pois você as usará enquanto executar o procedimento.

> **Note**
>
> Com esse procedimento no macOS Big Sur, só é possível realizar pequenas atualizações, como a atualização do macOS Big Sur 11.7.3 para o macOS Big Sur 11.7.4. Para o macOS Monterey ou superior, é possível realizar grandes atualizações de software.

Para acessar o disco interno

1. No computador local, no terminal, conecte-se à instância Mac com chip Apple usando SSH com o comando a seguir. Para obter mais informações, consulte Conectar-se à instância usando SSH.

```
ssh -i /path/key-pair-name.pem ec2-user@instance-public-dns-name
```

2. Instale e inicie o compartilhamento de tela do macOS usando o comando a seguir.

```
[ec2-user ~]$ sudo launchctl enable system/com.apple.screensharing
```

```
sudo launchctl load -w /System/Library/LaunchDaemons/
com.apple.screensharing.plist
```

3. Defina uma senha para `ec2-user` com o comando a seguir. Lembre-se da senha, pois você a usará mais tarde.

```
[ec2-user ~]$ sudo /usr/bin/dscl . -passwd /Users/ec2-user
```

4. Desconecte-se da instância digitando exit e pressionando return.
5. No seu computador local, no terminal, reconecte-se à sua instância com um túnel SSH para a porta VNC usando o comando a seguir.

```
ssh -i /path/key-pair-name.pem -L 5900:localhost:5900 ec2-user@instance-public-
dns-name
```

> **Note**
>
> Não saia dessa sessão SSH até que as seguintes etapas de conexão VNC e GUI sejam concluídas. Quando a instância for reiniciada, a conexão se fechará automaticamente.

6. No computador local, conecte-se a `localhost:5900` usando as etapas a seguir:
   a. Abra o Finder e selecione Ir.
   b. Selecione Conectar ao servidor.
   c. No campo Endereço do servidor, insira `vnc://localhost:5900`.
7. Na janela do macOS, conecte-se à sessão remota da instância Mac com chip Apple como `ec2-user` com a senha que você criou na etapa 3.
8. Acesse o disco interno, chamado InternalDisk, usando uma das opções a seguir.
   a. Para macOS Ventura ou superior: abra as Configurações do sistema, selecione Geral no painel esquerdo e depois Disco de startup no canto inferior direito do painel.
   b. Para macOS Monterey ou inferior: abra as Preferências do sistema, selecione Disco de startup e desbloqueie o painel escolhendo o ícone de cadeado no canto inferior esquerdo da janela.

> **Dica de solução de problemas**
>
> Se você precisar montar o disco interno, execute o comando a seguir no terminal.
>
> ```
> APFSVolumeName="InternalDisk" ; SSDContainer=$(diskutil list | grep
>  "Physical Store disk0" -B 3 | grep "/dev/disk" | awk {'print $1'} ) ;
>  diskutil apfs addVolume $SSDContainer APFS $APFSVolumeName
> ```

9. Escolha o disco interno, chamado InternalDisk, e selecione Reiniciar. Selecione Reiniciar novamente quando solicitado.

> **Important**
>
> Se o disco interno for denominado Macintosh HD em vez de InternalDisk, sua instância precisará ser interrompida e reiniciada para que o host dedicado possa ser atualizado. Para obter mais informações, consulte Parar ou terminar a instância do Mac no Amazon EC2.

Use o procedimento a seguir para delegar a propriedade ao usuário administrativo. Ao se reconectar à sua instância com SSH, você fará a inicialização a partir do disco interno usando o usuário administrativo especial (`aws-managed-user`). A senha inicial de `aws-managed-user` é em branco, então você precisa sobrescrevê-la em sua primeira conexão. Em seguida, você precisará repetir as etapas para instalar e iniciar o compartilhamento de tela do macOS, pois o volume de inicialização foi alterado.

Para delegar a propriedade ao administrador de um volume do Amazon EBS

1. No seu computador local, no terminal, conecte-se à sua instância Mac com chip Apple usando o comando a seguir.

```
ssh -i /path/key-pair-name.pem aws-managed-user@instance-public-dns-name
```

2. Ao receber o aviso `WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!`, use um dos comandos a seguir para resolver esse problema.

a. Limpe os hosts conhecidos usando o comando a seguir. Em seguida, repita a etapa anterior.

```
rm ~/.ssh/known_hosts
```

b. Adicione o seguinte ao comando SSH na etapa anterior.

```
-o UserKnownHostsFile=/dev/null -o StrictHostKeyChecking=no
```

3. Defina a senha do `aws-managed-user` com o comando a seguir. A senha inicial de `aws-managed-user` é em branco, então você precisa sobrescrevê-la em sua primeira conexão.

a.
```
[aws-managed-user ~]$ sudo /usr/bin/dscl . -passwd /Users/aws-managed-user password
```

b. Ao receber o prompt `Permission denied. Please enter user's old password:`, pressione enter.

> **Dica de solução de problemas**
>
> Se você receber o erro `passwd: DS error: eDSAuthFailed`, use o comando a seguir.
>
> ```
> [aws-managed-user ~]$ sudo passwd aws-managed-user
> ```

4. Instale e inicie o compartilhamento de tela do macOS usando o comando a seguir.

```
[aws-managed-user ~]$ sudo launchctl enable system/com.apple.screensharing
sudo launchctl load -w /System/Library/LaunchDaemons/
com.apple.screensharing.plist
```

5. Desconecte-se da instância digitando exit e pressionando return.
6. No seu computador local, no terminal, reconecte-se à sua instância com um túnel SSH para a porta VNC usando o comando a seguir.

```
ssh -i /path/key-pair-name.pem -L 5900:localhost:5900 aws-managed-user@instance-public-dns-name
```

7. No computador local, conecte-se a `localhost:5900` usando as etapas a seguir:

a. Abra o Finder e selecione Ir.

b. Selecione Conectar ao servidor.

c. No campo Endereço do servidor, insira `vnc://localhost:5900`.

8. Na janela do macOS, conecte-se à sessão remota da instância Mac com chip Apple como `aws-managed-user` com a senha que você criou na etapa 3.

> **Note**
>
> Quando solicitado a fazer login com seu Apple ID, selecione Configurar mais tarde.

9. Acesse o volume do Amazon EBS usando uma das opções a seguir.

a. Para macOS Ventura ou superior: abra as Configurações do sistema, selecione Geral no painel esquerdo e depois Disco de startup no canto inferior direito do painel.

b. Para macOS Monterey ou inferior: abra as Preferências do sistema, selecione Disco de startup e desbloqueie o painel escolhendo o ícone de cadeado no canto inferior esquerdo da janela.

> **Note**
>
> Até que a reinicialização ocorra, quando for solicitada uma senha de administrador, use a senha que você definiu acima para `aws-managed-user`. Essa senha pode ser diferente da que você definiu para o `ec2-user` ou a conta de administrador padrão em sua instância. As instruções a seguir especificam quando usar a senha de administrador da sua instância.

10. Selecione o volume Amazon EBS (o volume não denominado InternalDisk na janela Disco de startup) e escolha Reiniciar.

> **Note**
>
> Se você tiver vários volumes inicializáveis do Amazon EBS anexados à instância Mac com chip Apple, certifique-se de usar um nome exclusivo para cada volume.

11. Confirme a reinicialização e escolha Autorizar usuários quando solicitado.

12. No painel Autorizar usuário neste volume, verifique se o usuário administrativo (`ec2-user`, por padrão) está selecionado e selecione Autorizar.
13. Digite a senha do `ec2-user` que você criou na Etapa 3 do procedimento anterior e selecione Continuar.
14. Digite a senha do usuário administrativo especial (`aws-managed-user`) quando solicitado.
15. No computador local, no terminal, reconecte-se à instância usando SSH com o nome de usuário `ec2-user`.

    > **Dica de solução de problemas**
    >
    > Se você receber o aviso `WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!`, execute o comando a seguir e reconecte-se à sua instância usando SSH.
    >
    > ```
    > rm ~/.ssh/known_hosts
    > ```

16. Para realizar a atualização do software, use os comandos em Atualizar o software em instâncias x86 do Mac.

Atualizar o software em instâncias x86 do Mac

Em instâncias Mac x86, é possível instalar atualizações do sistema operacional da Apple usando o comando `softwareupdate`.

Para instalar atualizações do sistema operacional da Apple em instâncias Mac x86

1. Liste os pacotes com atualizações disponíveis usando o seguinte comando.

   ```
   [ec2-user ~]$ softwareupdate --list
   ```

2. Instale todas as atualizações ou apenas atualizações específicas. Para instalar atualizações específicas, use o seguinte comando.

   ```
   [ec2-user ~]$ sudo softwareupdate --install label
   ```

   Para instalar todas as atualizações, use o seguinte comando.

   ```
   [ec2-user ~]$ sudo softwareupdate --install --all --restart
   ```

Os administradores de sistemas podem usar o AWS Systems Manager para implementar atualizações pré-aprovadas do sistema operacional em instâncias Mac x86. Para obter mais informações, consulte o Guia do usuário do AWS Systems Manager.

É possível usar o Homebrew para instalar atualizações em pacotes nas AMIs do EC2 para o macOS a fim de obter a versão mais recente desses pacotes nas instâncias. Também é possível usar o Homebrew para instalar e executar aplicações macOS comuns no macOS do Amazon EC2. Para obter mais informações, consulte a Documentação do Homebrew.

Para instalar atualizações usando o Homebrew

1. Atualize o Homebrew usando o seguinte comando.

```
[ec2-user ~]$ brew update
```

2. Liste os pacotes com atualizações disponíveis usando o seguinte comando.

```
[ec2-user ~]$ brew outdated
```

3. Instale todas as atualizações ou apenas atualizações específicas. Para instalar atualizações específicas, use o seguinte comando.

```
[ec2-user ~]$ brew upgrade package name
```

   Para instalar todas as atualizações, use o seguinte comando.

```
[ec2-user ~]$ brew upgrade
```

Aumente o tamanho de um volume do EBS na instância do Mac

É possível aumentar o tamanho dos volumes do Amazon EBS na sua instância do Mac. Para obter mais informações, consulte Volumes Elásticos do Amazon EBS no Guia do usuário do Amazon EBS.

Depois de aumentar o tamanho do volume, é necessário aumentar o tamanho do contêiner APFS da forma a seguir.

Disponibilizar maior espaço em disco para uso

1. Determine se uma reinicialização é necessária. Se você redimensionou um volume do EBS existente em uma instância Mac em execução, será necessário reinicializar a instância para disponibilizar o novo tamanho. Se a modificação do espaço em disco tiver sido feita durante o tempo de lançamento, não será necessária uma reinicialização.

   Exibir o status atual dos tamanhos de disco:

   ```
   [ec2-user ~]$  diskutil list external physical
   /dev/disk0 (external, physical):
      #:                       TYPE NAME                    SIZE       IDENTIFIER
      0:                 GUID_partition_scheme            *322.1 GB     disk0
      1:                 EFI EFI                           209.7 MB     disk0s1
      2:                 Apple_APFS Container disk2        321.9 GB     disk0s2
   ```

2. Copie e cole o seguinte comando.

   ```
   [ec2-user ~]$ PDISK=$(diskutil list physical external | head -n1 | cut -d" " -f1)
   APFSCONT=$(diskutil list physical external | grep "Apple_APFS" | tr -s " " | cut -
   d" " -f8)
   yes | sudo diskutil repairDisk $PDISK
   ```

3. Copie e cole o seguinte comando.

   ```
   [ec2-user ~]$ sudo diskutil apfs resizeContainer $APFSCONT 0
   ```

Parar ou terminar a instância do Mac no Amazon EC2

Quando você interrompe uma instância do Mac, ela permanece no estado `stopping` por cerca de 15 minutos antes de entrar no estado `stopped`.

Quando uma instância do Mac é interrompida ou encerrada, o Amazon EC2 executa um fluxo de trabalho de depuração no host dedicado subjacente para apagar o SSD interno, limpar as variáveis NVRAM persistentes e, se necessário, atualizar o firmware do dispositivo para a versão mais recente. Isso garante que as instâncias Mac forneçam segurança e privacidade de dados semelhantes quando comparadas com outras instâncias do EC2 no Nitro. Isso também permite que você execute as AMIs mais recentes do macOS. Durante o fluxo de trabalho de depuração, o host dedicado entra temporariamente no estado de pendente. Em instâncias Mac x86, o fluxo de trabalho de limpeza pode levar até 50 minutos. Em instâncias Mac com chip Apple, o fluxo de

trabalho de limpeza pode levar até 110 minutos. Além disso, nas instâncias Mac x86, se o firmware do dispositivo precisar ser atualizado, o fluxo de trabalho de limpeza poderá demorar até 3 horas.

Não é possível iniciar a instância do Mac interrompida ou iniciar uma nova instância do Mac até que o fluxo de trabalho de depuração seja concluído, momento no qual o estado Host dedicado entra no estado `available`.

A medição e o faturamento são pausados quando o host dedicado entra no estado `pending`. Você não será cobrado pela duração do fluxo de trabalho de depuração.

Libere o Host dedicado para a sua instância do Mac

Quando você terminar de usar a instância Mac, poderá liberar o Host dedicado. Antes de liberar o Host dedicado, é necessário interromper ou encerrar a instância Mac. Você não pode liberar o host até que o período de alocação exceda o mínimo de 24 horas.

Para liberar o Host dedicado

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância e escolha Instance state (Estado da instância) e, em seguida, escolha Stop instance (Interromper instância) ou Terminate instance (Encerrar instância).
4. No painel de navegação, selecione Hosts dedicados.
5. Selecione o Host dedicado e escolha Actions (Ações), Release host (Liberar host).
6. Quando for solicitada a confirmação, escolha Release (Liberar).

Configurar a proteção da integridade do sistema para instâncias Mac do Amazon EC2

É possível configurar as opções da proteção da integridade do sistema (SIP) para instâncias Mac x86 e instâncias Mac com chip Apple. A SIP é um recurso de segurança essencial do macOS que ajuda a evitar a execução não autorizada de código e modificações no nível do sistema. Para obter mais informações, consulte Sobre a proteção da integridade do sistema.

É possível habilitar ou desabilitar completamente a SIP ou habilitar ou desabilitar seletivamente configurações específicas da proteção. Recomenda-se desabilitar a SIP apenas temporariamente para executar as tarefas necessárias e, em seguida, voltar a habilitá-la assim que possível. Manter a SIP desabilitada pode deixar sua instância vulnerável a códigos maliciosos.

A configuração da SIP é aceita em todas as regiões da AWS em que as instâncias Mac do Amazon EC2 são aceitas.

Tópicos

- Considerações
- Configurações de SIP padrão
- Verifique sua configuração de SIP
- Pré-requisitos para instâncias Mac com chip Apple
- Configurar as opções de SIP
- Verificar o status da tarefa de configuração de SIP

Considerações

- Os seguintes tipos de instância Mac do Amazon EC2 e versões do macOS são compatíveis:
  - Mac1 | Mac2 | Mac2-m1ultra: macOS Ventura (versão 13.0 ou posterior)
  - Mac2-m2 | Mac2-m2pro: macOS Ventura (versão 13.2 ou posterior)
  - Mac-M4 | Mac-M4Pro: macOS Sequoia (versão 15.6 ou posterior)

  > **Note**
  >
  > As versões beta e de prévia do macOS não são aceitas.

- É possível especificar uma configuração de SIP personalizada para habilitar ou desabilitar seletivamente configurações de SIP individuais. Se você implementar uma configuração personalizada, conecte-se à instância e verifique as configurações para garantir que seus requisitos sejam implementados adequadamente e funcionem conforme o esperado.

  As configurações de SIP podem mudar com as atualizações do macOS. Recomendamos revisar as configurações de SIP personalizadas após qualquer atualização da versão do macOS para garantir a compatibilidade contínua e a funcionalidade adequada das suas configurações de segurança.
- Para instâncias Mac x86, as configurações de SIP são aplicadas no nível da instância. Qualquer volume raiz associado à instância herdará automaticamente as configurações de SIP configuradas.

Para instâncias Mac com chip Apple, as configurações de SIP são aplicadas no nível do volume. Os volumes raiz associados à instância não herdam as configurações de SIP. Se você associar outro volume raiz, deverá alterar as configurações de SIP para o estado necessário.

- Até 90 minutos podem ser necessários para que as tarefas de configuração de SIP sejam concluídas. A instância permanece inacessível enquanto a tarefa de configuração do SIP está em andamento.
- As configurações de SIP não são transferidas para os snapshots ou AMIs criados posteriormente com base na instância.
- As instâncias Mac com chip Apple devem ter somente um volume inicializável, e cada volume associado pode ter somente um usuário administrador adicional.

Configurações de SIP padrão

A tabela a seguir lista a configuração de SIP padrão para instâncias Mac x86 e instâncias Mac com chip Apple.

	Instâncias Mac com chip Apple	Instâncias do Mac x86
Interno da Apple	Habilitado	Desabilitado
Proteções de sistema de arquivos	Habilitado	Desabilitado
Sistema base	Habilitado	Habilitado
Restrições de depuração	Habilitado	Habilitado
Restrições de acesso	Habilitado	Habilitado
Assinatura de Kext	Habilitado	Habilitado
Proteções de Nvram	Habilitado	Habilitado

Verifique sua configuração de SIP

Recomendamos que você verifique a configuração de SIP antes e depois de fazer alterações para garantir que ela esteja configurada conforme o esperado.

Para verificar a configuração de SIP de uma instância Mac do Amazon EC2

Conecte-se à instância usando SSH e execute o comando a seguir na linha de comando.

```
$ csrutil status
```

O seguinte é um exemplo de saída.

```
System Integrity Protection status: enabled.

Configuration:
    Apple Internal: enabled
    Kext Signing: disabled
    Filesystem Protections: enabled
    Debugging Restrictions: enabled
    DTrace Restrictions: enabled
    NVRAM Protections: enabled
    BaseSystem Verification: disabled
```

Pré-requisitos para instâncias Mac com chip Apple

Antes de configurar as configurações de SIP para instâncias Mac com chip Apple, é necessário definir uma senha e ativar o token seguro para o usuário administrativo do volume raiz do Amazon EBS (`ec2-user`).

> **Note**
>
> A senha e o token seguro são definidos na primeira vez que você se conecta a uma instância Mac com chip Apple usando a GUI. Se você já se conectou à instância usando a GUI, ou se estiver usando uma instância Mac x86, não será necessário executar essas etapas.

Para definir uma senha e ativar o token seguro para o usuário administrativo do volume raiz do EBS

1. Conecte-se à instância usando SSH.

2. Defina a senha do usuário `ec2-user`.

```
$ sudo /usr/bin/dscl . -passwd /Users/ec2-user
```

3. Ative o token seguro para o usuário `ec2-user`. Em `-oldPassword`, especifique a mesma senha da etapa anterior. Em `-newPassword`, especifique uma senha diferente. O comando a seguir pressupõe que suas senhas salvas antigas e novas estejam salvas em arquivos `.txt`.

```
$ sysadminctl -oldPassword `cat old_password.txt` -newPassword `cat
 new_password.txt`
```

4. Verifique se o token seguro está habilitado.

```
$ sysadminctl -secureTokenStatus ec2-user
```

Configurar as opções de SIP

Ao configurar as opções de SIP para sua instância, é possível habilitar ou desabilitar todas as configurações de SIP ou especificar uma configuração personalizada que habilite ou desabilite seletivamente configurações de SIP específicas.

> **Note**
>
> Se você implementar uma configuração personalizada, conecte-se à instância e verifique as configurações para garantir que seus requisitos sejam implementados adequadamente e funcionem conforme o esperado.
> As configurações de SIP podem mudar com as atualizações do macOS. Recomendamos revisar as configurações de SIP personalizadas após qualquer atualização da versão do macOS para garantir a compatibilidade contínua e a funcionalidade adequada das suas configurações de segurança.

Para configurar as opções de SIP para sua instância, é necessário criar uma tarefa de configuração de SIP. A tarefa de configuração de SIP especifica as configurações de SIP para sua instância.

Ao criar uma configuração de SIP para uma instância Mac com chip Apple, é necessário especificar as seguintes credenciais:

- Usuário administrativo do disco interno

  - Nome de usuário: somente o usuário administrativo padrão (`aws-managed-user`) é aceito e é usado por padrão. Não é possível especificar um usuário administrativo diferente.
  - Senha: se você não alterou a senha padrão para `aws-managed-user`, especifique a senha padrão, que está em branco. Caso contrário, especifique sua senha.
- Usuário administrativo do volume raiz do Amazon EBS
  - Nome de usuário: se você não alterou o usuário administrativo padrão, especifique `ec2-user`. Caso contrário, especifique o nome de usuário do seu usuário administrativo.
  - Senha: a senha deve ser sempre especificada.

Use os métodos a seguir para criar uma tarefa de configuração de SIP.

Console

Para criar uma tarefa de configuração de SIP 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, em seguida, selecione a instância Mac do Amazon EC2.
3. Na guia Segurança, escolha Modificar Mac, Modificar proteção de integridade do sistema.
4. Para habilitar todas as configurações de SIP, selecione Habilitar SIP. Para desabilitar todas as configurações de SIP, desmarque Habilitar SIP.
5. Para especificar uma configuração personalizada que habilite ou desabilite seletivamente configurações de SIP específicas, selecione Especificar uma configuração de SIP personalizada e, em seguida, selecione as configurações de SIP a serem habilitadas ou desmarque as configurações de SIP a serem desabilitadas.
6. Especifique as credenciais do usuário do volume raiz e do proprietário do disco interno.
7. Escolha Criar tarefa de modificação de SIP.

AWS CLI

Para criar uma tarefa de configuração de SIP usando a AWS CLI

Use o comando create-mac-system-integrity-protection-modification-task.

Habilitar ou desabilitar todas as configurações de SIP

Para habilitar ou desabilitar completamente todas as configurações de SIP, use somente o parâmetro `--mac-system-integrity-protection-status`.

O comando de exemplo a seguir habilita todas as configurações de SIP.

```
aws ec2 create-mac-system-integrity-protection-modification-task \
--instance-id i-0abcdef9876543210 \
--mac-system-integrity-protection-status enabled \
--mac-credentials file://mac-credentials.json
```

Especificar uma configuração de SIP personalizada

Para especificar uma configuração de SIP personalizada que habilite ou desabilite seletivamente configurações de SIP específicas, especifique os parâmetros `--mac-system-integrity-protection-status` e `--mac-system-integrity-protection-configuration`. Nesse caso, use `mac-system-integrity-protection-status` para especificar o status geral da SIP e use `mac-system-integrity-protection-configuration` para habilitar ou desabilitar seletivamente as configurações individuais de SIP.

O comando de exemplo a seguir cria uma tarefa de configuração de SIP para habilitar todas as configurações de SIP, exceto `NvramProtections` e `FilesystemProtections`.

```
aws ec2 create-mac-system-integrity-protection-modification-task \
--instance-id i-0abcdef9876543210 \
--mac-system-integrity-protection-status enabled \
--mac-system-integrity-protection-configuration
 "NvramProtections=disabled, FilesystemProtections=disabled" \
--mac-credentials file://mac-credentials.json
```

O comando de exemplo a seguir cria uma tarefa de configuração de SIP para desabilitar todas as configurações de SIP, exceto `DtraceRestrictions`.

```
aws ec2 create-mac-system-integrity-protection-modification-task \
--instance-id i-0abcdef9876543210 \
--mac-system-integrity-protection-status disabled \
--mac-system-integrity-protection-configuration "DtraceRestrictions=enabled" \
--mac-credentials file://mac-credentials.json
```

Conteúdo do arquivo **`mac-credentials.json`**

O conteúdo a seguir faz parte do arquivo `mac-credentials.json` mencionado nos exemplos anteriores.

```
{
  "internalDiskPassword":"internal-disk-admin_password",
  "rootVolumeUsername":"root-volume-admin_username",
  "rootVolumepassword":"root-volume-admin_password"
}
```

Verificar o status da tarefa de configuração de SIP

Use um dos métodos a seguir para verificar o estado das tarefas de configuração de SIP.

Console

Para visualizar tarefas de configuração de SIP 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, em seguida, selecione a instância Mac do Amazon EC2.
3. Na guia Segurança, role para baixo até a seção Tarefas de modificação do Mac.

AWS CLI

Para verificar o estado das tarefas de configuração de SIP usando a AWS CLI

Use o comando describe-mac-modification-tasks.

Encontrar versões do macOS compatíveis para seu host dedicado Mac do Amazon EC2

É possível ver as versões mais recentes do macOS compatíveis com seu host dedicado Mac do Amazon EC2. Com essa funcionalidade, será possível validar a compatibilidade do seu host dedicado com execuções de instância com suas versões preferenciais do macOS.

Cada versão do macOS requer uma versão mínima de firmware no Apple Mac subjacente para uma execução bem-sucedida. A versão de firmware do Apple Mac pode ficar desatualizada se um host dedicado do Mac alocado tiver ficado inativo por um longo período de tempo ou tiver uma instância em execução há muito tempo.

Para garantir a compatibilidade com as versões mais recentes do macOS, você pode interromper ou encerrar instâncias no host dedicado Mac alocado. Isso vai acionar o fluxo de trabalho de limpeza de host e atualizar o firmware no respectivo Apple Mac para compatibilidade com as versões mais recentes do macOS. Um host dedicado com uma instância em execução há muito tempo será atualizado automaticamente quando você interromper ou encerrar uma instância em execução.

Para obter mais informações sobre o fluxo de trabalho de limpeza, consulte Parar ou terminar a instância do Mac no Amazon EC2.

Para obter mais informações sobre como executar instâncias Mac, consulte Iniciar uma instância do Mac usando o Console de gerenciamento da AWS ou a AWS CLI.

É possível visualizar informações sobre as versões compatíveis mais recentes do macOS em seu host dedicado alocado usando o console do Amazon EC2 ou a AWS CLI.

Console

Para ver as informações do firmware do host dedicado usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Hosts dedicados.
3. Na página de Detalhes de hosts dedicados, em Versões mais recentes compatíveis do macOS, será possível ver as versões mais recentes do macOS compatíveis com o host.

AWS CLI

Para ver as informações do firmware do host dedicado usando a AWS CLI

Use o comando `describe-mac-hosts`, substituindo `region` pela Região da AWS adequada.

```
$ aws ec2 describe-mac-hosts --region us-east-1
  {
      "MacHosts": [
          {
              "HostId": "h-07879acf49EXAMPLE",
              "MacOSLatestSupportedVersions": [
                  "14.3",
                  "13.6.4",
                  "12.7.3"
              ]
```

```
            }
        ]
    }
```

Assinar notificações de AMI do macOS

Para ser notificado sobre o lançamento de novas AMIs ou atualizações do bridgeOS, inscreva-se em notificações usando o Amazon SNS.

Para obter mais informações sobre as AMIs do macOS para EC2, consulte Notas de lançamento das AMIs do Amazon EC2 para o macOS.

Para assinar notificações de AMI do macOS

1. Abra o console do Amazon SNS em https://console.aws.amazon.com/sns/v3/home.
2. Na barra de navegação, altere a região para Leste dos EUA (Norte da Virgínia), se necessário. Use essa região porque as notificações do SNS nas quais está se inscrevendo foram criadas nessa região.
3. No painel de navegação, escolha Subscriptions.
4. Selecione Create subscription.
5. Na caixa de diálogo Create subscription, faça o seguinte:

    a. Em Topic ARN, copie e cole um dos seguintes nomes de recursos da Amazon (ARNs):

    - **`arn:aws:sns:us-east-1:898855652048:amazon-ec2-macos-ami-updates`**
    - **`arn:aws:sns:us-east-1:898855652048:amazon-ec2-bridgeos-updates`**

    b. Em Protocolo, escolha uma das seguinte opções:

    - E-mail:

      Para Endpoint, digite um endereço de e-mail que é possível usar para receber as notificações. Após criar a assinatura, você receberá uma mensagem de confirmação com a linha de assunto `AWS Notification - Subscription Confirmation`. Abra o e-mail e escolha Confirm subscription para concluir a assinatura.
    - SMS:

      Em Endpoint, digite um número de telefone que é possível usar para receber as notificações.

- AWS Lambda, Amazon SQS, Amazon Data Firehose (as notificações são recebidas no formato JSON):

  Em Endpoint, insira o ARN da função Lambda, fila SQS ou transmissão do Firehose que é possível usar para receber notificações.

c. Selecione Create subscription.

Sempre que AMIs do macOS forem lançadas, enviaremos notificações aos assinantes do tópico `amazon-ec2-macos-ami-updates`. Sempre que houver uma atualização do bridgeOS , enviaremos notificações aos assinantes do tópico `amazon-ec2-bridgeos-updates`. Se não deseja mais receber essas notificações, use o procedimento a seguir para cancelar a assinatura.

Para cancelar a assinatura de notificações de AMIs do macOS

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

Recuperar IDs de AMI do macOS usando a API do AWS Systems Manager Parameter Store

Especifique uma AMI ao iniciar uma instância. Uma AMI é específica para uma Região da AWS, um sistema operacional e uma arquitetura de processador. É possível visualizar todas as AMIs do macOS em uma Região da AWS e recuperar a AMI mais recente do macOS consultando a API do AWS Systems Manager Parameter Store. Ao usar esses parâmetros públicos, não será necessário pesquisar manualmente IDs de AMI para o macOS. Os parâmetros públicos estão disponíveis para as AMIs x86 e ARM64 do macOS e podem ser integrados aos modelos do AWS CloudFormation existentes.

Permissões obrigatórias

Para realizar essa ação, a entidade principal do IAM deve ter permissões para chamar a ação da API `ssm:GetParameter`.

Para visualizar uma lista de todas as AMIs do macOS na Região da AWS atual usando a AWS CLI

Use o comando get-parameters-by-path para visualizar uma lista de todas as AMIs do macOS na região atual.

```
aws ssm get-parameters-by-path --path /aws/service/ec2-macos --recursive --query
 "Parameters[].Name"
```

Para recuperar o ID da AMI principal mais recente do macOS usando a AWS CLI

Use o seguinte comando get-parameter com o subparâmetro `image_id`. No exemplo a seguir, substitua `sonoma` por uma versão principal compatível do macOS, `x86_64_mac` pelo processador e `region-code` por uma Região da AWS compatível para a qual você deseja o ID de AMI mais recente do macOS.

```
aws ssm get-parameter --name /aws/service/ec2-macos/sonoma/x86_64_mac/latest/image_id
 --region region-code
```

Para obter mais informações, consulte Chamar parâmetros públicos da AMI para macOS no Guia do usuário do AWS Systems Manager.

Notas de lançamento das AMIs do Amazon EC2 para o macOS

As informações apresentadas a seguir fornecem detalhes sobre os pacotes incluídos por padrão nas AMIs do EC2 para o macOS e resumem as alterações para cada lançamento da AMI do EC2 para o macOS.

Para obter informações sobre como se tornar assinante de notificações da AMI para o macOS, consulte Assinar notificações de AMI do macOS.

As instâncias Mac podem executar um dos seguintes sistemas operacionais:

- macOS Mojave (versão 10.14) (somente instâncias Mac x86)
- macOS Catalina (versão 10.15) (somente instâncias Mac x86)
- macOS Big Sur (versão 11) (instâncias Mac x86 e M1)
- macOS Monterey (versão 12) (instâncias Mac x86 e M1)
- macOS Ventura (versão 13) (todas as instâncias Mac M2 e M2 Pro Mac são compatíveis com o macOS Ventura versão 13.2 ou posterior)
- macOS Sonoma (versão 14) (todas as instâncias do Mac)

- macOS Sequoia (versão 15) (todas as instâncias do Mac)

> **Note**
>
> As instâncias Mac M4 e M4 Pro são compatíveis com o macOS Sequoia versão 15.6 ou posterior.

Aprovar políticas de privacidade de rede local para macOS Sequoia

O macOS Sequoia (versão 15) tem um novo atributo de privacidade de rede local que afeta os usuários de serviços locais baseados em IP, incluindo serviço de metadados de instância (IMDS) do Amazon EC2.

> **Important**
>
> Para garantir que você tenha acesso ininterrupto aos serviços locais baseados em IP, use as etapas a seguir para aprovar as políticas de privacidade de rede local.

Para aprovar as políticas de privacidade de rede local

1. Conecte-se à interface gráfica do usuário (GUI).
2. Siga as instruções na tela para aprovar as políticas de privacidade de rede local.
3. Depois de aprovar as políticas, crie uma AMI da sua instância EC2 Mac. Para obter mais informações, consulte Criação de uma AMI baseada no Amazon EBS.

Todas as instâncias do EC2 Mac iniciadas a partir da AMI recém-criada reterão as permissões de privacidade de rede local.

Pacotes padrão incluídos nas AMIs do Amazon EC2 para o macOS

A tabela apresentada a seguir descreve os pacotes incluídos por padrão nas AMIs do EC2 para o macOS.

Pacotes	Notas da versão
EC2 macOS Init	https://github.com/aws/ec2-macos-init/tags

Pacotes	Notas da versão
EC2 macOS Utils	https://github.com/aws/ec2-macos-utils/tags
Amazon SSM Agent	https://github.com/aws/amazon-ssm-agent/releases
AWS Command Line Interface (AWS CLI) versão 2	https://raw.githubusercontent.com/aws/aws-cli/v2/CHANGELOG.rst
Ferramentas da linha de comando para Xcode	https://developer.apple.com/documentation/xcode-release-notes
Homebrew	https://github.com/Homebrew/brew/releases
EC2 Instance Connect	https://github.com/aws/aws-ec2-instance-connect-config/releases
Safari	https://developer.apple.com/documentation/safari-release-notes

Atualizações da AMI do Amazon EC2 para o macOS

A tabela apresentada a seguir descreve as alterações incluídas nos lançamentos da AMI do EC2 para o macOS. Observe que algumas alterações são aplicáveis a todas as AMIs do EC2 para o macOS, enquanto outras se aplicam apenas a um subconjunto dessas AMIs.

Atualizações da AMI do EC2 para o macOS

Versão	Alterações
26/12/2025	Todas as AMIs • Atualização da `awscli` para a versão 2.32.19 • Atualização do Homebrew para a versão 5.0.6 Lançamento do macOS Sonoma 14.8.3 • Conteúdo de segurança do macOS Sonoma 14.8.3

Versão	Alterações

	• Atualização do Safari para a versão 26.2
	  • Conteúdo de segurança do Safari 26.2
	
	Lançamento do macOS Sequoia 15.7.3
	
	• Conteúdo de segurança do macOS Sequoia 15.7.3
	• Atualização do Safari para a versão 26.2
	  • Conteúdo de segurança do Safari 26.2
	• Atualização das ferramentas de linha de comando para a versão 26.2
	
	Lançamento do macOS Tahoe 26.2
	
	• Conteúdo de segurança do macOS Tahoe 26.2
	• Atualização das ferramentas de linha de comando para a versão 26.2

Versão	Alterações

17/12/25	Todas as AMIs
	• Atualização da `awscli` para a versão 2.32.16
	• Atualização do Homebrew para a versão 5.0.5
	
	Lançamento do macOS Sonoma 14.8.2
	• Conteúdo de segurança do macOS Sonoma 14.8.2
	• Atualização do Safari para a versão 26.1
	  • Conteúdo de segurança do Safari 26.1
	
	Lançamento do macOS Sequoia 15.7.2
	• Conteúdo de segurança do macOS Sequoia 15.7.2
	• Atualização do Safari para a versão 26.1
	  • Conteúdo de segurança do Safari 26.1
	• Atualização das ferramentas de linha de comando para a versão 26.1
	
	Lançamento do macOS Tahoe 26.1
	• Conteúdo de segurança do macOS Tahoe 26.1
	• Atualização das ferramentas de linha de comando para a versão 26.1

Versão	Alterações

18/11/2025	Todas as AMIs
	
	• Atualização da `awscli` para a versão 2.31.35
	• Atualização de `ec2-macos-init` para a versão 1.5.13
	• Atualização de `ec2-macos-utils` para a versão 1.0.7
	• Atualização do Homebrew para a versão 5.0.1
	
	Lançamento do macOS Sonoma 14.8.1
	
	• Conteúdo de segurança do macOS Sonoma 14.8.1
	• Atualização do Safari para a versão 26.0.1
	  • Conteúdo de segurança do Safari 26.0.1
	
	Lançamento do macOS Sequoia 15.7.1
	
	• Conteúdo de segurança do macOS Sequoia 15.7.1
	• Atualização do Safari para a versão 26.0.1
	  • Conteúdo de segurança do Safari 18.6
	• Atualização das ferramentas de linha de comando para a versão 26.0
	
	Lançamento do macOS Tahoe 26.0.1
	
	• Conteúdo de segurança do macOS Tahoe 26.0.1
	• Atualização das ferramentas de linha de comando para a versão 26.0

Versão	Alterações
04/09/2025	Todas as AMIs • Atualização da `awscli` para a versão 2.28.19 • Atualização do Homebrew para a versão 4.6.7 Lançamento do macOS Ventura 13.7.8 • Conteúdo de segurança do macOS Ventura 13.7.8 Lançamento do macOS Sonoma 14.7.8 • Conteúdo de segurança do macOS Sonoma 14.7.8 Lançamento do macOS Sequoia 15.6.1 • Conteúdo de segurança do macOS Sequoia 15.6.1

Versão	Alterações

05/08/2025	Todas as AMIs
	• `awscli` atualizado para a versão 2.28.0
	• Homebrew atualizado para a versão 4.5.13
	
	Lançamento do macOS Ventura 13.7.7
	• Conteúdo de segurança do macOS Ventura 13.7.7
	• Safari atualizado para a versão 18.6
	  • Conteúdo de segurança do Safari 18.6
	
	Lançamento do macOS Sonoma 14.7.7
	• Conteúdo de segurança do macOS Sonoma 14.7.7
	• Safari atualizado para a versão 18.6
	  • Conteúdo de segurança do Safari 18.6
	
	Lançamento do macOS Sequoia 15.6
	• Conteúdo de segurança do macOS Sequoia 15.6
	• AWS ENA Ethernet atualizado para 2.0.0

Versão	Alterações

27/06/2025	Todas as AMIs
	• Atualização da `awscli` para a versão 2.27.40
	• Atualização do Homebrew para a versão 4.5.7
	• Imagens x86_64 migradas para o AWS ENA Ethernet dext
	
	Lançamento do macOS Ventura 13.7.6
	• Conteúdo de segurança do macOS Ventura 13.7.6
	• Atualização do Safari para a versão 18.5
	  • Conteúdo de segurança do Safari 18.5
	
	Lançamento do macOS Sonoma 14.7.6
	• Conteúdo de segurança do macOS Sonoma 14.7.6
	• Atualização do Safari para a versão 18.5
	  • Conteúdo de segurança do Safari 18.5
	
	Lançamento do macOS Sequoia 15.5
	• Conteúdo de segurança do macOS Sequoia 15.5
	• Atualização das ferramentas de linha de comando para a versão 16.4
	• AWS ENA Ethernet atualizado para 1.0.9

Versão	Alterações

21/05/2025	Todas as AMIs
	• Atualização da `awscli` para a versão 2.27.7
	• Atualização do `ec2-macos-init` para a versão 1.5.11
	• Atualização do `ec2-macos-utils` para a versão 1.0.5
	• Atualização do Homebrew para a versão 4.5.1
	
	Lançamento do macOS Ventura 13.7.5
	• Conteúdo de segurança do macOS Ventura 13.7.5
	• Atualização do Safari para a versão 18.4
	  • Conteúdo de segurança do Safari 18.4
	
	Lançamento do macOS Sonoma 14.7.5
	• Conteúdo de segurança do macOS Sonoma 14.7.5
	• Atualização do Safari para a versão 18.4
	  • Conteúdo de segurança do Safari 18.4
	
	Lançamento do macOS Sequoia 15.4.1
	• Conteúdo de segurança do macOS Sequoia 15.4.1
	• Atualização das ferramentas de linha de comando para a versão 16.3

Versão	Alterações

05/05/2025	Todas as AMIs
	• Atualização da `awscli` para a versão 2.27.1
	• Atualização do `ec2-macos-init` para a versão 1.5.11
	• Atualização do `ec2-macos-system-monitor` para a versão 1.3.1
	• Atualização do `ec2-macos-utils` para a versão 1.0.5
	• Atualização do Homebrew para a versão 4.4.32
	
	Lançamento do macOS Ventura 13.7.5
	• Conteúdo de segurança do macOS Ventura 13.7.5
	• Atualização do Safari para a versão 18.4
	  • Conteúdo de segurança do Safari 18.4
	
	Lançamento do macOS Sonoma 14.7.5
	• Conteúdo de segurança do macOS Sonoma 14.7.5
	• Atualização do Safari para a versão 18.4
	  • Conteúdo de segurança do Safari 18.4
	
	Lançamento do macOS Sequoia 15.4.1
	• Conteúdo de segurança do macOS Sequoia 15.4.1

Versão	Alterações
18/03/2025	Todas as AMIs • Atualização do `awscli` para a versão 2.24.2 • Atualização do Homebrew para 4.4.20 Lançamento do macOS Sequoia 15.3.1 • Conteúdo de segurança do macOS Sequoia 15.3.1 Lançamento do macOS Sonoma 14.7.4 • Conteúdo de segurança do macOS Sonoma 14.7.4 • Atualização do Safari para a versão 18.3 Lançamento do macOS Ventura 13.7.4 • Conteúdo de segurança do macOS Ventura 13.7.4 • Atualização do Safari para a versão 18.3

Versão	Alterações
24/01/2025	Todas as AMIs • Atualização do `awscli` para 2.22.33 • Atualização do Homebrew para 4.4.15 Lançamento do macOS Sequoia 15.2 • Conteúdo de segurança do macOS Sequoia 15.2 • Atualização das ferramentas de linha de comando para a versão 16.2 Lançamento do macOS Sonoma 14.7.2 • Conteúdo de segurança do macOS Sonoma 14.7.2 • Atualização do Safari para a versão 18.2 • Atualização das ferramentas de linha de comando para a versão 16.2 Lançamento do macOS Ventura 13.7.2 • Conteúdo de segurança do macOS Ventura 13.7.2 • Atualização do Safari para a versão 18.2

Versão	Alterações
20/12/2024	Todas as AMIs • Atualização do Homebrew para a versão 4.4.8 • Atualização da `aws-cli` para a versão 2.22.5 • Atualização de `amazon-ssm-agent` para a versão 3.3.987.0 Lançamento do macOS Sequoia 15.1.1 • Conteúdo de segurança do macOS Sequoia 15.1.1 Lançamento do macOS Sonoma 14.7.1 • Conteúdo de segurança do macOS Sonoma 14.7.1 • Atualização do Safari para a versão 18.1.1 Lançamento do macOS Ventura 13.7.1 • Conteúdo de segurança do macOS Ventura 13.7.1 • Atualização do Safari para a versão 18.1.1

Versão	Alterações

28/10/2024	Todas as AMIs
	• Atualização do Homebrew para a versão 4.4.2
	• Atualização da `aws-cli` para a versão 2.18.13
	• Atualização de `amazon-ssm-agent` para a versão 3.3.987.0
	• Atualização de `ec2-macos-init` para a versão 1.5.10
	• Atualização de `ec2-macos-utils` para a versão 1.0.4
	
	Lançamento do macOS Sequoia 15.0
	• Conteúdo de segurança do macOS Sequoia 15
	
	Lançamento do macOS Sonoma 14.7
	• Conteúdo de segurança do macOS Sonoma 14.7.
	• Atualização das ferramentas de linha de comando para a versão 16.0
	• Atualização do Safari para a versão 18.0.1
	  • Conteúdo de segurança do Safari 18
	
	Lançamento do macOS Ventura 13.7
	• Conteúdo de segurança do macOS Ventura 13.7
	• Atualização do Safari para a versão 18.0.1
	  • Conteúdo de segurança do Safari 18

Versão	Alterações

20/08/2024	Todas as AMIs
	• Atualização do Homebrew para a versão 4.3.14
	• Atualização da `aws-cli` para a versão 2.17.29
	
	Lançamento do macOS Sonoma 14.6.1
	• Nenhuma entrada de CVE publicada.
	
	Lançamento do macOS Ventura 13.6.9
	• Nenhuma entrada de CVE publicada.
	• Atualização do Safari para a versão 17.6
	  • Conteúdo de segurança do Safari 17.6
	
	Lançamento do macOS Monterey 12.7.6
	• Conteúdo de segurança do macOS Monterey 12.7.6
	• Atualização do Safari para a versão 17.6
	  • Conteúdo de segurança do Safari 17.6

Versão	Alterações

07/06/2024	Todas as AMIs
	• Atualização do Homebrew para a versão 4.3.1-1
	• Atualização da `aws-cli` para a versão 2.15.56
	• Atualização do `amazon-ssm-agent` para a versão 3.3.380.0-1
	
	Lançamento do macOS Sonoma 14.5
	• Conteúdo de segurança do macOS Sonoma 14.5
	
	Lançamento do macOS Ventura 13.6.7
	• Conteúdo de segurança do macOS Ventura 13.6.7
	• Atualização do Safari para a versão 17.5
	  • Conteúdo de segurança do Safari 17.5
	
	Lançamento do macOS Monterey 12.7.5
	• Conteúdo de segurança do macOS Monterey 12.7.5
	• Atualização do Safari para a versão 17.5
	  • Conteúdo de segurança do Safari 17.5

Versão	Alterações

12/04/2024	Todas as AMIs
	• Atualização do Homebrew para a versão 4.2.16-1
	• Atualização da `aws-cli` para a versão 2.15.36
	
	Lançamento do macOS Sonoma 14.4.1
	• Conteúdo de segurança do macOS Sonoma 14.4.1
	
	Lançamento do macOS Ventura 13.6.6
	• Conteúdo de segurança do macOS Ventura 13.6.6
	• Atualização do Safari para a versão 17.4.1
	  • Conteúdo de segurança do Safari 17.4.1
	
	Para macOS Monterey
	• Atualização do Safari para a versão 17.4.1
	  • Conteúdo de segurança do Safari 17.4.1

Tipos de instância otimizados para o Amazon EBS

As instâncias otimizadas para o Amazon EBS usam uma pilha de configuração otimizada e fornecem largura de banda dedicada adicional para E/S do Amazon EBS. Essa otimização proporciona a melhor performance para os volumes do EBS minimizando a contenção entre E/S do Amazon EBS e demais tráfego vindo da instância.

Quando anexados a uma instância otimizada para EBS, os volumes de SSD de uso geral (`gp2` e `gp3`) oferecem pelo menos 90 por cento da performance de IOPS provisionada 99% do tempo a cada ano, e os volumes de SSD com IOPS provisionadas (`io1` e `io2`) oferecem pelo menos 90 por cento da performance de IOPS provisionadas 99,9% do tempo a cada ano. O HDD otimizado para throughput (`st1`) e o HDD frio (`sc1`) fornecem pelo menos 90 por cento da performance de throughput esperada 99 por cento do tempo a cada ano. Os períodos não compatíveis são distribuídos com uniformidade aproximada, destinando 99% da throughput total esperada a cada

hora. Para obter mais informações, consulte Tipos de volumes do Amazon EBS no Guia do usuário do Amazon EBS.

Alguns tipos de instância são otimizados para EBS por padrão. Não há necessidade de habilitá-los, e tentar desabilitá-los não tem qualquer efeito. Outros tipos de instância são opcionalmente compatíveis com o EBS e você habilitá-los durante ou depois da execução por uma taxa adicional por hora. Alguns tipos de instância não são compatíveis com a otimização do EBS.

Para obter especificações detalhadas sobre os tipos de instância, consulte o Guia de tipos de instância do Amazon EC2.

Considerações

- A performance do EBS de uma instância é limitada pelos limites de performance do tipo de instância ou pela performance agregada dos volumes a ela anexados, a que for menor. Para alcançar a performance máxima do EBS, uma instância deve ter volumes anexados que forneçam uma performance combinada igual ou superior à performance máxima da instância. Por exemplo, para conseguir `80,000` IOPS para `r6i.16xlarge`, a instância deve ter pelo menos 5 volumes gp2provisionados com `16,000` IOPS cada (5 volumes x `16,000` IOPS = `80,000` IOPS) ou pode ter 1 volume gp3 provisionado com `80,000` IOPS. Recomendamos que você escolha um tipo de instância que forneça mais throughput dedicado do Amazon EBS do que o necessário para a aplicação. Caso contrário, a conexão entre o Amazon EBS e o Amazon EC2 pode se tornar um gargalo de performance.
- O número máximo de volumes do Amazon EBS que é possível anexar a uma instância depende do tipo e do tamanho da instância. Para obter mais informações, consulte Limites de volume do Amazon EBS para instâncias do Amazon EC2.
- Os limites máximos de IOPS e de throughput são interdependentes. Dependendo do tamanho da E/S, é possível atingir um limite antes do outro, o que pode afetar a performance geral. Para obter os melhores resultados, considere ambos os limites ao planejar sua workload.

Otimizados para EBS por padrão

Os tipos de instância a seguir são otimizados para EBS por padrão. Não é necessário habilitar a otimização para EBS, e nada ocorrerá se você desabilitá-la.

Instâncias

- Uso geral
- Otimizadas para computação

- Otimizado para memória
- Otimizada para armazenamento
- Computação acelerada
- Computação de alta performance

Uso geral

> **Note**
>
> Os tipos de instância M8a, M8g, M8gd, M8i, M8id, M8i-flex oferecem suporte a ponderações de largura de banda configuráveis. Com esses tipos de instância, é possível otimizar a largura de banda de uma instância para performance de rede ou performance do Amazon EBS. A tabela a seguir mostra a performance padrão de largura de banda do Amazon EBS para esses tipos de instância. Para obter mais informações, consulte Configuração de ponderação de largura de banda de instâncias do EC2.

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
a1.medium [1]	300	3500	37.50	437.50	2500	20000
a1.large [1]	525	3500	65.62	437.50	4000	20000
a1.xlarge [1]	800	3500	100.00	437.50	6000	20000
a1.2xlarge [1]	1750	3500	218,75	437.50	10000	20000
a1.4xlarge [2]	3500		437,5		20000	
a1.metal [2]	3500		437,5		20000	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
m4.large [2]	450		56,25		3600	
m4.xlarge [2]	750		93,75		6000	
m4.2xlarge [2]	1000		125.0		8000	
m4.4xlarge [2]	2000		250.0		16000	
m4.10xlarge [2]	4000		500.0		32000	
m4.16xlarge [2]	10000		1250.0		65000	
m5.large [1]	650	4750	81,25	593,75	3600	18750
m5.xlarge [1]	1150	4750	143,75	593,75	6000	18750
m5.2xlarge [1]	2300	4750	287.50	593,75	12000	18750
m5.4xlarge [2]	4750		593,75		18750	
m5.8xlarge [2]	6800		850.0		30000	
m5.12xlarge [2]	9500		1187,5		40000	
m5.16xlarge [2]	13600		1700.0		60000	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
m5.24xlarge [2]	19000		2375.0		80000	
m5.metal [2]	19000		2375.0		80000	
m5a.large [1]	650	2.880	81,25	360.00	3600	16000
m5a.xlarge [1]	1085	2.880	135.62	360.00	6000	16000
m5a.2xlarge [1]	1580	2.880	197.50	360.00	8333	16000
m5a.4xlarge [2]	2.880		360.0		16000	
m5a.8xlarge [2]	4750		593,75		20000	
m5a.12xlarge [2]	6780		847,5		30000	
m5a.16xlarge [2]	9500		1187,5		40000	
m5a.24xlarge [2]	13750		1718.75		60000	
m5ad.large [1]	650	2.880	81,25	360.00	3600	16000

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
m5ad.xlarge [1]	1085	2.880	135.62	360.00	6000	16000
m5ad.2xlarge [1]	1580	2.880	197.50	360.00	8333	16000
m5ad.4xlarge [2]	2.880		360.0		16000	
m5ad.8xlarge [2]	4750		593,75		20000	
m5ad.12xlarge [2]	6780		847,5		30000	
m5ad.16xlarge [2]	9500		1187,5		40000	
m5ad.24xlarge [2]	13750		1718.75		60000	
m5d.large [1]	650	4750	81,25	593,75	3600	18750
m5d.xlarge [1]	1150	4750	143,75	593,75	6000	18750
m5d.2xlarge [1]	2300	4750	287.50	593,75	12000	18750
m5d.4xlarge [2]	4750		593,75		18750	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
m5d.8xlarge [2]	6800		850.0		30000	
m5d.12xlarge [2]	9500		1187,5		40000	
m5d.16xlarge [2]	13600		1700.0		60000	
m5d.24xlarge [2]	19000		2375.0		80000	
m5d.metal [2]	19000		2375.0		80000	
m5dn.large [1]	650	4750	81,25	593,75	3600	18750
m5dn.xlarge [1]	1150	4750	143,75	593,75	6000	18750
m5dn.2xlarge [1]	2300	4750	287.50	593,75	12000	18750
m5dn.4xlarge [2]	4750		593,75		18750	
m5dn.8xlarge [2]	6800		850.0		30000	
m5dn.12xlarge [2]	9500		1187,5		40000	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
m5dn.16xlarge [2]	13600		1700.0		60000	
m5dn.24xlarge [2]	19000		2375.0		80000	
m5dn.metal [2]	19000		2375.0		80000	
m5n.large [1]	650	4750	81,25	593,75	3600	18750
m5n.xlarge [1]	1150	4750	143,75	593,75	6000	18750
m5n.2xlarge [1]	2300	4750	287.50	593,75	12000	18750
m5n.4xlarge [2]	4750		593,75		18750	
m5n.8xlarge [2]	6800		850.0		30000	
m5n.12xlarge [2]	9500		1187,5		40000	
m5n.16xlarge [2]	13600		1700.0		60000	
m5n.24xlarge [2]	19000		2375.0		80000	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
m5n.metal [2]	19000		2375.0		80000	
m5zn.large [1]	800	3170	100.00	396,25	3333	13333
m5zn.xlarge [1]	1564	3170	195.50	396,25	6667	13333
m5zn.2xlarge [2]	3170		396,25		13333	
m5zn.3xlarge [2]	4750		593,75		20000	
m5zn.6xlarge [2]	9500		1187,5		40000	
m5zn.12xlarge [2]	19000		2375.0		80000	
m5zn.metal [2]	19000		2375.0		80000	
m6a.large [1]	650	10000	81,25	1250.00	3600	40000
m6a.xlarge [1]	1250	10000	156,25	1250.00	6000	40000
m6a.2xlarge [1]	2500	10000	312.50	1250.00	12000	40000

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
m6a.4xlarge [1]	5000	10000	625.00	1250.00	20000	40000
m6a.8xlarge [2]	10000		1250.0		40000	
m6a.12xlarge [2]	15000		1875.0		60000	
m6a.16xlarge [2]	20000		2500.0		80000	
m6a.24xlarge [2]	30000		3750.0		120000	
m6a.32xlarge [2]	40000		5000.0		160000	
m6a.48xlarge [2]	40000		5000.0		240000	
m6a.metal [2]	40000		5000.0		240000	
m6g.medium [1]	315	4750	39.38	593,75	2500	20000
m6g.large [1]	630	4750	78,75	593,75	3600	20000
m6g.xlarge [1]	1188	4750	148.50	593,75	6000	20000

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
m6g.2xlarge [1]	2375	4750	296.88	593,75	12000	20000
m6g.4xlarge [2]	4750		593,75		20000	
m6g.8xlarge [2]	9500		1187,5		40000	
m6g.12xlarge [2]	14250		1781.25		50000	
m6g.16xlarge [2]	19000		2375.0		80000	
m6g.metal [2]	19000		2375.0		80000	
m6gd.medium [1]	315	4750	39.38	593,75	2500	20000
m6gd.large [1]	630	4750	78,75	593,75	3600	20000
m6gd.xlarge [1]	1188	4750	148.50	593,75	6000	20000
m6gd.2xlarge [1]	2375	4750	296.88	593,75	12000	20000
m6gd.4xlarge [2]	4750		593,75		20000	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
m6gd.8xlarge [2]	9500		1187,5		40000	
m6gd.12xlarge [2]	14250		1781.25		50000	
m6gd.16xlarge [2]	19000		2375.0		80000	
m6gd.metal [2]	19000		2375.0		80000	
m6i.large [1]	650	10000	81,25	1250.00	3600	40000
m6i.xlarge [1]	1250	10000	156,25	1250.00	6000	40000
m6i.2xlarge [1]	2500	10000	312.50	1250.00	12000	40000
m6i.4xlarge [1]	5000	10000	625.00	1250.00	20000	40000
m6i.8xlarge [2]	10000		1250.0		40000	
m6i.12xlarge [2]	15000		1875.0		60000	
m6i.16xlarge [2]	20000		2500.0		80000	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
m6i.24xlarge [2]	30000		3750.0		120000	
m6i.32xlarge [2]	40000		5000.0		160000	
m6i.metal [2]	40000		5000.0		160000	
m6id.large [1]	650	10000	81,25	1250.00	3600	40000
m6id.xlarge [1]	1250	10000	156,25	1250.00	6000	40000
m6id.2xlarge [1]	2500	10000	312.50	1250.00	12000	40000
m6id.4xlarge [1]	5000	10000	625.00	1250.00	20000	40000
m6id.8xlarge [2]	10000		1250.0		40000	
m6id.12xlarge [2]	15000		1875.0		60000	
m6id.16xlarge [2]	20000		2500.0		80000	
m6id.24xlarge [2]	30000		3750.0		120000	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
m6id.32xlarge [2]	40000		5000.0		160000	
m6id.metal [2]	40000		5000.0		160000	
m6idn.large [1]	1562	25000	195.31	3125.00	6250	100000
m6idn.xlarge [1]	3125	25000	390.62	3125.00	12500	100000
m6idn.2xlarge [1]	6250	25000	781.25	3125.00	25000	100000
m6idn.4xlarge [1]	12500	25000	1562.50	3125.00	50000	100000
m6idn.8xlarge [2]	25000		3125.0		100000	
m6idn.12xlarge [2]	37500		4687.5		150000	
m6idn.16xlarge [2]	50000		6250.0		200000	
m6idn.24xlarge [2]	75000		9375.0		300000	
m6idn.32xlarge [2]	100000		12500.0		400000	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
m6idn.metal [2]	100000		12500.0		400000	
m6in.large [1]	1562	25000	195.31	3125.00	6250	100000
m6in.xlarge [1]	3125	25000	390.62	3125.00	12500	100000
m6in.2xlarge [1]	6250	25000	781.25	3125.00	25000	100000
m6in.4xlarge [1]	12500	25000	1562.50	3125.00	50000	100000
m6in.8xlarge [2]	25000		3125.0		100000	
m6in.12xlarge [2]	37500		4687.5		150000	
m6in.16xlarge [2]	50000		6250.0		200000	
m6in.24xlarge [2]	75000		9375.0		300000	
m6in.32xlarge [2]	100000		12500.0		400000	
m6in.metal [2]	100000		12500.0		400000	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
m7a.medium [1]	325	10000	40.62	1250.00	2500	40000
m7a.large [1]	650	10000	81,25	1250.00	3600	40000
m7a.xlarge [1]	1250	10000	156,25	1250.00	6000	40000
m7a.2xlarge [1]	2500	10000	312.50	1250.00	12000	40000
m7a.4xlarge [1]	5000	10000	625.00	1250.00	20000	40000
m7a.8xlarge [2]	10000		1250.0		40000	
m7a.12xlarge [2]	15000		1875.0		60000	
m7a.16xlarge [2]	20000		2500.0		80000	
m7a.24xlarge [2]	30000		3750.0		120000	
m7a.32xlarge [2]	40000		5000.0		160000	
m7a.48xlarge [2]	40000		5000.0		240000	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
m7a.metal-48xl [2]	40000		5000.0		240000	
m7g.medium [1]	315	10000	39.38	1250.00	2500	40000
m7g.large [1]	630	10000	78,75	1250.00	3600	40000
m7g.xlarge [1]	1250	10000	156,25	1250.00	6000	40000
m7g.2xlarge [1]	2500	10000	312.50	1250.00	12000	40000
m7g.4xlarge [1]	5000	10000	625.00	1250.00	20000	40000
m7g.8xlarge [2]	10000		1250.0		40000	
m7g.12xlarge [2]	15000		1875.0		60000	
m7g.16xlarge [2]	20000		2500.0		80000	
m7g.metal [2]	20000		2500.0		80000	
m7gd.medium [1]	315	10000	39.38	1250.00	2500	40000

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
m7gd.large [1]	630	10000	78,75	1250.00	3600	40000
m7gd.xlarge [1]	1250	10000	156,25	1250.00	6000	40000
m7gd.2xlarge [1]	2500	10000	312.50	1250.00	12000	40000
m7gd.4xlarge [1]	5000	10000	625.00	1250.00	20000	40000
m7gd.8xlarge [2]	10000		1250.0		40000	
m7gd.12xlarge [2]	15000		1875.0		60000	
m7gd.16xlarge [2]	20000		2500.0		80000	
m7gd.metal [2]	20000		2500.0		80000	
m7i.large [1]	650	10000	81,25	1250.00	3600	40000
m7i.xlarge [1]	1250	10000	156,25	1250.00	6000	40000
m7i.2xlarge [1]	2500	10000	312.50	1250.00	12000	40000

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
m7i.4xlarge [1]	5000	10000	625.00	1250.00	20000	40000
m7i.8xlarge [2]	10000		1250.0		40000	
m7i.12xlarge [2]	15000		1875.0		60000	
m7i.16xlarge [2]	20000		2500.0		80000	
m7i.24xlarge [2]	30000		3750.0		120000	
m7i.48xlarge [2]	40000		5000.0		240000	
m7i.metal-24xl [2]	30000		3750.0		120000	
m7i.metal-48xl [2]	40000		5000.0		240000	
m7i-flex.large [1]	312	10000	39.06	1250.00	2500	40000
m7i-flex.xlarge [1]	625	10000	78.12	1250.00	3600	40000
m7i-flex.2xlarge [1]	1250	10000	156,25	1250.00	6000	40000

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
m7i-flex.4xlarge [1]	2500	10000	312.50	1250.00	12000	40000
m7i-flex.8xlarge [1]	5000	10000	625.00	1250.00	20000	40000
m7i-flex.12xlarge [1]	7500	15000	937.50	1875.00	30000	60000
m7i-flex.16xlarge [1]	10000	20000	1250.00	2500.00	40000	80000
m8a.medium [1]	325	10000	40.62	1250.00	2500	40000
m8a.large [1]	650	10000	81,25	1250.00	3600	40000
m8a.xlarge [1]	1250	10000	156,25	1250.00	6000	40000
m8a.2xlarge [1]	2500	10000	312.50	1250.00	12000	40000
m8a.4xlarge [1]	5000	10000	625.00	1250.00	20000	40000
m8a.8xlarge [2]	10000		1250.0		40000	
m8a.12xlarge [2]	15000		1875.0		60000	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
m8a.16xlarge [2]	20000		2500.0		80000	
m8a.24xlarge [2]	30000		3750.0		120000	
m8a.48xlarge [2]	60000		7500.0		240000	
m8a.metal-24xl [2]	30000		3750.0		120000	
m8a.metal-48xl [2]	60000		7500.0		240000	
m8azn.medium [1]	625	15000	78.12	1875.00	2500	60000
m8azn.large [1]	1250	15000	156,25	1875.00	5000	60000
m8azn.xlarge [1]	2500	15000	312.50	1875.00	10000	60000
m8azn.3xlarge [1]	7500	15000	937.50	1875.00	30000	60000
m8azn.6xlarge [2]	15000		1875.0		60000	
m8azn.12xlarge [2]	30000		3750.0		120000	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
m8azn.24xlarge [2]	60000		7500.0		240000	
m8azn.metal-12xl [2]	30000		3750.0		120000	
m8azn.metal-24xl [2]	60000		7500.0		240000	
m8g.medium [1]	315	10000	39.38	1250.00	2500	40000
m8g.large [1]	630	10000	78,75	1250.00	3600	40000
m8g.xlarge [1]	1250	10000	156,25	1250.00	6000	40000
m8g.2xlarge [1]	2500	10000	312.50	1250.00	12000	40000
m8g.4xlarge [1]	5000	10000	625.00	1250.00	20000	40000
m8g.8xlarge [2]	10000		1250.0		40000	
m8g.12xlarge [2]	15000		1875.0		60000	
m8g.16xlarge [2]	20000		2500.0		80000	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
m8g.24xlarge [2]	30000		3750.0		120000	
m8g.48xlarge [2]	40000		5000.0		240000	
m8g.metal-24xl [2]	30000		3750.0		120000	
m8g.metal-48xl [2]	40000		5000.0		240000	
m8gb.medium [1]	1562	25000	195.31	3125.00	7500	120000
m8gb.large [1]	3125	25000	390.62	3125.00	15000	120000
m8gb.xlarge [1]	6250	25000	781.25	3125.00	30000	120000
m8gb.2xlarge [1]	12500	25000	1562.50	3125.00	60000	120000
m8gb.4xlarge [2]	25000		3125.0		120000	
m8gb.8xlarge [2]	50000		6250.0		240000	
m8gb.12xlarge [2]	75000		9375.0		360000	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
m8gb.16xlarge [2]	100000		12500.0		480000	
m8gb.24xlarge [2]	150000		18750.0		720000	
m8gb.48xlarge [2]	300000		37500.0		1440000	
m8gd.medium [1]	315	10000	39.38	1250.00	2500	40000
m8gd.large [1]	630	10000	78,75	1250.00	3600	40000
m8gd.xlarge [1]	1250	10000	156,25	1250.00	6000	40000
m8gd.2xlarge [1]	2500	10000	312.50	1250.00	12000	40000
m8gd.4xlarge [1]	5000	10000	625.00	1250.00	20000	40000
m8gd.8xlarge [2]	10000		1250.0		40000	
m8gd.12xlarge [2]	15000		1875.0		60000	
m8gd.16xlarge [2]	20000		2500.0		80000	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
m8gd.24xlarge [2]	30000		3750.0		120000	
m8gd.48xlarge [2]	40000		5000.0		240000	
m8gd.metal-24xl [2]	30000		3750.0		120000	
m8gd.metal-48xl [2]	40000		5000.0		240000	
m8gn.medium [1]	760	10000	95.00	1250.00	2500	40000
m8gn.large [1]	1250	10000	156,25	1250.00	5000	40000
m8gn.xlarge [1]	2500	10000	312.50	1250.00	10000	40000
m8gn.2xlarge [1]	5000	10000	625.00	1250.00	20000	40000
m8gn.4xlarge [2]	10000		1250.0		40000	
m8gn.8xlarge [2]	20000		2500.0		80000	
m8gn.12xlarge [2]	30000		3750.0		120000	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
m8gn.16xlarge [2]	40000		5000.0		160000	
m8gn.24xlarge [2]	60000		7500.0		240000	
m8gn.48xlarge [2]	60000		7500.0		240000	
m8i.large [1]	650	10000	81,25	1250.00	3600	40000
m8i.xlarge [1]	1250	10000	156,25	1250.00	6000	40000
m8i.2xlarge [1]	2500	10000	312.50	1250.00	12000	40000
m8i.4xlarge [1]	5000	10000	625.00	1250.00	20000	40000
m8i.8xlarge [2]	10000		1250.0		40000	
m8i.12xlarge [2]	15000		1875.0		60000	
m8i.16xlarge [2]	20000		2500.0		80000	
m8i.24xlarge [2]	30000		3750.0		120000	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
m8i.32xlarge [2]	40000		5000.0		160000	
m8i.48xlarge [2]	60000		7500.0		240000	
m8i.96xlarge [2]	80000		10000.0		480000	
m8i.metal-48xl [2]	60000		7500.0		240000	
m8i.metal-96xl [2]	80000		10000.0		480000	
m8id.large [1]	650	10000	81,25	1250.00	3600	40000
m8id.xlarge [1]	1250	10000	156,25	1250.00	6000	40000
m8id.2xlarge [1]	2500	10000	312.50	1250.00	12000	40000
m8id.4xlarge [1]	5000	10000	625.00	1250.00	20000	40000
m8id.8xlarge [2]	10000		1250.0		40000	
m8id.12xlarge [2]	15000		1875.0		60000	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
m8id.16xlarge [2]	20000		2500.0		80000	
m8id.24xlarge [2]	30000		3750.0		120000	
m8id.32xlarge [2]	40000		5000.0		160000	
m8id.48xlarge [2]	60000		7500.0		240000	
m8id.96xlarge [2]	80000		10000.0		480000	
m8id.metal-48xl [2]	60000		7500.0		240000	
m8id.metal-96xl [2]	80000		10000.0		480000	
m8i-flex.large [1]	315	10000	39.38	1250.00	2500	40000
m8i-flex.xlarge [1]	630	10000	78,75	1250.00	3600	40000
m8i-flex.2xlarge [1]	1250	10000	156,25	1250.00	6000	40000
m8i-flex.4xlarge [1]	2500	10000	312.50	1250.00	12000	40000

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
m8i-flex.8xlarge [1]	5000	10000	625.00	1250.00	20000	40000
m8i-flex.12xlarge [1]	7500	15000	937.50	1875.00	30000	60000
m8i-flex.16xlarge [1]	10000	20000	1250.00	2500.00	40000	80000
mac1.metal [2]	14000		1750.0		80000	
mac2.metal [2]	10000		1250.0		55000	
mac2-m1ultra.metal [2]	10000		1250.0		55000	
mac2-m2.metal [2]	8000		1000.0		55000	
mac2-m2pro.metal [2]	8000		1000.0		55000	
mac-m4.metal [2]	8000		1000.0		55000	
mac-m4pro.metal [2]	8000		1000.0		55000	
t3.nano [1]	43	2085	5.38	260.62	250	11800
t3.micro [1]	87	2085	10.88	260.62	500	11800

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
t3.small [1]	174	2085	21.75	260.62	1000	11800
t3.medium [1]	347	2085	43.38	260.62	2000	11800
t3.large [1]	695	2780	86.88	347.50	4000	15700
t3.xlarge [1]	695	2780	86.88	347.50	4000	15700
t3.2xlarge [1]	695	2780	86.88	347.50	4000	15700
t3a.nano [1]	45	2085	5.62	260.62	250	11800
t3a.micro [1]	90	2085	11,25	260.62	500	11800
t3a.small [1]	175	2085	21,88	260.62	1000	11800
t3a.medium [1]	350	2085	43,75	260.62	2000	11800
t3a.large [1]	695	2780	86.88	347.50	4000	15700
t3a.xlarge [1]	695	2780	86.88	347.50	4000	15700
t3a.2xlarge [1]	695	2780	86.88	347.50	4000	15700
t4g.nano [1]	43	2085	5.38	260.62	250	11800
t4g.micro [1]	87	2085	10.88	260.62	500	11800
t4g.small [1]	174	2085	21.75	260.62	1000	11800
t4g.medium [1]	347	2085	43.38	260.62	2000	11800

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
t4g.large [1]	695	2780	86.88	347.50	4000	15700
t4g.xlarge [1]	695	2780	86.88	347.50	4000	15700
t4g.2xlarge [1]	695	2780	86.88	347.50	4000	15700

[1] Essas instâncias podem sustentar o desempenho máximo por 30 minutos pelo menos uma vez a cada 24 horas e depois revertem para o desempenho básico.

[2] Essas instâncias podem manter a performance declarada indefinidamente. Se a sua workload exigir performance máxima sustentado por mais de 30 minutos, selecione uma dessas instâncias.

Otimizadas para computação

> **Note**
>
> Os tipos de instância C8a, C8g, C8gd, C8i, C8id, C8i-flex oferecem suporte a com ponderações de larguras de bandas configuráveis. Com esses tipos de instância, é possível otimizar a largura de banda de uma instância para performance de rede ou performance do Amazon EBS. A tabela a seguir mostra a performance padrão de largura de banda do Amazon EBS para esses tipos de instância. Para obter mais informações, consulte Configuração de ponderação de largura de banda de instâncias do EC2.

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
c4.large [2]	500		62.5		4000	
c4.xlarge [2]	750		93,75		6000	
c4.2xlarge [2]	1000		125.0		8000	
c4.4xlarge [2]	2000		250.0		16000	
c4.8xlarge [2]	4000		500.0		32000	
c5.large [1]	650	4750	81,25	593,75	4000	20000
c5.xlarge [1]	1150	4750	143,75	593,75	6000	20000
c5.2xlarge [1]	2300	4750	287.50	593,75	10000	20000
c5.4xlarge [2]	4750		593,75		20000	
c5.9xlarge [2]	9500		1187,5		40000	
c5.12xlarge [2]	9500		1187,5		40000	
c5.18xlarge [2]	19000		2375.0		80000	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
c5.24xlarge [2]	19000		2375.0		80000	
c5.metal [2]	19000		2375.0		80000	
c5a.large [1]	200	3170	25.00	396,25	800	13300
c5a.xlarge [1]	400	3170	50.00	396,25	1600	13300
c5a.2xlarge [1]	800	3170	100.00	396,25	3200	13300
c5a.4xlarge [1]	1580	3170	197.50	396,25	6600	13300
c5a.8xlarge [2]	3170		396,25		13300	
c5a.12xlarge [2]	4750		593,75		20000	
c5a.16xlarge [2]	6300		787.5		26700	
c5a.24xlarge [2]	9500		1187,5		40000	
c5ad.large [1]	200	3170	25.00	396,25	800	13300
c5ad.xlarge [1]	400	3170	50.00	396,25	1600	13300

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
c5ad.2xlarge [1]	800	3170	100.00	396,25	3200	13300
c5ad.4xlarge [1]	1580	3170	197.50	396,25	6600	13300
c5ad.8xlarge [2]	3170		396,25		13300	
c5ad.12xlarge [2]	4750		593,75		20000	
c5ad.16xlarge [2]	6300		787.5		26700	
c5ad.24xlarge [2]	9500		1187,5		40000	
c5d.large [1]	650	4750	81,25	593,75	4000	20000
c5d.xlarge [1]	1150	4750	143,75	593,75	6000	20000
c5d.2xlarge [1]	2300	4750	287.50	593,75	10000	20000
c5d.4xlarge [2]	4750		593,75		20000	
c5d.9xlarge [2]	9500		1187,5		40000	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
c5d.12xlarge [2]	9500		1187,5		40000	
c5d.18xlarge [2]	19000		2375.0		80000	
c5d.24xlarge [2]	19000		2375.0		80000	
c5d.metal [2]	19000		2375.0		80000	
c5n.large [1]	650	4750	81,25	593,75	4000	20000
c5n.xlarge [1]	1150	4750	143,75	593,75	6000	20000
c5n.2xlarge [1]	2300	4750	287.50	593,75	10000	20000
c5n.4xlarge [2]	4750		593,75		20000	
c5n.9xlarge [2]	9500		1187,5		40000	
c5n.18xlarge [2]	19000		2375.0		80000	
c5n.metal [2]	19000		2375.0		80000	
c6a.large [1]	650	10000	81,25	1250.00	3600	40000
c6a.xlarge [1]	1250	10000	156,25	1250.00	6000	40000

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
c6a.2xlarge [1]	2500	10000	312.50	1250.00	12000	40000
c6a.4xlarge [1]	5000	10000	625.00	1250.00	20000	40000
c6a.8xlarge [2]	10000		1250.0		40000	
c6a.12xlarge [2]	15000		1875.0		60000	
c6a.16xlarge [2]	20000		2500.0		80000	
c6a.24xlarge [2]	30000		3750.0		120000	
c6a.32xlarge [2]	40000		5000.0		160000	
c6a.48xlarge [2]	40000		5000.0		240000	
c6a.metal [2]	40000		5000.0		240000	
c6g.medium [1]	315	4750	39.38	593,75	2500	20000
c6g.large [1]	630	4750	78,75	593,75	3600	20000
c6g.xlarge [1]	1188	4750	148.50	593,75	6000	20000

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
c6g.2xlarge [1]	2375	4750	296.88	593,75	12000	20000
c6g.4xlarge [2]	4750		593,75		20000	
c6g.8xlarge [2]	9500		1187,5		40000	
c6g.12xlarge [2]	14250		1781.25		50000	
c6g.16xlarge [2]	19000		2375.0		80000	
c6g.metal [2]	19000		2375.0		80000	
c6gd.medium [1]	315	4750	39.38	593,75	2500	20000
c6gd.large [1]	630	4750	78,75	593,75	3600	20000
c6gd.xlarge [1]	1188	4750	148.50	593,75	6000	20000
c6gd.2xlarge [1]	2375	4750	296.88	593,75	12000	20000
c6gd.4xlarge [2]	4750		593,75		20000	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
c6gd.8xlarge [2]	9500		1187,5		40000	
c6gd.12xlarge [2]	14250		1781.25		50000	
c6gd.16xlarge [2]	19000		2375.0		80000	
c6gd.metal [2]	19000		2375.0		80000	
c6gn.medium [1]	760	9500	95.00	1187.50	2500	40000
c6gn.large [1]	1235	9500	154.38	1187.50	5000	40000
c6gn.xlarge [1]	2375	9500	296.88	1187.50	10000	40000
c6gn.2xlarge [1]	4750	9500	593,75	1187.50	20000	40000
c6gn.4xlarge [2]	9500		1187,5		40000	
c6gn.8xlarge [2]	19000		2375.0		80000	
c6gn.12xlarge [2]	28500		3562.5		120000	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
c6gn.16xlarge [2]	38000		4750.0		160000	
c6i.large [1]	650	10000	81,25	1250.00	3600	40000
c6i.xlarge [1]	1250	10000	156,25	1250.00	6000	40000
c6i.2xlarge [1]	2500	10000	312.50	1250.00	12000	40000
c6i.4xlarge [1]	5000	10000	625.00	1250.00	20000	40000
c6i.8xlarge [2]	10000		1250.0		40000	
c6i.12xlarge [2]	15000		1875.0		60000	
c6i.16xlarge [2]	20000		2500.0		80000	
c6i.24xlarge [2]	30000		3750.0		120000	
c6i.32xlarge [2]	40000		5000.0		160000	
c6i.metal [2]	40000		5000.0		160000	
c6id.large [1]	650	10000	81,25	1250.00	3600	40000
c6id.xlarge [1]	1250	10000	156,25	1250.00	6000	40000

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
c6id.2xlarge [1]	2500	10000	312.50	1250.00	12000	40000
c6id.4xlarge [1]	5000	10000	625.00	1250.00	20000	40000
c6id.8xlarge [2]	10000		1250.0		40000	
c6id.12xlarge [2]	15000		1875.0		60000	
c6id.16xlarge [2]	20000		2500.0		80000	
c6id.24xlarge [2]	30000		3750.0		120000	
c6id.32xlarge [2]	40000		5000.0		160000	
c6id.metal [2]	40000		5000.0		160000	
c6in.large [1]	1562	25000	195.31	3125.00	6250	100000
c6in.xlarge [1]	3125	25000	390.62	3125.00	12500	100000
c6in.2xlarge [1]	6250	25000	781.25	3125.00	25000	100000

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
c6in.4xlarge [1]	12500	25000	1562.50	3125.00	50000	100000
c6in.8xlarge [2]	25000		3125.0		100000	
c6in.12xlarge [2]	37500		4687.5		150000	
c6in.16xlarge [2]	50000		6250.0		200000	
c6in.24xlarge [2]	75000		9375.0		300000	
c6in.32xlarge [2]	100000		12500.0		400000	
c6in.metal [2]	100000		12500.0		400000	
c7a.medium [1]	325	10000	40.62	1250.00	2500	40000
c7a.large [1]	650	10000	81,25	1250.00	3600	40000
c7a.xlarge [1]	1250	10000	156,25	1250.00	6000	40000
c7a.2xlarge [1]	2500	10000	312.50	1250.00	12000	40000

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
c7a.4xlarge [1]	5000	10000	625.00	1250.00	20000	40000
c7a.8xlarge [2]	10000		1250.0		40000	
c7a.12xlarge [2]	15000		1875.0		60000	
c7a.16xlarge [2]	20000		2500.0		80000	
c7a.24xlarge [2]	30000		3750.0		120000	
c7a.32xlarge [2]	40000		5000.0		160000	
c7a.48xlarge [2]	40000		5000.0		240000	
c7a.metal-48xl [2]	40000		5000.0		240000	
c7g.medium [1]	315	10000	39.38	1250.00	2500	40000
c7g.large [1]	630	10000	78,75	1250.00	3600	40000
c7g.xlarge [1]	1250	10000	156,25	1250.00	6000	40000

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
c7g.2xlarge [1]	2500	10000	312.50	1250.00	12000	40000
c7g.4xlarge [1]	5000	10000	625.00	1250.00	20000	40000
c7g.8xlarge [2]	10000		1250.0		40000	
c7g.12xlarge [2]	15000		1875.0		60000	
c7g.16xlarge [2]	20000		2500.0		80000	
c7g.metal [2]	20000		2500.0		80000	
c7gd.medium [1]	315	10000	39.38	1250.00	2500	40000
c7gd.large [1]	630	10000	78,75	1250.00	3600	40000
c7gd.xlarge [1]	1250	10000	156,25	1250.00	6000	40000
c7gd.2xlarge [1]	2500	10000	312.50	1250.00	12000	40000
c7gd.4xlarge [1]	5000	10000	625.00	1250.00	20000	40000

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
c7gd.8xlarge [2]	10000		1250.0		40000	
c7gd.12xlarge [2]	15000		1875.0		60000	
c7gd.16xlarge [2]	20000		2500.0		80000	
c7gd.metal [2]	20000		2500.0		80000	
c7gn.medium [1]	521	10000	65.12	1250.00	2083	40000
c7gn.large [1]	1042	10000	130.25	1250.00	4167	40000
c7gn.xlarge [1]	2083	10000	260.38	1250.00	8333	40000
c7gn.2xlarge [1]	4167	10000	520.88	1250.00	16667	40000
c7gn.4xlarge [1]	8333	10000	1041.62	1250.00	33333	40000
c7gn.8xlarge [1]	16667	20000	2083.38	2500.00	66667	80000
c7gn.12xlarge [1]	25000	30000	3125.00	3750.00	100000	120000

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
c7gn.16xlarge [1]	33333	40000	4166.62	5000.00	133333	160000
c7gn.metal [1]	33333	40000	4166.62	5000.00	133333	160000
c7i.large [1]	650	10000	81,25	1250.00	3600	40000
c7i.xlarge [1]	1250	10000	156,25	1250.00	6000	40000
c7i.2xlarge [1]	2500	10000	312.50	1250.00	12000	40000
c7i.4xlarge [1]	5000	10000	625.00	1250.00	20000	40000
c7i.8xlarge [2]	10000		1250.0		40000	
c7i.12xlarge [2]	15000		1875.0		60000	
c7i.16xlarge [2]	20000		2500.0		80000	
c7i.24xlarge [2]	30000		3750.0		120000	
c7i.48xlarge [2]	40000		5000.0		240000	
c7i.metal-24xl [2]	30000		3750.0		120000	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
c7i.metal-48xl [2]	40000		5000.0		240000	
c7i-flex.large [1]	312	10000	39.06	1250.00	2500	40000
c7i-flex.xlarge [1]	625	10000	78.12	1250.00	3600	40000
c7i-flex.2xlarge [1]	1250	10000	156,25	1250.00	6000	40000
c7i-flex.4xlarge [1]	2500	10000	312.50	1250.00	12000	40000
c7i-flex.8xlarge [1]	5000	10000	625.00	1250.00	20000	40000
c7i-flex.12xlarge [1]	7500	15000	937.50	1875.00	30000	60000
c7i-flex.16xlarge [1]	10000	20000	1250.00	2500.00	40000	80000
c8a.medium [1]	325	10000	40.62	1250.00	2500	40000
c8a.large [1]	650	10000	81,25	1250.00	3600	40000
c8a.xlarge [1]	1250	10000	156,25	1250.00	6000	40000

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
c8a.2xlarge [1]	2500	10000	312.50	1250.00	12000	40000
c8a.4xlarge [1]	5000	10000	625.00	1250.00	20000	40000
c8a.8xlarge [2]	10000		1250.0		40000	
c8a.12xlarge [2]	15000		1875.0		60000	
c8a.16xlarge [2]	20000		2500.0		80000	
c8a.24xlarge [2]	30000		3750.0		120000	
c8a.48xlarge [2]	60000		7500.0		240000	
c8a.metal-24xl [2]	30000		3750.0		120000	
c8a.metal-48xl [2]	60000		7500.0		240000	
c8g.medium [1]	315	10000	39.38	1250.00	2500	40000
c8g.large [1]	630	10000	78,75	1250.00	3600	40000

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
c8g.xlarge [1]	1250	10000	156,25	1250.00	6000	40000
c8g.2xlarge [1]	2500	10000	312.50	1250.00	12000	40000
c8g.4xlarge [1]	5000	10000	625.00	1250.00	20000	40000
c8g.8xlarge [2]	10000		1250.0		40000	
c8g.12xlarge [2]	15000		1875.0		60000	
c8g.16xlarge [2]	20000		2500.0		80000	
c8g.24xlarge [2]	30000		3750.0		120000	
c8g.48xlarge [2]	40000		5000.0		240000	
c8g.metal-24xl [2]	30000		3750.0		120000	
c8g.metal-48xl [2]	40000		5000.0		240000	
c8gb.medium [1]	1562	25000	195.31	3125.00	7500	120000

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
c8gb.large [1]	3125	25000	390.62	3125.00	15000	120000
c8gb.xlarge [1]	6250	25000	781.25	3125.00	30000	120000
c8gb.2xlarge [1]	12500	25000	1562.50	3125.00	60000	120000
c8gb.4xlarge [2]	25000		3125.0		120000	
c8gb.8xlarge [2]	50000		6250.0		240000	
c8gb.12xlarge [2]	75000		9375.0		360000	
c8gb.16xlarge [2]	100000		12500.0		480000	
c8gb.24xlarge [2]	150000		18750.0		720000	
c8gb.48xlarge [2]	300000		37500.0		1440000	
c8gb.metal-24xl [2]	150000		18750.0		720000	
c8gb.metal-48xl [2]	300000		37500.0		1440000	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
c8gd.medium [1]	315	10000	39.38	1250.00	2500	40000
c8gd.large [1]	630	10000	78,75	1250.00	3600	40000
c8gd.xlarge [1]	1250	10000	156,25	1250.00	6000	40000
c8gd.2xlarge [1]	2500	10000	312.50	1250.00	12000	40000
c8gd.4xlarge [1]	5000	10000	625.00	1250.00	20000	40000
c8gd.8xlarge [2]	10000		1250.0		40000	
c8gd.12xlarge [2]	15000		1875.0		60000	
c8gd.16xlarge [2]	20000		2500.0		80000	
c8gd.24xlarge [2]	30000		3750.0		120000	
c8gd.48xlarge [2]	40000		5000.0		240000	
c8gd.metal-24xl [2]	30000		3750.0		120000	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
c8gd.metal-48xl [2]	40000		5000.0		240000	
c8gn.medium [1]	760	10000	95.00	1250.00	2500	40000
c8gn.large [1]	1250	10000	156,25	1250.00	5000	40000
c8gn.xlarge [1]	2500	10000	312.50	1250.00	10000	40000
c8gn.2xlarge [1]	5000	10000	625.00	1250.00	20000	40000
c8gn.4xlarge [2]	10000		1250.0		40000	
c8gn.8xlarge [2]	20000		2500.0		80000	
c8gn.12xlarge [2]	30000		3750.0		120000	
c8gn.16xlarge [2]	40000		5000.0		160000	
c8gn.24xlarge [2]	60000		7500.0		240000	
c8gn.48xlarge [2]	60000		7500.0		240000	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
c8gn.metal-24xl [2]	60000		7500.0		240000	
c8gn.metal-48xl [2]	60000		7500.0		240000	
c8i.large [1]	650	10000	81,25	1250.00	3600	40000
c8i.xlarge [1]	1250	10000	156,25	1250.00	6000	40000
c8i.2xlarge [1]	2500	10000	312.50	1250.00	12000	40000
c8i.4xlarge [1]	5000	10000	625.00	1250.00	20000	40000
c8i.8xlarge [2]	10000		1250.0		40000	
c8i.12xlarge [2]	15000		1875.0		60000	
c8i.16xlarge [2]	20000		2500.0		80000	
c8i.24xlarge [2]	30000		3750.0		120000	
c8i.32xlarge [2]	40000		5000.0		160000	
c8i.48xlarge [2]	60000		7500.0		240000	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
c8i.96xlarge [2]	80000		10000.0		480000	
c8i.metal-48xl [2]	60000		7500.0		240000	
c8i.metal-96xl [2]	80000		10000.0		480000	
c8id.large [1]	650	10000	81,25	1250.00	3600	40000
c8id.xlarge [1]	1250	10000	156,25	1250.00	6000	40000
c8id.2xlarge [1]	2500	10000	312.50	1250.00	12000	40000
c8id.4xlarge [1]	5000	10000	625.00	1250.00	20000	40000
c8id.8xlarge [2]	10000		1250.0		40000	
c8id.12xlarge [2]	15000		1875.0		60000	
c8id.16xlarge [2]	20000		2500.0		80000	
c8id.24xlarge [2]	30000		3750.0		120000	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
c8id.32xlarge [2]	40000		5000.0		160000	
c8id.48xlarge [2]	60000		7500.0		240000	
c8id.96xlarge [2]	80000		10000.0		480000	
c8id.metal-48xl [2]	60000		7500.0		240000	
c8id.metal-96xl [2]	80000		10000.0		480000	
c8i-flex.large [1]	315	10000	39.38	1250.00	2500	40000
c8i-flex.xlarge [1]	630	10000	78,75	1250.00	3600	40000
c8i-flex.2xlarge [1]	1250	10000	156,25	1250.00	6000	40000
c8i-flex.4xlarge [1]	2500	10000	312.50	1250.00	12000	40000
c8i-flex.8xlarge [1]	5000	10000	625.00	1250.00	20000	40000
c8i-flex.12xlarge [1]	7500	15000	937.50	1875.00	30000	60000

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
c8i-flex.16xlarge [1]	10000	20000	1250.00	2500.00	40000	80000

[1] Essas instâncias podem sustentar o desempenho máximo por 30 minutos pelo menos uma vez a cada 24 horas e depois revertem para o desempenho básico.

[2] Essas instâncias podem manter a performance declarada indefinidamente. Se a sua workload exigir performance máxima sustentado por mais de 30 minutos, selecione uma dessas instâncias.

Otimizado para memória

> **Note**
>
> - Os tipos de instância R8a, R8g, R8gd, R8i, R8id, R8i-flex, X8g, X8aedz, X8i são compatíveis com ponderações de larguras de bandas configuráveis. Com esses tipos de instância, é possível otimizar a largura de banda de uma instância para performance de rede ou performance do Amazon EBS. A tabela a seguir mostra a performance padrão de largura de banda do Amazon EBS para esses tipos de instância. Para obter mais informações, consulte Configuração de ponderação de largura de banda de instâncias do EC2.
> - Para obter a performance máxima de IOPS com instâncias U7i, recomendamos que você use volumes do io2 BlockExpress.

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
r4.large [2]	425		53.125		3000	
r4.xlarge [2]	850		106,25		6000	
r4.2xlarge [2]	1700		212,5		12000	
r4.4xlarge [2]	3500		437,5		18750	
r4.8xlarge [2]	7000		875.0		37500	
r4.16xlarge [2]	14000		1750.0		75000	
r5.large [1]	650	4750	81,25	593,75	3600	18750
r5.xlarge [1]	1150	4750	143,75	593,75	6000	18750
r5.2xlarge [1]	2300	4750	287.50	593,75	12000	18750
r5.4xlarge [2]	4750		593,75		18750	
r5.8xlarge [2]	6800		850.0		30000	
r5.12xlarge [2]	9500		1187,5		40000	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
r5.16xlarge [2]	13600		1700.0		60000	
r5.24xlarge [2]	19000		2375.0		80000	
r5.metal [2]	19000		2375.0		80000	
r5a.large [1]	650	2.880	81,25	360.00	3600	16000
r5a.xlarge [1]	1085	2.880	135.62	360.00	6000	16000
r5a.2xlarge [1]	1580	2.880	197.50	360.00	8333	16000
r5a.4xlarge [2]	2.880		360.0		16000	
r5a.8xlarge [2]	4750		593,75		20000	
r5a.12xlarge [2]	6780		847,5		30000	
r5a.16xlarge [2]	9500		1187,5		40000	
r5a.24xlarge [2]	13570		1696.25		60000	
r5ad.large [1]	650	2.880	81,25	360.00	3600	16000

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
r5ad.xlarge [1]	1085	2.880	135.62	360.00	6000	16000
r5ad.2xlarge [1]	1580	2.880	197.50	360.00	8333	16000
r5ad.4xlarge [2]	2.880		360.0		16000	
r5ad.8xlarge [2]	4750		593,75		20000	
r5ad.12xlarge [2]	6780		847,5		30000	
r5ad.16xlarge [2]	9500		1187,5		40000	
r5ad.24xlarge [2]	13570		1696.25		60000	
r5b.large [1]	1250	10000	156,25	1250.00	5417	43333
r5b.xlarge [1]	2500	10000	312.50	1250.00	10833	43333
r5b.2xlarge [1]	5000	10000	625.00	1250.00	21667	43333
r5b.4xlarge [2]	10000		1250.0		43333	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
r5b.8xlarge [2]	20000		2500.0		86667	
r5b.12xlarge [2]	30000		3750.0		130000	
r5b.16xlarge [2]	40000		5000.0		173333	
r5b.24xlarge [2]	60000		7500.0		260000	
r5b.metal [2]	60000		7500.0		260000	
r5d.large [1]	650	4750	81,25	593,75	3600	18750
r5d.xlarge [1]	1150	4750	143,75	593,75	6000	18750
r5d.2xlarge [1]	2300	4750	287.50	593,75	12000	18750
r5d.4xlarge [2]	4750		593,75		18750	
r5d.8xlarge [2]	6800		850.0		30000	
r5d.12xlarge [2]	9500		1187,5		40000	
r5d.16xlarge [2]	13600		1700.0		60000	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
r5d.24xlarge [2]	19000		2375.0		80000	
r5d.metal [2]	19000		2375.0		80000	
r5dn.large [1]	650	4750	81,25	593,75	3600	18750
r5dn.xlarge [1]	1150	4750	143,75	593,75	6000	18750
r5dn.2xlarge [1]	2300	4750	287.50	593,75	12000	18750
r5dn.4xlarge [2]	4750		593,75		18750	
r5dn.8xlarge [2]	6800		850.0		30000	
r5dn.12xlarge [2]	9500		1187,5		40000	
r5dn.16xlarge [2]	13600		1700.0		60000	
r5dn.24xlarge [2]	19000		2375.0		80000	
r5dn.metal [2]	19000		2375.0		80000	
r5n.large [1]	650	4750	81,25	593,75	3600	18750

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
r5n.xlarge [1]	1150	4750	143,75	593,75	6000	18750
r5n.2xlarge [1]	2300	4750	287.50	593,75	12000	18750
r5n.4xlarge [2]	4750		593,75		18750	
r5n.8xlarge [2]	6800		850.0		30000	
r5n.12xlarge [2]	9500		1187,5		40000	
r5n.16xlarge [2]	13600		1700.0		60000	
r5n.24xlarge [2]	19000		2375.0		80000	
r5n.metal [2]	19000		2375.0		80000	
r6a.large [1]	650	10000	81,25	1250.00	3600	40000
r6a.xlarge [1]	1250	10000	156,25	1250.00	6000	40000
r6a.2xlarge [1]	2500	10000	312.50	1250.00	12000	40000
r6a.4xlarge [1]	5000	10000	625.00	1250.00	20000	40000

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
r6a.8xlarge [2]	10000		1250.0		40000	
r6a.12xlarge [2]	15000		1875.0		60000	
r6a.16xlarge [2]	20000		2500.0		80000	
r6a.24xlarge [2]	30000		3750.0		120000	
r6a.32xlarge [2]	40000		5000.0		160000	
r6a.48xlarge [2]	40000		5000.0		240000	
r6a.metal [2]	40000		5000.0		240000	
r6g.medium [1]	315	4750	39.38	593,75	2500	20000
r6g.large [1]	630	4750	78,75	593,75	3600	20000
r6g.xlarge [1]	1188	4750	148.50	593,75	6000	20000
r6g.2xlarge [1]	2375	4750	296.88	593,75	12000	20000
r6g.4xlarge [2]	4750		593,75		20000	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
r6g.8xlarge [2]	9500		1187,5		40000	
r6g.12xlarge [2]	14250		1781.25		50000	
r6g.16xlarge [2]	19000		2375.0		80000	
r6g.metal [2]	19000		2375.0		80000	
r6gd.medium [1]	315	4750	39.38	593,75	2500	20000
r6gd.large [1]	630	4750	78,75	593,75	3600	20000
r6gd.xlarge [1]	1188	4750	148.50	593,75	6000	20000
r6gd.2xlarge [1]	2375	4750	296.88	593,75	12000	20000
r6gd.4xlarge [2]	4750		593,75		20000	
r6gd.8xlarge [2]	9500		1187,5		40000	
r6gd.12xlarge [2]	14250		1781.25		50000	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
r6gd.16xlarge [2]	19000		2375.0		80000	
r6gd.metal [2]	19000		2375.0		80000	
r6i.large [1]	650	10000	81,25	1250.00	3600	40000
r6i.xlarge [1]	1250	10000	156,25	1250.00	6000	40000
r6i.2xlarge [1]	2500	10000	312.50	1250.00	12000	40000
r6i.4xlarge [1]	5000	10000	625.00	1250.00	20000	40000
r6i.8xlarge [2]	10000		1250.0		40000	
r6i.12xlarge [2]	15000		1875.0		60000	
r6i.16xlarge [2]	20000		2500.0		80000	
r6i.24xlarge [2]	30000		3750.0		120000	
r6i.32xlarge [2]	40000		5000.0		160000	
r6i.metal [2]	40000		5000.0		160000	
r6id.large [1]	650	10000	81,25	1250.00	3600	40000

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
r6id.xlarge [1]	1250	10000	156,25	1250.00	6000	40000
r6id.2xlarge [1]	2500	10000	312.50	1250.00	12000	40000
r6id.4xlarge [1]	5000	10000	625.00	1250.00	20000	40000
r6id.8xlarge [2]	10000		1250.0		40000	
r6id.12xlarge [2]	15000		1875.0		60000	
r6id.16xlarge [2]	20000		2500.0		80000	
r6id.24xlarge [2]	30000		3750.0		120000	
r6id.32xlarge [2]	40000		5000.0		160000	
r6id.metal [2]	40000		5000.0		160000	
r6idn.large [1]	1562	25000	195.31	3125.00	6250	100000
r6idn.xlarge [1]	3125	25000	390.62	3125.00	12500	100000

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
r6idn.2xlarge [1]	6250	25000	781.25	3125.00	25000	100000
r6idn.4xlarge [1]	12500	25000	1562.50	3125.00	50000	100000
r6idn.8xlarge [2]	25000		3125.0		100000	
r6idn.12xlarge [2]	37500		4687.5		150000	
r6idn.16xlarge [2]	50000		6250.0		200000	
r6idn.24xlarge [2]	75000		9375.0		300000	
r6idn.32xlarge [2]	100000		12500.0		400000	
r6idn.metal [2]	100000		12500.0		400000	
r6in.large [1]	1562	25000	195.31	3125.00	6250	100000
r6in.xlarge [1]	3125	25000	390.62	3125.00	12500	100000
r6in.2xlarge [1]	6250	25000	781.25	3125.00	25000	100000

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
r6in.4xlarge [1]	12500	25000	1562.50	3125.00	50000	100000
r6in.8xlarge [2]	25000		3125.0		100000	
r6in.12xlarge [2]	37500		4687.5		150000	
r6in.16xlarge [2]	50000		6250.0		200000	
r6in.24xlarge [2]	75000		9375.0		300000	
r6in.32xlarge [2]	100000		12500.0		400000	
r6in.metal [2]	100000		12500.0		400000	
r7a.medium [1]	325	10000	40.62	1250.00	2500	40000
r7a.large [1]	650	10000	81,25	1250.00	3600	40000
r7a.xlarge [1]	1250	10000	156,25	1250.00	6000	40000
r7a.2xlarge [1]	2500	10000	312.50	1250.00	12000	40000
r7a.4xlarge [1]	5000	10000	625.00	1250.00	20000	40000

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
r7a.8xlarge [2]	10000		1250.0		40000	
r7a.12xlarge [2]	15000		1875.0		60000	
r7a.16xlarge [2]	20000		2500.0		80000	
r7a.24xlarge [2]	30000		3750.0		120000	
r7a.32xlarge [2]	40000		5000.0		160000	
r7a.48xlarge [2]	40000		5000.0		240000	
r7a.metal-48xl [2]	40000		5000.0		240000	
r7g.medium [1]	315	10000	39.38	1250.00	2500	40000
r7g.large [1]	630	10000	78,75	1250.00	3600	40000
r7g.xlarge [1]	1250	10000	156,25	1250.00	6000	40000
r7g.2xlarge [1]	2500	10000	312.50	1250.00	12000	40000

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
r7g.4xlarge [1]	5000	10000	625.00	1250.00	20000	40000
r7g.8xlarge [2]	10000		1250.0		40000	
r7g.12xlarge [2]	15000		1875.0		60000	
r7g.16xlarge [2]	20000		2500.0		80000	
r7g.metal [2]	20000		2500.0		80000	
r7gd.medium [1]	315	10000	39.38	1250.00	2500	40000
r7gd.large [1]	630	10000	78,75	1250.00	3600	40000
r7gd.xlarge [1]	1250	10000	156,25	1250.00	6000	40000
r7gd.2xlarge [1]	2500	10000	312.50	1250.00	12000	40000
r7gd.4xlarge [1]	5000	10000	625.00	1250.00	20000	40000
r7gd.8xlarge [2]	10000		1250.0		40000	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
r7gd.12xlarge [2]	15000		1875.0		60000	
r7gd.16xlarge [2]	20000		2500.0		80000	
r7gd.metal [2]	20000		2500.0		80000	
r7i.large [1]	650	10000	81,25	1250.00	3600	40000
r7i.xlarge [1]	1250	10000	156,25	1250.00	6000	40000
r7i.2xlarge [1]	2500	10000	312.50	1250.00	12000	40000
r7i.4xlarge [1]	5000	10000	625.00	1250.00	20000	40000
r7i.8xlarge [2]	10000		1250.0		40000	
r7i.12xlarge [2]	15000		1875.0		60000	
r7i.16xlarge [2]	20000		2500.0		80000	
r7i.24xlarge [2]	30000		3750.0		120000	
r7i.48xlarge [2]	40000		5000.0		240000	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
r7i.metal-24xl [2]	30000		3750.0		120000	
r7i.metal-48xl [2]	40000		5000.0		240000	
r7iz.large [1]	792	10000	99.00	1250.00	3600	40000
r7iz.xlarge [1]	1584	10000	198.00	1250.00	6667	40000
r7iz.2xlarge [1]	3168	10000	396.00	1250.00	13333	40000
r7iz.4xlarge [1]	5000	10000	625.00	1250.00	20000	40000
r7iz.8xlarge [2]	10000		1250.0		40000	
r7iz.12xlarge [2]	19000		2375.0		76000	
r7iz.16xlarge [2]	20000		2500.0		80000	
r7iz.32xlarge [2]	40000		5000.0		160000	
r7iz.metal-16xl [2]	20000		2500.0		80000	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
r7iz.metal-32xl [2]	40000		5000.0		160000	
r8a.medium [1]	325	10000	40.62	1250.00	2500	40000
r8a.large [1]	650	10000	81,25	1250.00	3600	40000
r8a.xlarge [1]	1250	10000	156,25	1250.00	6000	40000
r8a.2xlarge [1]	2500	10000	312.50	1250.00	12000	40000
r8a.4xlarge [1]	5000	10000	625.00	1250.00	20000	40000
r8a.8xlarge [2]	10000		1250.0		40000	
r8a.12xlarge [2]	15000		1875.0		60000	
r8a.16xlarge [2]	20000		2500.0		80000	
r8a.24xlarge [2]	30000		3750.0		120000	
r8a.48xlarge [2]	60000		7500.0		240000	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
r8a.metal-24xl [2]	30000		3750.0		120000	
r8a.metal-48xl [2]	60000		7500.0		240000	
r8g.medium [1]	315	10000	39.38	1250.00	2500	40000
r8g.large [1]	630	10000	78,75	1250.00	3600	40000
r8g.xlarge [1]	1250	10000	156,25	1250.00	6000	40000
r8g.2xlarge [1]	2500	10000	312.50	1250.00	12000	40000
r8g.4xlarge [1]	5000	10000	625.00	1250.00	20000	40000
r8g.8xlarge [2]	10000		1250.0		40000	
r8g.12xlarge [2]	15000		1875.0		60000	
r8g.16xlarge [2]	20000		2500.0		80000	
r8g.24xlarge [2]	30000		3750.0		120000	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
r8g.48xlarge [2]	40000		5000.0		240000	
r8g.metal-24xl [2]	30000		3750.0		120000	
r8g.metal-48xl [2]	40000		5000.0		240000	
r8gb.medium [1]	1562	25000	195.31	3125.00	7500	120000
r8gb.large [1]	3125	25000	390.62	3125.00	15000	120000
r8gb.xlarge [1]	6250	25000	781.25	3125.00	30000	120000
r8gb.2xlarge [1]	12500	25000	1562.50	3125.00	60000	120000
r8gb.4xlarge [2]	25000		3125.0		120000	
r8gb.8xlarge [2]	50000		6250.0		240000	
r8gn.12xlarge [2]	75000		9375.0		360000	
r8gb.16xlarge [2]	100000		12500.0		480000	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
r8gb.24xlarge [2]	150000		18750.0		720000	
r8gn.48xlarge [2]	300000		37500.0		1440000	
r8gb.metal-24xl [2]	150000		18750.0		720000	
r8gb.metal-48xl [2]	300000		37500.0		1440000	
r8gd.medium [1]	315	10000	39.38	1250.00	2500	40000
r8gd.large [1]	630	10000	78,75	1250.00	3600	40000
r8gd.xlarge [1]	1250	10000	156,25	1250.00	6000	40000
r8gd.2xlarge [1]	2500	10000	312.50	1250.00	12000	40000
r8gd.4xlarge [1]	5000	10000	625.00	1250.00	20000	40000
r8gd.8xlarge [2]	10000		1250.0		40000	
r8gd.12xlarge [2]	15000		1875.0		60000	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
r8gd.16xlarge [2]	20000		2500.0		80000	
r8gd.24xlarge [2]	30000		3750.0		120000	
r8gd.48xlarge [2]	40000		5000.0		240000	
r8gd.metal-24xl [2]	30000		3750.0		120000	
r8gd.metal-48xl [2]	40000		5000.0		240000	
r8gn.medium [1]	760	10000	95.00	1250.00	2500	40000
r8gn.large [1]	1250	10000	156,25	1250.00	5000	40000
r8gn.xlarge [1]	2500	10000	312.50	1250.00	10000	40000
r8gn.2xlarge [1]	5000	10000	625.00	1250.00	20000	40000
r8gn.4xlarge [2]	10000		1250.0		40000	
r8gn.8xlarge [2]	20000		2500.0		80000	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
r8gn.12xlarge [2]	30000		3750.0		120000	
r8gn.16xlarge [2]	40000		5000.0		160000	
r8gn.24xlarge [2]	60000		7500.0		240000	
r8gn.48xlarge [2]	60000		7500.0		240000	
r8gn.metal-24xl [2]	60000		7500.0		240000	
r8gn.metal-48xl [2]	60000		7500.0		240000	
r8i.large [1]	650	10000	81,25	1250.00	3600	40000
r8i.xlarge [1]	1250	10000	156,25	1250.00	6000	40000
r8i.2xlarge [1]	2500	10000	312.50	1250.00	12000	40000
r8i.4xlarge [1]	5000	10000	625.00	1250.00	20000	40000
r8i.8xlarge [2]	10000		1250.0		40000	
r8i.12xlarge [2]	15000		1875.0		60000	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
r8i.16xlarge [2]	20000		2500.0		80000	
r8i.24xlarge [2]	30000		3750.0		120000	
r8i.32xlarge [2]	40000		5000.0		160000	
r8i.48xlarge [2]	60000		7500.0		240000	
r8i.96xlarge [2]	80000		10000.0		480000	
r8i.metal-48xl [2]	60000		7500.0		240000	
r8i.metal-96xl [2]	80000		10000.0		480000	
r8id.large [1]	650	10000	81,25	1250.00	3600	40000
r8id.xlarge [1]	1250	10000	156,25	1250.00	6000	40000
r8id.2xlarge [1]	2500	10000	312.50	1250.00	12000	40000
r8id.4xlarge [1]	5000	10000	625.00	1250.00	20000	40000

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
r8id.8xlarge [2]	10000		1250.0		40000	
r8id.12xlarge [2]	15000		1875.0		60000	
r8id.16xlarge [2]	20000		2500.0		80000	
r8id.24xlarge [2]	30000		3750.0		120000	
r8id.32xlarge [2]	40000		5000.0		160000	
r8id.48xlarge [2]	60000		7500.0		240000	
r8id.96xlarge [2]	80000		10000.0		480000	
r8id.metal-48xl [2]	60000		7500.0		240000	
r8id.metal-96xl [2]	80000		10000.0		480000	
r8i-flex.large [1]	315	10000	39.38	1250.00	2500	40000
r8i-flex.xlarge [1]	630	10000	78,75	1250.00	3600	40000

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
r8i-flex.2xlarge [1]	1250	10000	156,25	1250.00	6000	40000
r8i-flex.4xlarge [1]	2500	10000	312.50	1250.00	12000	40000
r8i-flex.8xlarge [1]	5000	10000	625.00	1250.00	20000	40000
r8i-flex.12xlarge [1]	7500	15000	937.50	1875.00	30000	60000
r8i-flex.16xlarge [1]	10000	20000	1250.00	2500.00	40000	80000
u-3tb1.56xlarge [2]	19000		2375.0		80000	
u-6tb1.56xlarge [2]	38000		4750.0		160000	
u-6tb1.112xlarge [2]	38000		4750.0		160000	
u-6tb1.metal [2]	38000		4750.0		160000	
u-9tb1.112xlarge [2]	38000		4750.0		160000	
u-9tb1.metal [2]	38000		4750.0		160000	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
u-12tb1.112xlarge [2]	38000		4750.0		160000	
u-12tb1.metal [2]	38000		4750.0		160000	
u-18tb1.112xlarge [2]	38000		4750.0		160000	
u-18tb1.metal [2]	38000		4750.0		160000	
u-24tb1.112xlarge [2]	38000		4750.0		160000	
u-24tb1.metal [2]	38000		4750.0		160000	
u7i-6tb.112xlarge [2]	100000		12500.0		560000	
u7i-8tb.112xlarge [2]	100000		12500.0		560000	
u7i-12tb.224xlarge [2]	100000		12500.0		560000	
u7in-16tb.224xlarge [2]	100000		12500.0		560000	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
u7in-24tb.224xlarge [2]	100000		12500.0		560000	
u7in-32tb.224xlarge [2]	100000		12500.0		560000	
u7inh-32tb.480xlarge [2]	160000		20000.0		840000	
x1.16xlarge [2]	7000		875.0		40000	
x1.32xlarge [2]	14000		1750.0		80000	
x1e.xlarge [2]	500		62.5		3700	
x1e.2xlarge [2]	1000		125.0		7400	
x1e.4xlarge [2]	1750		218,75		10000	
x1e.8xlarge [2]	3500		437,5		20000	
x1e.16xlarge [2]	7000		875.0		40000	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
x1e.32xlarge [2]	14000		1750.0		80000	
x2gd.medium [1]	315	4750	39.38	593,75	2500	20000
x2gd.large [1]	630	4750	78,75	593,75	3600	20000
x2gd.xlarge [1]	1188	4750	148.50	593,75	6000	20000
x2gd.2xlarge [1]	2375	4750	296.88	593,75	12000	20000
x2gd.4xlarge [2]	4750		593,75		20000	
x2gd.8xlarge [2]	9500		1187,5		40000	
x2gd.12xlarge [2]	14250		1781.25		60000	
x2gd.16xlarge [2]	19000		2375.0		80000	
x2gd.metal [2]	19000		2375.0		80000	
x2idn.16xlarge [2]	40000		5000.0		173333	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
x2idn.24xlarge [2]	60000		7500.0		260000	
x2idn.32xlarge [2]	80000		10000.0		260000	
x2idn.metal [2]	80000		10000.0		260000	
x2iedn.xlarge [1]	2500	20000	312.50	2500.00	8125	65000
x2iedn.2xlarge [1]	5000	20000	625.00	2500.00	16250	65000
x2iedn.4xlarge [1]	10000	20000	1250.00	2500.00	32500	65000
x2iedn.8xlarge [2]	20000		2500.0		65000	
x2iedn.16xlarge [2]	40000		5000.0		130000	
x2iedn.24xlarge [2]	60000		7500.0		195000	
x2iedn.32xlarge [2]	80000		10000.0		260000	
x2iedn.metal [2]	80000		10000.0		260000	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
x2iezn.2xlarge [2]	3170		396,25		13333	
x2iezn.4xlarge [2]	4750		593,75		20000	
x2iezn.6xlarge [2]	9500		1187,5		40000	
x2iezn.8xlarge [2]	12000		1500.0		55000	
x2iezn.12xlarge [2]	19000		2375.0		80000	
x2iezn.metal [2]	19000		2375.0		80000	
x8g.medium [1]	315	10000	39.38	1250.00	2500	40000
x8g.large [1]	630	10000	78,75	1250.00	3600	40000
x8g.xlarge [1]	1250	10000	156,25	1250.00	6000	40000
x8g.2xlarge [1]	2500	10000	312.50	1250.00	12000	40000
x8g.4xlarge [1]	5000	10000	625.00	1250.00	20000	40000

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
x8g.8xlarge [2]	10000		1250.0		40000	
x8g.12xlarge [2]	15000		1875.0		60000	
x8g.16xlarge [2]	20000		2500.0		80000	
x8g.24xlarge [2]	30000		3750.0		120000	
x8g.48xlarge [2]	40000		5000.0		240000	
x8g.metal-24xl [2]	30000		3750.0		120000	
x8g.metal-48xl [2]	40000		5000.0		240000	
x8aedz.large [1]	1250	15000	156,25	1875.00	5000	60000
x8aedz.xlarge [1]	2500	15000	312.50	1875.00	10000	60000
x8aedz.3xlarge [1]	7500	15000	937.50	1875.00	30000	60000
x8aedz.6xlarge [2]	15000		1875.0		60000	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
x8aedz.12xlarge [2]	30000		3750.0		120000	
x8aedz.24xlarge [2]	60000		7500.0		240000	
x8aedz.metal-12xl [2]	30000		3750.0		120000	
x8aedz.metal-24xl [2]	60000		7500.0		240000	
x8i.large [1]	650	10000	81,25	1250.00	3600	40000
x8i.xlarge [1]	1250	10000	156,25	1250.00	6000	40000
x8i.2xlarge [1]	2500	10000	312.50	1250.00	12000	40000
x8i.4xlarge [1]	5000	10000	625.00	1250.00	20000	40000
x8i.8xlarge [2]	10000		1250.0		40000	
x8i.12xlarge [2]	15000		1875.0		60000	
x8i.16xlarge [2]	20000		2500.0		80000	
x8i.24xlarge [2]	30000		3750.0		120000	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
x8i.32xlarge [2]	40000		5000.0		160000	
x8i.48xlarge [2]	60000		7500.0		240000	
x8i.64xlarge [2]	70000		8750.0		320000	
x8i.96xlarge [2]	80000		10000.0		480000	
x8i.metal-48xl [2]	60000		7500.0		240000	
x8i.metal-96xl [2]	80000		10000.0		480000	
z1d.large [1]	800	3170	100.00	396,25	3333	13333
z1d.xlarge [1]	1580	3170	197.50	396,25	6667	13333
z1d.2xlarge [2]	3170		396,25		13333	
z1d.3xlarge [2]	4750		593,75		20000	
z1d.6xlarge [2]	9500		1187,5		40000	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
z1d.12xlarge [2]	19000		2375.0		80000	
z1d.metal [2]	19000		2375.0		80000	

[1] Essas instâncias podem sustentar o desempenho máximo por 30 minutos pelo menos uma vez a cada 24 horas e depois revertem para o desempenho básico.

[2] Essas instâncias podem manter a performance declarada indefinidamente. Se a sua workload exigir performance máxima sustentado por mais de 30 minutos, selecione uma dessas instâncias.

Otimizada para armazenamento

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
d2.xlarge [2]	750		93,75		6000	
d2.2xlarge [2]	1000		125.0		8000	
d2.4xlarge [2]	2000		250.0		16000	
d2.8xlarge [2]	4000		500.0		32000	
d3.xlarge [1]	850	2800	106,25	350.00	5000	15000

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
d3.2xlarge [1]	1700	2800	212.50	350.00	10000	15000
d3.4xlarge [2]	2800		350.0		15000	
d3.8xlarge [2]	5000		625.0		30000	
d3en.xlarge [1]	850	2800	106,25	350.00	5000	15000
d3en.2xlarge [1]	1700	2800	212.50	350.00	10000	15000
d3en.4xlarge [2]	2800		350.0		15000	
d3en.6xlarge [2]	4000		500.0		25000	
d3en.8xlarge [2]	5000		625.0		30000	
d3en.12xlarge [2]	7000		875.0		40000	
h1.2xlarge [2]	1750		218,75		12000	
h1.4xlarge [2]	3500		437,5		20000	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
h1.8xlarge [2]	7000		875.0		40000	
h1.16xlarge [2]	14000		1750.0		80000	
i3.large [2]	425		53.125		3000	
i3.xlarge [2]	850		106,25		6000	
i3.2xlarge [2]	1700		212,5		12000	
i3.4xlarge [2]	3500		437,5		16000	
i3.8xlarge [2]	7000		875.0		32500	
i3.16xlarge [2]	14000		1750.0		65000	
i3.metal [2]	19000		2375.0		80000	
i3en.large [1]	576	4750	72.10	593,75	3000	20000
i3en.xlarge [1]	1153	4750	144.20	593,75	6000	20000
i3en.2xlarge [1]	2307	4750	288,39	593,75	12000	20000
i3en.3xlarge [1]	3800	4750	475.00	593,75	15000	20000
i3en.6xlarge [2]	4750		593,75		20000	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
i3en.12xlarge [2]	9500		1187,5		40000	
i3en.24xlarge [2]	19000		2375.0		80000	
i3en.metal [2]	19000		2375.0		80000	
i4g.large [1]	625	10000	78.12	1250.00	2500	40000
i4g.xlarge [1]	1250	10000	156,25	1250.00	5000	40000
i4g.2xlarge [1]	2500	10000	312.50	1250.00	10000	40000
i4g.4xlarge [1]	5000	10000	625.00	1250.00	20000	40000
i4g.8xlarge [2]	10000		1250.0		40000	
i4g.16xlarge [2]	20000		2500.0		80000	
i4i.large [1]	625	10000	78.12	1250.00	2500	40000
i4i.xlarge [1]	1250	10000	156,25	1250.00	5000	40000
i4i.2xlarge [1]	2500	10000	312.50	1250.00	10000	40000
i4i.4xlarge [1]	5000	10000	625.00	1250.00	20000	40000

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
i4i.8xlarge [2]	10000		1250.0		40000	
i4i.12xlarge [2]	15000		1875.0		60000	
i4i.16xlarge [2]	20000		2500.0		80000	
i4i.24xlarge [2]	30000		3750.0		120000	
i4i.32xlarge [2]	40000		5000.0		160000	
i4i.metal [2]	40000		5000.0		160000	
i7i.large [1]	625	10000	78.12	1250.00	2500	40000
i7i.xlarge [1]	1250	10000	156,25	1250.00	5000	40000
i7i.2xlarge [1]	2500	10000	312.50	1250.00	10000	40000
i7i.4xlarge [1]	5000	10000	625.00	1250.00	20000	40000
i7i.8xlarge [2]	10000		1250.0		40000	
i7i.12xlarge [2]	15000		1875.0		60000	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
i7i.16xlarge [2]	20000		2500.0		80000	
i7i.24xlarge [2]	30000		3750.0		120000	
i7i.48xlarge [2]	60000		7500.0		240000	
i7i.metal-24xl [2]	30000		3750.0		120000	
i7i.metal-48xl [2]	60000		7500.0		240000	
i7ie.large [1]	625	10000	78.12	1250.00	2500	40000
i7ie.xlarge [1]	1250	10000	156,25	1250.00	5000	40000
i7ie.2xlarge [1]	2500	10000	312.50	1250.00	10000	40000
i7ie.3xlarge [1]	3750	10000	468,75	1250.00	15000	40000
i7ie.6xlarge [1]	7500	10000	937.50	1250.00	30000	40000
i7ie.12xlarge [2]	15000		1875.0		60000	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
i7ie.18xlarge [2]	22500		2812.5		90000	
i7ie.24xlarge [2]	30000		3750.0		120000	
i7ie.48xlarge [2]	60000		7500.0		240000	
i7ie.metal-24xl [2]	30000		3750.0		120000	
i7ie.metal-48xl [2]	60000		7500.0		240000	
i8g.large [1]	625	10000	78.12	1250.00	2500	40000
i8g.xlarge [1]	1250	10000	156,25	1250.00	5000	40000
i8g.2xlarge [1]	2500	10000	312.50	1250.00	10000	40000
i8g.4xlarge [1]	5000	10000	625.00	1250.00	20000	40000
i8g.8xlarge [2]	10000		1250.0		40000	
i8g.12xlarge [2]	15000		1875.0		60000	
i8g.16xlarge [2]	20000		2500.0		80000	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
i8g.24xlarge [2]	30000		3750.0		120000	
i8g.48xlarge [2]	60000		7500.0		240000	
i8g.metal-24xl [2]	30000		3750.0		120000	
i8ge.large [1]	625	10000	78.12	1250.00	2500	40000
i8ge.xlarge [1]	1250	10000	156,25	1250.00	5000	40000
i8ge.2xlarge [1]	2500	10000	312.50	1250.00	10000	40000
i8ge.3xlarge [1]	3750	10000	468,75	1250.00	15000	40000
i8ge.6xlarge [1]	7500	10000	937.50	1250.00	30000	40000
i8ge.12xlarge [2]	15000		1875.0		60000	
i8ge.18xlarge [2]	22500		2812.5		90000	
i8ge.24xlarge [2]	30000		3750.0		120000	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
i8ge.48xlarge [2]	60000		7500.0		240000	
i8ge.metal-24xl [2]	30000		3750.0		120000	
i8ge.metal-48xl [2]	60000		7500.0		240000	
im4gn.large [1]	1250	10000	156,25	1250.00	5000	40000
im4gn.xlarge [1]	2500	10000	312.50	1250.00	10000	40000
im4gn.2xlarge [1]	5000	10000	625.00	1250.00	20000	40000
im4gn.4xlarge [2]	10000		1250.0		40000	
im4gn.8xlarge [2]	20000		2500.0		80000	
im4gn.16xlarge [2]	40000		5000.0		160000	
is4gen.medium [1]	625	10000	78.12	1250.00	2500	40000
is4gen.large [1]	1250	10000	156,25	1250.00	5000	40000

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
is4gen.xlarge [1]	2500	10000	312.50	1250.00	10000	40000
is4gen.2xlarge [1]	5000	10000	625.00	1250.00	20000	40000
is4gen.4xlarge [2]	10000		1250.0		40000	
is4gen.8xlarge [2]	20000		2500.0		80000	

[1] Essas instâncias podem sustentar o desempenho máximo por 30 minutos pelo menos uma vez a cada 24 horas e depois revertem para o desempenho básico.

[2] Essas instâncias podem manter a performance declarada indefinidamente. Se a sua workload exigir performance máxima sustentado por mais de 30 minutos, selecione uma dessas instâncias.

Computação acelerada

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
dl1.24xlarge [2]	19000		2375.0		80000	
dl2q.24xlarge [2]	19000		2375.0		80000	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
f1.2xlarge [2]	1700		212,5		12000	
f1.4xlarge [2]	3500		437,5		44000	
f1.16xlarge [2]	14000		1750.0		75000	
f2.6xlarge [2]	7500		937,5		30000	
f2.12xlarge [2]	15000		1875.0		60000	
f2.48xlarge [2]	60000		7500.0		240000	
g3.4xlarge [2]	3500		437,5		20000	
g3.8xlarge [2]	7000		875.0		40000	
g3.16xlarge [2]	14000		1750.0		80000	
g4ad.xlarge [1]	400	3170	50.00	396,25	1700	13333
g4ad.2xlarge [1]	800	3170	100.00	396,25	3400	13333
g4ad.4xlarge [1]	1580	3170	197.50	396,25	6700	13333

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
g4ad.8xlarge [2]	3170		396,25		13333	
g4ad.16xlarge [2]	6300		787.5		26667	
g4dn.xlarge [1]	950	3500	118,75	437.50	3000	20000
g4dn.2xlarge [1]	1150	3500	143,75	437.50	6000	20000
g4dn.4xlarge [2]	4750		593,75		20000	
g4dn.8xlarge [2]	9500		1187,5		40000	
g4dn.12xlarge [2]	9500		1187,5		40000	
g4dn.16xlarge [2]	9500		1187,5		40000	
g4dn.metal [2]	19000		2375.0		80000	
g5.xlarge [1]	700	3500	87.50	437.50	3000	15000
g5.2xlarge [1]	850	3500	106,25	437.50	3500	15000

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
g5.4xlarge [2]	4750		593,75		20000	
g5.8xlarge [2]	16000		2000.0		65000	
g5.12xlarge [2]	16000		2000.0		65000	
g5.16xlarge [2]	16000		2000.0		65000	
g5.24xlarge [2]	19000		2375.0		80000	
g5.48xlarge [2]	19000		2375.0		80000	
g5g.xlarge [1]	1188	4750	148.50	593,75	6000	20000
g5g.2xlarge [1]	2375	4750	296.88	593,75	12000	20000
g5g.4xlarge [2]	4750		593,75		20000	
g5g.8xlarge [2]	9500		1187,5		40000	
g5g.16xlarge [2]	19000		2375.0		80000	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
g5g.metal [2]	19000		2375.0		80000	
g6.xlarge [1]	1000	5000	125.00	625.00	4000	20000
g6.2xlarge [1]	2000	5000	250.00	625.00	8000	20000
g6.4xlarge [2]	8000		1000.0		32000	
g6.8xlarge [2]	16000		2000.0		64000	
g6.12xlarge [2]	20000		2500.0		80000	
g6.16xlarge [2]	20000		2500.0		80000	
g6.24xlarge [2]	30000		3750.0		120000	
g6.48xlarge [2]	60000		7500.0		240000	
g6e.xlarge [1]	1000	5000	125.00	625.00	4000	20000
g6e.2xlarge [1]	2000	5000	250.00	625.00	8000	20000
g6e.4xlarge [2]	8000		1000.0		32000	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
g6e.8xlarge [2]	16000		2000.0		64000	
g6e.12xlarge [2]	20000		2500.0		80000	
g6e.16xlarge [2]	20000		2500.0		80000	
g6e.24xlarge [2]	30000		3750.0		120000	
g6e.48xlarge [2]	60000		7500.0		240000	
g6f.large [1]	936	5000	117.00	625.00	3750	20000
g6f.xlarge [1]	1000	5000	125.00	625.00	4000	20000
g6e.2xlarge [1]	2000	5000	250.00	625.00	8000	20000
g6f.4xlarge [2]	6000		750.0		24000	
gr6.4xlarge [2]	8000		1000.0		32000	
gr6.8xlarge [2]	16000		2000.0		64000	
gr6f.4xlarge [2]	8000		1000.0		32000	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
g7e.2xlarge [1]	2000	5000	250.00	625.00	8000	20000
g7e.4xlarge [2]	8000		1000.0		32000	
g7e.8xlarge [2]	16000		2000.0		64000	
g7e.12xlarge [2]	25000		3125.0		100000	
g7e.24xlarge [2]	50000		6250.0		200000	
g7e.48xlarge [2]	100000		12500.0		400000	
inf1.xlarge [1]	1190	4750	148,75	593,75	4000	20000
inf1.2xlarge [1]	1190	4750	148,75	593,75	6000	20000
inf1.6xlarge [2]	4750		593,75		20000	
inf1.24xlarge [2]	19000		2375.0		80000	
inf2.xlarge [1]	1250	10000	156,25	1250.00	6000	40000

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
inf2.8xlarge [2]	10000		1250.0		40000	
inf2.24xlarge [2]	30000		3750.0		120000	
inf2.48xlarge [2]	60000		7500.0		240000	
p3.2xlarge [2]	1750		218,75		10000	
p3.8xlarge [2]	7000		875.0		40000	
p3.16xlarge [2]	14000		1750.0		80000	
p3dn.24xlarge [2]	19000		2375.0		80000	
p4d.24xlarge [2]	19000		2375.0		80000	
p4de.24xlarge [2]	19000		2375.0		80000	
p5.4xlarge [2]	10000		1250.0		32500	
p5.48xlarge [2]	80000		10000.0		260000	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
p5e.48xlarge [2]	80000		10000.0		260000	
p5en.48xlarge [2]	100000		12500.0		400000	
p6-b200.48xlarge [2]	100000		12500.0		400000	
p6-b300.48xlarge [2]	100000		12500.0		400000	
p6e-gb200.36xlarge [2]	60000		7500.0		240000	
trn1.2xlarge [1]	5000	20000	625.00	2500.00	16250	65000
trn1.32xlarge [2]	80000		10000.0		260000	
trn1n.32xlarge [2]	80000		10000.0		260000	
trn2.3xlarge [2]	5000		625.0		16250	
trn2.48xlarge [2]	80000		10000.0		260000	
trn2u.48xlarge [2]	80000		10000.0		260000	

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
vt1.3xlarge [1]	2375	4750	296.88	593,75	10000	20000
vt1.6xlarge [2]	4750		593,75		20000	
vt1.24xlarge [2]	19000		2375.0		80000	

[1] Essas instâncias podem sustentar o desempenho máximo por 30 minutos pelo menos uma vez a cada 24 horas e depois revertem para o desempenho básico.

[2] Essas instâncias podem manter a performance declarada indefinidamente. Se a sua workload exigir performance máxima sustentado por mais de 30 minutos, selecione uma dessas instâncias.

Computação de alta performance

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
hpc6a.48xlarge [1]	87	2085	10.88	260.62	500	11000
hpc6id.32xlarge [1]	87	2085	10.88	260.62	500	11000
hpc7a.12xlarge [1]	87	2085	10.88	260.62	500	11000

Tamanho da instância	Largura de banda da linha de base (Mbps)	Largura de banda máxima (Mbps)	Throughput de linha de base (MB/s, E/S de 128 KiB)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS da linha de base (E/S de 16 KiB)	IOPS máxima (16 KiB de E/S)
hpc7a.24xlarge [1]	87	2085	10.88	260.62	500	11000
hpc7a.48xlarge [1]	87	2085	10.88	260.62	500	11000
hpc7a.96xlarge [1]	87	2085	10.88	260.62	500	11000
hpc7g.4xlarge [1]	87	2085	10.88	260.62	500	11000
hpc7g.8xlarge [1]	87	2085	10.88	260.62	500	11000
hpc7g.16xlarge [1]	87	2085	10.88	260.62	500	11000
hpc8a.96xlarge [1]	87	2085	10.88	260.62	500	11000

[1] Essas instâncias podem sustentar o desempenho máximo por 30 minutos pelo menos uma vez a cada 24 horas e depois revertem para o desempenho básico.

[2] Essas instâncias podem manter a performance declarada indefinidamente. Se a sua workload exigir performance máxima sustentado por mais de 30 minutos, selecione uma dessas instâncias.

Suporte à otimização do EBS

Os tipos de instância a seguir oferecem suporte à otimização do EBS, mas essa otimização não está habilitada por padrão. Você precisa habilitar a otimização do EBS, por uma taxa horária adicional, durante ou após a execução para alcançar o nível de performance do EBS descrito.

Tamanho da instância	Largura de banda máxima (Mbps)	Throughput máxima (MB/s, 128 KiB E/S)	IOPS máxima (16 KiB de E/S)
c1.xlarge	1000	125.0	8000
c3.xlarge	500	62.5	4000
c3.2xlarge	1000	125.0	8000
c3.4xlarge	2000	250.0	16000
i2.xlarge	500	62.5	4000
i2.2xlarge	1000	125.0	8000
i2.4xlarge	2000	250.0	16000
m1.large	500	62.5	4000
m1.xlarge	1000	125.0	8000
m2.2xlarge	500	62.5	4000
m2.4xlarge	1000	125.0	8000
m3.xlarge	500	62.5	4000
m3.2xlarge	1000	125.0	8000
r3.xlarge	500	62.5	4000
r3.2xlarge	1000	125.0	8000
r3.4xlarge	2000	250.0	16000

> **Note**
>
> As instâncias `i2.8xlarge`, `c3.8xlarge` e `r3.8xlarge` não possuem largura de banda EBS dedicada e, portanto, não oferecem otimização de EBS. Nessas instâncias, o tráfego de rede e o trafego de Amazon EBS compartilham a mesma interface de rede de 10 gigabits.

Obter a máxima performance otimizada para o Amazon EBS

A performance do EBS de uma instância é limitada pelos limites de performance do tipo de instância ou pela performance agregada dos volumes a ela anexados, a que for menor. Para alcançar a performance máxima do EBS, uma instância deve ter volumes anexados que forneçam uma performance combinada igual ou superior à performance máxima da instância. Por exemplo, para conseguir `80,000` IOPS para `r6i.16xlarge`, a instância deve ter pelo menos 5 volumes gp2provisionados com `16,000` IOPS cada (5 volumes x `16,000` IOPS = `80,000` IOPS) ou pode ter 1 volume `gp3` provisionado com `80,000` IOPS. Recomendamos que você escolha um tipo de instância que forneça mais throughput dedicado do Amazon EBS do que o necessário para a aplicação. Caso contrário, a conexão entre o Amazon EBS e o Amazon EC2 pode se tornar um gargalo de performance.

> **Important**
>
> Ao usar ponderações de largura de banda configuráveis, os limites de largura de banda do EBS para sua instância podem mudar. Para instâncias com a configuração de ponderação `VPC-1`, que aumenta a largura de banda da rede, é possível experimentar um IOPS menor do que o esperado para volumes de EBS devido ao alcance do limite de largura de banda do EBS antes do limite de IOPS. Isso é particularmente perceptível com tamanhos maiores de E/S. Sempre teste sua workload específica para garantir que ela atenda aos requisitos de performance com a ponderação de largura de banda selecionada. Para obter mais informações, consulte Configuração de ponderação de largura de banda de instâncias do EC2.

É possível usar as métricas `EBSIOBalance%` e `EBSByteBalance%` para ajudá-lo a determinar se as instâncias estão dimensionadas corretamente. É possível visualizar essas métricas no console do CloudWatch e definir um alarme que é acionado com base nos limites especificados por você. Essas métricas são expressadas como uma porcentagem. As instâncias com uma

porcentagem de equilíbrio consistentemente baixa são candidatas à ampliação. As instâncias nas quais a porcentagem de equilíbrio jamais fica abaixo de 100% são candidatas à redução. Para obter mais informações, consulte Monitorar instâncias usando o CloudWatch.

As instâncias com mais memória foram projetadas para executar grandes bancos de dados na memória, incluindo implantações de produção do banco de dados na memória SAP HANA na nuvem. Para maximizar a performance do EBS, use instâncias com mais memória com um número par de volumes de `io1` ou `io2` com performance provisionada idêntica. Por exemplo, para workloads pesadas com relação às IOPS, use quatro volumes de `io1` ou `io2` com 40.000 IOPS provisionadas para obter o máximo de 160.000 IOPS de instância. Da mesma forma, para workloads pesadas com relação à throughput, use seis volumes de `io1` ou `io2` com 48.000 IOPS provisionadas para obter o máximo de 4.750 MB/s de throughput. Para obter recomendações adicionais, consulte Configuração de armazenamento para SAP HANA.

Considerações

- As instâncias G4dn, I3en, Inf1, M5a, M5ad, R5a, R5ad, T3, T3a e Z1d executadas após 26 de fevereiro de 2020 fornecem a performance máxima otimizada do EBS. Para obter a máxima performance de uma instância lançada antes de 26 de fevereiro de 2020, interrompa-a e inicie-a.
- As instâncias C5, C5d, C5n, M5, M5d, M5n, M5dn, R5, R5d, R5n, R5dn e P3dn executadas após 3 de dezembro de 2019 fornecem a performance máxima otimizada do EBS. Para obter a performance máxima de uma instância lançada antes de 3 de dezembro de 2019, interrompa-a e inicie-a.
- As instâncias `u-6tb1.metal`, `u-9tb1.metal` e `u-12tb1.metal` executadas após 12 de março de 2020 fornecem a performance máxima otimizada do EBS. As instâncias desses tipos lançadas antes de 12 de março de 2020 podem fornecer performance menor. Para obter a performance máxima de uma instância lançada antes de 12 de março de 2020, entre em contato com a equipe de conta para atualizar a instância sem custo adicional.

Encontrar os tipos de instância do EC2 otimizados para o EBS

É possível visualizar os tipos de instâncias compatíveis com a otimização do EBS em cada região.

Console

Para encontrar os tipos de instância otimizados para EBS por padrão

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

2. No painel de navegação, selecione Instance Types (Tipos de instância).
3. Adicione o filtro Suporte à otimização do EBS = padrão.
4. (Opcional) Clique no ícone Preferências e ative as colunas relevantes, como IOPS máximas do EBS e IOPS de referência do EBS.
5. (Opcional) Adicione filtros para ampliar o escopo de tipos específicos de instância de interesse.

AWS CLI

Para encontrar os tipos de instância otimizados para EBS por padrão

Use o comando describe-instance-types a seguir.

```
aws ec2 describe-instance-types \
--filters Name=ebs-info.ebs-optimized-support,Values=default  \
--query 'InstanceTypes[].{InstanceType:InstanceType,
 "MaxBandwidth(Mb/s)":EbsInfo.EbsOptimizedInfo.MaximumBandwidthInMbps,
 MaxIOPS:EbsInfo.EbsOptimizedInfo.MaximumIops, "MaxThroughput(MB/
s)":EbsInfo.EbsOptimizedInfo.MaximumThroughputInMBps}' \
--output=table
```

Para encontrar os tipos de instância com compatibilidade opcional com a otimização para EBS

Use o comando describe-instance-types a seguir.

```
aws ec2 describe-instance-types \
--filters Name=ebs-info.ebs-optimized-support,Values=supported \
--query 'InstanceTypes[].{InstanceType:InstanceType,
 "MaxBandwidth(Mb/s)":EbsInfo.EbsOptimizedInfo.MaximumBandwidthInMbps,
 MaxIOPS:EbsInfo.EbsOptimizedInfo.MaximumIops, "MaxThroughput(MB/
s)":EbsInfo.EbsOptimizedInfo.MaximumThroughputInMBps}' \
--output=table
```

Veja a seguir um exemplo de saída para o `eu-west-1`.

```
------------------------------------------------------------------------
|                        DescribeInstanceTypes                         |
+--------------+----------------------+----------+----------------------+
| InstanceType | MaxBandwidth(Mb/s)   | MaxIOPS  |  MaxThroughput(MB/s)  |
```

```
+--------------+----------------------+----------+-----------------------+
|  i2.2xlarge  |  1000                |  8000    |  125.0                |
|  m2.4xlarge  |  1000                |  8000    |  125.0                |
|  m2.2xlarge  |  500                 |  4000    |  62.5                 |
|  c1.xlarge   |  1000                |  8000    |  125.0                |
|  i2.xlarge   |  500                 |  4000    |  62.5                 |
|  m3.xlarge   |  500                 |  4000    |  62.5                 |
|  m1.xlarge   |  1000                |  8000    |  125.0                |
|  r3.4xlarge  |  2000                |  16000   |  250.0                |
|  r3.2xlarge  |  1000                |  8000    |  125.0                |
|  c3.xlarge   |  500                 |  4000    |  62.5                 |
|  m3.2xlarge  |  1000                |  8000    |  125.0                |
|  r3.xlarge   |  500                 |  4000    |  62.5                 |
|  i2.4xlarge  |  2000                |  16000   |  250.0                |
|  c3.4xlarge  |  2000                |  16000   |  250.0                |
|  c3.2xlarge  |  1000                |  8000    |  125.0                |
|  m1.large    |  500                 |  4000    |  62.5                 |
+--------------+----------------------+----------+-----------------------+
```

PowerShell

Para encontrar os tipos de instância otimizados para EBS por padrão

Use o cmdlet Get-EC2InstanceType.

```
Get-EC2InstanceType `
    -Filter @{Name="ebs-info.ebs-optimized-support"; Values="default"} | `
    Select InstanceType, `
        @{Name="MaxBandwidth(Mb/s)";
 Expression={($_.EbsInfo.EbsOptimizedInfo.MaximumBandwidthInMbps)}}, `
        @{Name="MaxIOPS"; Expression={($_.EbsInfo.EbsOptimizedInfo.MaximumIops)}}, `
        @{Name="MaxThroughput (MB/s)";
 Expression={($_.EbsInfo.EbsOptimizedInfo.MaximumThroughputInMBps)}}
```

Para encontrar os tipos de instância com compatibilidade opcional com a otimização para EBS

Use o cmdlet Get-EC2InstanceType.

```
Get-EC2InstanceType `
    -Filter @{Name="ebs-info.ebs-optimized-support"; Values="supported"} | `
    Select InstanceType, `
        @{Name="MaxBandwidth(Mb/s)";
 Expression={($_.EbsInfo.EbsOptimizedInfo.MaximumBandwidthInMbps)}}, `
```

```
        @{Name="MaxIOPS"; Expression={($_.EbsInfo.EbsOptimizedInfo.MaximumIops)}}, `
        @{Name="MaxThroughput (MB/s)";
 Expression={($_.EbsInfo.EbsOptimizedInfo.MaximumThroughputInMBps)}}
```

Veja a seguir um exemplo de saída para o `eu-west-1`.

```
InstanceType MaxBandwidth(Mb/s) MaxIOPS MaxThroughput (MB/s)
------------ ------------------ ------- --------------------
m2.4xlarge                1000    8000              125.000
i2.2xlarge                1000    8000              125.000
c1.xlarge                 1000    8000              125.000
m2.2xlarge                 500    4000               62.500
r3.2xlarge                1000    8000              125.000
m3.xlarge                  500    4000               62.500
r3.4xlarge                2000   16000              250.000
m1.xlarge                 1000    8000              125.000
i2.xlarge                  500    4000               62.500
c3.xlarge                  500    4000               62.500
c3.4xlarge                2000   16000              250.000
c3.2xlarge                1000    8000              125.000
i2.4xlarge                2000   16000              250.000
r3.xlarge                  500    4000               62.500
m3.2xlarge                1000    8000              125.000
m1.large                   500    4000               62.500
```

Habilitar a otimização do EBS para uma instância do Amazon EC2

Você só pode habilitar manualmente a otimização do EBS para os tipos de instâncias da geração anterior que sejam compatíveis opcionalmente com a otimização do EBS. Se você habilitar a otimização do EBS para esses tipos de instância, haverá uma tarifa adicional por hora

Pré-requisitos

- Verifique se o tipo de instância exige que você habilite a otimização do EBS. Para obter mais informações, consulte Suporte à otimização do EBS.
- Para habilitar a otimização do EBS após a inicialização, você deverá interromper a instância.

> **Warning**
>
> Quando você interrompe uma instância, os dados em todos os volumes de armazenamento de instâncias são apagados. Para manter dados longe dos volumes de armazenamento de instância, faça backup no armazenamento persistente.

Console

Para habilitar a otimização para o Amazon EBS durante a inicialização

No assistente de inicialização de instâncias, selecione o tipo de instância necessário. Expanda a seção Detalhes avançados e, depois, em Instância otimizada para o EBS, selecione Habilitar.

Se o tipo de instância selecionado não for compatível opcionalmente com o Amazon EBS, o menu suspenso estará desabilitado. Se o tipo de instância for otimizado para Amazon EBS por padrão, Habilitar já estará selecionado.

Para habilitar a otimização para o Amazon EBS depois da inicialização

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. Pare a instância. Escolha Actions (Ações), Instance state (Estado da instância), Stop instance (Interromper instância).
4. Com a instância ainda selecionada, escolha Actions (Ações), Instance settings (Configurações de instância), Change instance type (Alterar tipo de instância).
5. Selecione Otimizado para EBS e escolha Aplicar.

   Se o tipo de instância for otimizado para o Amazon EBS por padrão, ou se não for compatível com a otimização para o Amazon EBS, a caixa de seleção estará desabilitada.
6. Reinicie a instância. Escolha Instance state (Estado da instância) e Start instance (Iniciar instância).

AWS CLI

Para habilitar a otimização para o Amazon EBS durante a inicialização

Use o comando run-instances com a opção `--ebs-optimized`.

Para habilitar a otimização para o Amazon EBS depois da inicialização

1. Se a instância estiver em execução, interrompa-a usando comando stop-instances.

```
aws ec2 stop-instances --instance-ids i-1234567890abcdef0
```

2. Habilite a otimização do EBS usando o comando modify-instance-attribute com a opção `--ebs-optimized`.

```
aws ec2 modify-instance-attribute \
    --instance-id i-1234567890abcdef0 \
    --ebs-optimized
```

PowerShell

Para habilitar a otimização para o Amazon EBS durante a inicialização

Use o cmdlet New-EC2Instance com a opção `-EbsOptimized`.

Para habilitar a otimização para o Amazon EBS depois da inicialização

1. Se a instância estiver em execução, interrompa-a usando o cmdlet Stop-EC2Instance.

```
Stop-EC2Instance -InstanceId i-1234567890abcdef0
```

2. Habilite a otimização do EBS usando o cmdlet Edit-EC2InstanceAttribute com a opção `-EbsOptimized`.

```
Edit-EC2InstanceAttribute `
    -InstanceId i-1234567890abcdef0 `
    -EbsOptimized $true
```

Opções de CPU para instâncias do Amazon EC2

Muitas instâncias do Amazon EC2 oferecem suporte a multithreading simultâneo (SMT), o 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.

Na maioria dos casos, há um tipo de instância do Amazon EC2 que tem uma combinação de memória e número de vCPUs para atender às suas workloads. No entanto, para otimizar sua instância para workloads específicas ou necessidades comerciais, você pode especificar as seguintes opções de CPU durante e após o lançamento da instância:

- Número de núcleos de CPU: é possível personalizar o número de núcleos de CPU para a instância. É possível fazer isso para otimizar potencialmente os custos de licenciamento do software com uma instância que tenha quantidade suficiente de RAM para workloads com uso intensivo de memória, mas menos núcleos de CPU.
- Threads por núcleo: pode-se desabilitar o SMT especificando um único thread por núcleo de CPU. É possível fazer isso para determinadas workloads, como workloads de computação de alta performance (HPC).

Considerações

- Não é possível modificar o número de threads por núcleo para instâncias T2, C7a, M7a, R7a e Apple Silicon Mac, e instâncias baseadas no processador AWS Graviton.
- O número de instâncias que você pode executar é baseado nas vCPUs padrão dos tipos de instância usados. A forma como calculamos as vCPUs consumidas por uma instância não é afetada pela alteração das opções de CPU.

Preços

Não há cobrança adicional em razão da especificação das opções de CPU. Para instâncias do EC2 que sejam executadas a partir de AMIs do Windows e do SQL Server com licença incluída, é possível personalizar as opções de CPU para aproveitar o recurso de otimização de CPUs do EC2 e pagar taxas de licenciamento com base no número de vCPUs configuradas para sua instância. Para outras instâncias do EC2, a cobrança será igual à das instâncias inicializadas com as opções de CPU padrão.

Conteúdo

- Regras para especificar opções de CPU para uma instância do Amazon EC2
- Opções de CPU compatíveis com tipos de instância do Amazon EC2
- Especificar opções de CPU para uma instância do Amazon EC2

- Visualizar threads e núcleos de CPU para uma instância do Amazon EC2
- Otimização de CPUs para instâncias com licença incluída

Regras para especificar opções de CPU para uma instância do Amazon EC2

Para especificar as opções de CPU para a instância, lembre-se das seguintes regras:

- Não é possível especificar opções de CPU para instâncias bare metal.
- É possível especificar as opções de CPU durante ou depois da execução da instância.
- Para configurar opções de CPU, deve-se especificar o número de núcleos de CPU e threads por núcleo na solicitação. Por obter exemplos de solicitação, consulte Especificar opções de CPU para uma instância do Amazon EC2.
- 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, especifique um número válido de núcleos de CPU e threads por núcleo para o tipo de instância. Não deve-se exceder o número padrão de vCPUs para a instância. Para mais informações, consulte Opções de CPU compatíveis com tipos de instância do Amazon EC2.
- Para desabilitar o multithreading simultâneo (SMT), também conhecido como hyper-threading, especifique um thread por núcleo.
- No console, ao alterar o tipo de instância de uma instância existente, o Amazon EC2 aplica as configurações de opções de CPU da instância existente à nova instância, se possível. Se o novo tipo de instância não for compatível com essas configurações, as opções de CPU serão redefinidas como Usar as opções de CPU padrão. Essa opção usa o número padrão de vCPUs para o novo tipo de instância.

  Para atualizar as configurações da nova instância, selecione Especificar opções de CPU em Detalhes avançados na visualização Alterar tipo de instância.
- As opções de CPU especificadas ao se interromper, iniciar ou reinicializar uma instância.
- Se você usa instâncias reservadas, os descontos podem não ser aplicados ao configurar CPUs otimizadas para instâncias lançadas a partir de AMIs do Windows com licença incluída na mesma conta pagante. Recomendamos que você use o Savings Plans para reduzir os custos de licenciamento baseados em vCPU e oferecer economias comparáveis em seus custos de computação.

- Para economizar nos custos de licenciamento de instâncias lançadas a partir de AMIs incluídas na licença do Windows e do SQL Server, será necessário configurar no mínimo quatro vCPUs. Se você configurar menos de quatro vCPUs, o faturamento padrão será aplicado.
- Não há suporte à otimização de CPUs para instâncias com licença incluída nos tipos de instância T3.

Opções de CPU compatíveis com tipos de instância do Amazon EC2

As tabelas a seguir listam os tipos de instância que oferecem suporte à especificação de opções de CPU.

Conteúdo

- Instâncias de uso geral
- Instâncias otimizadas para computação
- Instâncias otimizadas para memória
- Instâncias otimizadas para armazenamento
- Instâncias computacionais aceleradas
- Instâncias de computação de alta performance

Instâncias de uso geral

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
m2.xlarge	2	2	1	1, 2	1
m2.2xlarge	4	4	1	1, 2, 3, 4	1
m2.4xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
m3.large	2	1	2	1	1, 2
m3.xlarge	4	2	2	1, 2	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
m3.2xlarge	8	4	2	1, 2, 3, 4	1, 2
m4.large	2	1	2	1	1, 2
m4.xlarge	4	2	2	1, 2	1, 2
m4.2xlarge	8	4	2	1, 2, 3, 4	1, 2
m4.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
m4.10xlarge	40	20	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20	1, 2
m4.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
m5.large	2	1	2	1	1, 2
m5.xlarge	4	2	2	2	1, 2
m5.2xlarge	8	4	2	2, 4	1, 2
m5.4xlarge	16	8	2	2, 4, 6, 8	1, 2
m5.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
m5.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
m5.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
m5.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
m5a.large	2	1	2	1	1, 2
m5a.xlarge	4	2	2	2	1, 2
m5a.2xlarge	8	4	2	2, 4	1, 2
m5a.4xlarge	16	8	2	2, 4, 6, 8	1, 2
m5a.8xlarge	32	16	2	4, 6, 8, 10, 12, 14, 16	1, 2
m5a.12xlarge	48	24	2	6, 12, 18, 24	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
m5a.16xlarge	64	32	2	8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
m5a.24xlarge	96	48	2	12, 18, 24, 36, 48	1, 2
m5ad.large	2	1	2	1	1, 2
m5ad.xlarge	4	2	2	2	1, 2
m5ad.2xlarge	8	4	2	2, 4	1, 2
m5ad.4xlarge	16	8	2	2, 4, 6, 8	1, 2
m5ad.8xlarge	32	16	2	4, 6, 8, 10, 12, 14, 16	1, 2
m5ad.12xlarge	48	24	2	6, 12, 18, 24	1, 2
m5ad.16xlarge	64	32	2	8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
m5ad.24xlarge	96	48	2	12, 18, 24, 36, 48	1, 2
m5d.large	2	1	2	1	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
m5d.xlarge	4	2	2	2	1, 2
m5d.2xlarge	8	4	2	2, 4	1, 2
m5d.4xlarge	16	8	2	2, 4, 6, 8	1, 2
m5d.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
m5d.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
m5d.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
m5d.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
m5dn.large	2	1	2	1	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
m5dn.xlarge	4	2	2	1, 2	1, 2
m5dn.2xlarge	8	4	2	2, 4	1, 2
m5dn.4xlarge	16	8	2	2, 4, 6, 8	1, 2
m5dn.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
m5dn.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
m5dn.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
m5dn.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
m5n.large	2	1	2	1	1, 2
m5n.xlarge	4	2	2	1, 2	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
m5n.2xlarge	8	4	2	2, 4	1, 2
m5n.4xlarge	16	8	2	2, 4, 6, 8	1, 2
m5n.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
m5n.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
m5n.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
m5n.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
m5zn.large	2	1	2	1	1, 2
m5zn.xlarge	4	2	2	1, 2	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
m5zn.2xlarge	8	4	2	2, 4	1, 2
m5zn.3xlarge	12	6	2	2, 4, 6	1, 2
m5zn.6xlarge	24	12	2	2, 4, 6, 8, 10, 12	1, 2
m5zn.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
m6a.large	2	1	2	1	1, 2
m6a.xlarge	4	2	2	1, 2	1, 2
m6a.2xlarge	8	4	2	1, 2, 3, 4	1, 2
m6a.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
m6a.8xlarge	32	16	2	4, 6, 8, 10, 12, 14, 16	1, 2
m6a.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 16, 24	1, 2
m6a.16xlarge	64	32	2	4, 6, 8, 10, 12, 14, 16, 32	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
m6a.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 32, 48	1, 2
m6a.32xlarge	128	64	2	8, 12, 16, 20, 24, 28, 32, 64	1, 2
m6a.48xlarge	192	96	2	8, 12, 16, 20, 24, 28, 32, 64, 96	1, 2
m6g.large	2	2	1	1, 2	1
m6g.xlarge	4	4	1	1, 2, 3, 4	1
m6g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
m6g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
m6g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
m6g.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
m6g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
m6gd.large	2	2	1	1, 2	1
m6gd.xlarge	4	4	1	1, 2, 3, 4	1
m6gd.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
m6gd.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
m6gd.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
m6gd.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
m6gd.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
m6i.large	2	1	2	1	1, 2
m6i.xlarge	4	2	2	1, 2	1, 2
m6i.2xlarge	8	4	2	2, 4	1, 2
m6i.4xlarge	16	8	2	2, 4, 6, 8	1, 2
m6i.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
m6i.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
m6i.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
m6i.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
m6i.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
m6id.large	2	1	2	1	1, 2
m6id.xlarge	4	2	2	1, 2	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
m6id.2xlarge	8	4	2	2, 4	1, 2
m6id.4xlarge	16	8	2	2, 4, 6, 8	1, 2
m6id.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
m6id.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
m6id.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
m6id.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
m6id.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
m6idn.large	2	1	2	1	1, 2
m6idn.xlarge	4	2	2	1, 2	1, 2
m6idn.2xlarge	8	4	2	1, 2, 3, 4	1, 2
m6idn.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
m6idn.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
m6idn.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
m6idn.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2
m6idn.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
m6idn.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
m6in.large	2	1	2	1	1, 2
m6in.xlarge	4	2	2	1, 2	1, 2
m6in.2xlarge	8	4	2	1, 2, 3, 4	1, 2
m6in.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
m6in.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
m6in.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
m6in.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2
m6in.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
m6in.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
m7a.large	2	2	1	1, 2	1
m7a.xlarge	4	4	1	1, 2, 3, 4	1
m7a.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
m7a.4xlarge	16	16	1	1, 2, 4, 6, 8, 10, 12, 14, 16	1
m7a.8xlarge	32	32	1	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32	1
m7a.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 12, 18, 24, 30, 36, 42, 48	1
m7a.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 16, 24, 32, 40, 48, 56, 64	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
m7a.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 24, 36, 48, 60, 72, 84, 96	1
m7a.32xlarge	128	128	1	4, 6, 8, 10, 12, 14, 16, 32, 48, 64, 80, 96, 112, 128	1
m7a.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 48, 72, 96, 120, 144, 168, 192	1
m7g.large	2	2	1	1, 2	1
m7g.xlarge	4	4	1	1, 2, 3, 4	1
m7g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
m7g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
m7g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
m7g.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
m7g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
m7gd.large	2	2	1	1, 2	1
m7gd.xlarge	4	4	1	1, 2, 3, 4	1
m7gd.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
m7gd.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
m7gd.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
m7gd.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
m7gd.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
m7i.large	2	1	2	1	1, 2
m7i.xlarge	4	2	2	1, 2	1, 2
m7i.2xlarge	8	4	2	1, 2, 3, 4	1, 2
m7i.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
m7i.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
m7i.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
m7i.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
m7i.24xlarge	96	48	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1, 2
m7i.48xlarge	192	96	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
m7i-flex.large	2	1	2	1	1, 2
m7i-flex.xlarge	4	2	2	1, 2	1, 2
m7i-flex.2xlarge	8	4	2	1, 2, 3, 4	1, 2
m7i-flex.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
m7i-flex.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
m7i-flex.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
m7i-flex.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
m8a.medium	1	1	1	1	1
m8a.large	2	2	1	1, 2	1
m8a.xlarge	4	4	1	1, 2, 3, 4	1
m8a.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
m8a.4xlarge	16	16	1	1, 2, 4, 6, 8, 10, 12, 14, 16	1
m8a.8xlarge	32	32	1	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32	1
m8a.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 12, 18, 24, 30, 36, 42, 48	1
m8a.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 16, 24, 32, 40, 48, 56, 64	1
m8a.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 24, 36, 48, 60, 72, 84, 96	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
m8a.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 48, 72, 96, 120, 144, 168, 192	1
m8azn.medium	1	1	1	1	1
m8azn.large	2	2	1	1, 2	1
m8azn.xlarge	4	4	1	1, 2, 3, 4	1
m8azn.3xlarge	12	12	1	1, 2, 4, 6, 8, 10, 12	1
m8azn.6xlarge	24	24	1	1, 2, 3, 4, 8, 12, 16, 20, 24	1
m8azn.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 16, 24, 32, 40, 48	1
m8azn.24xlarge	96	96	1	4, 6, 8, 10, 12, 14, 16, 32, 48, 64, 80, 96	1
m8g.large	2	2	1	1, 2	1
m8g.xlarge	4	4	1	1, 2, 3, 4	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
m8g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
m8g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
m8g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
m8g.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
m8g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
m8g.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
m8g.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96, 98, 100, 102, 104, 106, 108, 110, 112, 114, 116, 118, 120, 122, 124, 126, 128, 130, 132, 134, 136, 138, 140, 142, 144, 146, 148, 150, 152, 154, 156, 158, 160, 162, 164,	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
				166, 168, 170, 172, 174, 176, 178, 180, 182, 184, 186, 188, 190, 192	
m8gb.large	2	2	1	1, 2	1
m8gb.xlarge	4	4	1	1, 2, 3, 4	1
m8gb.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
m8gb.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
m8gb.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
m8gb.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
m8gb.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
m8gb.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
m8gb.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96, 98, 100, 102, 104, 106, 108, 110, 112, 114, 116, 118, 120, 122, 124, 126, 128, 130, 132, 134, 136, 138, 140, 142, 144, 146, 148, 150, 152, 154, 156, 158, 160, 162, 164,	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
				166, 168, 170, 172, 174, 176, 178, 180, 182, 184, 186, 188, 190, 192	
m8gd.large	2	2	1	1, 2	1
m8gd.xlarge	4	4	1	1, 2, 3, 4	1
m8gd.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
m8gd.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
m8gd.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
m8gd.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
m8gd.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
m8gd.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
m8gd.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96, 98, 100, 102, 104, 106, 108, 110, 112, 114, 116, 118, 120, 122, 124, 126, 128, 130, 132, 134, 136, 138, 140, 142, 144, 146, 148, 150, 152, 154, 156, 158, 160, 162, 164,	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
				166, 168, 170, 172, 174, 176, 178, 180, 182, 184, 186, 188, 190, 192	
m8gn.large	2	2	1	1, 2	1
m8gn.xlarge	4	4	1	1, 2, 3, 4	1
m8gn.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
m8gn.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
m8gn.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
m8gn.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
m8gn.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
m8gn.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
m8gn.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96, 98, 100, 102, 104, 106, 108, 110, 112, 114, 116, 118, 120, 122, 124, 126, 128, 130, 132, 134, 136, 138, 140, 142, 144, 146, 148, 150, 152, 154, 156, 158, 160, 162, 164,	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
				166, 168, 170, 172, 174, 176, 178, 180, 182, 184, 186, 188, 190, 192	
m8i.large	2	1	2	1	1, 2
m8i.xlarge	4	2	2	1, 2	1, 2
m8i.2xlarge	8	4	2	1, 2, 3, 4	1, 2
m8i.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
m8i.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
m8i.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
m8i.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2
m8i.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
m8i.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
m8i.48xlarge	192	96	2	6, 9, 12, 15, 18, 21, 24, 27, 30, 33, 36, 39, 42, 45, 48, 51, 54, 57, 60, 63, 66, 69, 72, 75, 78, 81, 84, 87, 90, 93, 96	1, 2
m8i.96xlarge	384	192	2	12, 18, 24, 30, 36, 42, 48, 54, 60, 66, 72, 78, 84, 90, 96, 102, 108, 114, 120, 126, 132, 138, 144, 150, 156, 162, 168, 174, 180, 186, 192	1, 2
m8id.large	2	1	2	1	1, 2
m8id.xlarge	4	2	2	1, 2	1, 2
m8id.2xlarge	8	4	2	1, 2, 3, 4	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
m8id.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
m8id.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
m8id.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
m8id.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2
m8id.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
m8id.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
m8id.48xlarge	192	96	2	6, 9, 12, 15, 18, 21, 24, 27, 30, 33, 36, 39, 42, 45, 48, 51, 54, 57, 60, 63, 66, 69, 72, 75, 78, 81, 84, 87, 90, 93, 96	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
m8id.96xlarge	384	192	2	12, 18, 24, 30, 36, 42, 48, 54, 60, 66, 72, 78, 84, 90, 96, 102, 108, 114, 120, 126, 132, 138, 144, 150, 156, 162, 168, 174, 180, 186, 192	1, 2
m8i-flex.large	2	1	2	1	1, 2
m8i-flex.xlarge	4	2	2	1, 2	1, 2
m8i-flex.2xlarge	8	4	2	1, 2, 3, 4	1, 2
m8i-flex.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
m8i-flex.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
m8i-flex.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
m8i-flex.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	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
t3a.nano	2	1	2	1	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
t3a.micro	2	1	2	1	1, 2
t3a.small	2	1	2	1	1, 2
t3a.medium	2	1	2	1	1, 2
t3a.large	2	1	2	1	1, 2
t3a.xlarge	4	2	2	2	1, 2
t3a.2xlarge	8	4	2	2, 4	1, 2
t4g.nano	2	2	1	1, 2	1
t4g.micro	2	2	1	1, 2	1
t4g.small	2	2	1	1, 2	1
t4g.medium	2	2	1	1, 2	1
t4g.large	2	2	1	1, 2	1
t4g.xlarge	4	4	1	1, 2, 3, 4	1
t4g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Instâncias otimizadas para computação

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
c3.large	2	1	2	1	1, 2
c3.xlarge	4	2	2	1, 2	1, 2
c3.2xlarge	8	4	2	1, 2, 3, 4	1, 2
c3.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
c3.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
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

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
c5.4xlarge	16	8	2	2, 4, 6, 8	1, 2
c5.9xlarge	36	18	2	2, 4, 6, 8, 10, 12, 14, 16, 18	1, 2
c5.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
c5.18xlarge	72	36	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36	1, 2
c5.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
c5a.large	2	1	2	1	1, 2
c5a.xlarge	4	2	2	1, 2	1, 2
c5a.2xlarge	8	4	2	1, 2, 3, 4	1, 2
c5a.4xlarge	16	8	2	1, 2, 3, 4, 8	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
c5a.8xlarge	32	16	2	1, 2, 3, 4, 8, 12, 16	1, 2
c5a.12xlarge	48	24	2	1, 2, 3, 4, 8, 12, 16, 20, 24	1, 2
c5a.16xlarge	64	32	2	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32	1, 2
c5a.24xlarge	96	48	2	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48	1, 2
c5ad.large	2	1	2	1	1, 2
c5ad.xlarge	4	2	2	1, 2	1, 2
c5ad.2xlarge	8	4	2	1, 2, 3, 4	1, 2
c5ad.4xlarge	16	8	2	1, 2, 3, 4, 8	1, 2
c5ad.8xlarge	32	16	2	1, 2, 3, 4, 8, 12, 16	1, 2
c5ad.12xlarge	48	24	2	1, 2, 3, 4, 8, 12, 16, 20, 24	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
c5ad.16xlarge	64	32	2	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32	1, 2
c5ad.24xlarge	96	48	2	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48	1, 2
c5d.large	2	1	2	1	1, 2
c5d.xlarge	4	2	2	2	1, 2
c5d.2xlarge	8	4	2	2, 4	1, 2
c5d.4xlarge	16	8	2	2, 4, 6, 8	1, 2
c5d.9xlarge	36	18	2	2, 4, 6, 8, 10, 12, 14, 16, 18	1, 2
c5d.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
c5d.18xlarge	72	36	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
c5d.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
c5n.large	2	1	2	1	1, 2
c5n.xlarge	4	2	2	2	1, 2
c5n.2xlarge	8	4	2	2, 4	1, 2
c5n.4xlarge	16	8	2	2, 4, 6, 8	1, 2
c5n.9xlarge	36	18	2	2, 4, 6, 8, 10, 12, 14, 16, 18	1, 2
c5n.18xlarge	72	36	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36	1, 2
c6a.large	2	1	2	1	1, 2
c6a.xlarge	4	2	2	1, 2	1, 2
c6a.2xlarge	8	4	2	1, 2, 3, 4	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
c6a.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
c6a.8xlarge	32	16	2	4, 6, 8, 10, 12, 14, 16	1, 2
c6a.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 16, 24	1, 2
c6a.16xlarge	64	32	2	4, 6, 8, 10, 12, 14, 16, 32	1, 2
c6a.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 32, 48	1, 2
c6a.32xlarge	128	64	2	8, 12, 16, 20, 24, 28, 32, 64	1, 2
c6a.48xlarge	192	96	2	8, 12, 16, 20, 24, 28, 32, 64, 96	1, 2
c6g.large	2	2	1	1, 2	1
c6g.xlarge	4	4	1	1, 2, 3, 4	1
c6g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
c6g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
c6g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
c6g.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
c6g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
c6gd.large	2	2	1	1, 2	1
c6gd.xlarge	4	4	1	1, 2, 3, 4	1
c6gd.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
c6gd.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
c6gd.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
c6gd.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
c6gd.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
c6gn.medium	1	1	1	1	1
c6gn.large	2	2	1	1, 2	1
c6gn.xlarge	4	4	1	1, 2, 3, 4	1
c6gn.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
c6gn.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
c6gn.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
c6gn.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
c6gn.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
c6i.large	2	1	2	1	1, 2
c6i.xlarge	4	2	2	1, 2	1, 2
c6i.2xlarge	8	4	2	2, 4	1, 2
c6i.4xlarge	16	8	2	2, 4, 6, 8	1, 2
c6i.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
c6i.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
c6i.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
c6i.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
c6i.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
c6id.large	2	1	2	1	1, 2
c6id.xlarge	4	2	2	1, 2	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
c6id.2xlarge	8	4	2	2, 4	1, 2
c6id.4xlarge	16	8	2	2, 4, 6, 8	1, 2
c6id.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
c6id.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
c6id.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
c6id.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
c6id.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
c6in.large	2	1	2	1	1, 2
c6in.xlarge	4	2	2	1, 2	1, 2
c6in.2xlarge	8	4	2	1, 2, 3, 4	1, 2
c6in.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
c6in.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
c6in.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
c6in.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2
c6in.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
c6in.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
c7a.large	2	2	1	1, 2	1
c7a.xlarge	4	4	1	1, 2, 3, 4	1
c7a.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
c7a.4xlarge	16	16	1	1, 2, 4, 6, 8, 10, 12, 14, 16	1
c7a.8xlarge	32	32	1	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32	1
c7a.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 12, 18, 24, 30, 36, 42, 48	1
c7a.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 16, 24, 32, 40, 48, 56, 64	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
c7a.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 24, 36, 48, 60, 72, 84, 96	1
c7a.32xlarge	128	128	1	4, 6, 8, 10, 12, 14, 16, 32, 48, 64, 80, 96, 112, 128	1
c7a.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 48, 72, 96, 120, 144, 168, 192	1
c7g.large	2	2	1	1, 2	1
c7g.xlarge	4	4	1	1, 2, 3, 4	1
c7g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
c7g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
c7g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
c7g.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
c7g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
c7gd.large	2	2	1	1, 2	1
c7gd.xlarge	4	4	1	1, 2, 3, 4	1
c7gd.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
c7gd.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
c7gd.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
c7gd.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
c7gd.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
c7gn.large	2	2	1	1, 2	1
c7gn.xlarge	4	4	1	1, 2, 3, 4	1
c7gn.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
c7gn.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
c7gn.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
c7gn.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
c7gn.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
c7i.large	2	1	2	1	1, 2
c7i.xlarge	4	2	2	1, 2	1, 2
c7i.2xlarge	8	4	2	1, 2, 3, 4	1, 2
c7i.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
c7i.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
c7i.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
c7i.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
c7i.24xlarge	96	48	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1, 2
c7i.48xlarge	192	96	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
c7i-flex.large	2	1	2	1	1, 2
c7i-flex.xlarge	4	2	2	1, 2	1, 2
c7i-flex.2xlarge	8	4	2	1, 2, 3, 4	1, 2
c7i-flex.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
c7i-flex.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
c7i-flex.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
c7i-flex.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
c8a.medium	1	1	1	1	1
c8a.large	2	2	1	1, 2	1
c8a.xlarge	4	4	1	1, 2, 3, 4	1
c8a.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
c8a.4xlarge	16	16	1	1, 2, 4, 6, 8, 10, 12, 14, 16	1
c8a.8xlarge	32	32	1	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32	1
c8a.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 12, 18, 24, 30, 36, 42, 48	1
c8a.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 16, 24, 32, 40, 48, 56, 64	1
c8a.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 24, 36, 48, 60, 72, 84, 96	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
c8a.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 48, 72, 96, 120, 144, 168, 192	1
c8g.large	2	2	1	1, 2	1
c8g.xlarge	4	4	1	1, 2, 3, 4	1
c8g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
c8g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
c8g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
c8g.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
c8g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
c8g.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
c8g.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96, 98, 100, 102, 104, 106, 108, 110, 112, 114, 116, 118, 120, 122, 124, 126, 128, 130, 132, 134, 136, 138, 140, 142, 144, 146, 148, 150, 152, 154, 156, 158, 160, 162, 164,	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
				166, 168, 170, 172, 174, 176, 178, 180, 182, 184, 186, 188, 190, 192	
c8gb.large	2	2	1	1, 2	1
c8gb.xlarge	4	4	1	1, 2, 3, 4	1
c8gb.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
c8gb.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
c8gb.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
c8gb.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
c8gb.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
c8gb.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
c8gb.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96, 98, 100, 102, 104, 106, 108, 110, 112, 114, 116, 118, 120, 122, 124, 126, 128, 130, 132, 134, 136, 138, 140, 142, 144, 146, 148, 150, 152, 154, 156, 158, 160, 162, 164,	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
				166, 168, 170, 172, 174, 176, 178, 180, 182, 184, 186, 188, 190, 192	
c8gd.large	2	2	1	1, 2	1
c8gd.xlarge	4	4	1	1, 2, 3, 4	1
c8gd.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
c8gd.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
c8gd.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
c8gd.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
c8gd.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
c8gd.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
c8gd.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96, 98, 100, 102, 104, 106, 108, 110, 112, 114, 116, 118, 120, 122, 124, 126, 128, 130, 132, 134, 136, 138, 140, 142, 144, 146, 148, 150, 152, 154, 156, 158, 160, 162, 164,	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
				166, 168, 170, 172, 174, 176, 178, 180, 182, 184, 186, 188, 190, 192	
c8gn.large	2	2	1	1, 2	1
c8gn.xlarge	4	4	1	1, 2, 3, 4	1
c8gn.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
c8gn.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
c8gn.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
c8gn.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
c8gn.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
c8gn.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
c8gn.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96, 98, 100, 102, 104, 106, 108, 110, 112, 114, 116, 118, 120, 122, 124, 126, 128, 130, 132, 134, 136, 138, 140, 142, 144, 146, 148, 150, 152, 154, 156, 158, 160, 162, 164,	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
				166, 168, 170, 172, 174, 176, 178, 180, 182, 184, 186, 188, 190, 192	
c8i.large	2	1	2	1	1, 2
c8i.xlarge	4	2	2	1, 2	1, 2
c8i.2xlarge	8	4	2	1, 2, 3, 4	1, 2
c8i.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
c8i.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
c8i.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
c8i.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2
c8i.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
c8i.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
c8i.48xlarge	192	96	2	6, 9, 12, 15, 18, 21, 24, 27, 30, 33, 36, 39, 42, 45, 48, 51, 54, 57, 60, 63, 66, 69, 72, 75, 78, 81, 84, 87, 90, 93, 96	1, 2
c8i.96xlarge	384	192	2	12, 18, 24, 30, 36, 42, 48, 54, 60, 66, 72, 78, 84, 90, 96, 102, 108, 114, 120, 126, 132, 138, 144, 150, 156, 162, 168, 174, 180, 186, 192	1, 2
c8id.large	2	1	2	1	1, 2
c8id.xlarge	4	2	2	1, 2	1, 2
c8id.2xlarge	8	4	2	1, 2, 3, 4	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
c8id.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
c8id.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
c8id.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
c8id.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2
c8id.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
c8id.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
c8id.48xlarge	192	96	2	6, 9, 12, 15, 18, 21, 24, 27, 30, 33, 36, 39, 42, 45, 48, 51, 54, 57, 60, 63, 66, 69, 72, 75, 78, 81, 84, 87, 90, 93, 96	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
c8id.96xlarge	384	192	2	12, 18, 24, 30, 36, 42, 48, 54, 60, 66, 72, 78, 84, 90, 96, 102, 108, 114, 120, 126, 132, 138, 144, 150, 156, 162, 168, 174, 180, 186, 192	1, 2
c8i-flex.large	2	1	2	1	1, 2
c8i-flex.xlarge	4	2	2	1, 2	1, 2
c8i-flex.2xlarge	8	4	2	1, 2, 3, 4	1, 2
c8i-flex.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
c8i-flex.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
c8i-flex.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
c8i-flex.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2

Instâncias otimizadas para memória

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
r3.large	2	1	2	1	1, 2
r3.xlarge	4	2	2	1, 2	1, 2
r3.2xlarge	8	4	2	1, 2, 3, 4	1, 2
r3.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
r3.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
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
r5.2xlarge	8	4	2	2, 4	1, 2
r5.4xlarge	16	8	2	2, 4, 6, 8	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
r5.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
r5.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
r5.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
r5.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
r5a.large	2	1	2	1	1, 2
r5a.xlarge	4	2	2	2	1, 2
r5a.2xlarge	8	4	2	2, 4	1, 2
r5a.4xlarge	16	8	2	2, 4, 6, 8	1, 2
r5a.8xlarge	32	16	2	4, 6, 8, 10, 12, 14, 16	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
r5a.12xlarge	48	24	2	6, 12, 18, 24	1, 2
r5a.16xlarge	64	32	2	8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
r5a.24xlarge	96	48	2	12, 18, 24, 36, 48	1, 2
r5ad.large	2	1	2	1	1, 2
r5ad.xlarge	4	2	2	2	1, 2
r5ad.2xlarge	8	4	2	2, 4	1, 2
r5ad.4xlarge	16	8	2	2, 4, 6, 8	1, 2
r5ad.8xlarge	32	16	2	4, 6, 8, 10, 12, 14, 16	1, 2
r5ad.12xlarge	48	24	2	6, 12, 18, 24	1, 2
r5ad.16xlarge	64	32	2	8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
r5ad.24xlarge	96	48	2	12, 18, 24, 36, 48	1, 2
r5b.large	2	1	2	1	1, 2
r5b.xlarge	4	2	2	1, 2	1, 2
r5b.2xlarge	8	4	2	2, 4	1, 2
r5b.4xlarge	16	8	2	2, 4, 6, 8	1, 2
r5b.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
r5b.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
r5b.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
r5b.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
r5d.large	2	1	2	1	1, 2
r5d.xlarge	4	2	2	2	1, 2
r5d.2xlarge	8	4	2	2, 4	1, 2
r5d.4xlarge	16	8	2	2, 4, 6, 8	1, 2
r5d.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
r5d.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
r5d.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
r5d.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
r5dn.large	2	1	2	1	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
r5dn.xlarge	4	2	2	1, 2	1, 2
r5dn.2xlarge	8	4	2	2, 4	1, 2
r5dn.4xlarge	16	8	2	2, 4, 6, 8	1, 2
r5dn.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
r5dn.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
r5dn.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
r5dn.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
r5n.large	2	1	2	1	1, 2
r5n.xlarge	4	2	2	1, 2	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
r5n.2xlarge	8	4	2	2, 4	1, 2
r5n.4xlarge	16	8	2	2, 4, 6, 8	1, 2
r5n.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
r5n.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
r5n.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
r5n.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
r6a.large	2	1	2	1	1, 2
r6a.xlarge	4	2	2	1, 2	1, 2
r6a.2xlarge	8	4	2	1, 2, 3, 4	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
r6a.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
r6a.8xlarge	32	16	2	4, 6, 8, 10, 12, 14, 16	1, 2
r6a.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 16, 24	1, 2
r6a.16xlarge	64	32	2	4, 6, 8, 10, 12, 14, 16, 32	1, 2
r6a.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 32, 48	1, 2
r6a.32xlarge	128	64	2	8, 12, 16, 20, 24, 28, 32, 64	1, 2
r6a.48xlarge	192	96	2	8, 12, 16, 20, 24, 28, 32, 64, 96	1, 2
r6g.large	2	2	1	1, 2	1
r6g.xlarge	4	4	1	1, 2, 3, 4	1
r6g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
r6g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
r6g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
r6g.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
r6g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
r6gd.large	2	2	1	1, 2	1
r6gd.xlarge	4	4	1	1, 2, 3, 4	1
r6gd.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
r6gd.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
r6gd.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
r6gd.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
r6gd.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
r6i.large	2	1	2	1	1, 2
r6i.xlarge	4	2	2	1, 2	1, 2
r6i.2xlarge	8	4	2	2, 4	1, 2
r6i.4xlarge	16	8	2	2, 4, 6, 8	1, 2
r6i.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
r6i.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
r6i.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
r6i.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
r6i.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
r6id.large	2	1	2	1	1, 2
r6id.xlarge	4	2	2	1, 2	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
r6id.2xlarge	8	4	2	2, 4	1, 2
r6id.4xlarge	16	8	2	2, 4, 6, 8	1, 2
r6id.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
r6id.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
r6id.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
r6id.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
r6id.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
r6idn.large	2	1	2	1	1, 2
r6idn.xlarge	4	2	2	1, 2	1, 2
r6idn.2xlarge	8	4	2	1, 2, 3, 4	1, 2
r6idn.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
r6idn.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
r6idn.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
r6idn.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2
r6idn.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
r6idn.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
r6in.large	2	1	2	1	1, 2
r6in.xlarge	4	2	2	1, 2	1, 2
r6in.2xlarge	8	4	2	1, 2, 3, 4	1, 2
r6in.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
r6in.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
r6in.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
r6in.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2
r6in.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
r6in.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
r7a.large	2	2	1	1, 2	1
r7a.xlarge	4	4	1	1, 2, 3, 4	1
r7a.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
r7a.4xlarge	16	16	1	1, 2, 4, 6, 8, 10, 12, 14, 16	1
r7a.8xlarge	32	32	1	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32	1
r7a.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 12, 18, 24, 30, 36, 42, 48	1
r7a.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 16, 24, 32, 40, 48, 56, 64	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
r7a.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 24, 36, 48, 60, 72, 84, 96	1
r7a.32xlarge	128	128	1	4, 6, 8, 10, 12, 14, 16, 32, 48, 64, 80, 96, 112, 128	1
r7a.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 48, 72, 96, 120, 144, 168, 192	1
r7g.large	2	2	1	1, 2	1
r7g.xlarge	4	4	1	1, 2, 3, 4	1
r7g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
r7g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
r7g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
r7g.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
r7g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
r7gd.large	2	2	1	1, 2	1
r7gd.xlarge	4	4	1	1, 2, 3, 4	1
r7gd.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
r7gd.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
r7gd.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
r7gd.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
r7gd.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
r7i.large	2	1	2	1	1, 2
r7i.xlarge	4	2	2	1, 2	1, 2
r7i.2xlarge	8	4	2	1, 2, 3, 4	1, 2
r7i.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
r7i.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
r7i.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
r7i.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
r7i.24xlarge	96	48	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1, 2
r7i.48xlarge	192	96	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
r7iz.large	2	1	2	1	1, 2
r7iz.xlarge	4	2	2	1, 2	1, 2
r7iz.2xlarge	8	4	2	1, 2, 3, 4	1, 2
r7iz.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
r7iz.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
r7iz.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
r7iz.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
r7iz.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
r8a.medium	1	1	1	1	1
r8a.large	2	2	1	1, 2	1
r8a.xlarge	4	4	1	1, 2, 3, 4	1
r8a.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
r8a.4xlarge	16	16	1	1, 2, 4, 6, 8, 10, 12, 14, 16	1
r8a.8xlarge	32	32	1	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32	1
r8a.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 12, 18, 24, 30, 36, 42, 48	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
r8a.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 16, 24, 32, 40, 48, 56, 64	1
r8a.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 24, 36, 48, 60, 72, 84, 96	1
r8a.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 48, 72, 96, 120, 144, 168, 192	1
r8g.large	2	2	1	1, 2	1
r8g.xlarge	4	4	1	1, 2, 3, 4	1
r8g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
r8g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
r8g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
r8g.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
r8g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
r8g.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
r8g.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96, 98, 100, 102, 104, 106, 108, 110, 112, 114, 116, 118, 120, 122, 124, 126, 128, 130, 132, 134, 136, 138, 140, 142, 144, 146, 148, 150, 152, 154, 156, 158, 160, 162, 164,	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
				166, 168, 170, 172, 174, 176, 178, 180, 182, 184, 186, 188, 190, 192	
r8gb.large	2	2	1	1, 2	1
r8gb.xlarge	4	4	1	1, 2, 3, 4	1
r8gb.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
r8gb.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
r8gb.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
r8gb.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
r8gb.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
r8gb.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
r8gb.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96, 98, 100, 102, 104, 106, 108, 110, 112, 114, 116, 118, 120, 122, 124, 126, 128, 130, 132, 134, 136, 138, 140, 142, 144, 146, 148, 150, 152, 154, 156, 158, 160, 162, 164,	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
				166, 168, 170, 172, 174, 176, 178, 180, 182, 184, 186, 188, 190, 192	
r8gd.large	2	2	1	1, 2	1
r8gd.xlarge	4	4	1	1, 2, 3, 4	1
r8gd.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
r8gd.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
r8gd.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
r8gd.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
r8gd.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
r8gd.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
r8gd.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96, 98, 100, 102, 104, 106, 108, 110, 112, 114, 116, 118, 120, 122, 124, 126, 128, 130, 132, 134, 136, 138, 140, 142, 144, 146, 148, 150, 152, 154, 156, 158, 160, 162, 164,	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
				166, 168, 170, 172, 174, 176, 178, 180, 182, 184, 186, 188, 190, 192	
r8gn.large	2	2	1	1, 2	1
r8gn.xlarge	4	4	1	1, 2, 3, 4	1
r8gn.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
r8gn.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
r8gn.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
r8gn.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
r8gn.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
r8gn.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
r8gn.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96, 98, 100, 102, 104, 106, 108, 110, 112, 114, 116, 118, 120, 122, 124, 126, 128, 130, 132, 134, 136, 138, 140, 142, 144, 146, 148, 150, 152, 154, 156, 158, 160, 162, 164,	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
				166, 168, 170, 172, 174, 176, 178, 180, 182, 184, 186, 188, 190, 192	
r8i.large	2	1	2	1	1, 2
r8i.xlarge	4	2	2	1, 2	1, 2
r8i.2xlarge	8	4	2	1, 2, 3, 4	1, 2
r8i.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
r8i.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
r8i.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
r8i.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2
r8i.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
r8i.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
r8i.48xlarge	192	96	2	6, 9, 12, 15, 18, 21, 24, 27, 30, 33, 36, 39, 42, 45, 48, 51, 54, 57, 60, 63, 66, 69, 72, 75, 78, 81, 84, 87, 90, 93, 96	1, 2
r8i.96xlarge	384	192	2	12, 18, 24, 30, 36, 42, 48, 54, 60, 66, 72, 78, 84, 90, 96, 102, 108, 114, 120, 126, 132, 138, 144, 150, 156, 162, 168, 174, 180, 186, 192	1, 2
r8id.large	2	1	2	1	1, 2
r8id.xlarge	4	2	2	1, 2	1, 2
r8id.2xlarge	8	4	2	1, 2, 3, 4	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
r8id.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
r8id.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
r8id.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
r8id.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2
r8id.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
r8id.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
r8id.48xlarge	192	96	2	6, 9, 12, 15, 18, 21, 24, 27, 30, 33, 36, 39, 42, 45, 48, 51, 54, 57, 60, 63, 66, 69, 72, 75, 78, 81, 84, 87, 90, 93, 96	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
r8id.96xlarge	384	192	2	12, 18, 24, 30, 36, 42, 48, 54, 60, 66, 72, 78, 84, 90, 96, 102, 108, 114, 120, 126, 132, 138, 144, 150, 156, 162, 168, 174, 180, 186, 192	1, 2
r8i-flex.large	2	1	2	1	1, 2
r8i-flex.xlarge	4	2	2	1, 2	1, 2
r8i-flex.2xlarge	8	4	2	1, 2, 3, 4	1, 2
r8i-flex.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
r8i-flex.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
r8i-flex.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
r8i-flex.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2
u-3tb1.56xlarge	224	112	2	8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48, 52, 56, 60, 64, 68, 72, 76, 80, 84, 88, 92, 96, 100, 104, 108, 112	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
u-6tb1.56xlarge	224	224	1	16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224	1
u-6tb1.112xlarge	448	224	2	16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
u-9tb1.112xlarge	448	224	2	16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224	1, 2
u-12tb1.112xlarge	448	224	2	16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
u-18tb1.112xlarge	448	224	2	16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224	1, 2
u-24tb1.112xlarge	448	224	2	16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
u7i-6tb.112xlarge	448	224	2	8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48, 52, 56, 60, 64, 68, 72, 76, 80, 84, 88, 92, 96, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 144, 148, 152, 156, 160, 164, 168, 172, 176, 180, 184, 188, 192, 196, 200, 204, 208, 212, 216, 220, 224	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
u7i-8tb.112xlarge	448	224	2	8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48, 52, 56, 60, 64, 68, 72, 76, 80, 84, 88, 92, 96, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 144, 148, 152, 156, 160, 164, 168, 172, 176, 180, 184, 188, 192, 196, 200, 204, 208, 212, 216, 220, 224	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
u7i-12tb.224xlarge	896	448	2	16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224, 232, 240, 248, 256, 264, 272, 280, 288, 296, 304, 312, 320, 328, 336, 344, 352, 360, 368, 376, 384, 392, 400, 408, 416, 424, 432, 440, 448	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
u7in-16tb.224xlarge	896	448	2	16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224, 232, 240, 248, 256, 264, 272, 280, 288, 296, 304, 312, 320, 328, 336, 344, 352, 360, 368, 376, 384, 392, 400, 408, 416, 424, 432, 440, 448	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
u7in-24tb.224xlarge	896	448	2	16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224, 232, 240, 248, 256, 264, 272, 280, 288, 296, 304, 312, 320, 328, 336, 344, 352, 360, 368, 376, 384, 392, 400, 408, 416, 424, 432, 440, 448	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
u7in-32tb.224xlarge	896	448	2	16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224, 232, 240, 248, 256, 264, 272, 280, 288, 296, 304, 312, 320, 328, 336, 344, 352, 360, 368, 376, 384, 392, 400, 408, 416, 424, 432, 440, 448	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
u7inh-32tb.480xlarge	1920	960	2	32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240, 256, 272, 288, 304, 320, 336, 352, 368, 384, 400, 416, 432, 448, 464, 480, 496, 512, 528, 544, 560, 576, 592, 608, 624, 640, 656, 672, 688, 704, 720, 736, 752, 768, 784, 800, 816, 832, 848, 864, 880, 896, 912, 928, 944, 960	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
x1.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
x1.32xlarge	128	64	2	4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48, 52, 56, 60, 64	1, 2
x1e.xlarge	4	2	2	1, 2	1, 2
x1e.2xlarge	8	4	2	1, 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

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
x1e.32xlarge	128	64	2	4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48, 52, 56, 60, 64	1, 2
x2gd.large	2	2	1	1, 2	1
x2gd.xlarge	4	4	1	1, 2, 3, 4	1
x2gd.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
x2gd.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
x2gd.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
x2gd.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
x2gd.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
x2idn.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
x2idn.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
x2idn.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
x2iedn.xlarge	4	2	2	1, 2	1, 2
x2iedn.2xlarge	8	4	2	2, 4	1, 2
x2iedn.4xlarge	16	8	2	2, 4, 6, 8	1, 2
x2iedn.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
x2iedn.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
x2iedn.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
x2iedn.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
x2iezn.2xlarge	8	4	2	2, 4	1, 2
x2iezn.4xlarge	16	8	2	2, 4, 6, 8	1, 2
x2iezn.6xlarge	24	12	2	2, 4, 6, 8, 10, 12	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
x2iezn.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
x2iezn.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
x8g.large	2	2	1	1, 2	1
x8g.xlarge	4	4	1	1, 2, 3, 4	1
x8g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
x8g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
x8g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
x8g.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
x8g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
x8g.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
x8g.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96, 98, 100, 102, 104, 106, 108, 110, 112, 114, 116, 118, 120, 122, 124, 126, 128, 130, 132, 134, 136, 138, 140, 142, 144, 146, 148, 150, 152, 154, 156, 158, 160, 162, 164,	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
				166, 168, 170, 172, 174, 176, 178, 180, 182, 184, 186, 188, 190, 192	
x8aedz.large	2	2	1	1, 2	1
x8aedz.xlarge	4	4	1	1, 2, 3, 4	1
x8aedz.3xlarge	12	12	1	1, 2, 4, 6, 8, 10, 12	1
x8aedz.6xlarge	24	24	1	1, 2, 3, 4, 8, 12, 16, 20, 24	1
x8aedz.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 16, 24, 32, 40, 48	1
x8aedz.24xlarge	96	96	1	4, 6, 8, 10, 12, 14, 16, 32, 48, 64, 80, 96	1
x8i.large	2	1	2	1	1, 2
x8i.xlarge	4	2	2	1, 2	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
x8i.2xlarge	8	4	2	1, 2, 3, 4	1, 2
x8i.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
x8i.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
x8i.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
x8i.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
x8i.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
x8i.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
x8i.48xlarge	192	96	2	6, 9, 12, 15, 18, 21, 24, 27, 30, 33, 36, 39, 42, 45, 48, 51, 54, 57, 60, 63, 66, 69, 72, 75, 78, 81, 84, 87, 90, 93, 96	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
x8i.64xlarge	256	128	2	8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48, 52, 56, 60, 64, 68, 72, 76, 80, 84, 88, 92, 96, 100, 104, 108, 112, 116, 120, 124, 128	1, 2
x8i.96xlarge	384	192	2	12, 18, 24, 30, 36, 42, 48, 54, 60, 66, 72, 78, 84, 90, 96, 102, 108, 114, 120, 126, 132, 138, 144, 150, 156, 162, 168, 174, 180, 186, 192	1, 2
z1d.large	2	1	2	1	1, 2
z1d.xlarge	4	2	2	1, 2	1, 2
z1d.2xlarge	8	4	2	2, 4	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
z1d.3xlarge	12	6	2	2, 4, 6	1, 2
z1d.6xlarge	24	12	2	2, 4, 6, 8, 10, 12	1, 2
z1d.12xlarge	48	24	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2

Instâncias otimizadas para armazenamento

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
d2.xlarge	4	2	2	1, 2	1, 2
d2.2xlarge	8	4	2	1, 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
d3.xlarge	4	2	2	1, 2	1, 2
d3.2xlarge	8	4	2	2, 4	1, 2
d3.4xlarge	16	8	2	2, 4, 6, 8	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
d3.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
d3en.xlarge	4	2	2	1, 2	1, 2
d3en.2xlarge	8	4	2	2, 4	1, 2
d3en.4xlarge	16	8	2	2, 4, 6, 8	1, 2
d3en.6xlarge	24	12	2	2, 4, 6, 8, 10, 12	1, 2
d3en.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
d3en.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
h1.2xlarge	8	4	2	1, 2, 3, 4	1, 2
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

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
h1.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
i2.xlarge	4	2	2	1, 2	1, 2
i2.2xlarge	8	4	2	1, 2, 3, 4	1, 2
i2.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
i2.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	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

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
i3.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
i3en.large	2	1	2	1	1, 2
i3en.xlarge	4	2	2	1, 2	1, 2
i3en.2xlarge	8	4	2	2, 4	1, 2
i3en.3xlarge	12	6	2	2, 4, 6	1, 2
i3en.6xlarge	24	12	2	2, 4, 6, 8, 10, 12	1, 2
i3en.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
i3en.24xlarge	96	48	2	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
i4g.large	2	2	1	1, 2	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
i4g.xlarge	4	4	1	1, 2, 3, 4	1
i4g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
i4g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
i4g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
i4g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
i4i.large	2	1	2	1	1, 2
i4i.xlarge	4	2	2	1, 2	1, 2
i4i.2xlarge	8	4	2	1, 2, 3, 4	1, 2
i4i.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
i4i.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
i4i.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
i4i.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
i4i.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
i4i.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
i7i.large	2	1	2	1	1, 2
i7i.xlarge	4	2	2	1, 2	1, 2
i7i.2xlarge	8	4	2	1, 2, 3, 4	1, 2
i7i.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
i7i.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
i7i.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
i7i.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2
i7i.24xlarge	96	48	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
i7i.48xlarge	192	96	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96	1, 2
i7ie.large	2	1	2	1	1, 2
i7ie.xlarge	4	2	2	1, 2	1, 2
i7ie.2xlarge	8	4	2	1, 2, 3, 4	1, 2
i7ie.3xlarge	12	6	2	1, 2, 3, 4, 5, 6	1, 2
i7ie.6xlarge	24	12	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
i7ie.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
i7ie.18xlarge	72	36	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
i7ie.24xlarge	96	48	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1, 2
i7ie.48xlarge	192	96	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96	1, 2
i8g.large	2	2	1	1, 2	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
i8g.xlarge	4	4	1	1, 2, 3, 4	1
i8g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
i8g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
i8g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
i8g.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
i8g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
i8g.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
i8g.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96, 98, 100, 102, 104, 106, 108, 110, 112, 114, 116, 118, 120, 122, 124, 126, 128, 130, 132, 134, 136, 138, 140, 142, 144, 146, 148, 150, 152, 154, 156, 158, 160, 162, 164,	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
				166, 168, 170, 172, 174, 176, 178, 180, 182, 184, 186, 188, 190, 192	
i8ge.large	2	2	1	1, 2	1
i8ge.xlarge	4	4	1	1, 2, 3, 4	1
i8ge.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
i8ge.3xlarge	12	12	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12	1
i8ge.6xlarge	24	24	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
i8ge.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
i8ge.18xlarge	72	72	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
i8ge.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
i8ge.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96, 98, 100, 102, 104, 106, 108, 110, 112, 114, 116, 118, 120, 122, 124, 126, 128, 130, 132, 134, 136, 138, 140, 142, 144, 146, 148, 150, 152, 154, 156, 158, 160, 162, 164,	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
				166, 168, 170, 172, 174, 176, 178, 180, 182, 184, 186, 188, 190, 192	
im4gn.large	2	2	1	1, 2	1
im4gn.xlarge	4	4	1	1, 2, 3, 4	1
im4gn.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
im4gn.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
im4gn.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
im4gn.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
is4gen.medium	1	1	1	1	1
is4gen.large	2	2	1	1, 2	1
is4gen.xlarge	4	4	1	1, 2, 3, 4	1
is4gen.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
is4gen.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
is4gen.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Instâncias computacionais aceleradas

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
dl1.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
dl2q.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28,	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
				30, 32, 34, 36, 38, 40, 42, 44, 46, 48	
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
f2.6xlarge	24	12	2	1, 2, 3, 6, 9, 12	1, 2
f2.12xlarge	48	24	2	1, 2, 3, 6, 9, 12, 15, 18, 21, 24	1, 2
f2.48xlarge	192	96	2	4, 6, 8, 10, 12, 24, 36, 48, 60, 72, 84, 96	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

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
g3.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
g4ad.xlarge	4	2	2	2	1, 2
g4ad.2xlarge	8	4	2	2, 4	1, 2
g4ad.4xlarge	16	8	2	2, 4, 8	1, 2
g4ad.8xlarge	32	16	2	2, 4, 8, 16	1, 2
g4ad.16xlarge	64	32	2	2, 4, 8, 16, 32	1, 2
g4dn.xlarge	4	2	2	2	1, 2
g4dn.2xlarge	8	4	2	2, 4	1, 2
g4dn.4xlarge	16	8	2	2, 4, 6, 8	1, 2
g4dn.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
g4dn.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
g4dn.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
g5g.xlarge	4	4	1	1, 2, 3, 4	1
g5g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
g5g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
g5g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
g5g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
g6.xlarge	4	2	2	1, 2	1, 2
g6.2xlarge	8	4	2	1, 2, 3, 4	1, 2
g6.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
g6.8xlarge	32	16	2	1, 2, 4, 6, 8, 10, 12, 14, 16	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
g6.12xlarge	48	24	2	1, 2, 3, 6, 9, 12, 15, 18, 21, 24	1, 2
g6.16xlarge	64	32	2	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32	1, 2
g6.24xlarge	96	48	2	1, 2, 3, 4, 5, 6, 12, 18, 24, 30, 36, 42, 48	1, 2
g6.48xlarge	192	96	2	4, 6, 8, 10, 12, 24, 36, 48, 60, 72, 84, 96	1, 2
g6e.xlarge	4	2	2	1, 2	1, 2
g6e.2xlarge	8	4	2	1, 2, 3, 4	1, 2
g6e.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
g6e.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
g6e.12xlarge	48	24	2	3, 6, 9, 12, 15, 18, 21, 24	1, 2
g6e.16xlarge	64	32	2	4, 8, 12, 16, 20, 24, 28, 32	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
g6e.24xlarge	96	48	2	6, 12, 18, 24, 30, 36, 42, 48	1, 2
g6e.48xlarge	192	96	2	12, 24, 36, 48, 60, 72, 84, 96	1, 2
g6f.large	2	1	2	1	1, 2
g6f.xlarge	4	2	2	1, 2	1, 2
g6f.2xlarge	8	4	2	1, 2, 3, 4	1, 2
g6f.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
gr6.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
gr6.8xlarge	32	16	2	1, 2, 4, 6, 8, 10, 12, 14, 16	1, 2
gr6f.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
g7e.2xlarge	8	4	2	1, 2, 3, 4	1, 2
g7e.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
g7e.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
g7e.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
g7e.24xlarge	96	48	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
g7e.48xlarge	192	96	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96	1, 2
inf1.xlarge	4	2	2	2	1, 2
inf1.2xlarge	8	4	2	2, 4	1, 2
inf1.6xlarge	24	12	2	2, 4, 6, 8, 10, 12	1, 2
inf1.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
inf2.xlarge	4	2	2	1, 2	1, 2
inf2.8xlarge	32	16	2	4, 6, 8, 10, 12, 14, 16	1, 2
inf2.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 32, 48	1, 2
inf2.48xlarge	192	96	2	4, 8, 12, 16, 20, 24, 28, 32, 64, 96	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

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
p3dn.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
p4d.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
p4de.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
p5.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
p5.48xlarge	192	96	2	12, 24, 36, 48, 60, 72, 84, 96	1, 2
p5e.48xlarge	192	96	2	12, 24, 36, 48, 60, 72, 84, 96	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
p5en.48xlarge	192	96	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96	1, 2
p6-b200.48xlarge	192	96	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
p6-b300.48xlarge	192	96	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
p6e-gb200.36xlarge	144	144	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96, 97, 98, 99, 100,	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
				101, 102, 103, 104, 105, 106, 107, 108, 109, 110, 111, 112, 113, 114, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124, 125, 126, 127, 128, 129, 130, 131, 132, 133, 134, 135, 136, 137, 138, 139, 140, 141, 142, 143, 144	
`trn1.2xlarge`	8	4	2	2, 4	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
trn1.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
trn1n.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
trn2.3xlarge	12	6	2	1, 2, 3, 4, 5, 6	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
trn2.48xlarge	192	96	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96	1, 2
trn2u.48xlarge	192	96	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
vt1.3xlarge	12	6	2	6	1, 2
vt1.6xlarge	24	12	2	6, 12	1, 2
vt1.24xlarge	96	48	2	6, 12, 48	1, 2

Instâncias de computação de alta performance

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
hpc6id.32xlarge	64	64	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1
hpc8a.96xlarge	192	192	1	24, 48, 72, 96, 120, 144, 168, 192	1

Especificar opções de CPU para uma instância do Amazon EC2

É possível especificar as opções de CPU durante ou após a instância ser iniciada.

Tarefas

- Desabilitar multithreading simultâneo
- Especificar um número personalizado de vCPUs na inicialização
- Especificar um número personalizado de vCPUs em um modelo de execução
- Alterar opções de CPU para a instância do EC2

Desabilitar multithreading simultâneo

Para desabilitar o multithreading simultâneo (SMT), também conhecido como hyper-threading, especifique um thread por núcleo.

Console

Desabilitar o SMT durante a inicialização da instância

1. Siga o procedimento Executar uma instância do EC2 usando o assistente de inicialização de instâncias no console e configure sua instância conforme necessário.
2. Expanda Detalhes avançados e marque a caixa de seleção Especificar opções de CPU.
3. Em Contagem de núcleos, defina o número de núcleos de CPU necessário. Neste exemplo, para especificar a contagem de núcleos de CPU para uma instância `r5.4xlarge`, selecione 8.
4. Para desabilitar o SMT, em Threads por núcleo, selecione 1.
5. No painel Resumo, analise a configuração da instância e selecione Iniciar instância. Para obter mais informações, consulte Executar uma instância do EC2 usando o assistente de inicialização de instâncias no console.

AWS CLI

Desabilitar o SMT durante a inicialização da instância

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 `r7i.4xlarge`, especifique um valor de 8.

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --instance-type r7i.4xlarge \
    --cpu-options "CoreCount=8,ThreadsPerCore=1" \
    --key-name my-key-pair
```

PowerShell

Desabilitar o SMT durante a inicialização da instância

Use o comando New-EC2Instance e especifique um valor 1 para `ThreadsPerCore` no parâmetro `-CpuOptions`. Em `CoreCount`, especifique o número de núcleos de CPU. Neste exemplo, para especificar a contagem de núcleos de CPU padrão para uma instância `r7i.4xlarge`, especifique um valor de 8.

```
New-EC2Instance `
    -ImageId 'ami-0abcdef1234567890' `
    -InstanceType 'r7i.4xlarge' `
    -CpuOptions @{CoreCount=8; ThreadsPerCore=1} `
    -KeyName 'my-key-pair'
```

> **Note**
>
> Para desabilitar o SMT para uma instância existente, siga o processo mostrado em Alterar opções de CPU para a instância do EC2 e altere o número de threads executados por núcleo para 1.

Especificar um número personalizado de vCPUs na inicialização

É possível personalizar o número de núcleos de CPU e de thread por núcleo da instância ao iniciar uma instância do console do EC2 ou da AWS CLI. Os exemplos nesta seção usam um tipo de instância `r5.4xlarge`, que tem as seguintes configurações padrão:

- Núcleos de CPU: 8
- Threads por núcleo: 2

Por padrão, as instâncias são iniciadas com o número máximo de vCPUs disponíveis para o tipo de instância. Para esse tipo de instância, são 16 vCPUs no total (8 núcleos executando 2 threads cada). Para obter mais informações sobre este tipo de instância, consulte Instâncias otimizadas para memória.

O exemplo apresentado a seguir inicia uma instância `r5.4xlarge` com quatro vCPUs.

Console

Para especificar um número personalizado de vCPUs durante a execução da instância

1. Siga o procedimento Executar uma instância do EC2 usando o assistente de inicialização de instâncias no console e configure sua instância conforme necessário.
2. Expanda Detalhes avançados e marque a caixa de seleção Especificar opções de CPU.
3. Para obter quatro vCPUs, especifique dois núcleos de CPU e dois threads por núcleo, da seguinte forma:
   - Em Contagem de núcleos, selecione 2.
   - For Threads por núcleo, selecione 2.
4. No painel Resumo, analise a configuração da instância e selecione Iniciar instância. Para mais informações, consulte Executar uma instância do EC2 usando o assistente de inicialização de instâncias no console.

AWS CLI

Para especificar um número personalizado de vCPUs durante a execução da instância

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`. É possível especificar dois núcleos de CPU e dois threads por núcleo para obter quatro vCPUs.

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --instance-type r7i.4xlarge \
    --cpu-options "CoreCount=2,ThreadsPerCore=2" \
    --key-name my-key-pair
```

Como alternativa, especifique quatro núcleos de CPU e um thread por núcleo (desabilitar o SMT) para obter quatro vCPUs:

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --instance-type r7i.4xlarge \
    --cpu-options "CoreCount=4,ThreadsPerCore=1" \
    --key-name my-key-pair
```

PowerShell

Para especificar um número personalizado de vCPUs durante a execução da instância

Use o comando New-EC2Instance e especifique o número de núcleos de CPU e o número de threads no parâmetro `-CpuOptions`. É possível especificar dois núcleos de CPU e dois threads por núcleo para obter quatro vCPUs.

```
New-EC2Instance `
    -ImageId 'ami-0abcdef1234567890' `
    -InstanceType 'r7i.4xlarge' `
    -CpuOptions @{CoreCount=2; ThreadsPerCore=2} `
    -KeyName 'my-key-pair'
```

Como alternativa, especifique quatro núcleos de CPU e um thread por núcleo (desabilitar o SMT) para obter quatro vCPUs:

```
New-EC2Instance `
    -ImageId 'ami-0abcdef1234567890' `
    -InstanceType 'r7i.4xlarge' `
    -CpuOptions @{CoreCount=4; ThreadsPerCore=1} `
    -KeyName 'my-key-pair'
```

Especificar um número personalizado de vCPUs em um modelo de execução

É possível personalizar o número de núcleos de CPU e de threads por núcleo para a instância em um modelo de execução. Os exemplos nesta seção usam um tipo de instância `r5.4xlarge`, que tem as seguintes configurações padrão:

- Núcleos de CPU: 8
- Threads por núcleo: 2

Por padrão, as instâncias são iniciadas com o número máximo de vCPUs disponíveis para o tipo de instância. Para esse tipo de instância, são 16 vCPUs no total (8 núcleos executando 2 threads cada). Para obter mais informações sobre este tipo de instância, consulte Instâncias otimizadas para memória.

O exemplo apresentado a seguir cria um modelo de execução que especifica a configuração para uma instância `r5.4xlarge` com quatro vCPUs.

Console

Para especificar um número personalizado de vCPUs em um modelo de execução

1. Siga o procedimento Criar um modelo de execução especificando parâmetros e configure seu modelo de execução conforme necessário.
2. Expanda Detalhes avançados e marque a caixa de seleção Especificar opções de CPU.
3. Para obter quatro vCPUs, especifique dois núcleos de CPU e dois threads por núcleo, da seguinte forma:
   - Em Contagem de núcleos, selecione 2.
   - For Threads por núcleo, selecione 2.
4. No painel Resumo, analise a configuração da sua instância e selecione Criar modelo de execução. Para mais informações, consulte Armazenar os parâmetros de execução de instâncias nos modelos de execução do Amazon EC2.

AWS CLI

Para especificar um número personalizado de vCPUs em um modelo de execução

Use o comando create-launch-template da AWS CLI e especifique o número de núcleos de CPU e o número de threads no parâmetro `CpuOptions`. É possível especificar dois núcleos de CPU e dois threads por núcleo para obter quatro vCPUs.

```
aws ec2 create-launch-template \
    --launch-template-name TemplateForCPUOptions \
    --version-description CPUOptionsVersion1 \
    --launch-template-data file://template-data.json
```

Veja a seguir um exemplo de arquivo JSON que contém os dados do modelo de execução, que incluem as opções de CPU, para a configuração da instância para este exemplo.

```
{
    "NetworkInterfaces": [{
        "AssociatePublicIpAddress": true,
        "DeviceIndex": 0,
        "Ipv6AddressCount": 1,
        "SubnetId": "subnet-0abcdef1234567890"
    }],
    "ImageId": "ami-0abcdef1234567890",
    "InstanceType": "r5.4xlarge",
    "TagSpecifications": [{
        "ResourceType": "instance",
        "Tags": [{
            "Key":"Name",
            "Value":"webserver"
        }]
    }],
    "CpuOptions": {
        "CoreCount":2,
        "ThreadsPerCore":2
    }
}
```

Outra alternativa é especificar quatro núcleos de CPU e um thread por núcleo (desabilite o SMT) para obter quatro vCPUs:

```
{
    "NetworkInterfaces": [{
        "AssociatePublicIpAddress": true,
        "DeviceIndex": 0,
        "Ipv6AddressCount": 1,
        "SubnetId": "subnet-0abcdef1234567890"
    }],
    "ImageId": "ami-0abcdef1234567890",
    "InstanceType": "r5.4xlarge",
    "TagSpecifications": [{
        "ResourceType": "instance",
        "Tags": [{
            "Key":"Name",
            "Value":"webserver"
        }]
    }],
    "CpuOptions": {
        "CoreCount":4,
```

```
        "ThreadsPerCore":1
    }
}
```

PowerShell

Para especificar um número personalizado de vCPUs em um modelo de execução

Use o New-EC2LaunchTemplate.

```
New-EC2LaunchTemplate `
    -LaunchTemplateName 'TemplateForCPUOptions' `
    -VersionDescription 'CPUOptionsVersion1' `
    -LaunchTemplateData (Get-Content -Path 'template-data.json' | ConvertFrom-Json)
```

Alterar opções de CPU para a instância do EC2

À medida que suas necessidades mudam com o tempo, talvez seja necessário alterar a configuração das opções de CPU para uma instância existente. Cada thread executado na instância é conhecido como CPU virtual (vCPU). É possível alterar o número total de vCPUs que são executadas em uma instância existente no console, na AWS CLI, na API ou nos SDKs do Amazon EC2. O estado da instância deve ser `Stopped` antes que se possa fazer essa alteração.

Para visualizar as etapas do console ou da linha de comando, selecione a guia que corresponde ao ambiente. Para obter informações sobre solicitações e respostas de API, consulte ModifyInstanceCpuOptions na Referência de API do Amazon EC2.

Console

Siga este procedimento para alterar o número de vCPUs ativas para sua instância usando o Console de gerenciamento da AWS.

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação à esquerda, selecione Instâncias. Esse procedimento abre a lista de instâncias definidas para a Região da AWS atual.
3. Na lista de Instâncias, selecione a instância. Outra alternativa é selecionar o link da instância para abrir a página de detalhes da instância.
4. Caso a instância esteja em execução, é necessário interrompê-la antes de continuar. No menu Estado da instância, selecione Interromper instância.

5. Para alterar a configuração de vCPU, selecione Alterar opções de CPU em Configurações de instância no menu Ações. Esse procedimento abre a página Alterar opções de CPU.
6. Selecione uma das seguintes opções de CPU para alterar a configuração da instância.

   Usar as opções de CPU padrão

   Essa opção redefine sua instância para o número padrão de vCPUs para o tipo de instância. O padrão é executar todos os threads para todos os núcleos da CPU.

   Especificar opções de CPU

   Essa opção permite a configuração do número de vCPUs em execução na sua instância.
7. Se você escolher Especificar opções de CPU, os campos vCPUs ativas ficarão visíveis.

   - Utilize o primeiro seletor para configurar o número de threads para cada núcleo de CPU. Para desabilitar o multithreading simultâneo, selecione 1.
   - Utilize o segundo seletor para configurar o número de CPUs que serão executadas na sua instância.

   Os campos a seguir serão atualizados dinamicamente à medida que você fizer alterações nos seletores de opções da CPU:

   - vCPUs ativas: o número total de núcleos de CPU multiplicado pelos threads por núcleo, com base nas seleções realizadas. Por exemplo, caso tenha selecionado 2 threads e 4 núcleos, isso equivaleria a 8 vCPUs.
   - Total de vCPUs: o número máximo de vCPUs para o tipo de instância. Por exemplo, para um tipo de instância `m6i.4xlarge`, são 16 vCPUs (8 núcleos executando 2 threads cada).
8. Para aplicar suas atualizações, selecione Alterar.

AWS CLI

Siga este procedimento para alterar o número de vCPUs ativas para sua instância usando o AWS CLI.

Use o comando modify-instance-cpu-options e especifique o número de núcleos de CPU que são executados no parâmetro `--core-count` e o número de threads executados por núcleo no parâmetro `--threads-per-core`.

Os exemplos a seguir mostram duas configurações possíveis em um tipo de instância `m6i.4xlarge` para executar 8 vCPUs na instância especificada. O padrão para esse tipo de instância é 16 vCPUs (8 núcleos executando 2 threads cada).

Exemplo 1: execute 4 núcleos de CPU com 2 threads por núcleo, totalizando 8 vCPUs.

```
aws ec2 modify-instance-cpu-options \
    --instance-id i-1234567890abcdef0 \

    --core-count=4 \
    --threads-per-core=2
```

Exemplo 2: desabilite o multithreading simultâneo alterando o número de threads executados por núcleo para 1. A configuração resultante também executa um total de 8 vCPUs (8 núcleos de CPU com 1 thread por núcleo).

```
aws ec2 modify-instance-cpu-options \
    --instance-id 1234567890abcdef0 \
    --core-count=8 \
    --threads-per-core=1
```

PowerShell

Para alterar o número de vCPUs ativas para uma instância

Use o cmdlet Edit-EC2InstanceCpuOption e especifique o número de núcleos de CPU em execução no parâmetro `-CoreCount` e o número de threads executados por núcleo no parâmetro `ThreadsPerCore`.

Exemplo 1: execute 4 núcleos de CPU com 2 threads por núcleo, totalizando 8 vCPUs.

```
Edit-EC2InstanceCpuOption `
    -InstanceId 'i-1234567890abcdef0' `
    -CoreCount 4 `
    -ThreadsPerCore 2
```

Exemplo 2: desabilite o multithreading simultâneo alterando o número de threads executados por núcleo para 1. A configuração resultante também executa um total de 8 vCPUs (8 núcleos de CPU com 1 thread por núcleo).

```
Edit-EC2InstanceCpuOption `
```

```
    -InstanceId 'i-1234567890abcdef0' `
    -CoreCount 8 `
    -ThreadsPerCore 1
```

Visualizar threads e núcleos de CPU para uma instância do Amazon EC2

É possível visualizar as opções de CPU de uma instância existente descrevendo a instância.

Console

Para visualizar as opções de CPU para uma instância

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação à esquerda, selecione Instâncias e selecione a instância.
3. Na guia Detalhes, em Host e grupo de posicionamento, localize Número de vCPUs.

AWS CLI

Para visualizar as opções de CPU para uma instância

Use o comando describe-instances.

```
aws ec2 describe-instances \
    --instance-ids i-1234567890abcdef0 \
    --query Reservations[].Instances[].CpuOptions
```

O seguinte é um exemplo de saída. O campo `CoreCount` indica o número de núcleos para a instância. O campo `ThreadsPerCore` indica o número de threads por núcleo.

```
[
    {
        "CoreCount": 24,
        "ThreadsPerCore": 2
    },
]
```

PowerShell

Para visualizar as opções de CPU para uma instância

Use o cmdlet Get-EC2Instance.

```
(Get-EC2Instance `
    -InstanceId 'i-1234567890abcdef0').Instances.CpuOptions
```

O seguinte é um exemplo de saída.

```
AmdSevSnp CoreCount ThreadsPerCore
--------- --------- --------------
          24        2
```

Outra alternativa para visualizar as informações da CPU é conectar-se à sua instância e usar uma das seguintes ferramentas do sistema:

- O Windows `Task Manager` na instância do Windows
- O comando lscpu na instância do Linux

É possível usar o AWS Config para fazer registros, auditorias e avaliações de alterações de configuração para instâncias, incluindo instâncias encerradas. Para obter mais informações, consulte Conceitos básicos do AWS Config no Guia do desenvolvedor do AWS Config.

Otimização de CPUs para instâncias com licença incluída

Workloads como o Microsoft SQL Server geralmente exigem altos níveis de memória e IOPS, mas uma baixa contagem de vCPUs. A AWS fornece um amplo conjunto de tipos de instâncias que podem cobrir a maioria das suas necessidades de infraestrutura. No entanto, para reduzir os custos de licenciamento baseados em vCPUs para Windows e Microsoft SQL Server, é possível personalizar o número de vCPUs em execução na sua instância do EC2, mantendo a mesma memória e IOPS. Para configurar as opções de CPU em sua instância e economizar nos custos de licenciamento baseados em vCPU para workloads com licença incluída e traga a sua própria licença (BYOL), use o recurso de otimização de CPUs.

Para obter mais informações, consulte esta publicação do blog sobre práticas recomendadas para otimizar CPUs em workloads do SQL Server.

Tipos de licença com suporte

A otimização de CPUs oferece suporte ao faturamento com base no número de CPUs ativas para os tipos a seguir de configurações de licença para instâncias lançadas a partir de uma AMI com licença

incluída. Para obter mais informações sobre tipos de licença, consulte Campos de informações de faturamento da AMI.

Faturamento de instâncias de AMI com licença incluída

Licenças incluídas	Operação de uso	Preço por hora de vCPU
Windows Server	RunInstances:0002	USD 0,046
Windows Server com SQL Server Enterprise	RunInstances:0102	USD 0,421
Windows Server com SQL Server Standard	RunInstances:0006	USD 0,166
Windows Server com SQL Server Web	RunInstances:0202	USD 0,063

Opções de compra com suporte

A otimização de CPUs oferece suporte às opções a seguir para a compra de instâncias com licença incluída:

- Sob demanda
- Savings Plans

> **Warning**
>
> Se você usar instâncias reservadas, os descontos podem não ser aplicados ao configurar a otimização de CPUs para instâncias incluídas na licença na mesma conta pagadora. Recomendamos que você use o Savings Plans para reduzir os custos de licenciamento baseados em vCPU e oferecer economias comparáveis em seus custos de computação. As contas que usavam CPUs otimizadas e instâncias reservadas para Windows e SQL Server no mesmo tipo de instância antes de 15 de outubro de 2025 foram adicionadas a uma lista de exclusão para manter sua experiência de cobrança atual. Para aproveitar as

vantagens da economia de licenças de CPU otimizadas, entre em contato com a Central de AWS Support para ser removido da lista de exclusão.

Como a otimização de CPUs funciona para economizar nas taxas de licenciamento

Os exemplos a seguir ajudam a ilustrar a economia de custos que é possível quando você configura o uso da sua CPU.

Exemplo 1: faturamento padrão este exemplo mostra uma instância r7i.8xlarge iniciada a partir de uma AMI do Windows e do SQL Server Enterprise com licença incluída que foi executada por 100 horas com a configuração de CPU padrão de 32 vCPUs para o tipo de instância (3.200 horas de vCPU).

A fatura mostra um item de linha com uma taxa combinada que inclui taxas de uso e de licenciamento.

For illustration purposes only **Amazon Web Services, Inc. charges by service** **Total services: 1** **Description**	**Usage Quantity**	**Total charges** **$1,558.88** **Amount in USD**
Elastic Compute Cloud		$1,558.88
|- US East (N. Virginia)		$1,558.88
|- Amazon Elastic Compute Cloud running Windows and SQL Server Enterprise		$1,558.88
| |- $15.5888 per On Demand Windows with SQL Server Enterprise r7i.8xlarge Instance Hour	100 Hrs	$1,558.88

Exemplo 2: faturamento de CPUs otimizadas este exemplo mostra uma instância r7i.8xlarge iniciada a partir de uma AMI do Windows e do SQL Server Enterprise com licença incluída. Para economizar nas taxas de licença, o número de CPUs ativas foi reduzido para 16 vCPUs. Em seguida, a instância foi executada por 100 horas com a nova configuração.

A fatura mostra os dois itens de linha a seguir.

Descrição do faturamento: Elastic Compute Cloud

O item da primeira linha mostra o custo básico da instância do Windows e do SQL Server que foi executada por 100 horas (USD 211,68).

Descrição do faturamento: A licença de CPU otimizada do Amazon EC2 inclui taxas de terceiros

O segundo item de linha cobre as taxas de licenciamento com base no número de vCPUs que estavam ativas durante o período de cobrança (673,60 USD).

For illustration purposes only **Amazon Web Services, Inc. charges by service** **Total services: 2** **Description**	**Usage Quantity**	**Total charges** **$885.28** **Amount in USD**
Elastic Compute Cloud		$211.68
|- US East (N. Virginia)		$211.68
|- Amazon Elastic Compute Cloud running Windows and SQL Server Enterprise		$211.68
| |- $2.1168 per On Demand Windows and SQL Server Enterprise without licenses r7i.8xlarge Instance Hr	100 Hrs	$211.68
Amazon EC2 Optimize CPU License Included Third Party Fees		$673.60
|- US East (N. Virginia)		$673.60
|- Amazon Elastic Compute Cloud running Windows and SQL Server Enterprise		$673.60
| |- $0.421 per vCPU-Hour of On Demand Windows with SQL Server licenses on r7i Instance	1,600 vCPU-Hrs	$673.60

Exemplo 3: faturamento de CPUs otimizadas com Savings Plans este exemplo mostra uma instância r7i.8xlarge iniciada a partir de uma AMI do Windows e do SQL Server Enterprise com licença incluída. Para economizar nas taxas de licença, o número de CPUs ativas foi reduzido para 16 vCPUs. Em seguida, a instância foi executada por 100 horas com a nova configuração.

O Savings Plans para computação sem taxas iniciais de um ano com um compromisso de USD 1,60 por hora (arredondado) proporciona economias adicionais que reduzem o custo básico da instância do Windows e do SQL Server. O compromisso do Savings Plan cobre o uso total de 100 horas da instância r7i.8xlarge por uma taxa de 1,53362 USD/hora do Savings Plans.

A fatura mostra os itens de linha a seguir.

Descrição do faturamento: Uso do Savings Plans para computação

O item da primeira linha mostra o compromisso do Savings Plans para o uso total de 100 horas (USD 160,00).

Descrição do faturamento: Elastic Compute Cloud

O item da segunda linha contém duas entradas. A primeira entrada mostra qual teria sido o custo base da instância do Windows e do SQL Server executada por 100 horas sem Savings Plans (USD 211,68). A segunda entrada mostra que o custo básico total foi coberto pelo Savings Plans para computação (USD -211,68), o que gera um custo líquido de zero para esse item de linha.

Descrição do faturamento: A licença de CPU otimizada do Amazon EC2 inclui taxas de terceiros

O terceiro item de linha cobre as taxas de licenciamento com base no número de vCPUs que estavam ativas durante o período de cobrança (USD 673,60).

For illustration purposes only Amazon Web Services, Inc. charges by service Total services: 3 Description	Usage Quantity	Total charges $833.60 Amount in USD
Savings Plans for Compute usage		$160.00
|- Any		$160.00
|- Compute Savings Plans		$160.00
| |- 1 year No Upfront Compute Savings Plan	100 Hrs	$160.00
Elastic Compute Cloud		$0.00
|- US East (N. Virginia)		$0.00
|- Amazon Elastic Compute Cloud running Windows and SQL Server Enterprise		$0.00
| |- $2.1168 per On Demand Windows and SQL Server Enterprise without licenses r7i.8xlarge Instance Hr	100 Hrs	$211.68
| |- r7i.8xlarge Windows with SQL Server Enterprise without licenses instance usage covered by CSP	100 Hrs	($211.68)
Amazon EC2 Optimize CPU License Included Third Party Fees		$673.60
|- US East (N. Virginia)		$673.60
|- Amazon Elastic Compute Cloud running Windows and SQL Server Enterprise		$673.60
| |- $0.421 per vCPU-Hour of On Demand Windows with SQL Server licenses on r7i Instance	1,600 vCPU-Hrs	$673.60

AMD SEV-SNP para instâncias do Amazon EC2

O AMD Secure Encrypted Virtualization-Secure Nested Paging (AMD SEV-SNP) é um recurso de CPU que fornece as seguintes propriedades:

- Declaração: o AMD SEV-SNP permite que você recupere um relatório de declaração assinado que contém uma medida criptográfica que pode ser usada para validar o estado e a identidade da instância e se ela está sendo executada em hardware original da AMD. Para obter mais informações, consulte Atestar uma instância do Amazon EC2 com o AMD SEV-SNP.
- Criptografia de memória: começando com os processadores AMD EPYC (Milan), AWS Graviton2 e Intel Xeon Scalable (Ice Lake), a memória da instância é sempre criptografada. As instâncias habilitadas para o AMD SEV-SNP usam uma chave específica da instância para sua criptografia de memória.

Conteúdo

- Conceitos e terminologia
- Requisitos
- Considerações
- Preços
- Encontrar tipos de instância do EC2 que são compatíveis com o AMD SEV-SNP
- Habilitar o AMD SEV-SNP para uma instância do EC2
- Atestar uma instância do Amazon EC2 com o AMD SEV-SNP

Conceitos e terminologia

Antes de começar a usar o AMD SEV-SNP, certifique-se de estar familiarizado com os conceitos e a terminologia a seguir.

Relatório de declaração AMD SEV-SNP

O relatório de declaração AMD SEV-SNP é um documento que uma instância pode solicitar para a CPU. O relatório de declaração AMD SEV-SNP pode ser usado para validar o estado e a identidade de uma instância e para verificar se ela está sendo executada em um ambiente AMD sancionado. O relatório inclui uma medição de inicialização, que é um hash criptográfico do estado inicial de inicialização de uma instância, incluindo o conteúdo da memória da instância inicial e o estado inicial das vCPUs. O relatório de declaração AMD SEV-SNP é assinado com uma assinatura VLEK que remonta a uma raiz de confiança da AMD.

VLEK

A Versioned Loaded Endossement Key (VLEK) é uma chave de assinatura versionada certificada pela AMD e usada pela CPU da AMD para assinar os relatórios de declaração do AMD SEV-SNP. As assinaturas VLEK podem ser validadas usando certificados fornecidos pela AMD.

Binário OVMF

O Open Virtual Machine Firmware (OVMF) é o código de inicialização antecipada usado para fornecer um ambiente UEFI para a instância. O código de inicialização antecipada é executado antes que o código na AMI seja inicializado. O OVMF também encontra e executa o carregador de inicialização fornecido na AMI. Para obter mais informações, consulte o repositório do OVMF.

Requisitos

Para usar o AMD SEV-SNP, você deve fazer o seguinte:

- Use um dos seguintes tipos de instância com suporte:
  - Uso geral: `m6a.large` | `m6a.xlarge` | `m6a.2xlarge` | `m6a.4xlarge` | `m6a.8xlarge`
  - Otimizadas para computação: `c6a.large` | `c6a.xlarge` | `c6a.2xlarge` | `c6a.4xlarge` | `c6a.8xlarge` | `c6a.12xlarge` | `c6a.16xlarge`
  - Otimizadas para memória: `r6a.large` | `r6a.xlarge` | `r6a.2xlarge` | `r6a.4xlarge`
- Execute sua instância em um Região da AWS com suporte. Atualmente, há suporte apenas para Leste dos EUA (Ohio) e Europa (Irlanda).

- Use uma AMI com modo de inicialização `uefi` ou `uefi-preferred` e um sistema operacional com suporte a AMD SEV-SNP. Para obter mais informações sobre o suporte ao AMD SEV-SNP em seu sistema operacional, consulte a documentação do respectivo sistema operacional. Na AWS, o AMD SEV-SNP é compatível com AL2023, RHEL 9.3, SLES 15 SP4 e Ubuntu 23.04 e posterior.

Considerações

Você só pode habilitar o AMD SEV-SNP ao iniciar uma instância. Quando o AMD SEV-SNP está habilitado para a inicialização da instância, as regras a seguir se aplicam.

- Uma vez habilitado, o AMD SEV-SNP não poderá ser desabilitado. Ele permanece habilitado durante todo o ciclo de vida da instância.
- É possível alterar o tipo de instância somente para outro tipo de instância com suporte para o AMD SEV-SNP.
- Não há suporte para o Hibernation e o Nitro Enclaves.
- Não há suporte para hosts dedicados.
- Se o host subjacente para a instância estiver programado para manutenção, você receberá uma notificação do evento programado 14 dias antes do evento. Você deverá interromper ou reiniciar manualmente sua instância para movê-la para um novo host.

Preços

Quando você inicia uma instância do Amazon EC2 com o AMD SEV-SNP habilitado, é cobrada uma taxa adicional de uso por hora que equivale a 10% da taxa horária sob demanda do tipo de instância selecionada.

Essa taxa de uso do AMD SEV-SNP é uma cobrança separada do uso da instância do Amazon EC2. Instâncias reservadas, Savings Plans e uso do sistema operacional não afetam essa taxa.

Se você configurar uma instância spot para iniciar com o AMD SEV-SNP habilitado, uma tarifa adicional de uso por hora será cobrada. Essa tarifa equivale a 10% da taxa horária sob demanda do tipo de instância selecionada. Se a estratégia de alocação usar o preço como entrada, a frota spot não incluirá essa tarifa adicional; somente o preço spot será usado.

Encontrar tipos de instância do EC2 que são compatíveis com o AMD SEV-SNP

É possível encontrar tipos de instância compatíveis com o AMD SEV-SNP. O console do Amazon EC2 não exibe essas informações para um tipo de instância.

AWS CLI

Para encontrar os tipos de instância compatíveis com o AMD SEV-SNP

Use o seguinte comando describe-instance-types:

```
aws ec2 describe-instance-types \
    --filters Name=processor-info.supported-features,Values=amd-sev-snp \
    --query 'InstanceTypes[*].[InstanceType]' \
    --output text | sort
```

O seguinte é um exemplo de saída.

```
c6a.12xlarge
c6a.16xlarge
c6a.2xlarge
c6a.4xlarge
c6a.8xlarge
c6a.large
c6a.xlarge
m6a.2xlarge
m6a.4xlarge
m6a.8xlarge
m6a.large
m6a.xlarge
r6a.2xlarge
r6a.4xlarge
r6a.large
r6a.xlarge
```

PowerShell

Para encontrar os tipos de instância compatíveis com o AMD SEV-SNP

Use o cmdlet Get-EC2InstanceType.

```
(Get-EC2InstanceType `
```

```
    -Filter @{Name="processor-info.supported-features"; Values="amd-sev-
snp"}).InstanceType.Value | Sort-Object
```

O seguinte é um exemplo de saída.

```
c6a.12xlarge
c6a.16xlarge
c6a.2xlarge
c6a.4xlarge
c6a.8xlarge
c6a.large
c6a.xlarge
m6a.2xlarge
m6a.4xlarge
m6a.8xlarge
m6a.large
m6a.xlarge
r6a.2xlarge
r6a.4xlarge
r6a.large
r6a.xlarge
```

Habilitar o AMD SEV-SNP para uma instância do EC2

É possível iniciar uma instância com o AMD SEV-SNP habilitado. Não é possível habilitar o AMD SEV-SNP após a inicialização.

Iniciar uma instância com o AMD SEV-SNP habilitado

Não é possível habilitar o AMD SEV-SNP usando o console do Amazon EC2.

AWS CLI

Para iniciar uma instância com o AMD SEV-SNP habilitado

Use o comando run-instances com a opção `--cpu-options`. Para obter requisitos adicionais, consulte Requisitos do AMD SEV-SNP.

```
--cpu-options AmdSevSnp=enabled
```

PowerShell

Para iniciar uma instância com o AMD SEV-SNP habilitado

Use o cmdlet New-EC2Instance com o parâmetro `-CpuOption`.

```
-CpuOption @{AmdSevSnp="enabled"}
```

Verificar se uma instância do EC2 está habilitada para o AMD SEV-SNP

É possível encontrar instâncias que estão habilitadas para o AMD SEV-SNP. O console do Amazon EC2 não exibe essas informações.

AWS CLI

Para verificar se o AMD SEV-SNP está habilitado para uma instância

Use o comando describe-instances.

```
aws ec2 describe-instances \
    --instance-ids i-1234567890abcdef0 \
    --query Reservations[].Instances[].CpuOptions
```

O seguinte é um exemplo de saída. Se `AmdSevSnp` não estiver presente em `CpuOptions`, o AMD SEV-SNP está desabilitado.

```
[
    {
        "AmdSevSnp": "enabled",
        "CoreCount": 1,
        "ThreadsPerCore": 2
    }
]
```

PowerShell

Para verificar se o AMD SEV-SNP está habilitado para uma instância

Use o cmdlet Get-EC2Instance.

```
(Get-EC2Instance `
    -InstanceId i-1234567890abcdef0).Instances.CpuOptions
```

O seguinte é um exemplo de saída. Se o valor de `AmdSevSnp` não estiver presente, o AMD SEV-SNP está desabilitado.

```
AmdSevSnp CoreCount ThreadsPerCore
--------- --------- --------------
enabled   1         2
```

AWS CloudTrail

No evento do AWS CloudTrail para a solicitação de inicialização da instância, a propriedade a seguir indica que o AMD SEV-SNP está habilitado para a instância.

```
"cpuOptions": {"AmdSevSnp": "enabled"}
```

Atestar uma instância do Amazon EC2 com o AMD SEV-SNP

A declaração é um processo que permite que sua instância prove seu estado e sua identidade. Após habilitar o AMD SEV-SNP para a instância, será possível solicitar um relatório de atestado do AMD SEV-SNP para o processador subjacente. O relatório de declaração do AMD SEV-SNP contém um hash criptográfico, chamado de medição de lançamento, do conteúdo inicial da memória do convidado e do estado inicial da vCPU. O relatório de declaração é assinado com uma assinatura VLEK que remonta a uma raiz de confiança da AMD. É possível usar a medida de inicialização incluída no relatório de declaração para validar se a instância está sendo executada em um ambiente AMD genuíno e para validar o código de inicialização inicial usado para iniciar a instância.

Pré-requisito

Iniciar uma instância habilitada para o AMD SEV-SNP. Para obter mais informações, consulte Habilitar o AMD SEV-SNP para uma instância do EC2.

Etapas

- Etapa 1: obter o relatório de declaração
- Etapa 2: validar a assinatura do relatório de atestado

Etapa 1: obter o relatório de declaração

Nessa etapa, você instala e cria o utilitário `snpguest` e, em seguida, usa-o para solicitar o relatório de atestado e os certificados do AMD SEV-SNP.

1. Conecte-se à sua instância.
2. Execute os comandos apresentados a seguir para desenvolver o utilitário `snpguest` usando o repositório snpguest repository.

   ```
   $ git clone https://github.com/virtee/snpguest.git
   $ cd snpguest
   $ cargo build -r
   $ cd target/release
   ```

3. Gere uma solicitação para o relatório de atestado. O utilitário solicita o relatório de atestado usando o host e o grava em um arquivo binário com os dados de solicitação fornecidos.

   O exemplo apresentado a seguir cria uma string de solicitação randômica e a utiliza como arquivo de solicitação (`request-file.txt`). Quando o comando retorna o relatório de atestado, ele é armazenado no caminho do arquivo especificado (`report.bin`). Nesse caso, o utilitário armazena o relatório no diretório atual.

   ```
   $ ./snpguest report report.bin request-file.txt --random
   ```

4. Solicite os certificados usando a memória do host e armazene-os como arquivos PEM. O exemplo apresentado a seguir armazena os arquivos no mesmo diretório do utilitário `snpguest`. Se já existirem certificados no diretório especificado, esses certificados serão substituídos.

   ```
   $ ./snpguest certificates PEM ./
   ```

Etapa 2: validar a assinatura do relatório de atestado

O relatório de declaração é assinado com um certificado, chamado Versioned Loaded Endossement Key (VLEK), emitido pela AMD para a AWS. Nessa etapa, é possível validar se o certificado VLEK é emitido pela AMD e se o relatório de atestado é assinado por esse certificado VLEK.

1. Faça o download dos certificados VLEK de raiz de confiança do site oficial da AMD para o diretório atual.

```
$ sudo curl --proto '=https' --tlsv1.2 -sSf https://kdsintf.amd.com/vlek/v1/Milan/
cert_chain -o ./cert_chain.pem
```

2. Use `openssl` para validar se o certificado VLEK está assinado pela raiz dos certificados de confiança da AMD.

```
$ sudo openssl verify --CAfile ./cert_chain.pem vlek.pem
```

O seguinte é um exemplo de saída.

```
vlek.pem: OK
```

3. Use o utilitário `snpguest` para validar se o relatório de declaração foi assinado pelo certificado VLEK.

```
$ ./snpguest verify attestation ./ report.bin
```

O seguinte é um exemplo de saída.

```
Reported TCB Boot Loader from certificate matches the attestation report.
Reported TCB TEE from certificate matches the attestation report.
Reported TCB SNP from certificate matches the attestation report.
Reported TCB Microcode from certificate matches the attestation report.
VEK signed the Attestation Report!
```

Controle do estado do processador para instâncias Linux do Amazon EC2

C-states controlam os níveis de suspensão que um núcleo pode assumir quando está ocioso. 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).

P-states controlam a performance desejada (na frequência da CPU) de um núcleo. Os P-states são numerados começando com P0 (a configuração de performance mais elevada em que o núcleo pode usar a Intel Turbo Boost Technology para aumentar a frequência, se possível) e vão de P1 (o P-state que solicita a frequência máxima de linha de base) até P15 (a frequência mais baixa possível).

> **Note**
>
> AWSOs processadores Graviton da têm modos de economia de energia integrados e operam em uma frequência fixa. Portanto, eles não fornecem a capacidade para o sistema operacional controlar os C-states e P-states.

Estados C e estados P

Os tipos de instâncias a seguir oferecem a capacidade de um sistema operacional de controlar C-states e P-states:

- Uso geral: `m4.10xlarge` | `m4.16xlarge`
- Otimizadas para computação: `c4.8xlarge`
- Otimizadas para memória: `r4.8xlarge` | `r4.16xlarge` | `x1.16xlarge` | `x1.32xlarge` | `x1e.8xlarge` | `x1e.16xlarge` | `x1e.32xlarge`
- Otimizadas para armazenamento: `d2.8xlarge` | `i3.8xlarge` | `i3.16xlarge` | `h1.8xlarge` | `h1.16xlarge`
- Computação acelerada: `f1.16xlarge` | `g3.16xlarge` | `p2.16xlarge` | `p3.16xlarge`
- Bare metal: todas as instâncias bare metal com processadores Intel e AMD

Somente estados C

Os tipos de instâncias a seguir oferecem a capacidade de um sistema operacional de controlar C-states:

- Uso geral: `m5.12xlarge` | `m5.24xlarge` | `m5d.12xlarge` | `m5d.24xlarge` | `m5n.12xlarge` | `m5n.24xlarge` | `m5dn.12xlarge` | `m5dn.24xlarge` | `m5zn.6xlarge` | `m5zn.12xlarge` | `m6a.24xlarge` | `m6a.48xlarge` | `m6i.16xlarge` | `m6i.32xlarge` | `m6id.16xlarge` | `m6id.32xlarge` | `m6idn.16xlarge` | `m6in.16xlarge` | `m6in.32xlarge` | `m7a.medium` | `m7a.large` | `m7a.xlarge` | `m7a.2xlarge` | `m7a.4xlarge` | `m7a.8xlarge` | `m7a.12xlarge` | `m7a.16xlarge` | `m7a.24xlarge` | `m7a.32xlarge` | `m7a.48xlarge` | `m7i.large` | `m7i.xlarge` | `m7i.2xlarge` | `m7i.4xlarge` | `m7i.8xlarge` | `m7i.12xlarge` | `m7i.16xlarge` | `m7i.24xlarge` | `m7i.48xlarge` | `m8a.medium` | `m8a.large` | `m8a.xlarge` | `m8a.2xlarge` | `m8a.4xlarge` | `m8a.8xlarge` | `m8a.12xlarge` | `m8a.16xlarge` | `m8a.24xlarge` | `m8a.48xlarge` | `m8azn.medium` | `m8azn.large` | `m8azn.xlarge` | `m8azn.3xlarge` | `m8azn.6xlarge` | `m8azn.12xlarge` | `m8azn.24xlarge` | `m8i.large`

| m8i.xlarge | m8i.2xlarge | m8i.4xlarge | m8i.8xlarge | m8i.12xlarge | m8i.16xlarge | m8i.24xlarge | m8i.32xlarge | m8i.48xlarge | m8i.96xlarge | m8id.large | m8id.xlarge | m8id.2xlarge | m8id.4xlarge | m8id.8xlarge | m8id.12xlarge | m8id.16xlarge | m8id.24xlarge | m8id.32xlarge | m8id.48xlarge | m8id.96xlarge

- Otimizadas para computação: c5.9xlarge | c5.12xlarge | c5.18xlarge | c5.24xlarge | c5a.24xlarge | c5ad.24xlarge | c5d.9xlarge | c5d.12xlarge | c5d.18xlarge | c5d.24xlarge | c5n.9xlarge | c5n.18xlarge | c6a.24xlarge | c6a.32xlarge | c6a.48xlarge | c6i.16xlarge | c6i.32xlarge | c6id.24xlarge | c6id.32xlarge | c6in.32xlarge | c7a.medium | c7a.large | c7a.xlarge | c7a.2xlarge | c7a.4xlarge | c7a.8xlarge | c7a.12xlarge | c7a.16xlarge | c7a.24xlarge | c7a.32xlarge | c7a.48xlarge | c7i.large | c7i.xlarge | c7i.2xlarge | c7i.4xlarge | c7i.8xlarge | c7i.12xlarge | c7i.16xlarge | c7i.24xlarge | c7i.48xlarge | c8a.medium | c8a.large | c8a.xlarge | c8a.2xlarge | c8a.4xlarge | c8a.8xlarge | c8a.12xlarge | c8a.16xlarge | c8a.24xlarge | c8a.48xlarge | c8i.large | c8i.xlarge | c8i.2xlarge | c8i.4xlarge | c8i.8xlarge | c8i.12xlarge | c8i.16xlarge | c8i.24xlarge | c8i.32xlarge | c8i.48xlarge | c8i.96xlarge | c8id.large | c8id.xlarge | c8id.2xlarge | c8id.4xlarge | c8id.8xlarge | c8id.12xlarge | c8id.16xlarge | c8id.24xlarge | c8id.32xlarge | c8id.48xlarge | c8id.96xlarge x8i.large | x8i.xlarge | x8i.2xlarge | x8i.4xlarge | x8i.8xlarge | x8i.12xlarge | x8i.16xlarge | x8i.24xlarge | x8i.32xlarge | x8i.48xlarge | x8i.48xlarge | x8i.96xlarge
- Otimizadas para memória: r5.12xlarge | r5.24xlarge | r5b.12xlarge | r5d.12xlarge | r5d.24xlarge | r5n.12xlarge | r5n.24xlarge | r5dn.12xlarge | r5dn.24xlarge | r6a.24xlarge | r6a.48xlarge | r6i.16xlarge | r6i.32xlarge | r6id.16xlarge | r6id.32xlarge | r6in.16xlarge | r6in.32xlarge | r7a.medium | r7a.large | r7a.xlarge | r7a.2xlarge | r7a.4xlarge | r7a.8xlarge | r7a.12xlarge | r7a.16xlarge | r7a.24xlarge | r7a.32xlarge | r7a.48xlarge | r7i.large | r7i.xlarge | r7i.2xlarge | r7i.4xlarge | r7i.8xlarge | r7i.12xlarge | r7i.16xlarge | r7i.24xlarge | r7i.48xlarge | r7iz.large | r7iz.xlarge | r7iz.2xlarge | r7iz.4xlarge | r7iz.8xlarge | r7iz.12xlarge | r7iz.16xlarge | r7iz.32xlarge | r8a.medium | r8a.large | r8a.xlarge | r8a.2xlarge | r8a.4xlarge | r8a.8xlarge | r8a.12xlarge | r8a.16xlarge | r8a.24xlarge | r8a.48xlarge | r8i.large | r8i.xlarge | r8i.2xlarge | r8i.4xlarge | r8i.8xlarge | r8i.12xlarge | r8i.16xlarge | r8i.24xlarge | r8i.32xlarge | r8i.48xlarge | r8i.96xlarge | r8id.large | r8id.xlarge | r8id.2xlarge | r8id.4xlarge |

r8id.8xlarge | r8id.12xlarge | r8id.16xlarge | r8id.24xlarge | r8id.32xlarge | r8id.48xlarge | r8id.96xlarge | u-3tb1.56xlarge | u-6tb1.56xlarge | u-6tb1.112xlarge | u-9tb1.112xlarge | u-12tb1.112xlarge | u-18tb1.112xlarge | u-24tb1.112xlarge | u7i-6tb.112xlarge | u7i-8tb.112xlarge | u7i-12tb.224xlarge | u7in-16tb.224xlarge | u7in-24tb.224xlarge | u7in-32tb.224xlarge | u7inh-32tb.480xlarge | x2idn.32xlarge | x2iedn.16xlarge | x2iedn.32xlarge | x2iezn.12xlarge | x8aedz.large | x8aedz.xlarge | x8aedz.3xlarge | x8aedz.6xlarge | x8aedz.12xlarge | x8aedz.24xlarge | z1d.6xlarge | z1d.12xlarge

- Otimizadas para armazenamento: d3en.12xlarge | dl1.24xlarge | i3en.12xlarge | i3en.24xlarge | i4i.16xlarge | i7i.large | i7i.xlarge | i7i.2xlarge | i7i.4xlarge | i7i.8xlarge | i7i.12xlarge | i7i.16xlarge | i7i.24xlarge | i7i.48xlarge | i7ie.large | i7ie.xlarge | i7ie.2xlarge | i7ie.3xlarge | i7ie.6xlarge | i7ie.12xlarge | i7ie.18xlarge | i7ie.24xlarge | i7ie.48xlarge | r5b.12xlarge | r5b.24xlarge
- Computação acelerada: dl1.24xlarge | f2.6xlarge | f2.12xlarge | f2.48xlarge | g5.24xlarge | g5.48xlarge | g6.24xlarge | g6.48xlarge | g6e.12xlarge | g6e.24xlarge | g6e.48xlarge | g7e.2xlarge | g7e.4xlarge | g7e.8xlarge | g7e.12xlarge | g7e.24xlarge | g7e.48xlarge | inf1.24xlarge | p3dn.24xlarge | p4d.24xlarge | p4de.24xlarge | p5.48xlarge | p5e.48xlarge | p5en.48xlarge | p6-b200.48xlarge | p6-b300.48xlarge | trn1.32xlarge | trn2.3xlarge | trn2.48xlarge | trn2a.3xlarge | trn2a.48xlarge | trn2n.3xlarge | trn2n.48xlarge | trn2p.48xlarge | trn2u.48xlarge | vt1.24xlarge
- Computação de alta performance: hpc7a.12xlarge | hpc7a.24xlarge | hpc7a.48xlarge | hpc7a.96xlarge | hpc8a.96xlarge

Talvez você queira alterar as configurações de C-state ou P-state para aumentar a consistência de performance do processador, reduzir a latência ou ajustar sua instância para uma workload específica. As configurações padrão de C-state e P-state proporcionam o performance máxima, que é o ideal para a maioria das workloads. Contudo, se sua aplicação se beneficiaria de latência reduzida ao custo de frequências superiores de single ou dual core, ou de uma performance consistente em frequências menores em oposição às frequências Turbo Boost expansíveis, considere experimentar as configurações de C-state ou P-state que estão disponíveis para essas instâncias.

Para obter informações sobre diferentes configurações de processador e como monitorar os efeitos da configuração para o Amazon Linux, consulte Processor state control for Amazon EC2 Amazon

Linux instance no Amazon Linux 2 User Guide. Esses procedimentos foram escritos para o Amazon Linux e se aplicam a ele, mas também podem funcionar para outras distribuições do Linux com o kernel do Linux versão 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.

Instâncias gerenciadas do Amazon EC2

Uma instância gerenciada do Amazon EC2 é uma instância do EC2 que é provisionada e gerenciada por um provedor de serviços designado, como o Amazon EKS por meio do Modo Automático do EKS. As instâncias gerenciadas fornecem uma maneira simplificada de executar workloads computacionais no Amazon EC2, permitindo que você delegue o controle operacional da instância a um provedor de serviços.

O controle delegado é a única alteração introduzida para instâncias gerenciadas. As especificações técnicas e o faturamento permanecem os mesmos das instâncias do EC2 não gerenciadas. Como as instâncias gerenciadas permitem delegar o controle ao provedor de serviços, é possível se beneficiar da experiência operacional e das melhores práticas do provedor de serviços. Quando uma instância é gerenciada, o provedor de serviços é responsável por tarefas como provisionar a instância, configurar o software, dimensionar a capacidade, lidar com falhas e substituições de instâncias e encerrar essa instância.

Não é possível modificar diretamente as configurações de uma instância gerenciada ou encerrá-la. O serviço e as operações específicas são determinados pelo acordo entre você e o provedor de serviços. No entanto, é possível adicionar, modificar ou remover tags das suas instâncias gerenciadas, permitindo categorizá-las em seu ambiente da AWS.

Conteúdo

- Faturamento de instâncias gerenciadas
- Identificar instâncias gerenciadas
- Conceitos básicos das instâncias gerenciadas

Faturamento de instâncias gerenciadas

Uma instância gerenciada do Amazon EC2 incorre na mesma cobrança básica de uma instância não gerenciada do Amazon EC2, além de uma taxa separada para o provedor de serviços. Essa taxa adicional é cobrada pelo provedor de serviços que gerencia sua instância e é faturada

separadamente. Ela cobre o custo dos serviços fornecidos para operar e manter sua instância gerenciada.

Todas as opções de compra do Amazon EC2 estão disponíveis para instâncias gerenciadas, incluindo instâncias sob demanda, instâncias reservadas, instâncias spot e Savings Plans. Ao adquirir sua computação diretamente do EC2 e fornecê-la ao seu provedor de serviços, você se beneficia de quaisquer instâncias reservadas ou Savings Plans existentes aplicados à sua conta, garantindo o uso da capacidade computacional mais econômica disponível.

Por exemplo, ao usar o Modo Automático do Amazon EKS, você paga a taxa padrão de instância EC2 para as instâncias subjacentes, além de uma cobrança adicional do Amazon EKS pelo gerenciamento das instâncias em seu nome. Se você decidir se inscrever em Savings Plans, a taxa de instância do EC2 será reduzida pelos Savings Plans, enquanto a cobrança adicional do Amazon EKS permanecerá inalterada.

Identificar instâncias gerenciadas

As instâncias gerenciadas são identificadas por um valor true no campo Gerenciada. O provedor de serviços é identificado no campo Operador (no console) ou no campo `Principal` (na CLI).

Use os procedimentos a seguir para identificar instâncias gerenciadas.

Console

Para identificar uma instância gerenciada

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância que você deseja verificar.
4. Na guia Detalhs (se você marcou a caixa de seleção) ou na área de resumo (se você selecionou o ID da instância), localize o campo Gerenciada.
   - Um valor de true indica uma instância gerenciada.
   - Um valor de false indica uma instância não gerenciada.
5. Se Gerenciada estiver definido como true, o campo Operador exibirá um valor identificando o provedor de serviços responsável pelo gerenciamento da instância. Por exemplo, um valor de eks.amazonaws.com identifica o Amazon EKS como o provedor de serviços.

AWS CLI

Para identificar uma instância gerenciada

Use o comando describe-instances e especifique o ID da instância.

```
aws ec2 describe-instances \
    --instance-ids i-1234567890abcdef0 \
    --query Reservations[].Instances[].Operator
```

O seguinte é um exemplo de saída. Se `Managed` for `true`, a instância é uma instância gerenciada e um `Principal` será incluído. A entidade principal é o provedor de serviços que gerencia a instância. Por exemplo, um valor de `eks.amazonaws.com` identifica o Amazon EKS como o provedor de serviços.

```
[
    {
        "Managed": true,
        "Principal": "eks.amazonaws.com"
    }
]
```

Para encontrar suas instâncias gerenciadas

Use o comando describe-instances e especifique o filtro `operator.managed` com um valor de `true`. A opção `--query` exibe somente os IDs das instâncias gerenciadas.

```
aws ec2 describe-instances \
    --filters "Name=operator.managed,Values=true" \
    --query Reservations[*].Instances[].InstanceId
```

PowerShell

Para identificar uma instância gerenciada

Use o cmdlet Get-EC2Instance.

```
(Get-EC2Instance -InstanceId i-1234567890abcdef0).Instances.Operator
```

O seguinte é um exemplo de saída.

```
Managed Principal
```

```
------- ---------
True    eks.amazonaws.com
```

Para encontrar suas instâncias gerenciadas

Use o cmdlet Get-EC2Instance. Este exemplo exibe somente os IDs das instâncias gerenciadas.

```
(Get-EC2Instance -Filter @{Name="operator.managed";
 Values="true"}).Instances.InstanceId
```

Conceitos básicos das instâncias gerenciadas

Para obter orientação sobre o uso de instâncias gerenciadas, consulte Automatizar a infraestrutura de cluster com o Modo Automático do EKS no Guia do usuário do Amazon EKS.

Use a virtualização aninhada para executar hipervisores em instâncias do Amazon EC2

A virtualização aninhada permite que você execute hipervisores como Hyper-V e KVM dentro de instâncias virtuais do Amazon EC2. As instâncias virtuais do EC2 não são instâncias bare metal. Esse recurso amplia a flexibilidade da virtualização ao adicionar suporte de virtualização em nível de processador às instâncias virtuais do EC2, permitindo que um hipervisor em execução na sua instância crie e gerencie máquinas virtuais.

A virtualização aninhada pode ajudar quando você executa ferramentas de desenvolvimento como Docker Desktop, Windows Subsystem for Linux 2 (WSL2), emuladores do Android Studio ou QEMU em seu fluxo de trabalho de desenvolvimento, pois permite escolher entre uma ampla variedade de tipos de instâncias virtuais padrão do Amazon EC2 que atendem aos seus requisitos específicos de desempenho e preço.

Não há custo adicional para usar a virtualização aninhada.

Conteúdo

- Como funcionam
- Considerações
- Iniciar uma nova instância com a virtualização aninhada
- Configurar uma instância existente para usar a virtualização aninhada

Como funcionam

As instâncias virtuais do EC2 são executadas em um host físico que tem o hipervisor Nitro. Para oferecer suporte à virtualização aninhada, o Sistema Nitro transfere as extensões do processador, como Intel VT-x, para instâncias para facilitar a execução de máquinas virtuais aninhadas. A arquitetura de virtualização aninhada consiste em três camadas: a infraestrutura física da AWS e o hipervisor Nitro (L0), sua instância EC2 executando um hipervisor (L1) e uma ou mais máquinas virtuais criadas nessa instância (L2).

Considerações

Antes de começar a usar a virtualização aninhada, considere o seguinte:

- Tipos de instância compatíveis: atualmente, a virtualização aninhada é compatível com instâncias C8i, M8i e R8i.
- Hipervisores compatíveis: atualmente, o KVM e o Hyper-V são os hipervisores L1 compatíveis.
- Instâncias do Windows: quando a virtualização aninhada está habilitada em uma instância do Windows:
  - Credential Guard: o Virtual Secure Mode (VSM) é automaticamente desativado.
  - Hibernação: a hibernação e a retomada da instância não são compatíveis.
  - Limite de CPU: não é compatível em instâncias do Windows com mais de 192 CPUs, como `m8i.96xl`.
- Responsabilidades de segurança: ao usar a virtualização aninhada em instâncias do EC2, a AWS é responsável pela “segurança da nuvem”, protegendo a infraestrutura subjacente e mantendo os fortes limites de isolamento entre as instâncias do EC2 fornecidos pelo AWS Nitro System. Os clientes são responsáveis pela “segurança na nuvem”, que inclui proteger o sistema operacional, o hipervisor, as máquinas virtuais aninhadas, os sistemas operacionais convidados, as aplicações e os dados nas instâncias do EC2.
- Desempenho: a AWS recomenda que os clientes que desejam executar workloads que exijam acesso a extensões de virtualização de hardware, sejam sensíveis ao desempenho ou tenham requisitos rígidos de latência, avaliem instâncias bare metal.

Iniciar uma nova instância com a virtualização aninhada

Ao iniciar uma nova instância, você pode ativar a virtualização aninhada para executar hipervisores e máquinas virtuais nela.

Pré-requisitos

É necessário ter as permissões do IAM exigidas para iniciar uma instância do Amazon EC2.

Console

Para habilitar um virtualização aninhada durante o início da instância

1. Siga o procedimento the section called “Usar o assistente de execução de instância” e configure sua instância conforme necessário.
2. Verifique se um tipo de instância compatível está selecionado.
3. Expanda os detalhes avançados e em Virtualização aninhada, escolha Habilitar.
4. No painel Resumo, analise a configuração da instância e selecione Iniciar instância.

AWS CLI

Para iniciar uma instância com a virtualização aninhada habilitada

Use o comando run-instances.

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --instance-type r8i.4xlarge \
    --cpu-options "NestedVirtualization=enabled" \
    --key-name my-key-pair \
    --placement "Tenancy=host"
```

PowerShell

Para iniciar uma instância com a virtualização aninhada habilitada

Use o comando New-EC2Instance.

```
New-EC2Instance `
    -ImageId ami-0abcdef1234567890 `
    -InstanceType r8i.4xlarge `
    -CpuOption @{NestedVirtualization='enabled'} `
    -KeyName my-key-pair `
    -Placement_Tenancy host
```

Configurar uma instância existente para usar a virtualização aninhada

Você pode ativar a virtualização aninhada em uma instância existente do Amazon EC2.

Pré-requisitos

- A instância deve se encontrar no estado `stopped`.
- O tipo de instância deve permitir a virtualização aninhada.

Console

Para habilitar a virtualização aninhada em 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 que você deseja modificar na tabela de instâncias.
4. Escolha Ações, Configurações de instância, Alterar opções de CPU.
5. Na página Alterar opções de CPU, para Virtualização aninhada, escolha uma das seguintes opções:
   - Habilitar: ativa a virtualização aninhada para a instância
   - Desabilitar: desativa a virtualização aninhada para a instância
6. Confira suas alterações e escolha Alterar para aplicar as novas opções de CPU.

AWS CLI

Para habilitar a virtualização aninhada em uma instância existente

Primeiro, interrompa a instância e use o comando modify-instance-cpu-options.

```
aws ec2 modify-instance-cpu-options \
    --instance-id i-1234567890abcdef0 \
    --core-count 4 \
    --threads-per-core 2 \
    --nested-virtualization enabled
```

PowerShell

Para habilitar a virtualização aninhada em uma instância existente

Primeiro, interrompa a instância e use o comando Edit-EC2InstanceCpuOption.

```
Edit-EC2InstanceCpuOption `
    -InstanceId i-1234567890abcdef0 `
    -CoreCount 4 `
    -ThreadsPerCore 2 `
    -NestedVirtualization enabled
```

Opções de faturamento e compra do Amazon EC2

É possível usar as seguintes opções para otimizar seus custos para o Amazon EC2:

- Instâncias sob demanda: pague por segundo as instâncias que você iniciar.
- Savings Plans: reduza os custos do Amazon EC2 se comprometendo com uma quantidade consistente de uso, em USD por hora, pelo prazo de um ou de três anos.
- Instâncias reservadas: reduza os custos do Amazon EC2 se comprometendo com uma configuração consistente de instância, incluindo tipo de instância e região, pelo prazo de um ou de três anos.
- Instâncias spot: solicite instâncias do EC2 não utilizadas, o que pode reduzir significativamente os custos do Amazon EC2.
- Hosts dedicados: pague por um host físico totalmente dedicado à execução de suas instâncias e use as licenças existentes de software por soquete, por núcleo ou por VM para reduzir os custos.
- Instâncias dedicadas: pague por hora as instâncias executadas em hardware de locatário único.
- Reservas de capacidade: reserve capacidade para as instâncias do EC2 em uma zona de disponibilidade específica.

Se você não puder se comprometer com uma configuração de instância específica, mas puder se comprometer com uma quantidade de uso, adquira Savings Plans para reduzir seus custos de instâncias sob demanda. Se você precisar de uma reserva de capacidade, compre instâncias reservadas ou Reservas de Capacidade para uma zona de disponibilidade específica. Os blocos de capacidade podem ser usados para reservar um cluster de instâncias de GPU. As instâncias spot são uma opção econômica se houver flexibilidade quanto ao momento em que as aplicações serão executados e se poderão ser interrompidas. Os hosts dedicados ou as instâncias dedicadas podem ajudar você a atender aos requisitos de conformidade e reduzir custos usando as licenças de software associadas ao servidor.

Para obter mais informações, consulte Definição de preços do Amazon EC2 e Instâncias gerenciadas do Amazon EC2.

Como comprar instâncias sob demanda para o Amazon EC2

Com instâncias sob demanda, você paga pela capacidade computacional por segundo, sem qualquer compromisso de longo prazo. Você tem pleno controle sobre o ciclo de vida da instância: você decide quando executar, interromper, hibernar, iniciar, reiniciar ou encerrá-la.

Não há compromisso de longo prazo ao comprar Instâncias on-demand. Você paga apenas pelos segundos em que suas instâncias sob demanda estiverem no estado `running`, com um mínimo de 60 segundos. O preço por segundo para uma instância sob demanda em execução é fixo e está listado na página de preços sob demanda, preços do Amazon EC2.

Recomendamos o uso de Instâncias on-demand para aplicações com workloads de curto prazo e irregulares que não podem ser interrompidas.

Para economias significativas com relação a instâncias sob demanda, use AWS Savings Plans, Instâncias spot ou Visão geral de instâncias reservadas para o Amazon EC2.

Sumário

- Cotas de instância sob demanda
  - Monitorar cotas e uso de instância sob demanda
  - Solicitar um aumento da cota
- Consulte os preços das instâncias sob demanda

Cotas de instância sob demanda

Há cotas para o número de instâncias sob demanda em execução por Conta da AWS por região. As cotas de instância sob demanda são gerenciadas em termos do número de unidades de processamento central virtual (vCPUs) que as instâncias sob demanda em execução estão usando, independentemente do tipo de instância. Cada tipo de cota especifica o número máximo de vCPUs para uma ou mais famílias de instâncias.

Sua conta inclui as cotas apresentadas a seguir para as instâncias sob demanda. As instâncias que estão nos estados pendente, em interrupção, interrompida e hibernada não entram na contagem das cotas de instância sob demanda. Reservas de capacidade entram na contagem das cotas de instância sob demanda, mesmo que não sejam utilizadas.

Name	Padrão	Ajustável
Execução de instâncias DL sob demanda	0	Sim
Execução de instâncias F sob demanda	0	Sim
Execução de instâncias G e VT sob demanda	0	Sim
Executar todas as instâncias HPC sob demanda	0	Sim
Executar instâncias com mais memória sob demanda	0	Sim
Execução de instâncias Inf sob demanda	0	Sim
Execução de instâncias P sob demanda	0	Sim
Execução de instâncias padrão sob demanda (A, C, D, H, I, M, R, T, Z)	5	Sim
Executar instâncias Trn sob demanda	0	Sim
Execução de instâncias X sob demanda	0	Sim

Para obter informações sobre as diferentes famílias, gerações e tamanhos de instâncias, consulte o Guia de tipos de instância do Amazon EC2.

É possível executar qualquer combinação de tipos de instância que atenda às necessidades em constante mudança da sua aplicação, desde que o número de vCPUs não exceda a cota da sua conta. Por exemplo: com uma cota de instância padrão de 256 vCPUs, é possível iniciar 32 instâncias `m5.2xlarge` (32 x 8 vCPUs) ou 16 instâncias `c5.4xlarge` (16 x 16 vCPUs). Para mais informações, consulte Limites de instância sob demanda do EC2.

Tarefas

- Monitorar cotas e uso de instância sob demanda
- Solicitar um aumento da cota

Monitorar cotas e uso de instância sob demanda

É possível visualizar e gerenciar suas cotas de instância sob demanda usando os métodos a seguir.

Para visualizar as cotas atuais usando o console do Service Quotas

1. Abra o console do Service Quotas em https://console.aws.amazon.com/servicequotas/home/services/ec2/quotas/.
2. Na barra de navegação, selecione uma região.
3. No campo de filtro, insira **`On-Demand`**.
4. A coluna Valor da cota aplicada exibe o número máximo de vCPUs para cada tipo de cota de instância sob demanda da sua conta.

Para visualizar as cotas atuais usando o console do AWS Trusted Advisor

Abra a página Limites do serviço no console do AWS Trusted Advisor.

Para configurar os alarmes do CloudWatch

Com a integração de métricas do Amazon CloudWatch, é possível monitorar o uso do EC2 em relação às cotas. Também é possível configurar alarmes para alertar quando estiver chegando próximo da cota. Para obter mais informações, consulte Alarmes do Service Quotas e do Amazon Cloudwatch no Guia do usuário do Service Quotas.

Solicitar um aumento da cota

Mesmo que o Amazon EC2 aumente automaticamente suas cotas de instância sob demanda com base em seu uso, é possível solicitar um aumento de cota, se for o caso. Por exemplo, se você pretender iniciar mais instâncias do que o permitido por sua cota atual, é possível solicitar um aumento de cota usando console do Service Quotas, descrito em Service Quotas do Amazon EC2.

Consulte os preços das instâncias sob demanda

É possível usar a API do serviço de lista de preços ou a API da lista de preços da AWS para consultar os preços de instâncias sob demanda. Para obter mais informações, consulte Uso da API da lista de preços da AWS no Guia do usuário do AWS Billing.

Visão geral de instâncias reservadas para o Amazon EC2

> **Important**
>
> Recomendamos utilizar Savings Plans em vez de instâncias reservadas. Os Savings Plans são a maneira mais fácil e flexível de economizar dinheiro em seus custos de computação da AWS e oferecem preços mais baixos (até 72% de desconto sobre os preços sob demanda), assim como as instâncias reservadas. No entanto, os Savings Plans são diferentes das instâncias reservadas. Com as instâncias reservadas, você se compromete com uma configuração de instância específica, enquanto que com Savings Plans você tem a flexibilidade de usar as configurações de instância que melhor atendam às suas necessidades. Para usar o Savings Plans, você se compromete com uma quantidade consistente de uso, medida em USD por hora. Para obter mais informações, consulte o Guia do usuário do AWS Savings Plans.

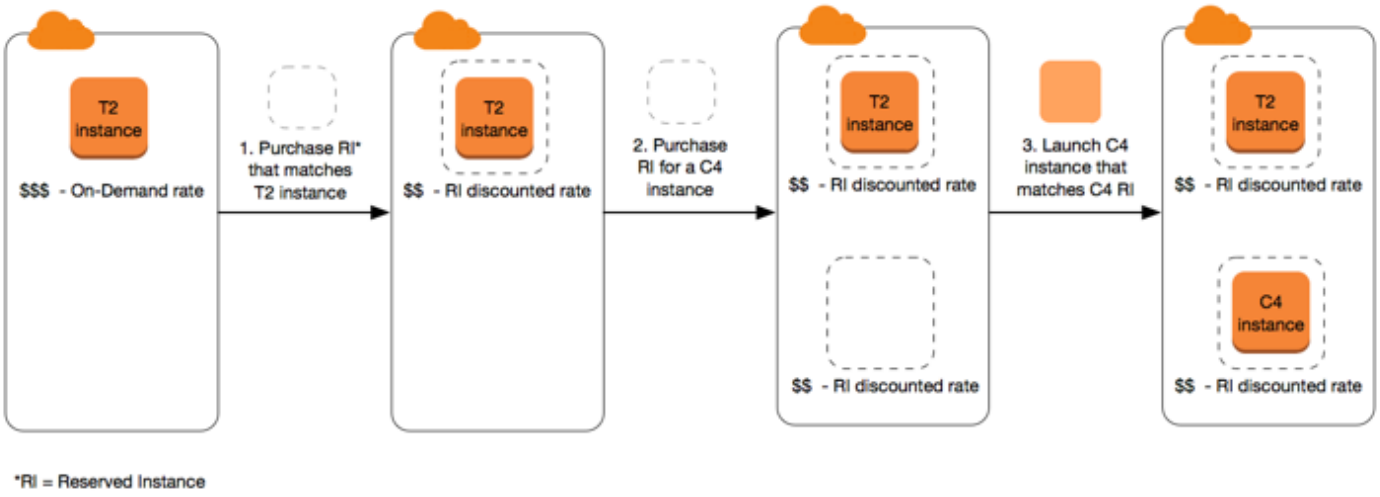
As instâncias reservadas proporcionam economia significativa em seus custos do Amazon EC2 em comparação com os preços de instâncias sob demanda. As instâncias reservadas não são instâncias físicas, mas um desconto na fatura aplicado na sua conta pelo uso de instâncias sob demanda. Essas Instâncias on-demand devem corresponder a determinados atributos, como o tipo de instância e a região, para que você possa aproveitar os benefícios do desconto de faturamento.

Tópicos de Instâncias reservadas

- Exemplo de cenário de instâncias reservadas
- Principais variáveis que determinam a definição de preço da Instância reservada
- Instâncias reservadas regionais e zonais (escopo)
- Tipos de Instâncias reservadas (classes de oferta)
- Como descontos em instâncias reservadas são aplicados
- Use as suas Instâncias reservadas
- Como o faturamento funciona com instâncias reservadas
- Comprar instâncias reservadas para o Amazon EC2
- Vender instâncias reservadas para o Amazon EC2 no Marketplace de instâncias reservadas
- Modificar a Instâncias reservadas
- Trocar Instâncias reservadas conversíveis
- Cotas de instâncias reservadas

Exemplo de cenário de instâncias reservadas

O diagrama a seguir mostra um cenário básico da compra e do uso de instâncias reservadas.



Neste cenário, você tem uma instância sob demanda (T2) em execução na sua conta, pela qual paga atualmente as tarifas sob demanda. Você compra uma Instância reservada que corresponde aos atributos da instância em execução, e o benefício do faturamento é aplicado imediatamente. Em seguida, você compra uma Instância reservada para uma instância C4. Você não tem nenhuma instância em execução na conta que corresponda aos atributos dessa Instância reservada. Na etapa final, execute uma instância que corresponda aos atributos da Instância reservada C4 para que o benefício do faturamento seja aplicado imediatamente.

Principais variáveis que determinam a definição de preço da Instância reservada

A definição de preço de Instância reservada é determinada pelas principais variáveis a seguir.

Atributos da instância

Uma instância reservada tem quatro atributos de instância que determinam seu preço.

- Tipo de instância: Por exemplo, `m4.large`. Isso é composto pela família de instâncias (por exemplo, `m4`) e pelo tamanho da instância (por exemplo, `large`).
- Região: a região na qual a Instância reservada é comprada.
- Locação: Se sua instância é executada em hardware compartilhado (padrão) ou com grupo de usuários único (dedicado). Para obter mais informações, consulte Instâncias dedicadas do Amazon EC2.
- Plataforma: O sistema operacional; por exemplo, Windows ou Linux/Unix. Para obter mais informações, consulte Escolher uma plataforma.

Compromisso com o período de vigência

É possível comprar uma Instância reservada para um compromisso de um ou três anos, sendo que há um grande desconto para o compromisso de três anos.

- Um ano: o compromisso de um ano é definido como 31536000 segundos (365 dias).
- Três anos: o compromisso de três anos é definido como 94608000 segundos (1095 dias).

As Instâncias reservadas não são renovadas automaticamente; quando elas expiram, é possível 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.

> **Important**
>
> Após adquirir uma Instância reservada, você não poderá cancelar a compra. Contudo, será possível modificar, trocar ou vender a Instância reservada caso suas necessidades mudem.

Opções de pagamento

As seguintes opções de pagamento estão disponíveis para Instâncias reservadas:

- Pagamento adiantado integral: o pagamento integral é feito no início do período de vigência, sem outros custos ou cobranças por hora incorridos pelo restante do período, independentemente das horas usadas.
- Adiantamento parcial: uma parte do custo deve ser paga adiantada, e as horas restantes do período de vigência são faturadas em uma taxa por hora com desconto, independentemente de a Instância reservada estar ou não sendo usada.
- Sem pagamento adiantado: é cobrada a tarifa por hora com desconto para cada hora do período de vigência, independentemente de a Instância reservada estar ou não sendo usada. Nenhum pagamento adiantado é necessário.

> **Note**
>
> As Instâncias reservadas sem pagamento adiantado têm como base uma obrigação contratual de pagamento mensal pelo período de vigência da reserva. Por esse motivo,

é necessário ter um histórico de faturamento de sucesso para que seja possível comprar Instâncias reservadas sem pagamento adiantado.

Em linhas gerais, é possível economizar mais ao fazer um pagamento adiantado maior pelas Instâncias reservadas. Também é possível encontrar instâncias reservadas oferecidas por vendedores terceirizados a preços menores e períodos de vigência mais curtos no Marketplace de instâncias reservadas. Para obter mais informações, consulte Vender instâncias reservadas para o Amazon EC2 no Marketplace de instâncias reservadas.

Classe de oferta

Se sua computação precisar de uma mudança, você talvez consiga modificar ou trocar a Instância reservada, dependendo da classe de oferta.

- Padrão: fornece o desconto mais significativo, mas só pode ser modificada. As Instâncias reservadas não podem ser alteradas.
- Conversível: fornece um desconto menor que o das Instâncias reservadas padrão, mas pode ser trocada por outra Instância reservada conversível com atributos de instância diferentes. As Instâncias reservadas conversíveis também podem ser modificadas.

Para obter mais informações, consulte Tipos de Instâncias reservadas (classes de oferta).

Important

Após adquirir uma Instância reservada, você não poderá cancelar a compra. Contudo, será possível modificar, trocar ou vender a Instância reservada caso suas necessidades mudem.

Para obter mais informações, consulte a página Definição de preço de instâncias reservadas do Amazon EC2.

Instâncias reservadas regionais e zonais (escopo)

Ao comprar uma Instância reservada, você determina o escopo da Instância reservada. O escopo pode ser regional ou zonal.

- Regional: quando você compra uma Instância reservada para uma região, ela é chamada de Instância reservada regional.

- Zonal: quando você compra uma Instância reservada para uma zona de disponibilidade específica, ela é chamada de Instância reservada zonal.

O escopo não afeta o preço. Você paga o mesmo preço por um Instância reservada regional ou zonal. Para obter mais informações sobre Instância reserva da definição de preço, consulte Principais variáveis que determinam a definição de preço da Instância reservada and Definição de preço de instâncias reservadas do Amazon EC2.

Para saber mais sobre como especificar o escopo de uma instância reservada, consulte Atributos da RI, especificamente o marcador Zona de disponibilidade.

Diferenças entre Instâncias reservadas regionais e zonais

A tabela a seguir destaca algumas das principais diferenças entre regionais Instâncias reservadas e zonais Instâncias reservadas:

	Instâncias reservadas regionais	Instâncias reservadas zonais
Capacidade de reservar capacidade	Uma Instância reservada regional não reserva capacidade.	Uma Instância reservada zonal reserva capacidade na zona de disponibilidade especificada.
Flexibilidade da zona de disponibilidade	O desconto da Instância reservada se aplica ao uso da instância em qualquer zona de disponibilidade na região especificada.	Sem flexibilidade da zona de disponibilidade — o desconto da Instância reservada se aplica ao uso da instância somente na zona de disponibilidade especificada.
Flexibilidade de tamanho da instância	O desconto da Instância reservada se aplica ao uso da instância na família de instâncias, independentemente do tamanho.	Sem flexibilidade de tamanho da instância — o desconto da Instância reservada se aplica ao uso da instância somente

	Instâncias reservadas regionais	Instâncias reservadas zonais
	Compatível somente com Instâncias reservadas de Linux/Unix da Amazon com locação padrão. Para obter mais informações, consulte Flexibilidade de tamanho da instância determinada pelo fator de normalização.	para o tamanho e o tipo de instância especificados.
Enfileiramento de uma compra	É possível enfileirar compras para instâncias reservadas regionais.	Você não pode enfileirar compras para instâncias reservadas zonais.

Para obter mais informações e exemplos, consulte Como descontos em instâncias reservadas são aplicados.

Tipos de Instâncias reservadas (classes de oferta)

A classe de oferta de uma Instância reservada é padrão ou conversível. Uma Instância reservada padrão oferece um desconto mais significativo do que uma Instância reservada conversível, mas você não pode trocar uma Instância reservada padrão. É possível trocar Instâncias reservadas conversíveis. É possível modificar Instâncias reservadas padrão e conversíveis.

A configuração de uma Instância reservada compreende um único tipo de instância, plataforma, escopo e locação ao longo de um termo. Se as suas necessidades de computação mudarem, talvez seja possível modificar ou trocar a sua Instância reservada.

Diferenças entre Instâncias reservadas padrão e conversível

A seguir estão as diferenças entre as classes de oferta da Instâncias reservadas padrão e conversível.

	Instância reservada padrão	Convertible Reserved Instance
Modificar a Instâncias reservadas	Alguns atributos podem ser modificados. Para obter mais informações, consulte Modificar a Instâncias reservadas.	Alguns atributos podem ser modificados. Para obter mais informações, consulte Modificar a Instâncias reservadas.
Trocar instâncias reservadas	Não pode ser trocada.	Pode ser trocada durante o período de vigência por outra Instância reservada convertível com novos atributos, incluindo a família de instâncias, o tipo de instância, a plataforma, o escopo ou a locação. Para obter mais informações, consulte Trocar Instâncias reservadas conversíveis.
Vender no Marketplace de instâncias reservadas	Pode ser vendida no Marketplace de instâncias reservadas.	Não pode ser vendida no Marketplace de instâncias reservadas.
Comprar no marketplace de instâncias reservadas	Pode ser comprada no Marketplace de instâncias reservadas.	Não pode ser comprada no Marketplace de instâncias reservadas.

Como descontos em instâncias reservadas são aplicados

As instâncias reservadas não são instâncias físicas, mas um desconto na fatura aplicado às instâncias sob demanda em execução em sua conta. As instâncias sob demanda devem atendem a determinadas especificações de instâncias reservadas para que possam se beneficiar do desconto na fatura.

Se você adquirir uma instância reservada e já tiver uma instância sob demanda em execução que atenda às especificações e instância reservada, o desconto na fatura será aplicado

automaticamente. Você não tem de reiniciar suas instâncias. Se você não tiver uma instância sob demanda qualificada em execução, inicie uma instância sob demanda com as mesmas especificações da instância reservada Para obter mais informações, consulte Use as suas Instâncias reservadas.

A classe de oferta (padrão ou conversível) da instância reservada não afeta a forma como o desconto da fatura é aplicado.

Tópicos

- Como as Instâncias reservadas zonais são aplicadas
- Como as Instâncias reservadas regionais são aplicadas
- Flexibilidade de tamanho da instância
- Exemplos de aplicação da Instâncias reservadas

Como as Instâncias reservadas zonais são aplicadas

Uma instância reservada que é comprada para reservar capacidade em uma zona de disponibilidade específica é denominada instância reservada zonal.

- O desconto de instância reservada se aplica ao uso correspondente da instância nessa zona de disponibilidade.
- 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.

Por exemplo, se você tiver adquirido duas instâncias reservadas de locação padrão `c4.xlarge` na zona de disponibilidade us-east-1a, até duas instâncias do 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.

Como as Instâncias reservadas regionais são aplicadas

Uma instâncias reservada comprada para uma região é denominada instância reservada regional e fornece flexibilidade de zona de disponibilidade e tamanho de instância.

- O desconto da Instância reservada se aplica ao uso da instância em qualquer zona de disponibilidade nessa região.

- O desconto da instância reservada se aplica ao uso da instância na família de instâncias, independentemente do tamanho; isso é conhecido como flexibilidade de tamanho de instância.

Flexibilidade de tamanho da instância

Com a flexibilidade de tamanho de instâncias, o desconto de instâncias reservadas aplica-se ao uso de instâncias que têm a mesma família. A instância reservada é aplicada do menor para o maior tamanho de instância na família de instâncias com base no fator de normalização. Para obter um exemplo de como o desconto de instância reservada é aplicado, consulte Cenário 2: Instâncias reservadas em uma única conta usando o fator de normalização.

Limitações

- Com suporte: só há suporte para a flexibilidade do tamanho da instância para instâncias reservadas regionais.
- Sem suporte: a flexibilidade do tamanho da instância não tem suporte nas seguintes instâncias reservadas:
  - Instâncias reservadas compradas para uma zona de disponibilidade específica (Instâncias reservadas zonal)
  - Instâncias reservadas para instâncias G4ad, G4dn, G5, G5g, G6, G6e, G6f, Gr6, Gr6f, hpc7a, P5, Inf1, Inf2, u7i-6tb e u7i-8tb
  - Instâncias reservadas para Windows Server, Windows Server com SQL Standard, Windows Server com SQL Server Enterprise, Windows Server com SQL Server Web, RHEL e SUSE Linux Enterprise Server
  - Instâncias reservadas com locação dedicada

Flexibilidade de tamanho da instância determinada pelo fator de normalização

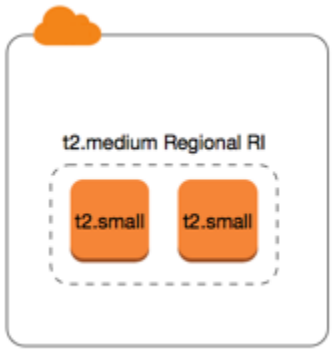
A flexibilidade de tamanho da instância é determinada pelo fator de normalização do tamanho da instância. O desconto se aplica total ou parcialmente às instâncias em execução da mesma família de instâncias, dependendo do tamanho da instância da reserva, em qualquer zona de disponibilidade na região. Os únicos atributos que devem ser correspondentes são a locação, a plataforma e a família de instâncias.

A tabela a seguir descreve os diferentes tamanhos em uma família de instâncias e o fator de normalização correspondente. Essa escala é usada para aplicar a taxa de desconto de Instâncias reservadas ao uso normalizado da família de instâncias.

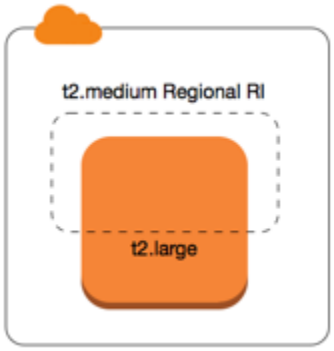
Tamanho da instância	Fator de normalização
nano	0.25
micro	0,5
small	1
medium	2
large	4
xlarge	8
2xlarge	16
3xlarge	24
4xlarge	32
6xlarge	48
8xlarge	64
9xlarge	72
10xlarge	80
12xlarge	96
16xlarge	128
18xlarge	144
24xlarge	192
32xlarge	256
48xlarge	384
56xlarge	448

Tamanho da instância	Fator de normalização
112xlarge	896

Por exemplo, uma instância `t2.medium` tem um fator de normalização de 2. Se você tiver adquirido uma Instância reservada `t2.medium` de Linux/Unix da Amazon de locação padrão na US East (N. Virginia) e tiver duas instâncias `t2.small` em execução em sua conta nessa região, o benefício de faturamento será aplicado integralmente às duas instâncias.



Ou, se você tiver uma instância `t2.large` em execução em sua conta na região US East (N. Virginia) o benefício de faturamento será aplicado a 50% do uso da instância.



O fator de normalização é aplicado também ao modificar Instâncias reservadas. Para obter mais informações, consulte Modificar a Instâncias reservadas.

Fator de normalização para instâncias bare metal

A flexibilidade de tamanho da instância também se aplica a instâncias bare metal na família de instâncias. Se você tem Instâncias reservadas regionais de Linux/Unix da Amazon com locação compartilhada em instâncias bare metal, é possível se beneficiar das economias de Instância reservada na mesma família de instâncias. O inverso também é verdadeiro: se você tem Instâncias

reservadas regionais de Linux/Unix da Amazon com locação compartilhada em instâncias na mesma família que uma instância bare metal, é possível se beneficiar das economias de Instância reservada na instância bare metal.

O tamanho da instância `metal` não tem um único fator de normalização. Uma instância bare metal tem o mesmo fator de normalização que o tamanho de instância virtualizada equivalente na mesma família de instâncias. Por exemplo, uma instância `i3.metal` tem o mesmo fator de normalização que uma instância `i3.16xlarge`.

Tamanho da instância	Fator de normalização
`a1.metal`	32
`m5zn.metal` | `x2iezn.metal` `z1d.metal`	96
`c6g.metal` | `c6gd.metal` | `i3.metal` | `m6g.metal` | `m6gd.metal` | `r6g.metal` | `r6gd.metal` | `x2gd.metal`	128
`c5n.metal`	144
`c5.metal` | `c5d.metal` | `i3en.metal` | `m5.metal` | `m5d.metal` | `m5dn.metal` | `m5n.metal` | `r5.metal` | `r5b.metal` | `r5d.metal` | `r5dn.metal` | `r5n.metal`	192
`c6i.metal` | `c6id.metal` | `m6i.metal` | `m6id.metal` | `r6d.metal` | `r6id.metal`	256
`u-18tb1.metal` | `u-24tb1.metal`	448
`u-6tb1.metal` | `u-9tb1.metal` | `u-12tb1.metal`	896

Por exemplo, uma instância `i3.metal` tem um fator de normalização de 128. Se você comprar uma Instância reservada `i3.metal` de Linux/Unix da Amazon de locação padrão na US East (N. Virginia), o benefício de faturamento poderá ser aplicado da seguinte maneira:

- Se você tem uma instância `i3.16xlarge` em execução em sua conta nessa região, o benefício de faturamento é aplicado integralmente à instância `i3.16xlarge` (fator de normalização da `i3.16xlarge` = 128).

- Ou, se você tem duas instâncias `i3.8xlarge` em execução em sua conta nessa região, o benefício de faturamento é aplicado integralmente a ambas as instâncias `i3.8xlarge` (fator de normalização da `i3.8xlarge` = 64).
- Ou, se você tem quatro instâncias `i3.4xlarge` em execução em sua conta nessa região, o benefício de faturamento é aplicado integralmente a todas as quatro instâncias `i3.4xlarge` (fator de normalização da `i3.4xlarge` = 32).

O inverso também é verdadeiro. Por exemplo, se você comprar duas Instâncias reservadas `i3.8xlarge` de Linux/Unix da Amazon de locação padrão na US East (N. Virginia) e tiver uma instância `i3.metal` em execução nessa região, o benefício de faturamento será aplicado integralmente à instância `i3.metal`.

Exemplos de aplicação da Instâncias reservadas

Os cenários a seguir abrangem as maneiras como as Instâncias reservadas são aplicadas.

- Cenário 1: Instâncias reservadas em uma única conta
- Cenário 2: Instâncias reservadas em uma única conta usando o fator de normalização
- Cenário 3: Instâncias reservadas regionais em contas vinculadas
- Cenário 4: Instâncias reservadas zonais em uma conta vinculada

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 completo de faturamento de uso das duas instâncias `m4.xlarge`.
- A Instância reservada `c4.large` regional em us-east-1 fornece flexibilidade de zona de disponibilidade e de tamanho da instância, pois é uma Instância reservada Amazon Linux regional com locação padrão e se aplica à instância `c4.xlarge`. Uma instância `c4.large` é equivalente a 4 unidades normalizadas/hora e a uma `c4.xlarge` é equivalente a 8 unidades normalizadas/hora.

  Nesse caso, a `c4.large` Instância reservada regional fornece benefício parcial para uso de `c4.xlarge`. Isso ocorre porque a Instância reservada `c4.large` equivale a 4 unidades normalizadas/hora de uso, mas a instância `c4.xlarge` requer 8 unidades normalizadas/hora. Portanto, o desconto de faturamento da Instância reservada `c4.large` aplica-se a 50% do uso de `c4.xlarge`. O uso `c4.xlarge` restante é cobrado na tarifa sob demanda.

Cenário 2: Instâncias reservadas em uma única conta usando o fator de normalização

Você está executando as seguintes Instâncias on-demand na conta A:

- 2 x instâncias do Amazon Linux `m3.xlarge` de locação padrão na zona de disponibilidade us-east-1b
- 2 x instâncias do Amazon Linux `m3.large` de locação padrão na zona de disponibilidade us-east-1b

Você adquire as seguintes Instâncias reservadas na conta A:

- 1 x Instância reservada `m3.2xlarge` de locação padrão do Amazon Linux na região us-east-1

Os benefícios da Instância reservada são aplicados da seguinte maneira:

- A Instância reservada regional `m3.2xlarge` 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 . Ele se aplica primeiro às instâncias `m3.large` e, em seguida, às instâncias `m3.xlarge`, porque a aplicação é do menor para o maior tamanho de instância na família de instâncias com base no fator de normalização.

  Uma instância `m3.large` é equivalente a 4 unidades normalizadas/hora.

  Uma instância `m3.xlarge` é equivalente a 8 unidades normalizadas/hora.

  Uma instância `m3.2xlarge` é equivalente a 16 unidades normalizadas/hora.

  O benefício é aplicado da seguinte forma:

  A instância reservada regional `m3.2xlarge` oferece total benefício para uso de 2 x `m3.large`, porque juntas essas instâncias representam 8 unidades normalizadas/hora. Isso deixa 8 unidades normalizadas/hora para serem aplicadas às instâncias `m3.xlarge`.

  Com as restantes 8 unidades/hora normalizadas, a instância reservada regional `m3.2xlarge` oferece total benefício para uso de 1 x `m3.xlarge`, porque cada instância `m3.xlarge` é equivalente a 8 unidades normalizadas/hora. O uso `m3.xlarge` restante é cobrado na tarifa sob demanda.

Cenário 3: 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. Para Instâncias reservadas regionais que oferecem flexibilidade de tamanho de instância, o benefício é aplicado do menor para o maior tamanho de instância na família de instâncias.

Você está executando a seguinte Instâncias on-demand na conta A (a conta de compra):

- 2 x instâncias do Linux `m4.xlarge` de locação padrão na zona de disponibilidade us-east-1a

- 1 x instâncias do Linux `m4.2xlarge` de locação padrão na zona de disponibilidade us-east-1b
- 2 x instâncias do Linux `c4.xlarge` de locação padrão na zona de disponibilidade us-east-1a
- 1 x instâncias do Linux `c4.2xlarge` de locação padrão na zona de disponibilidade us-east-1b

Outro cliente está executando as seguintes Instâncias on-demand na conta B — uma conta vinculada:

- 2 x instâncias do Linux `m4.xlarge` de locação padrão na zona de disponibilidade us-east-1a

Você adquire as seguintes Instâncias reservadas regionais na conta A:

- 4 x Instâncias reservadas `m4.xlarge` de locação padrão do Linux na região us-east-1
- 2 x Instâncias reservadas `c4.xlarge` de locação padrão do Linux na região us-east-1

Os benefícios da Instância reservada regional são aplicados da seguinte maneira:

- O desconto das quatro Instâncias reservadas `m4.xlarge` é usado pelas duas instâncias `m4.xlarge` e pela única instância `m4.2xlarge` na conta A (conta de compra). Todas as três instâncias têm atributos correspondentes (locação, plataforma região e família de instâncias). O desconto é aplicado às instâncias da conta de compra (conta A) primeiro, mesmo que a conta B (conta vinculada) tenha duas `m4.xlarge` que também correspondam às Instâncias reservadas. Não há reserva de capacidade, pois as Instâncias reservadas são regionais Instâncias reservadas.
- O desconto das duas Instâncias reservadas `c4.xlarge` se aplica às duas instâncias `c4.xlarge`, porque eles são um tamanho de instância menor que a instância `c4.2xlarge`. Não há reserva de capacidade, pois as Instâncias reservadas são regionais Instâncias reservadas.

Cenário 4: 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 Understanding your reservations no AWS Cost and Usage Report.

> **Note**
>
> As instâncias reservadas de zona reservam capacidade somente para a conta proprietária e não podem ser compartilhadas com outras Contas da AWS. Se você precisar compartilhar a capacidade com outras Contas da AWS, use Reservar capacidade computacional com reservas de capacidade sob demanda do EC2.

Use as suas Instâncias reservadas

As Instâncias reservadas são aplicadas automaticamente às Instâncias on-demand em execução, desde que as especificações sejam correspondentes. Se você não tiver nenhuma Instâncias on-demand que corresponda às especificações de sua Instância reservada, a Instância reservada não será utilizada até que você execute uma instância com as especificações necessárias.

Se você estiver iniciando uma instância para aproveitar o benefício de fatura de uma instância reservada, especifique as informações a seguir quando configurar a instância sob demanda:

Plataforma

Especifique 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` para a instância reservada, pode iniciar uma instância de uma AMI do Amazon Linux AMI ou do Ubuntu.

Tipo de instância

Se você comprou uma instância reservada zonal, especifique o mesmo tipo de instância da instância reservada; por exemplo, `t3.large`. Para obter mais informações, consulte Como as Instâncias reservadas zonais são aplicadas.

Se você comprou uma instância reservada regional, deverá especificar um tipo de instância da mesma família de instâncias que o tipo de instância da instância reservada. Por exemplo, se você tiver especificado `t3.xlarge` para a instância reservada, deverá iniciar a instância na família T3, mas poderá especificar qualquer tamanho, por exemplo, `t3.medium`. Para obter mais informações, consulte Como as Instâncias reservadas regionais são aplicadas.

Zona de disponibilidade

Se você adquiriu uma instância reservada para uma zona de disponibilidade específica, deve iniciar a instância na mesma zona de disponibilidade.

Se adquiriu uma instância reservada regional, pode iniciar a instância em qualquer zona de disponibilidade da região que especificou para a instância reservada.

Locação

A locação (`dedicated` ou `shared`) da instância deve corresponder à locação da instância reservada. Para obter mais informações, consulte Instâncias dedicadas do Amazon EC2.

Para obter exemplos de como as instâncias reservadas são aplicadas às instâncias sob demanda em execução, consulte Como descontos em instâncias reservadas são aplicados. Para obter mais informações, consulte Por que minhas instâncias reservadas do Amazon EC2 não estão sendo aplicadas à minha fatura da AWS da forma que eu esperava?

É possível usar vários métodos para iniciar as instâncias sob demanda que usem o desconto de instância reservada. Para obter informações sobre os diferentes métodos de lançamento, consulte Iniciar uma instância do Amazon EC2. É possível usar o Amazon EC2 Auto Scaling para iniciar instâncias dedicadas. Para mais informações, consulte o Guia do usuário do Amazon EC2 Auto Scaling.

Como o faturamento funciona com instâncias reservadas

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. É possível optar por pagar pela Instância reservada adiantado, parcialmente adiantado ou mensalmente, dependendo da opção de pagamento especificada para a Instância reservada.

Quando as Instâncias reservadas expirarem, serão cobradas taxas sob demanda pelo uso da instância do EC2. É possível colocar uma Instância reservada em uma fila para compra por até três anos de maneira antecipada. Isso pode ajudar a garantir que você tenha cobertura ininterrupta. Para obter mais informações, consulte Enfileirar sua compra.

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, o preço padrão será cobrado. Para mais informações, consulte Nível gratuito da AWS.

Conteúdo

- Faturamento do uso
- Visualizar sua fatura
- Instâncias reservadas e faturamento consolidado
- Níveis de definição de preço com desconto da Instância reservada

Faturamento do uso

As Instâncias reservadas são cobradas a cada hora fechada durante o período de vigência selecionado, independentemente de uma instância estar sendo executada ou não. Cada hora

fechada começa na hora (zero minutos e zero segundos após a hora) de um relógio padrão de 24 horas. Por exemplo, 1:00:00 a 1:59:59 é uma hora fechada. Para obter mais informações sobre os estados da instância, consulte Alterações do estado de instâncias do Amazon EC2.

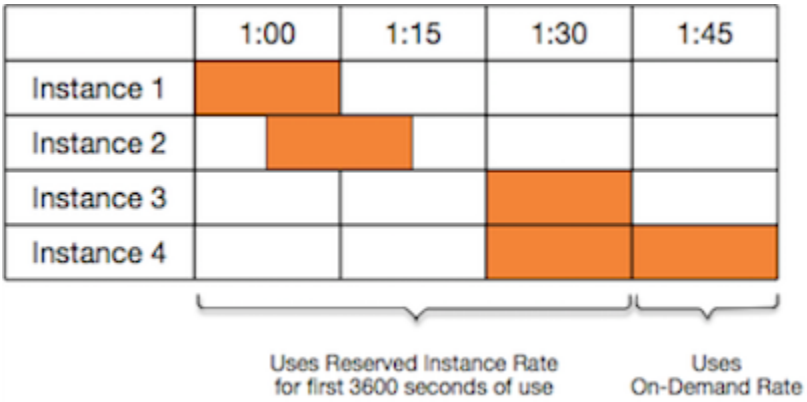
Um benefício do faturamento de Instância reservada pode ser aplicado a uma instância em execução com base em uma taxa por segundo. O faturamento por segundo está disponível para instâncias que usam uma distribuição de código aberto do Linux, como o Amazon Linux e o Ubuntu. O faturamento por hora é usado para distribuições comerciais do Linux, como o Red Hat Enterprise Linux e o SUSE Linux Enterprise Server.

Um dos benefícios de faturamento da Instância reservada pode ser aplicado a um máximo de 3600 segundos (uma hora) de uso de instância por hora fechada. É possível executar várias instâncias simultaneamente, mas só pode receber o benefício do desconto de Instância reservada por um total de 3600 segundos por hora. O uso de instância que ultrapassar 3600 segundos em uma hora será faturado com base na taxa sob demanda.

Por exemplo, se você adquirir uma Instância reservada `m4.xlarge` e executar quatro instâncias `m4.xlarge` simultaneamente por uma hora, uma instância será cobrada em uma hora de uso de Instância reservada, enquanto as outras três instâncias serão cobradas em três horas de uso sob demanda.

Contudo, se você adquirir uma Instância reservada `m4.xlarge` e executar quatro instâncias `m4.xlarge` por 15 minutos (900 segundos) cada uma 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.

Se várias instâncias qualificadas estiverem sendo executadas simultaneamente, o benefício de faturamento de Instância reservada será aplicado a todas as instâncias ao mesmo tempo até um máximo de 3600 segundos em uma hora. Depois disso, serão cobradas taxas sob demanda.



O Cost Explorer no console do Billing and Cost Management permite que você analise as economias com base nas Instâncias on-demand em execução. As perguntas frequentes sobre Instâncias reservadas incluem um exemplo de um cálculo de valor de tabela.

Se você fechar sua conta na AWS, o faturamento sob demanda dos seus recursos será interrompido. Contudo, se você tiver Instâncias reservadas na conta, continuará recebendo a fatura delas até que elas expirem.

Visualizar sua fatura

Você encontrará mais informações sobre as cobranças e as taxas da sua conta ao visualizar o console do AWS Billing and Cost Management.

- O Painel exibe um resumo de gastos da sua conta.
- Na página Bills (Faturas), em Details (Detalhes), expanda a seção Elastic Compute Cloud e a região para obter informações de faturamento sobre suas Instâncias reservadas.

É possível visualizar as cobranças online ou baixar um arquivo CSV.

Também é possível monitorar a utilização da instância reservada usando o Relatório de uso e de custos da AWS. Para obter mais informações, consulte Noções básicas das suas reservas.

Instâncias reservadas e faturamento consolidado

Os benefícios da definição de preços das Instâncias reservadas são compartilhados quando a conta que faz a compra é parte de um conjunto de contas faturadas sob uma conta pagante de faturamento consolidado. O uso da instância em todas as contas-membro é agregada na conta pagante todos os meses. Em geral, isso é útil para empresas em que há equipes ou grupos funcionais diferentes; dessa forma, a lógica usual da Instância reservada é aplicada para calcular a conta. Para obter mais informações, consulte Faturamento consolidado para o AWS Organizations.

Se você fechar a conta que comprou a Instância reservada, a conta pagante será cobrada pela Instância reservada até que a instância reservada expire. Depois que a conta encerrada for excluída permanentemente em 90 dias, as contas de membro não se beneficiarão mais do desconto de faturamento da instância reservada.

> **Note**
>
> As instâncias reservadas de zona reservam capacidade somente para a conta proprietária e não podem ser compartilhadas com outras Contas da AWS. Se você precisar compartilhar a capacidade com outras Contas da AWS, use Reservar capacidade computacional com reservas de capacidade sob demanda do EC2.

Níveis de definição de preço com desconto da Instância reservada

Se sua conta se qualificar para uma camada de preços com desconto, ela receberá automaticamente descontos nas taxas de uso de instância e com pagamento adiantado nas compras de Instância reservada que você fizer nessa camada, desse ponto em diante. Para se qualificar para um desconto, o valor de tabela das Instâncias reservadas na região deverá ser de 500.000 USD ou mais.

As seguintes regras se aplicam:

- As camadas de preços e descontos relacionados aplicam-se somente às compras das Amazon EC2 padrão do Instâncias reservadas.
- As camadas de preços não se aplicam às Instâncias reservadas para Windows com SQL Server Standard, SQL Server Web e SQL Server Enterprise.
- Os níveis de preços não se aplicam a Instâncias reservadas para Linux com SQL Server de qualquer tipo.
- Os descontos do nível de preços aplicam-se somente às compras feitas pela AWS. Eles não se aplicam a compras de Instâncias reservadas de terceiros.
- As camadas de preços com desconto atualmente não são aplicáveis a compras de Instância reservada convertível.

Tópicos

- Calcular descontos de preço de Instância reservada

- Comprar com nível de desconto
- Cruzamento de níveis de definição de preço
- Faturamento consolidado para níveis de definição de preço

Calcular descontos de preço de Instância reservada

É possível determinar a camada da definição de preço de sua conta ao calcular o valor de tabela de todas as Instâncias reservadas em uma região. Multiplique o preço recorrente por hora de cada reserva pelo número total de horas do período de vigência e adicione o preço adiantado sem desconto (conhecido também como preço fixo) no momento da compra. Como o valor de tabela se no preço sem desconto (público), ele não será afetado se você se qualificar para um desconto por volume ou se o preço cair depois de você comprar suas Instâncias reservadas.

```
List value = fixed price + (undiscounted recurring hourly price * hours in term)
```

Por exemplo, para uma `t2.small` Instância reservada com adiantamento parcial de 1 ano, supõe-se que o preço inicial seja 60,00 USD e a taxa por hora seja 0,007 USD. Isso fornece um valor de tabela de 121,32 USD.

```
121.32 = 60.00 + (0.007 * 8760)
```

Para ver os valores de preço fixo das Instâncias reservadas usando o console do Amazon EC2

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Instâncias reservadas.
3. Para exibir a coluna Preço para pagamento adiantado, selecione o ícone de configurações ( ) no canto superior direito, ative Preço para pagamento adiantado e escolha Confirmar.

Para ver os valores de preço fixo das Instâncias reservadas usando a linha de comando

- describe-reserved-instances (AWS CLI)
- Get-EC2ReservedInstance (AWS Tools for Windows PowerShell)

Comprar com nível de desconto

Quando você comprar Instâncias reservadas, o Amazon EC2 aplicará automaticamente todos os descontos à parte da sua compra que estiver dentro do nível de preço com desconto. Você não precisará fazer nada diferente e poderá comprar as Instâncias reservadas usando qualquer ferramenta do Amazon EC2. Para obter mais informações, consulte Comprar instâncias reservadas para o Amazon EC2.

Depois que o valor de tabela das Instâncias reservadas ativas em uma região ultrapassar um nível de definição de preço com desconto, qualquer compra futura de Instâncias reservadas nessa região será cobrada com uma taxa com desconto. Se com uma única compra de Instâncias reservadas em uma região você ultrapassar o limite de uma camada com desconto, a parte da compra que estiver acima do limite de preço será cobrada com a taxa com desconto. Para obter mais informações sobre os IDs de Instância reservada temporária criados durante o processo de compra, consulte Cruzamento de níveis de definição de preço.

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 quatros cenários possíveis durante a compra de Instâncias reservadas:

- Sem desconto — sua compra em uma região ainda está abaixo do limite para desconto.
- Desconto parcial — sua compra em uma região ultrapassa o limite do primeiro nível de desconto. Nenhum desconto é aplicado a uma ou mais reservas e a taxa com desconto é aplicada nas reservas restantes.
- Desconto total — sua compra inteira em uma região cai em um nível de desconto e recebe o desconto apropriado.
- Duas taxas com desconto — sua compra em uma região ultrapassa um nível inferior de desconto para um nível superior de desconto. Serão cobradas duas taxas diferentes: uma ou mais reservas na taxa desconto inferior e as reservas restantes com a taxa desconto maior.

Cruzamento de níveis de definição de preço

Se sua compra cruzar um nível de preços com desconto, você verá múltiplas entradas para essa compra: uma para a parte da compra cobrada em preço normal e outra para essa a parte da compra cobrada na taxa de desconto aplicável.

O serviço Instância reservada gera vários IDs de Instância reservada porque sua compra passou de um nível sem desconto ou de um nível com desconto para outro. Há um ID para cada conjunto de reservas em um nível. Portanto, o ID retornado pelo comando de compra da CLI ou pela ação da API é diferente do ID real das novas Instâncias reservadas.

Faturamento consolidado para níveis de definição de preço

Uma conta de faturamento consolidado agrega 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.

Comprar instâncias reservadas para o Amazon EC2

Para comprar uma instância reservada para o Amazon EC2, você pode usar o console do Amazon EC2, uma ferramenta de linha de comandos ou um SDK para pesquisar 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. Ao realizar a compra de uma instância reservada de um vendedor terceirizado no Marketplace de instâncias reservadas do Amazon EC2, se houver ofertas semelhantes à sua escolha, mas com um preço inicial mais baixo, a AWS venderá para você as ofertas com preços iniciais 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. É possível enfileirar uma compra para uma data futura e cancelar a compra enfileirada antes do horário agendado.

Para comprar e modificar instâncias reservadas, certifique-se de que seu usuário tenha as permissões apropriadas, como a capacidade de descrever zonas de disponibilidade. Para obter informações, consulte the section called “Trabalhar com Instâncias reservadas” (API) ou the section called “Trabalhar com Instâncias reservadas” (console).

Tarefas

- Escolher uma plataforma
- Enfileirar sua compra
- Comprar Instâncias reservadas padrão
- Comprar Instâncias reservadas conversíveis
- Comprar do Marketplace da Instância reservada
- Como cancelar uma compra colocada na fila
- Renovar uma Instância reservada

Escolher uma plataforma

O Amazon EC2 é compatível com as seguintes plataformas para as instâncias reservadas:

- Linux/UNIX
- Linux com SQL Server Standard
- Linux com SQL Server Web
- Linux com SQL Server Enterprise
- SUSE Linux
- Red Hat Enterprise Linux
- Red Hat Enterprise Linux com HA
- Windows
- Windows com SQL Server Standard
- Windows com SQL Server Web
- Windows com SQL Server Enterprise

Considerações

- Se você trouxer sua assinatura existente (BYOS) para o Red Hat Enterprise Linux, SUSE Linux ou Ubuntu Pro, deverá escolher uma oferta para a plataforma Linux/Unix.
- Não há suporte a instâncias reservadas para instâncias que executam macOS ou Ubuntu Pro (assinatura do EC2 incluída, ou seja, não BYOS). Para economizar com os preços de instâncias sob demanda, recomendamos usar instâncias do macOS e do Ubuntu Pro (assinatura do EC2 incluída) com os Savings Plans. Para obter mais informações, consulte o Guia do usuário do Savings Plans.

Para garantir que uma instância seja executada em uma instância reservada específica, a plataforma da instância reservada deve corresponder à plataforma da AMI usada para iniciar a instância. Para AMIs do Linux, é importante verificar se a plataforma da AMI usa o valor geral Linux/UNIX ou um valor mais específico, como SUSE Linux.

Console

Para verificar a plataforma da AMI

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione AMIs.
3. Selecione a AMI.
4. Na guia Detalhes, anote o valor de Detalhes da plataforma.

AWS CLI

Para verificar a plataforma da AMI

Utilize o comando describe-images e verifique o valor de `PlatformDetails`.

```
aws ec2 describe-images \
    --image-id ami-0abcdef1234567890 \
    --query Images[*].PlatformDetails
```

O seguinte é um exemplo de saída.

```
[
    "Linux/UNIX"
```

```
]
```

PowerShell

Para verificar a plataforma da AMI

Use o cmdlet Get-EC2Image e verifique o valor de `PlatformDetails`.

```
Get-EC2Image `
    -ImageId ami-0abcdef1234567890 | `
    Select PlatformDetails
```

O seguinte é um exemplo de saída.

```
PlatformDetails
---------------
Linux/UNIX
```

Enfileirar sua compra

Por padrão, quando você compra uma Instância reservada, a compra é feita imediatamente. Se preferir, será possível colocar as compras na fila para uma data e hora futura. Por exemplo, é possível colocar uma compra na fila para o momento próximo da expiração de uma Instância reservada existente. Isso pode ajudar a garantir que você tenha cobertura ininterrupta.

É possível colocar compras na fila para uma Instâncias reservadas regional, mas não para uma Instâncias reservadas zonal ou uma Instâncias reservadas de outros vendedores. É possível colocar uma compra na fila por até três anos de maneira antecipada. Na data e hora programadas, a compra será executada usando a forma de pagamento padrão. Após o pagamento ser feito com êxito, os benefícios de faturamento serão aplicados.

É possível definir uma data para suas compras enfileiradas no console do Amazon EC2, e a compra ficará enfileirada até 00:00 UTC dessa data. Para especificar um horário diferente para a compra enfileirada, use um SDK da AWS ou uma ferramenta de linha de comandos.

É possível visualizar as compras colocadas na fila no console do Amazon EC2. O status de uma compra na fila é queued (na fila). É possível cancelar uma compra na fila a qualquer momento antes da hora programada. Para obter mais detalhes, consulte Como cancelar uma compra colocada na fila.

Comprar Instâncias reservadas padrão

É possível comprar as Instâncias reservadas padrão em uma zona de disponibilidade específica e obter uma reserva de capacidade. Como alternativa, é possível abandonar a reserva de capacidade e comprar uma Instância reservada padrão regional;.

Após concluir a compra, se você já tiver uma instância em execução que corresponda às especificações da Instância reservada, o benefício de faturamento será aplicado imediatamente. Você não precisa reiniciar suas instâncias. Se você não tiver uma instância adequada em execução, inicie uma instância que atenda aos mesmos critérios especificados para a instância reservada. Para obter mais informações, consulte Use as suas Instâncias reservadas.

Para obter exemplos de como as Instâncias reservadas são aplicadas às instâncias em execução, consulte Como descontos em instâncias reservadas são aplicados.

Console

Para comprar instâncias reservadas padrão

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Reserved Instances (Instâncias reservadas) e Purchase Instâncias reservadas (Comprar Instâncias reservadas).
3. Para Offering class (Classe da oferta), escolha Standard (Padrão) para exibir as Instâncias reservadas padrão.
4. Para comprar uma reserva de capacidade, escolha Only show offerings that reserve capacity (Mostrar apenas ofertas que reservam capacidade) no canto superior direito da tela de compra. Quando você ativa essa configuração, o campo Availability Zone (Zona de disponibilidade) é exibido.

   Para comprar um Instância reservada regional, desative essa configuração. Quando você desativa essa configuração, o campo Availability Zone (Zona de disponibilidade) desaparece.
5. Selecione outras configurações conforme necessário e escolha Search (Pesquisar).
6. Para cada Instância reservada que você deseja comprar, insira a quantidade e escolha Add to cart (Adicionar ao carrinho).

   Para comprar uma instância reservada padrão no Marketplace de instâncias reservadas, procure por 3rd Party (terceiros) na coluna Seller (Vendedor) dos resultados de pesquisa. A coluna Termo exibe os termos não padrão. Para obter mais informações, consulte Comprar do Marketplace da Instância reservada.

7. Para ver um resumo das Instâncias reservadas selecionadas, escolha View cart (Visualizar carrinho).
8. Se Order on (Pedir em) for Now (Agora), a compra será concluída imediatamente após você escolher Order all (Pedir tudo). Para colocar uma compra na fila, selecione Now (Agora) e selecione uma data. É possível selecionar uma data diferente para cada oferta elegível no carrinho. A compra é enfileirada até às 00:00 UTC da data selecionada.
9. Para concluir o pedido, selecione Order all (Pedir tudo).

   Se, no momento de fazer o pedido, houver ofertas semelhantes à sua escolha, mas com um preço menor, a AWS venderá as ofertas pelo preço mais baixo.
10. Escolha Close (Fechar).

    O status do seu pedido é listado na coluna State (Estado). Quando o pedido estiver concluído, veja o valor Estado mudar de `Payment-pending` para `Active`. Quando a Instância reservada for `Active`, ela estará pronta para ser usada.

    Se o status for para `Retired`, a AWS pode não ter recebido seu pagamento.

AWS CLI

Para comprar uma instância reservada padrão

1. Localize as Instâncias reservadas disponíveis usando o comando describe-reserved-instances-offerings. Especifique `standard` para a opção `--offering-class` para retornar somente instâncias reservadas padrão. É possível aplicar critérios adicionais para restringir os resultados. Por exemplo, use o comando a seguir para comprar uma instância reservada regional `t2.large` com uma locação padrão para `Linux/UNIX` durante um período de vigência de somente 1 ano.

```
aws ec2 describe-reserved-instances-offerings \
    --instance-type t2.large \
    --offering-class standard \
    --product-description "Linux/UNIX" \
    --instance-tenancy default \
    --filters Name=duration,Values=31536000 \
              Name=scope,Values=Region
```

Para localizar as instâncias reservadas somente no Marketplace de instâncias reservadas, use o filtro `marketplace` e não especifique uma duração na solicitação, pois o período de vigência pode ser mais curto que o período de 1 ou 3 anos.

```
aws ec2 describe-reserved-instances-offerings \
    --instance-type t2.large \
    --offering-class standard \
    --product-description "Linux/UNIX" \
    --instance-tenancy default \
    --filters Name=marketplace,Values=true
```

Quando encontrar uma Instância reservada que atenda às suas necessidades, anote o ID da oferta. Por exemplo:

```
"ReservedInstancesOfferingId": "bec624df-a8cc-4aad-a72f-4f8abc34caf2"
```

2. Use o comando purchase-reserved-instances-offering para comprar sua Instância reservada. Especifique o ID de oferta da Instância reservada obtido na etapa anterior e o número de instâncias da reserva.

```
aws ec2 purchase-reserved-instances-offering \
    --reserved-instances-offering-id bec624df-a8cc-4aad-a72f-4f8abc34caf2 \
    --instance-count 1
```

Por padrão, a compra será concluída imediatamente. Se preferir, para colocar a compra na fila, adicione a opção a seguir à chamada anterior.

```
--purchase-time "2020-12-01T00:00:00Z"
```

3. Use o comando describe-reserved-instances para obter o status da Instância reservada.

```
aws ec2 describe-reserved-instances \
    --reserved-instances-ids b847fa93-e282-4f55-b59a-1342fec06327 \
    --query ReservedInstances[].State
```

PowerShell

Para comprar uma instância reservada padrão

1. Encontre as instâncias reservadas disponíveis usando o cmdlet Get-EC2ReservedInstancesOffering. Especifique `standard` para o parâmetro `-OfferingClass` apresentar somente Instâncias reservadas padrão. É possível aplicar critérios adicionais para restringir os resultados. Por exemplo, use o comando a seguir para comprar uma instância reservada regional `t2.large` com uma locação padrão para `Linux/UNIX` durante um período de vigência de somente 1 ano.

```
Get-EC2ReservedInstancesOffering `
    -InstanceType "t2.large" `
    -OfferingClass "standard" `
    -ProductDescription "Linux/UNIX" `
    -InstanceTenancy "default" `
    -Filters @{Name="duration"; Values="31536000"} `
             @{Name="scope"; Values="Region"
```

Para localizar as instâncias reservadas somente no Marketplace de instâncias reservadas, use o filtro `marketplace` e não especifique uma duração na solicitação, pois o período de vigência pode ser mais curto que o período de 1 ou 3 anos.

```
Get-EC2ReservedInstancesOffering `
    -InstanceType t2.large `
    -OfferingClass "standard" `
    -ProductDescription "Linux/UNIX" `
    -InstanceTenancy default `
    -Filters @{Name="marketplace"; Values="true"}
```

Quando encontrar uma Instância reservada que atenda às suas necessidades, anote o ID da oferta. Por exemplo:

```
bec624df-a8cc-4aad-a72f-4f8abc34caf2
```

2. Use o cmdlet New-EC2ReservedInstance para comprar sua instância reservada. Especifique o ID de oferta da Instância reservada obtido na etapa anterior e o número de instâncias da reserva.

```
New-EC2ReservedInstance `
```

```
    -ReservedInstancesOfferingId "bec624df-a8cc-4aad-a72f-4f8abc34caf2" `
    -InstanceCount 1
```

Por padrão, a compra será concluída imediatamente. Se preferir, para colocar a compra na fila, adicione o parâmetro a seguir à chamada anterior.

```
-PurchaseTime "2020-12-01T00:00:00Z"
```

3. Use o cmdlet Get-EC2ReservedInstance para obter o status da sua instância reservada.

```
Get-EC2ReservedInstance `
    -ReservedInstancesId b847fa93-e282-4f55-b59a-1342fec06327 | `
    Select State
```

Comprar Instâncias reservadas conversíveis

É possível comprar Instâncias reservadas conversíveis em uma zona de disponibilidade específica e obter uma reserva de capacidade. Como alternativa, é possível abandonar a reserva de capacidade e comprar uma Instância reservada convertível regional.

Se você já tiver uma instância em execução que corresponda às especificações da Instância reservada, o benefício de faturamento será imediatamente aplicado. Você não tem de reiniciar suas instâncias. Se você não tiver uma instância em execução adequada, execute uma instância atendendo aos mesmos critérios especificados para a Instância reservada. Para obter mais informações, consulte Use as suas Instâncias reservadas.

Para obter exemplos de como as Instâncias reservadas são aplicadas às instâncias em execução, consulte Como descontos em instâncias reservadas são aplicados.

Console

Para comprar instâncias reservadas conversíveis

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Reserved Instances (Instâncias reservadas) e Purchase Instâncias reservadas (Comprar Instâncias reservadas).
3. Em Offering class (Classe da oferta), escolha Convertible (Conversível) para exibir as Instâncias reservadas conversíveis.

4. Para comprar uma reserva de capacidade, escolha Only show offerings that reserve capacity (Mostrar apenas ofertas que reservam capacidade) no canto superior direito da tela de compra. Quando você ativa essa configuração, o campo Availability Zone (Zona de disponibilidade) é exibido.

   Para comprar um Instância reservada regional, desative essa configuração. Quando você desativa essa configuração, o campo Availability Zone (Zona de disponibilidade) desaparece.
5. Selecione outras configurações conforme o necessário e escolha Pesquisar.
6. Para cada Instância reservada convertível que você deseja comprar, insira a quantidade e escolha Add to cart (Adicionar ao carrinho).
7. Para ver um resumo da sua seleção, escolha View cart (Visualizar carrinho).
8. Se Order on (Pedir em) for Now (Agora), a compra será concluída imediatamente após você escolher Order all (Pedir tudo). Para colocar uma compra na fila, selecione Now (Agora) e selecione uma data. É possível selecionar uma data diferente para cada oferta elegível no carrinho. A compra é enfileirada até às 00:00 UTC da data selecionada.
9. Para concluir o pedido, selecione Order all (Pedir tudo).

   Se, no momento de fazer o pedido, houver ofertas semelhantes à sua escolha, mas com um preço menor, a AWS venderá as ofertas pelo preço mais baixo.
10. Escolha Close (Fechar).

    O status do seu pedido é listado na coluna State (Estado). Quando o pedido estiver concluído, veja o valor Estado mudar de `Payment-pending` para `Active`. Quando a Instância reservada for `Active`, ela estará pronta para ser usada.

    Se o status for para `Retired`, a AWS pode não ter recebido seu pagamento.

AWS CLI

Para comprar uma instância reservada conversível

1. Localize as Instâncias reservadas disponíveis usando o comando describe-reserved-instances-offerings. Especifique `convertible` para a opção `--offering-class` para retornar somente instâncias reservadas conversíveis. É possível aplicar critérios adicionais para restringir os resultados. Por exemplo, use o comando a seguir para comprar uma instância reservada regional `t2.large` com uma locação padrão para `Linux/UNIX`.

```
aws ec2 describe-reserved-instances-offerings \
    --instance-type t2.large \
    --offering-class convertible \
    --product-description "Linux/UNIX" \
    --instance-tenancy default \
    --filters Name=scope,Values=Region
```

Quando encontrar uma Instância reservada que atenda às suas necessidades, anote o ID da oferta. Por exemplo:

```
"ReservedInstancesOfferingId": "bec624df-a8cc-4aad-a72f-4f8abc34caf2"
```

2. Use o comando purchase-reserved-instances-offering para comprar sua Instância reservada. Especifique o ID de oferta da Instância reservada obtido na etapa anterior e o número de instâncias da reserva.

```
aws ec2 purchase-reserved-instances-offering \
    --reserved-instances-offering-id bec624df-a8cc-4aad-a72f-4f8abc34caf2 \
    --instance-count 1
```

Por padrão, a compra será concluída imediatamente. Se preferir, para colocar a compra na fila, adicione a opção a seguir à chamada anterior.

```
--purchase-time "2020-12-01T00:00:00Z"
```

3. Use o comando describe-reserved-instances para obter o status da Instância reservada.

```
aws ec2 describe-reserved-instances \
    --reserved-instances-ids b847fa93-e282-4f55-b59a-1342fec06327 \
    --query ReservedInstances[].State
```

PowerShell

Para comprar uma instância reservada conversível

1. Encontre as instâncias reservadas disponíveis usando o cmdlet Get-EC2ReservedInstancesOffering. Especifique `convertible` para o parâmetro `-OfferingClass` apresentar somente Instâncias reservadas conversíveis. É possível aplicar

critérios adicionais para restringir os resultados. Por exemplo, use o comando a seguir para comprar uma instância reservada regional `t2.large` com uma locação padrão para `Linux/UNIX`.

```
Get-EC2ReservedInstancesOffering `
    -InstanceType "t2.large" `
    -OfferingClass "convertible" `
    -ProductDescription "Linux/UNIX" `
    -InstanceTenancy "default" `
    -Filters @{Name="scope"; Values="Region"
```

Quando encontrar uma Instância reservada que atenda às suas necessidades, anote o ID da oferta. Por exemplo:

```
bec624df-a8cc-4aad-a72f-4f8abc34caf2
```

2. Use o cmdlet New-EC2ReservedInstance para comprar sua instância reservada. É necessário especificar o ID da oferta de instância reservada obtido na etapa anterior e o número de instâncias da reserva.

```
New-EC2ReservedInstance `
    -ReservedInstancesOfferingId "bec624df-a8cc-4aad-a72f-4f8abc34caf2" `
    -InstanceCount 1
```

Por padrão, a compra será concluída imediatamente. Se preferir, para colocar a compra na fila, adicione o parâmetro a seguir à chamada anterior.

```
-PurchaseTime "2020-12-01T00:00:00Z"
```

3. Use o cmdlet Get-EC2ReservedInstance para obter o status da sua instância reservada.

```
Get-EC2ReservedInstance `
    -ReservedInstancesId b847fa93-e282-4f55-b59a-1342fec06327 | `
    Select State
```

Comprar do Marketplace da Instância reservada

É possível adquirir instâncias reservadas de vendedores terceiros que tenham instâncias reservadas de que não precisam mais do Marketplace de instâncias reservadas. É possível fazer isso usando o

console do Amazon EC2 ou a ferramenta da linha de comando. O processo é semelhante à compra de instâncias reservadas da AWS. Para obter mais informações, consulte Comprar Instâncias reservadas padrão.

Existem poucas diferenças entre instâncias reservadas adquiridas no Marketplace de instâncias reservadas e adquiridas diretamente da AWS:

- Período de vigência: as instâncias reservadas que você compra de terceiros têm menos que um período de vigência padrão completo restante. Os períodos de vigência completos da AWS são de um ano ou três anos.
- Preço adiantado: as instâncias reservadas de terceiros podem ser vendidas em preços adiantados diferentes. As taxas de uso ou recorrentes são as mesmas que as taxas definidas quando as instâncias reservadas foram adquiridas originalmente da AWS.
- Tipos de instâncias reservadas: somente instâncias reservadas padrão do Amazon EC2 podem ser adquiridas no Marketplace de instâncias reservadas. Instâncias reservadas conversíveis, Amazon RDS e Amazon ElastiCache não estão disponíveis para compra no Marketplace de instâncias reservadas.

Informações básicas sobre você são compartilhadas com o vendedor – por exemplo, seu código postal e as informações do país.

Essas informações permitem que os vendedores calculem os impostos de transação necessários que precisam remeter ao governo (como impostos sobre vendas ou imposto sobre valor agregado) e são fornecidas na forma de um relatório de desembolso. Em raras circunstâncias, a AWS pode ter de fornecer ao vendedor seu endereço de e-mail, de forma que possam entrar em contato com você sobre as perguntas relacionadas à venda (por exemplo, dúvidas sobre impostos).

Por motivos semelhantes, a AWS compartilha a razão social do vendedor na fatura de compra do comprador. Se você precisar de mais informações sobre o vendedor para fins de impostos ou algo relacionado, entre em contato com o Suporte.

Como cancelar uma compra colocada na fila

É possível colocar uma compra na fila por até três anos de maneira antecipada. É possível cancelar uma compra na fila a qualquer momento antes da hora programada.

Console

Como cancelar uma compra colocada na fila

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Instâncias reservadas.
3. Selecione uma ou mais Instâncias reservadas.
4. Selecione Actions (Ações), Delete Queued Reserved Instances (Excluir instâncias reservadas na fila).
5. Quando a confirmação for solicitada, insira Delete (Excluir) e escolha Close (Fechar).

AWS CLI

Como cancelar uma compra colocada na fila

Use o comando delete-queued-reserved-instances.

```
aws ec2 delete-queued-reserved-instances \
    --reserved-instances-ids b847fa93-e282-4f55-b59a-1342fec06327
```

PowerShell

Como cancelar uma compra colocada na fila

Use o cmdlet Remove-EC2QueuedReservedInstance.

```
Remove-EC2QueuedReservedInstance `
    -ReservedInstancesId b847fa93-e282-4f55-b59a-1342fec06327
```

Renovar uma Instância reservada

É possível renovar uma Instância reservada antes que ela esteja programada para expirar. Renovar uma Instância reservada coloca a compra de uma Instância reservada na fila com a mesma configuração até que a Instância reservada atual expire.

Você deve renovar uma instância Reservada usando o console do Amazon EC2.

Para renovar uma instância reservada usando uma compra em fila

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

2. No painel de navegação, selecione Instâncias reservadas.
3. Selecione a instância reservada para renovar.
4. Escolha Actions (Ações), Renew Reserved Instances (Renovar instâncias reservadas).
5. Para concluir o pedido, escolha Order all (Pedir tudo) e, em seguida, Close (Fechar).

Vender instâncias reservadas para o Amazon EC2 no Marketplace de instâncias reservadas

O Marketplace de instâncias reservadas do Amazon EC2 é uma plataforma que facilita a venda de instâncias reservadas padrão não utilizadas de clientes da AWS e vendedores terceirizados. Essas instâncias reservadas podem variar em termos de duração e opções de preços. Talvez você queira vender suas instâncias reservadas quando não precisar mais delas, como quando você move as instâncias para uma nova Região da AWS, muda para um tipo de instância diferente, conclui projetos antes que o prazo da instância reservada expire, suas necessidades comerciais mudam ou você tem excesso de capacidade.

Assim que você oferecer suas instâncias reservadas no Marketplace de instâncias reservadas, elas serão disponibilizadas para que possíveis compradores as encontrem. Todas as Instâncias reservadas são agrupadas de acordo com a duração do período de vigência restante e do preço por hora.

Para atender à solicitação de um comprador que deseja comprar uma instância reservada de um vendedor terceirizado por meio do Marketplace de instâncias reservadas, a AWS primeiro vende a instância reservada com o preço inicial mais baixo no agrupamento especificado. Em seguida, a AWS vende a instância reservada com o menor preço até que o pedido inteiro do comprador seja cumprido. A AWS então processa as transações e transfere a propriedade das instâncias reservadas ao comprador.

Você manterá a propriedade da Instância reservada até ela ser vendida. Após venda, você abre mão da reserva de capacidade e das taxas recorrentes com desconto. Se você continuar a usar sua instância, a AWS cobrará de você o preço sob demanda, a partir do momento em que sua instância reservada foi vendida.

Se você quiser vender suas instâncias reservadas não utilizadas no Marketplace de instâncias reservadas, deverá atender a determinados critérios de elegibilidade.

Para obter mais informações sobre como comprar instâncias reservadas no Marketplace de instâncias reservadas, consulte Comprar do Marketplace da Instância reservada.

Tópicos

- Restrições e limitações
- Registre-se como vendedor
- Conta de banco para desembolso
- Informações fiscais
- Precificar suas Instâncias reservadas
- Liste as suas Instâncias reservadas
- Estados de listagem da Instância reservada
- Ciclo de vida de uma lista
- Depois que a Instância reservada é vendida
- Recebimentos
- Informações compartilhadas com o comprador

Restrições e limitações

Antes que você possa vender suas reservas não utilizadas, é necessário registrar-se como vendedor no Marketplace de instâncias reservadas. Para obter mais informações, consulte Registre-se como vendedor.

As seguintes limitações e restrições são aplicáveis na venda da Instâncias reservadas:

- Somente as instâncias regional padrão e reservada zonal do Amazon EC2 podem ser vendidas no Marketplace de instâncias reservadas.
- Instâncias reservadas conversíveis do Amazon EC2 não podem ser vendidas no Marketplace de instâncias reservadas.
- Instâncias reservadas de outros serviços da AWS, como o Amazon RDS e o Amazon ElastiCache, não podem ser vendidas no Marketplace de instâncias reservadas.
- Deve haver pelo menos um mês restante no período de vigência da Instância reservada padrão.
- Você não pode vender uma instância reservada padrão em uma região que é desabilitada por padrão.
- O preço mínimo permitido no Marketplace de instâncias reservadas é 0,00 USD.
- É possível vender instâncias reservadas sem adiantamento, com adiantamento parcial ou adiantamento integral no Marketplace de instâncias reservadas, desde que estejam ativas em sua

conta há pelo menos 30 dias. Além disso, se houver um pagamento antecipado em uma instância reservada, ela só poderá ser vendida após a AWS ter recebido o pagamento adiantado.

- Você não poderá vender uma instância reservada no Marketplace de instâncias reservadas caso a tenha comprado usando um desconto por volume.
- Você não pode modificar diretamente sua oferta no Marketplace de instâncias reservadas. No entanto, é possível alterar sua lista primeiro cancelando-a e depois criando outra lista com os parâmetros novos. Para obter mais informações, consulte Precificar suas Instâncias reservadas. Também é possível modificar as Instâncias reservadas antes de listá-las. Para obter mais informações, consulte Modificar a Instâncias reservadas.
- AWSA cobra uma taxa de serviço de 12% do preço inicial total de cada instância reservada padrão que você vender no Marketplace de instâncias reservadas. O preço inicial é aquele que o vendedor está cobrando pela Instância reservada padrão;.
- Quando você se registra como vendedor, o banco especificado deve ter um endereço nos EUA. Para obter mais informações, consulte Requisitos adicionais do vendedor para produtos pagos no Guia do vendedor do AWS Marketplace.
- Os clientes da Amazon Web Services India Private Limited (AWS India) não podem se registrar como vendedores no Reserved Instance Marketplace do EC2 e não podem listar nem vender instâncias reservadas no Reserved Instance Marketplace do EC2 mesmo que tenham conta bancária nos EUA. Para obter mais informações, consulte Quais são as diferenças entre as Contas da AWS e as contas da AWS India?
- Se você alterar seu vendedor registrado para a Amazon Web Services India Private Limited (AWS India), seu registro como vendedor será cancelado no Reserved Instance Marketplace do EC2 e todas as suas ofertas ativas existentes no Reserved Instance Marketplace do EC2 serão removidas. Para restaurar seu status de vendedor, você deve alterar o local da sua conta para outro país, que não seja a Índia, e realizar o processo de registro de vendedor novamente.

Registre-se como vendedor

> **Note**
>
> Somente o Usuário raiz da conta da AWS pode registrar uma conta como vendedor.

Para vender no Marketplace de instâncias reservadas, é necessário se registrar como vendedor. Durante o registro, você fornecerá as seguintes informações:

- Informações bancárias: a AWS deve ter suas informações bancárias para desembolsar os fundos recolhidos da venda das suas reservas. O banco que você especificar deverá ter um endereço nos EUA. Para obter mais informações, consulte Conta de banco para desembolso.
- 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.

Depois que a AWS receber o registro preenchido do vendedor, você receberá um e-mail confirmando seu registro e informando que é possível começar a vender no Marketplace de instâncias reservadas.

Conta de banco para desembolso

AWSA deverá ter suas informações bancárias para pagar os fundos recolhidos quando você vender a instância reservada. O banco que você especificar deverá ter um endereço nos EUA. Para obter mais informações, consulte Requisitos adicionais do vendedor para produtos pagos no Guia do vendedor do AWS Marketplace.

Para registrar uma conta de banco padrão para desembolsos

1. Abra a página Reserved Instance Marketplace Seller Registration (Registro do vendedor do Marketplace de instâncias reservadas) e faça login usando as credenciais da AWS.
2. Na página Gerenciar conta bancária, forneça as informações a seguir sobre o banco para receber o pagamento:
   - Nome do titular da conta
   - Número de roteamento
   - Número da conta
   - Tipo de conta bancária

> **Note**
>
> Se você estiver usando uma conta bancária corporativa, será solicitado que envie as informações sobre a conta bancária via fax (1-206-765-3424).

Após o registro, a conta bancária fornecida é definida como padrão, ficando pendente a verificação com o banco. Pode demorar até duas semanas para verificar uma conta bancária nova, e durante esse tempo você não poderá receber desembolsos. Para uma conta estabelecida, geralmente leva cerca de dois dias para os desembolsos serem concluídos.

Para alterar a conta de banco padrão para o desembolso

1. Na página Reserved Instance Marketplace Seller Registration (Registro do vendedor do Marketplace de instâncias reservadas), faça login na conta que você usou ao se registrar.
2. Na página Gerenciar conta bancária, adicione uma conta bancária nova ou modifique a conta bancária padrão conforme necessário.

Informações fiscais

A venda de Instâncias reservadas pode estar sujeita a um imposto baseado em transação, como imposto sobre vendas ou imposto sobre valor agregado. É necessário verificar com os departamentos fiscal, jurídico, financeiro ou contábil da sua empresa para determinar a aplicabilidade dos impostos de transação. Você é responsável para coletar e enviar impostos de transação para a devida autoridade fiscal.

Como parte do processo de registro do vendedor, é necessário completar uma entrevista sobre impostos no Portal de registro do vendedor. O entrevista coleta suas informações sobre impostos e preenche um formulário W-9, W-8BEN ou W-8BEN-E de IRS, que é usado para determinar todas as obrigações de declaração de impostos necessárias.

As informações sobre impostos inseridas como parte da entrevista sobre impostos pode diferir dependendo se você opera como um indivíduo ou como um negócio, e se você ou o seu negócio são ou não uma pessoa ou entidade dos EUA. Enquanto preenche a entrevista fiscal, tenha em mente o seguinte:

- Informações fornecidas pela AWS, inclusive as informações deste tópico, não constituem orientações jurídicas, fiscais ou profissional de alguma outra forma. Para descobrir como os requisitos de relatório da IRS podem afetar seu negócio, ou se você tiver outras dúvidas, entre em contato com seu orientador fiscal, jurídico ou profissional.
- Para atender os requisitos de relatório da IRS da forma mais eficiente possível, responda todas as perguntas e insira todas as informações solicitadas durante a entrevista.
- Verifique suas respostas. Evite erros de ortografia ou inserir números de identificação fiscal incorretos. Eles podem resultar em um formulário de impostos invalidado.

Com base nas respostas da entrevista fiscal e nos limites de declaração de imposto de renda, a Amazon pode registrar o Formulário 1099-K. A Amazon envia uma cópia do Formulário 1099-K em 31 de janeiro, ou antes disso, do ano seguinte ao ano em que sua conta fiscal chegar aos níveis do limite. Por exemplo, se sua conta atingir o limite em 2018, o formulário 1099-K será enviado até 31 de janeiro de 2019.

Para obter mais informações sobre os requisitos do IRS e o Formulário 1099-K, consulte Perguntas frequentes sobre o formulário 1099-K no site do IRS.

Precificar suas Instâncias reservadas

Ao definir o preço para suas instâncias reservadas, considere o seguinte:

- Preço para pagamento adiantado: o preço para pagamento adiantado é o único preço que pode ser especificado para a instância reservada que você está vendendo. O preço para pagamento à vista é o preço total que o comprador paga ao adquirir cada instância reservada.

  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, é possível os preços iniciais diferentes com base nas vendas da sua reserva. Por exemplo, se sua Instância reservada tiver nove meses de prazo restante, é possível 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.

  O preço mínimo permitido no Marketplace de instâncias reservadas é 0,00 USD.
- Limites: os limites para venda de instâncias reservadas a seguir se aplicam à vida útil de sua Conta da AWS. Eles não são limites anuais e não podem ser aumentados.
  - É possível vender até 50.000 USD em Instâncias reservadas.
  - É possível vender até 5.000 Instâncias reservadas.
- Não é possível modificar: você não pode modificar diretamente sua lista. No entanto, é possível alterar sua lista primeiro cancelando-a e depois criando outra lista com os parâmetros novos.
- É possível cancelar: 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.

Liste as suas Instâncias reservadas

Como vendedor registrado, é possível optar por vender uma ou mais de suas Instâncias reservadas. É possível escolher vender todos eles em uma lista ou em partes. Além disso, é possível listar as Instâncias reservadas com qualquer configuração de tipo de instância, plataforma e escopo.

O console determina um preço sugerido. Ele verifica as ofertas que correspondem à Instância reservada e relaciona a que tiver o preço mais baixo. Caso contrário, ele calcula um preço sugerido com base no custo da Instância reservada pelo tempo restante. Se o valor calculado for menor que 1,01 USD, o preço sugerido será de 1,01 USD.

Se você cancelar sua lista e parte da lista tiver sido vendida, o cancelamento não será eficiente na parte que foi vendida. Somente a parte não vendida da oferta não estará mais disponível no Marketplace de instâncias reservadas.

Console

Listar uma instância reservada no Marketplace de instâncias reservadas usando

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Instâncias reservadas.
3. Selecione as Instâncias reservadas para listar e escolha Actions (Ações) e Sell Instâncias reservadas (Vender Instâncias reservadas).
4. Na página Configurar a lista de Instância reservada, defina o número de instâncias para vender e o preço inicial para o prazo restante nas colunas relevantes. Veja como o valor de sua reserva muda com o restante do período ao selecionar a seta ao lado da coluna Meses restantes.
5. Se você for um usuário avançado e quiser personalizar o preço, poderá inserir valores diferentes nos meses subsequentes. Para retornar à queda de preço linear padrão, escolha Redefinir.
6. Escolha Continuar quando você tiver terminado de configurar sua lista.
7. Confirme os detalhes da sua lista na página Confirmar a lista da sua Instância reservada e, se estiver satisfeito, escolha Listar instância reservada.

Para visualizar suas listas no console 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. Selecione a Instância reservada listada e escolha a guia My Listings (Minhas ofertas) na parte inferior da página.

AWS CLI

Para gerenciar instâncias reservadas no marketplace de instâncias reservadas

1. Obtenha a lista das suas Instâncias reservadas usando o comando describe-reserved-instances. Anote o ID da instância reservada que deseja listar.
2. Use o comando create-reserved-instances-listing. Especifique o ID da Instância reservada, o número de instâncias e a programação de preços.
3. Para visualizar sua lista, use o comando describe-reserved-instances-listings.
4. Para cancelar sua lista, use o comando cancel-reserved-instances-listings.

PowerShell

Para gerenciar instâncias reservadas no marketplace de instâncias reservadas

1. Obtenha uma lista das suas instâncias reservadas usando o cmdlet Get-EC2ReservedInstance. Anote o ID da instância reservada que deseja listar.
2. Use o cmdlet New-EC2ReservedInstancesListing. Especifique o ID da Instância reservada, o número de instâncias e a programação de preços.
3. Para visualizar sua listagem, use o cmdlet Get-EC2ReservedInstancesListing.
4. Para cancelar sua listagem, use o cmdlet Stop-EC2ReservedInstancesListing.

Estados de listagem da Instância reservada

O Estado da lista na guia Minhas listagens da página de Instâncias reservadas exibe o status atual das listagens:

As informações exibidas por Listing State (Estado da oferta) se referem ao status de sua oferta no Marketplace de instâncias reservadas. Isso é diferente das informações de status exibidas na coluna Estado da página Instâncias reservadas. Essas informações de Estado são sobre sua reserva.

- ativa—A lista está disponível para compra.

- canceled (cancelada): a oferta foi cancelada e não está disponível para compra no Marketplace de instâncias reservadas.
- closed—A Instância reservada não é listada. Uma Instância reservada pode ser `closed`, pois a venda da listagem foi concluída.

Ciclo de vida de uma lista

Quando todas as instâncias na sua lista forem correspondidas e vendidas, a guia Minhas listas visualizará que a Contagem de instâncias totais corresponde à contagem listada em Vendido. Além disso, não há instâncias Disponíveis deixadas para sua listagem, e o Status é `closed`.

Quando apenas parte da sua oferta é vendida, a AWS remove as instâncias reservadas na oferta e cria o número de instâncias reservadas igual ao das instâncias reservadas restantes na contagem. Assim, o ID da listagem e a listagem que a representa, que agora tem menos reservas à venda, ainda estão ativas.

Todas as vendas futuras das Instâncias reservadas nessa listagem serão processadas dessa maneira. Quando todas as instâncias reservadas na oferta forem vendidas, a AWS marcará a lista como `closed`.

Por exemplo, você cria um ID de listagem de Instâncias reservadas 5ec28771-05ff-4b9b-aa31-9e57dexample com uma contagem de 5.

A guia Minhas listas na página do console da Instância reservada exibirá a lista desta forma:

ID de listagem de Instância reservada 5ec28771-05ff-4b9b-aa31-9e57dexample

- Contagem total da reserva = 5
- Vendidas = 0
- Disponíveis = 5
- Status = ativos

Um comprador compra duas das reservas, que deixa uma contagem de três reservas ainda disponíveis para venda. Por conta dessa venda parcial, a AWS cria uma nova reserva com uma contagem de três para representar as reservas restantes que ainda estão à venda.

Sua lista tem a seguinte forma na guia Minha lista:

ID de listagem de Instância reservada 5ec28771-05ff-4b9b-aa31-9e57dexample

- Contagem total da reserva = 5
- Vendidas = 2
- Disponíveis = 3
- Status = ativos

Se você cancelar sua lista e parte da lista já tiver sido vendida, o cancelamento não será eficiente na parte que foi vendida. Somente a parte não vendida da oferta não estará mais disponível no Marketplace de instâncias reservadas.

Depois que a Instância reservada é vendida

Quando a instância reservada for vendida, a AWS enviará uma notificação por e-mail. Cada dia em que houver qualquer tipo de atividade, você receberá uma notificação por e-mail capturando todas as atividades do dia. As atividades podem incluir a criação ou a venda de uma oferta ou o envio de recursos financeiros para sua conta pela AWS.

Console

Para rastrear o status de uma listagem de instância reservada

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Na página de navegação, escolha Reserved Instances (Instâncias reservadas).
3. Na guia Minhas listagens, procure o valor de Estado da listagem. A guia também contém informações sobre o período, o preço de tabela e um detalhamento de quantas instâncias na listagem estão disponíveis, pendentes, vendidas e canceladas.

AWS CLI

Para rastrear o status de uma listagem de instância reservada

Use o comando describe-reserved-instances-listings com o filtro apropriado para obter informações sobre suas listagens.

```
aws ec2 describe-reserved-instances-listings
```

PowerShell

Para rastrear o status de uma listagem de instância reservada

Use o cmdlet New-EC2ReservedInstancesListing.

```
Get-EC2ReservedInstancesListing
```

Recebimentos

Assim que a AWS receber os valores do comprador, será enviada uma mensagem ao e-mail da conta do proprietário registrado para a instância reservada vendida.

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. Os desembolsos ocorrem uma vez por dia. Você receberá um e-mail com o relatório de desembolso após o recurso financeiro ser liberado. Lembre-se de que você não poderá receber desembolsos até que a AWS tenha recebido verificação do seu banco. Isso pode levar até duas semanas.

A Instância reservada que você vendeu continua aparecendo quando você descreve as Instâncias reservadas.

Você recebe um reembolso em dinheiro pelas instâncias reservadas por meio de uma transferência eletrônica feita diretamente na sua conta bancária. A AWS cobra uma taxa de serviço de 12% do preço inicial total de cada instância reservada vendida no Marketplace de instâncias reservadas.

Informações compartilhadas com o comprador

Quando você vender no Marketplace de instâncias reservadas, a AWS compartilhará o nome legal da empresa no extrato do comprador, de acordo com as normas dos EUA. Além disso, se o comprador acessar o suporte da Suporte porque precisa entrar em contato com você para obter uma fatura ou por outro motivo relacionado a impostos, a AWS pode precisar fornecer ao comprador no seu endereço de e-mail, de modo que ele possa entrar em contato diretamente com você.

Por motivos semelhantes, as informações de código postal do comprador e do país são fornecidas ao vendedor no relatório de desembolso. Como vendedor, é possível 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 Suporte.

Modificar a Instâncias reservadas

Quando suas necessidades mudarem, será possível modificar seu padrão ou Instâncias reservadas conversíveis e continuar usufruindo o benefício de faturamento. É possível modificar atributos como a zona de disponibilidade, tamanho da instância (na mesma família e geração de instâncias), e escopo de sua Instância reservada.

> **Note**
>
> Também é possível trocar uma Instância reservada convertível por outra Instância reservada convertível com uma configuração diferente. Para obter mais informações, consulte Trocar Instâncias reservadas conversíveis.

É possível modificar todas as Instâncias reservadas ou um subconjunto delas. É possível 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`.

Também é possível mesclar duas ou mais Instâncias reservadas em uma única Instância reservada. Por exemplo, se você tiver quatro `t2.small` Instâncias reservadas de uma instância cada, poderá mesclá-las para criar uma `t2.large` Instância reservada. Para obter mais informações, consulte Suporte para modificar tamanhos de instância.

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. É possível obter a data efetiva das Instâncias reservadas modificadas usando o comando describe-reserved-instances.

- A reserva original é desativada. A data final é a data inicial da nova reserva, e a data final da nova reserva é a mesma que a data final da Instância reservada original. Se você modificar uma reserva de três anos com 16 meses sobrando de período de vigência, a reserva modificada resultante será uma reserva de 16 meses com a mesma data final que a original.
- A reserva alterada lista um preço fixo de 0 USD e não o preço fixo da reserva original.
- O preço fixo da reserva modificada não afeta os cálculos da camada de preços com desconto aplicados à sua conta, que são baseados no preço fixo da reserva original.

Se sua solicitação de modificação falhar, as Instâncias reservadas manterão a configuração original e serão imediatamente disponibilizadas para outra solicitação de modificação.

Não há taxas para a modificação e você não receber nenhuma conta ou fatura novas.

É possível 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, é possível enviar outra solicitação de modificação para reverter as alterações que fez, se necessário.

Tópicos

- Requisitos e restrições para modificação
- Suporte para modificar tamanhos de instância
- Enviar solicitações de modificação
- Solucionar problemas de solicitações de modificação

Requisitos e restrições para modificação

É possível modificar esses atributos da maneira a seguir.

Atributo modificável	Plataformas compatíveis	Limitações e considerações
Alterar as zonas de disponibilidade na mesma região	Linux e Windows	-
	Linux e Windows	Uma instância reservada por zona tem escopo para uma

Atributo modificável	Plataformas compatíveis	Limitações e considerações
Alterar o escopo de zona de disponibilidade para região e vice-versa		zona de disponibilidade e reserva capacidade nessa zona de disponibilidade. Se você alterar o escopo de zona de disponibilidade para região (de zonal para regional), você perderá o benefício da reserva de capacidade. Uma instância reservada por região tem escopo para uma região. O desconto para instância reservada se aplica a instâncias executadas em qualquer zona de disponibilidade nessa região. Além disso, o desconto da instância reservada se aplica ao uso da instância em todos os tamanhos na família de instâncias selecionada. Se você alterar o escopo de região para zona de disponibilidade (ou seja, de regional para zonal), você perderá a flexibilidade da zona de disponibilidade e a flexibilidade de tamanho de instância (se aplicável). Para obter mais informações, consulte Como descontos em instâncias reservadas são aplicados.

Atributo modificável	Plataformas compatíveis	Limitações e considerações
Alterar o tamanho da instância na mesma família e geração de instâncias	Somente Linux/UNIX A flexibilidade do tamanho da instância não está disponível para Instâncias reservadas nas outras plataformas, que incluem Linux com SQL Server Standard, Linux com SQL Server Web, Linux com SQL Server Enterprise, Red Hat Enterprise Linux, SUSE Linux, Windows, Windows com SQL Standard, Windows com SQL Server Enterprise e Windows com SQL Server Web.	A reserva deve usar a locação padrão. Para algumas famílias de instâncias não há suporte, pois não há outros tamanhos disponíveis. Para obter mais informações, consulte . Suporte para modificar tamanhos de instância

Requisitos

O Amazon EC2 processará sua solicitação de modificação se houver capacidade suficiente para sua nova configuração (se aplicável) e se as seguintes condições forem atendidas:

- A Instância reservada não pode ser modificada antes ou ao mesmo tempo da compra
- a Instância reservada deve estar ativa.
- Não pode haver uma solicitação de modificação pendente
- A instância reservada não está listada no Marketplace de instâncias reservadas
- Deve haver correspondência entre o tamanho ocupado pela instância da reserva original e a nova configuração. Para obter mais informações, consulte Suporte para modificar tamanhos de instância.
- As Instâncias reservadas de entrada são todas Instâncias reservadas standard ou todas as Instâncias reservadas conversíveis, e não algumas de cada tipo
- As Instâncias reservadas de entrada deverão expirar na mesma hora, se forem Instâncias reservadas standard

- Para modificar o tamanho da instância, a instância reservada deve oferecer suporte à flexibilidade do tamanho da instância. Para ver a lista de instâncias reservadas que não oferecem suporte à flexibilidade do tamanho da instância, consulte Flexibilidade de tamanho da instância.

Suporte para modificar tamanhos de instância

É possível modificar o tamanho da instância de um Instância reservada se os seguintes requisitos forem atendidos.

Requisitos

- A plataforma é Linux/UNIX.
- Você deve selecionar outro tamanho de instância na mesma família de instâncias (indicada por uma letra, p. ex., T) e geração (indicada por um número, p. ex., 2).

  Por exemplo, você pode modificar uma instância reservada de `t2.small` para `t2.large`, pois ambas estão na mesma família e geração T2. Porém, você não pode modificar uma instância reservada de T2 para M2 ou de T2 para T3, porque nesses dois exemplos, a família e a geração de instâncias de destino não são as mesmas da instância reservada original.
- Você só pode modificar o tamanho de uma instância reservada se ela oferecer suporte à flexibilidade do tamanho da instância. Para ver a lista de instâncias reservadas que não oferecem suporte à flexibilidade do tamanho da instância, consulte Flexibilidade de tamanho da instância.
- Você não pode modificar o tamanho de instâncias reservadas para instâncias `t1.micro`, porque `t1.micro` tem apenas um tamanho.
- As Instância reservada original e modificada devem ter o mesmo espaço para tamanho de instância.

Tópicos

- Espaço para tamanho da instância
- Fatores de normalização para instâncias bare metal

Espaço para tamanho da instância

Cada Instância reservada tem um espaço para tamanho da instância, que é determinado pelo fator de normalização do tamanho de instância e pelo número de instâncias na reserva. Ao modificar os tamanhos da instância em uma Instância reservada, o espaço da nova configuração deverá

ser equivalente ao da configuração original; caso contrário, a solicitação de modificação não será processada.

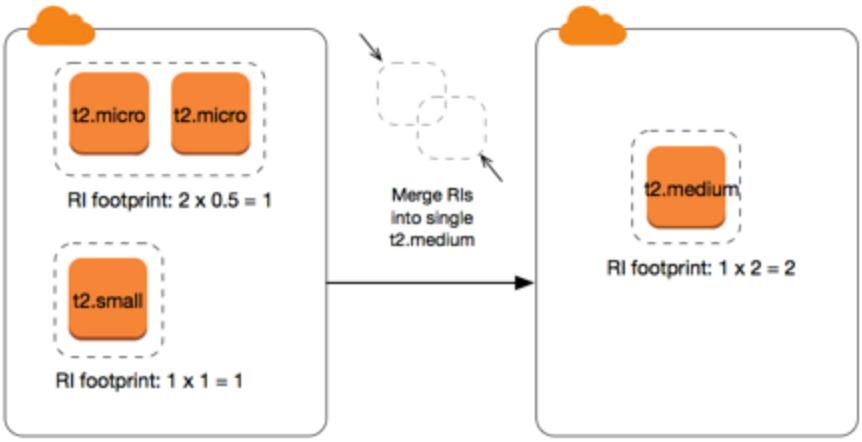
Para calcular o espaço para tamanho de instância de uma Instância reservada, multiplique o número de instâncias pelo fator de normalização. No console do Amazon EC2, o fator de normalização é medido em unidades. A tabela a seguir descreve o fator de normalização para os tamanhos de instância em uma família de instâncias. Por exemplo, `t2.medium` tem um fator de normalização de 2, por isso, uma reserva para quatro instâncias `t2.medium` tem um espaço de 8 unidades.

Tamanho da instância	Fator de normalização
nano	0.25
micro	0,5
small	1
medium	2
large	4
xlarge	8
2xlarge	16
3xlarge	24
4xlarge	32
6xlarge	48
8xlarge	64
9xlarge	72
10xlarge	80
12xlarge	96
16xlarge	128

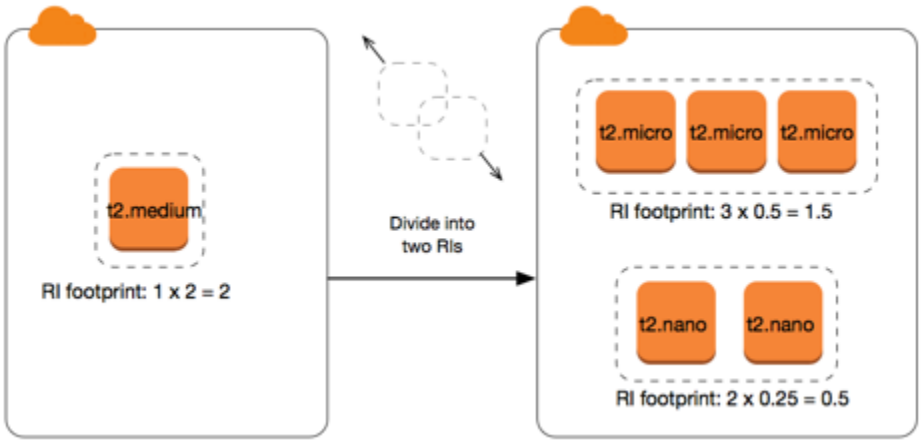
Tamanho da instância	Fator de normalização
18xlarge	144
24xlarge	192
32xlarge	256
48xlarge	384
56xlarge	448
112xlarge	896

É possível alocar suas reservas para tamanhos de instância diferentes na mesma família de instâncias, desde que o espaço para o tamanho da instância da sua reserva permaneça o mesmo. Por exemplo, é possível dividir uma reserva para uma instância `t2.large` (1 @ 4 unidades) em quatro instâncias `t2.small` (4 @ 1 unidade). Da mesma forma, é possível combinar uma reserva para quatro instâncias `t2.small` em uma instância `t2.large`. No entanto, você não pode alterar sua reserva para duas instâncias `t2.small` em uma instância `t2.large` porque o espaço da nova reserva (4 unidades) é maior que o espaço da reserva original (2 unidades).

No exemplo a seguir, você tem uma reserva com duas instâncias `t2.micro` (1 unidade) e uma reserva com uma instância `t2.small` (1 unidade). Se você mesclar ambas as reservas em uma única reserva com uma instância `t2.medium` (2 unidades), o espaço da nova reserva será igual ao espaço das reservas combinadas.



Também é possível modificar uma reserva para dividi-la em duas ou mais reservas. No exemplo a seguir, você tem uma reserva com uma instância `t2.medium` (2 unidades). É possível dividir a reserva em duas reservas, uma com duas instâncias `t2.nano` (0,5 unidades) e a outra com três instâncias `t2.micro` (1,5 unidades).



Fatores de normalização para instâncias bare metal

É possível modificar uma reserva com instâncias `metal` usando outros tamanhos na mesma família de instâncias. É possível modificar uma reserva com instâncias diferentes de instâncias bare metal usando o tamanho `metal` na mesma família de instâncias. Geralmente, uma instância bare metal tem o mesmo tamanho que o maior tamanho de instância disponível na mesma família de instâncias. Por exemplo, uma instância `i3.metal` é do mesmo tamanho que uma instância `i3.16xlarge`. Portanto, elas têm o mesmo fator de normalização.

A tabela a seguir descreve o fator de normalização para os tamanhos de instâncias bare metal em famílias de instâncias com instâncias bare metal. O fator de normalização para instâncias `metal` depende da família de instâncias, ao contrário dos outros tamanhos de instância.

Tamanho da instância	Fator de normalização
`a1.metal`	32
`m5zn.metal` | `x2iezn.metal` `z1d.metal`	96
`c6g.metal` | `c6gd.metal` | `i3.metal` | `m6g.metal` | `m6gd.metal` | `r6g.metal` | `r6gd.metal` | `x2gd.metal`	128

Tamanho da instância	Fator de normalização
c5n.metal	144
c5.metal | c5d.metal | i3en.metal | m5.metal | m5d.metal | m5dn.metal | m5n.metal | r5.metal | r5b.metal | r5d.metal | r5dn.metal | r5n.metal	192
c6i.metal | c6id.metal | m6i.metal | m6id.metal | r6d.metal | r6id.metal	256
u-18tb1.metal | u-24tb1.metal	448
u-6tb1.metal | u-9tb1.metal | u-12tb1.metal	896

Por exemplo, uma instância `i3.metal` tem um fator de normalização de 128. Se você comprar uma Instância reservada `i3.metal` de Linux/Unix da Amazon de locação padrão, será possível dividir a reserva da seguinte maneira:

- Uma instância `i3.16xlarge` é do mesmo tamanho que uma instância `i3.metal`, portanto, seu fator de normalização é de 128 (128/1). A reserva para uma instância `i3.metal` pode ser modificada para uma instância `i3.16xlarge`.
- Uma instância `i3.8xlarge` tem a metade do tamanho de uma instância `i3.metal`, portanto, seu fator de normalização é de 64 (128/2). A reserva para uma instância `i3.metal` pode ser dividida em duas instâncias `i3.8xlarge`.
- Uma instância `i3.4xlarge` é um quarto do tamanho de uma instância `i3.metal`, portanto, seu fator de normalização é de 32 (128/4). A reserva para uma instância `i3.metal` pode ser dividida em quatro instâncias `i3.4xlarge`.

Enviar solicitações de modificação

Antes de realizar modificações nas instâncias reservadas, certifique-se de ter lido as restrições aplicáveis. Antes de realizar modificações no tamanho da instância, calcule a área de ocupação do tamanho da instância das reservas originais que deseja modificar e certifique-se de que essa área corresponda à área de ocupação do tamanho da instância das suas novas configurações.

Console

Para modificar suas instâncias reservadas

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Na página Reserved Instances (Instâncias reservadas), selecione uma ou mais Instâncias reservadas para modificar e escolha Actions (Ações), Modify Reserved Instances (Modificar instâncias reservadas).

   Se as Instâncias reservadas não estiverem no estado ativo ou não puderem ser modificadas, a opção Modificar Instâncias reservadas estará desativada.
3. A primeira entrada na tabela de modificação exibe os atributos da Instâncias reservadas selecionada e pelo menos uma configuração de destino abaixo dela. A coluna Unidades exibe o espaço para tamanho total da instância. Escolha Adicionar para cada nova configuração a ser adicionada. Modifique os atributos conforme necessário para cada configuração.

   - Scope (Escopo): escolha se a configuração se aplica a uma zona de disponibilidade ou a toda a região.
   - Zona de disponibilidade: Escolha a zona de disponibilidade necessária. Não aplicável para Instâncias reservadas regionais.
   - Tipo de instância: selecione o tipo de instância necessário. As configurações combinadas devem ser iguais ao tamanho da instância das configurações originais.
   - Count (Contagem): especifique o número de instâncias. Para dividir as Instâncias reservadas em várias configurações, reduza a contagem, escolha Add (Adicionar) e especifique uma contagem para a configuração adicional. Por exemplo, se você tiver uma única configuração com uma contagem de 10, poderá alterar sua contagem para 6 e adicionar uma configuração com uma contagem de 4. Esse processo desativa a Instância reservada original assim que as novas Instâncias reservadas são ativadas.
4. Escolha Continue.
5. Para confirmar suas escolhas quando terminar de especificar as configurações de destino, selecione Submit modifications (Enviar modificações).
6. É possível determinar o status de sua solicitação da modificação analisando a coluna State (Estado) na tela de Instâncias reservadas. Os estados possíveis são os seguintes.

   - ativo (modificação pendente) — estado de transição das Instâncias reservadas originais.

- desativado (modificação pendente) — estado de transição das Instâncias reservadas originais enquanto as novas Instâncias reservadas são criadas
- desativado — Instâncias reservadas modificadas e substituídas com êxito
- ativo — uma das seguintes opções:
  - Novas Instâncias reservadas criadas com base em uma solicitação de modificação bem-sucedida
  - Instâncias reservadas originais após falha na solicitação da modificação

AWS CLI

Para modificar suas instâncias reservadas

Use o comando modify-reserved-instances. É possível fornecer os detalhes da configuração em um arquivo JSON.

```
aws ec2 modify-reserved-instances \
    --reserved-instances-ids b847fa93-e282-4f55-b59a-1342f5bd7c02 \
    --target-configurations file://configuration.json
```

Para obter o status de sua solicitação de modificação

Use o comando describe-reserved-instances-modifications. O status é `processing`, `fulfilled` ou `failed`.

```
aws ec2 describe-reserved-instances-modifications \
    --reserved-instances-modification-ids rimod-d3ed4335-b1d3-4de6-ab31-0f13aaf46687
 \
    --query ReservedInstancesModifications[].Status
```

PowerShell

Para modificar suas instâncias reservadas

Use o cmdlet Edit-EC2ReservedInstance. É possível fornecer os detalhes da configuração em um objeto do tipo `Amazon.EC2.Model.ReservedInstancesConfiguration`.

```
Edit-EC2ReservedInstance `
    -ReservedInstancesId b847fa93-e282-4f55-b59a-1342f5bd7c02 `
```

```
    -TargetConfiguration $configuration
```

Para obter o status de sua solicitação de modificação

Use o cmdlet Get-EC2ReservedInstancesModification. O status é `processing`, `fulfilled` ou `failed`.

```
Get-EC2ReservedInstancesModification `
    -ReservedInstancesModificationId rimod-d3ed4335-b1d3-4de6-ab31-0f13aaf46687 | `
    Select Status
```

Solucionar problemas de solicitações de modificação

Se as configurações de destino solicitadas forem exclusivas, você receberá uma mensagem de que sua solicitação está sendo processada. Neste ponto, o Amazon EC2 só determinou que os parâmetros da sua solicitação de modificação são válidos. A solicitação da modificação ainda pode falhar durante o processo em função de capacidade indisponível.

Em algumas situações, é possível 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 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, é possível obter versões diferentes da mensagem.

O Amazon EC2 exibe os motivos pelos quais sua requisição não pode ser processada. Por exemplo, é possível 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

É possível 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 quantas vezes você realiza uma troca, desde que a nova Instância reservada conversível tenha valor igual ou superior às Instâncias reservadas conversíveis que você está trocando.

Ao trocar sua instância reservada conversível, o número de instâncias da sua reserva atual é trocado por um número de instâncias que cobrem o valor igual ou superior da configuração da nova instância reservada conversível. O Amazon EC2 calcula o número de instâncias reservadas que é possível receber como resultado da troca.

Você não pode trocar Instâncias reservadas padrão, mas pode modificá-las. Para obter mais informações, consulte Modificar a Instâncias reservadas .

Tópicos

- Requisitos para trocar de Instâncias reservadas conversíveis
- Calcular trocas de Instâncias reservadas conversíveis
- Mesclar Instâncias reservadas conversíveis
- Trocar uma parte de uma Instância reservada convertível
- Enviar solicitações de troca

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
- Tenha pelo menos 24 horas restantes do prazo de validade

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 conversível por uma instância reservada conversível de outra região.
- Para trocar uma instância reservada conversível zonal, a AWS precisa ter capacidade suficiente para o novo o tipo de instância na região.
- É possível trocar uma ou mais Instâncias reservadas conversíveis por vez por uma única Instância reservada convertível somente.
- Para trocar parte de uma Instância reservada convertível, é possível 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. Para obter mais informações sobre como modificar Instâncias reservadas, consulte Modificar a Instâncias reservadas.
- 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 USD 0,00, a AWS fornecerá automaticamente uma quantidade de instâncias na instância reservada conversível que garantirá o custo alinhado de USD 0,00 ou mais.

> **Note**
>
> Se o valor total (preço adiantado + preço por hora * número de horas restantes) da nova instância reservada conversível for menor do que o valor total da instância reservada conversível que foi trocada, a AWS fornecerá automaticamente uma quantidade de instâncias na instância reservada conversível que garantirá um valor total igual ou superior ao valor da instância reservada conversível trocada.

- Para se beneficiar com preços melhores, é possível trocar uma Instância reservada convertível sem adiantamento por uma Instância reservada convertível com adiantamento total ou parcial.
- Você não pode trocar Instâncias reservadas conversíveis pagas total ou parcialmente à vista por instâncias reservadas conversíveis sem pagamento antecipado.

- Só é possível trocar uma Instância reservada convertível sem adiantamento por uma outra Instância reservada convertível sem adiantamento se o preço por hora da nova Instância reservada convertível for igual ou superior ao preço por hora da Instância reservada convertível que foi trocada.

  > **Note**
  >
  > Se o valor total (preço por hora * número de horas restantes) da nova instância reservada conversível for menor do que o valor total da instância reservada conversível que foi trocada, a AWS fornecerá automaticamente uma quantidade de instâncias na instância reservada conversível que garantirá um valor total igual ou superior ao valor da instância reservada conversível trocada.

- Se você trocar várias Instâncias reservadas conversíveis com datas de expiração diferentes, a data de expiração da nova Instância reservada convertível será a data futura mais longe.
- Se você trocar uma única Instância reservada convertível, ela deverá ter o mesmo período de vigência (um ano ou três anos) da nova Instância reservada convertível. Se você mesclar várias Instâncias reservadas conversíveis com períodos de vigência diferentes, a nova Instância reservada convertível terá um período de vigência de três anos. Para obter mais informações, consulte Mesclar Instâncias reservadas conversíveis.
- Quando o Amazon EC2 troca uma instância reservada conversível, ele retira a reserva associada e transfere a data de término para a nova reserva. Após a troca, o Amazon EC2 define a data de término da reserva antiga e a data de início da nova reserva como a data da troca. Por exemplo, se você trocar uma reserva de três anos com 16 meses restantes do período de vigência, a nova reserva será uma reserva de 16 meses com a mesma data de término que a reserva da Instância reservada conversível que você trocou.

Calcular trocas de Instâncias reservadas conversíveis

A troca de Instâncias reservadas conversíveis são gratuitas. Porém, pode ser necessário pagar o custo diferencial, que é o custo à vista pro rata da diferença entre as Instâncias reservadas conversíveis que você tinha e as novas Instâncias reservadas conversíveis que você recebe na 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 é possível 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
```

É possível trocar sua Instância reservada convertível por três Instâncias reservadas conversíveis de US$ 10. Não é possível adquirir meias reservas; portanto, é necessário comprar uma Instância reservada convertível adicional que cubra o restante:

```
3.5 = 3 whole Convertible Reserved Instances + 1 additional Convertible Reserved
 Instance
```

A quarta Instância reservada convertível tem a mesma data de término das outras três. Se você estiver trocando Instâncias reservadas conversíveis com adiantamento integral ou parcial, pagará o custo alinhado da quarta reserva. Se o custos iniciais restante das Instâncias reservadas conversíveis forem USD 500 e a reserva de destino custar normalmente USD 600 pro rata, será cobrado de você USD 100.

```
$600 prorated upfront cost of new reservations - $500 remaining upfront cost of old
 reservations = $100 difference
```

Mesclar Instâncias reservadas conversíveis

Se você combinar duas ou mais Instâncias reservadas conversíveis, o termo da nova Instância reservada conversível deverá ser o mesmo das instâncias reservadas conversíveis originais ou o mais alto das instâncias reservadas conversíveis originais. 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

- É possível 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.
- É possível mesclar `bbbb2222` e `cccc3333` e trocá-las por uma Instância reservada convertível de três anos. Você não pode trocá-las por uma Instância reservada convertível de um ano. A data de expiração da nova Instância reservada convertível é 31/07/2018.
- É possível mesclar `cccc3333` e `dddd4444` e trocá-las por uma Instância reservada convertível de três anos. Você não pode trocá-las por uma Instância reservada convertível de um ano. A data de expiração da nova Instância reservada convertível é 31/12/2019.

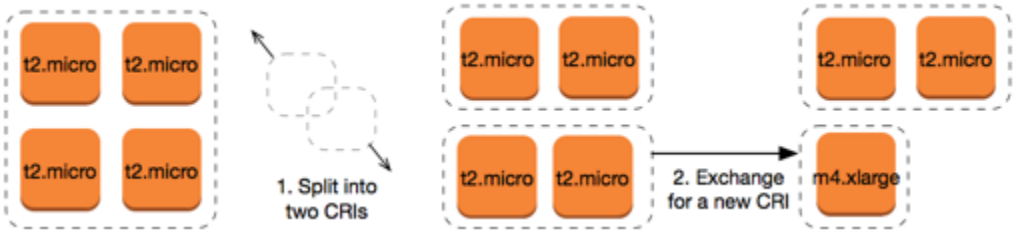
Trocar uma parte de uma Instância reservada convertível

É possível 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`:

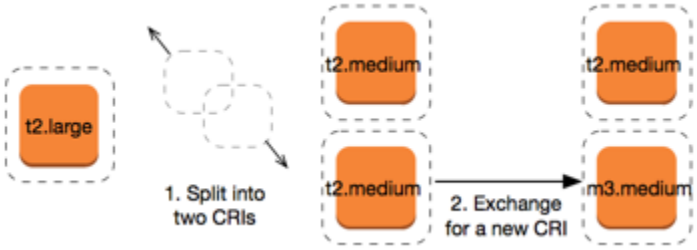
1. Modifique a `t2.micro` Instância reservada convertível dividindo-a em duas `t2.micro` Instâncias reservadas conversíveis com duas instâncias cada uma.
2. Troque uma das novas `t2.micro` Instâncias reservadas conversíveis por uma `m4.xlarge` Instância reservada convertível.



Example Exemplo: Instância reservada convertível com uma única instância

Neste exemplo, você tem uma `t2.large` Instância reservada convertível. Para transformá-la em uma instância `t2.medium` menor e em uma instância `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`.
2. Troque uma das novas `t2.medium` Instâncias reservadas conversíveis por uma `m3.medium` Instância reservada convertível.



Para obter mais informações, consulte Suporte para modificar tamanhos de instância e Enviar solicitações de troca.

Enviar solicitações de troca

É possível trocar suas instâncias reservadas conversíveis. As instâncias reservadas trocadas são desativadas.

Console

Para trocar instâncias reservadas conversíveis

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Escolha Instâncias reservadas, selecione as Instâncias reservadas conversíveis a serem trocadas e escolha Ações, Trocar Instância reservada.
3. Selecione os atributos da configuração desejada e escolha Find offering (Localizar oferta).
4. Selecione uma nova Instância reservada convertível. Na parte inferior da tela, é possível visualizar o número da Instâncias reservadas que você receber para a troca, além de quaisquer custos adicionais.
5. Ao selecionar uma Instância reservada convertível que atenda às suas necessidades, escolha Review (Revisar).
6. Escolha Exchange (Troca) e, em seguida, Close (Fechar).

AWS CLI

Para trocar uma instância reservada conversível

1. Encontre uma nova instância reservada conversível que atenda às suas necessidades usando o comando describe-reserved-instances-offerings.
2. Obtenha uma cotação para a troca usando o comando get-reserved-instances-exchange-quote. Isso inclui o número de instâncias reservadas obtidas na troca e o custo alinhado da troca:
3. Faça a troca usando o comando accept-reserved-instances-exchange-quote.

PowerShell

Para trocar uma instância reservada conversível

1. Encontre uma nova instância reservada conversível que atenda às suas necessidades usando o cmdlet Get-EC2ReservedInstancesOffering.
2. Obtenha uma cotação para a troca usando o cmdlet Get-EC2ReservedInstancesExchangeQuote. Isso inclui o número de instâncias reservadas obtidas na troca e o custo alinhado da troca:
3. Faça a troca usando o cmdlet Approve-EC2ReservedInstancesExchangeQuote

Cotas de instâncias reservadas

É possívelrá comprar novas instâncias reservadas a cada mês. O número de novas instâncias reservadas que é possível comprar por mês é determinado por sua cota mensal, da seguinte forma:

Descrição da cota	Cota padrão
Novas instâncias reservadas regionais	20 por região por mês
Novas instâncias reservadas zonais	20 por zona de disponibilidade por mês

Por exemplo, em uma região com três zonas de disponibilidade, a cota padrão é de 80 novas instâncias reservadas por mês, calculada da seguinte forma:

- 20 instâncias reservadas regionais para a região

- Mais 60 instâncias reservadas zonais (20 para cada uma das três zonas de disponibilidade)

As instâncias no estado `running` contam para sua cota. As instâncias que estão nos estados `pending`, `stopping`, `stopped` e `hibernated` não contam para sua cota.

Visualizar o número de instâncias reservadas que você comprou

O número de instâncias reservadas compradas por você é indicado pelo campo Instance count (Contagem de instâncias) (console) ou o parâmetro `InstanceCount` (AWS CLI). Quando você compra novas instâncias reservadas, a cota é medida em relação à contagem total de instâncias. Por exemplo, se você comprar uma única configuração de instância reservada com uma contagem de instâncias igual 10, a compra contará para sua cota como 10, e não como 1.

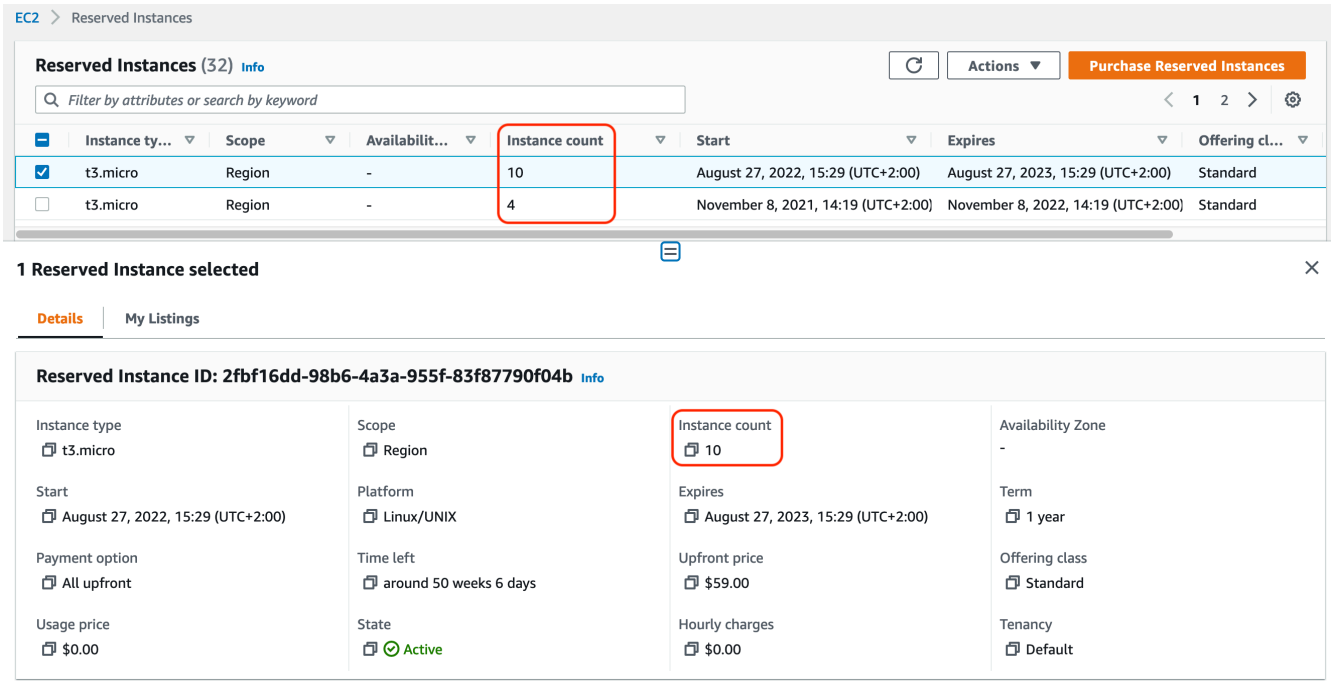
É possível ver quantas instâncias reservadas você comprou usando o Amazon EC2 ou a AWS CLI.

Console

Para ver o número de instâncias reservadas que você comprou

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Instâncias reservadas.
3. Selecione uma configuração de instância reservada na tabela e verifique o campo Instance count (Contagem de instâncias).

   Na captura de tela a seguir, a linha selecionada representa uma única configuração de instância reservada para um tipo de instância `t3.micro`. A coluna Instance count (Contagem de instâncias) na visualização da tabela e no campo Instance count (Contagem de instâncias) na visualização detalhada (descrito na captura de tela) indica que há 10 instâncias reservadas para essa configuração.



AWS CLI

Para ver o número de instâncias reservadas que você comprou

Use o comando describe-reserved-instances e especifique o ID da configuração da instância reservada.

```
aws ec2 describe-reserved-instances \
    --reserved-instances-ids a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
    --output table
```

O seguinte é um exemplo de saída. O campo `InstanceCount` indica que há 10 instâncias reservadas para essa configuração.

```
-------------------------------------------------------------------
|                   DescribeReservedInstances                     |
+-----------------------------------------------------------------+
||                       ReservedInstances                       ||
|+----------------------+----------------------------------------+|
||  CurrencyCode        |  USD                                   ||
||  Duration            |  31536000                              ||
||  End                 |  2023-08-27T13:29:44+00:00             ||
||  FixedPrice          |  59.0                                  ||
||  InstanceCount       |  10                                    ||
```

```
||  InstanceTenancy     |  default                                  ||
||  InstanceType        |  t3.micro                                 ||
||  OfferingClass       |  standard                                 ||
||  OfferingType        |  All Upfront                              ||
||  ProductDescription  |  Linux/UNIX                               ||
||  ReservedInstancesId |  a1b2c3d4-5678-90ab-cdef-EXAMPLE11111     ||
||  Scope               |  Region                                   ||
||  Start               |  2022-08-27T13:29:45.938000+00:00         ||
||  State               |  active                                   ||
||  UsagePrice          |  0.0                                      ||
|+---------------------+-------------------------------------------+|
|||                      RecurringCharges                          |||
||+----------------------------------+--------------------------+||
|||  Amount                          |  0.0                     |||
|||  Frequency                       |  Hourly                  |||
||+----------------------------------+--------------------------+||
```

PowerShell

Para ver o número de instâncias reservadas que você comprou

Use o cmdlet Get-EC2ReservedInstance e especifique o ID da configuração da instância reservada.

```
Get-EC2ReservedInstance -ReservedInstancesId a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

O seguinte é um exemplo de saída. O campo `InstanceCount` indica que há 10 instâncias reservadas para essa configuração.

```
AvailabilityZone    :
CurrencyCode        : USD
Duration            : 31536000
End                 : 1/12/2017 8:57:08 PM
FixedPrice          : 0
InstanceCount       : 10
InstanceTenancy     : default
InstanceType        : t3.medium
OfferingClass       : standard
OfferingType        : All Upfront
ProductDescription  : Windows
RecurringCharges    : {}
ReservedInstancesId : a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

```
Scope               : Region
Start               : 10/12/2016 4:00:00 PM
State               : active
Tags                : {}
UsagePrice          : 0
```

Considerações

Um regional Instância reservada aplica um desconto para um instância sob demanda em execução. O instância sob demanda padrão é 20. Não é possível exceder o limite de execução do instância sob demanda, comprando regional Instâncias reservadas. Por exemplo, se você já tem 20 Instâncias on-demand em execução e você adquiri 20 regional Instâncias reservadas, essas 20 regional Instâncias reservadas serão usadas para aplicar desconto nas 20 Instâncias on-demand em execução. Se você compra mais regional Instâncias reservadas, não será possível iniciar mais instâncias porque alcançou seu limite do instância sob demanda.

Antes de comprar Instâncias reservadas regionais, verifique se o limite de instância sob demanda corresponde ou excede o número de Instâncias reservadas regionais que você pretende ter. Se necessário, solicite um aumento de seu limite de instância sob demanda antes de comprar mais Instâncias reservadas regionais.

Uma instância reservada zonal (uma Instância reservada que é comprada para uma zona de disponibilidade específica) e que fornece reserva de capacidade, bem como um desconto. É possível 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, é possível 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.

Visualize suas cotas de instância reservada e solicite um aumento de cota

O console do Amazon EC2 fornece informações sobre as cotas. Também é possível solicitar um aumento em suas cotas. Para obter mais informações, consulte Visualizar as cotas atuais e Solicitar um aumento.

Instâncias spot

Uma instância spot é uma instância que usa capacidade adicional do EC2 que está disponível por um valor mais baixo que o preço sob demanda. Como as Instâncias spot permitem que você solicite

instâncias do EC2 não usadas com descontos consideráveis, é possível reduzir seus custos do Amazon EC2 significativamente. O preço por hora de uma instância spot é chamado de preço spot. O preço spot de cada tipo de instância em cada zona de disponibilidade é definido pelo Amazon EC2 e ajustado gradualmente com base na oferta e a demanda de longo prazo das Instâncias spot. Sua instância spot executará sempre que houver capacidade disponível.

As Instâncias spot são uma opção econômica se houver flexibilidade quanto ao momento em que as aplicações serão executadas e se as aplicações poderão ser interrompidas. Por exemplo, as Instâncias spot são adequadas para análise de dados, trabalhos em lote, processamento em segundo plano e tarefas opcionais. Para obter mais informações, consulte Instâncias spot do Amazon EC2.

Para obter uma comparação das diferentes opções de compra de instância do EC2, consulte Opções de faturamento e compra do Amazon EC2.

Conceitos

Antes de começar a trabalhar com as Instâncias spot, é necessário se familiarizar com os seguintes conceitos:

- Grupo de capacidade spot: um conjunto de instâncias do EC2 não utilizadas com o mesmo tipo de instância (por exemplo, `m5.large`) e zona de disponibilidade.
- Preço spot: o preço atual de uma instância spot por hora.
- Solicitação de instância Spot: solicita uma instância spot. Quando houver capacidade disponível, o Amazon EC2 atenderá à solicitação. Uma solicitação de instância spot é única ou persistente. O Amazon EC2 reenvia automaticamente uma solicitação de instância spot persistente depois que a instância spot associada à solicitação for interrompida.
- Recomendação de rebalanceamento de instância do EC2: o Amazon EC2 emite um sinal de recomendação de rebalanceamento de instância para avisar que uma instância spot apresenta risco elevado de interrupção. Esse sinal fornece uma oportunidade de rebalancear proativamente as workloads entre instâncias spot novas ou existentes sem que seja necessário aguardar o aviso de interrupção de dois minutos da instância spot.
- Interrupção de instância spot: o Amazon EC2 encerra, interrompe ou coloca em hibernação a instância spot quando o Amazon EC2 precisa novamente da capacidade. O Amazon EC2 fornece um aviso de interrupção da instância spot, enviando à instância um aviso de dois minutos antes que ela seja interrompida.

Diferenças entre instâncias spot e instâncias sob demanda

A tabela a seguir lista as principais diferenças entre instâncias spot e instâncias sob demanda.

	Spot Instances	On-Demand Instances
Horário do lançamento	Só poderá ser executado imediatamente se a solicitação da instância spot estiver ativa e a capacidade estiver disponível.	Só poderá ser executado imediatamente se você fizer uma solicitação de execução manual e se a capacidade estiver disponível.
Capacidade disponível	Se a capacidade não estiver disponível, a solicitação de instância spot continuará a fazer a solicitação de inicialização automaticamente até que a capacidade seja disponibilizada.	Se a capacidade não estiver disponível quando você fizer uma solicitação de execução, você receberá um erro de capacidade insuficiente (ICE).
Custo por hora	O preço por hora das instâncias spot varia de acordo com a demanda e oferta de longo prazo.	O preço por hora de Instâncias on-demand é estático.
Recomendação de rebalanceamento	O sinal que o Amazon EC2 emite para uma instância spot em execução quando a instância possui risco elevado de interrupção.	Você determina quando uma instância sob demanda é interrompida (parada ou encerrada).
Interrupção de instância	É possível interromper e iniciar uma instância spot baseada no Amazon EBS. Além disso, o Amazon EC2 poderá interromper uma instância spot individual se a capacidade não estiver mais disponível.	Você determina quando uma instância sob demanda é interrompida (parada ou encerrada).

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. Suas Instâncias spot serão executadas até que você as encerre, a capacidade não esteja mais disponível ou seu grupo do Amazon EC2 Auto Scaling as encerre durante o processo de reduzir a escala horizontalmente.

Se você ou o Amazon EC2 interromper uma instância spot em execução, você será cobrado pelos segundos usados ou pela hora completa, ou então não será cobrado, dependendo do sistema operacional usado e de quem interrompeu a instância spot. Para obter mais informações, consulte Faturamento para Instâncias spot interrompidas.

As instâncias spot não são cobertas pelos Savings Plans. Se tiver um Savings Plan, ele não oferecerá vantagens econômicas adicionais, além das que você já obtém com o uso de instâncias spots. Além disso, seus gastos com instâncias spot não aplicam os compromissos dos Savings Plans para computação.

Visualizar preços

Para ver o menor preço atual de instâncias spot (atualizado a cada cinco minutos) por Região da AWS e tipo de instância, consulte a página Definição de preço de instâncias spot do Amazon EC2.

Para visualizar o histórico de preços de spot dos últimos três meses, use o console do Amazon EC2 ou o comando describe-spot-price-history. Para obter mais informações, consulte Visualizar o histórico de preços de instância spot.

Mapeamos as zonas de disponibilidade para os códigos de cada Conta da AWS de maneira independente. Portanto, é possível obter resultados diferentes para o mesmo código de zona de disponibilidade (por exemplo, `us-west-2a`) entre contas diferentes.

Visualizar economias

É possível visualizar as economias feitas com o uso de instâncias spot para uma única frota spot ou para todas as instâncias spot. É possível 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.

Exibir faturamento

Sua fatura fornece detalhes sobre seu uso do serviço. Para obter mais informações, consulte Exibição da sua fatura no Guia do usuário do AWS Billing.

Práticas recomendadas para instâncias spot do Amazon EC2

O Amazon EC2 fornece acesso à capacidade computacional sobressalente do EC2 na Nuvem AWS que está disponível por meio de instâncias spot com um desconto de até 90% em comparação com os preços de instâncias sob demanda. A única diferença entre instâncias sob demanda e instâncias spot é que as instâncias spot poderão ser interrompidas pelo Amazon EC2, com dois minutos de notificação, se o Amazon EC2 precisar recuperar capacidade. Para garantir a melhor experiência com instâncias Spot, é importante entender e aplicar as práticas recomendadas de uso.

As Instâncias spot são recomendadas para aplicações flexíveis, tolerantes a falhas e sem estado. Por exemplo, as Instâncias spot funcionam bem para big data, workloads em contêineres, CI/CD, servidores Web sem estado, computação de alta performance (HPC) e workloads de renderização.

Durante a execução, as Instâncias spot são exatamente as mesmos que as Instâncias on-demand. No entanto, o Spot não garante que você possa manter as instâncias em execução tempo suficiente para concluir as workloads. O Spot também não garante que você possa obter disponibilidade imediata das instâncias que está procurando, nem que sempre possa obter a capacidade agregada solicitada. Além disso, as interrupções e a capacidade da instância spot podem mudar ao longo do tempo porque a disponibilidade da instância spot varia de acordo com a oferta e a demanda, e a performance passada não é uma garantia de resultados futuros.

As Instâncias spot não são adequadas para workloads que são inflexíveis, com estado, intolerantes a falhas ou fortemente acopladas entre nós de instância. As instâncias spot também não são recomendadas para workloads que não sejam tolerantes a períodos ocasionais em que a capacidade-alvo não está totalmente disponível. Seguir as práticas recomendadas para spot de ser flexível em termos de tipos de instância e zonas de disponibilidade é a melhor chance de ter alta disponibilidade, mas isso não garante que haverá capacidade disponível, pois os picos na demanda de instâncias sob demanda podem perturbar as workloads nas instâncias spot.

Não é recomendável usar instâncias spot para essas workloads nem tentar fazer failover para instâncias sob demanda como forma de lidar com interrupções ou períodos de indisponibilidade. Fazer failover para instâncias sob demanda pode inadvertidamente causar interrupções em outras instâncias spot. Além disso, se as instâncias spot de uma combinação de tipo de instância e zona de disponibilidade forem interrompidas, poderá ser difícil obter instâncias sob demanda com a mesma combinação.

Independentemente de você ser um usuário spot experiente ou iniciante na utilização de instâncias spot, se estiver enfrentando problemas com interrupções ou disponibilidade de instâncias spot no momento, recomendamos que siga essas práticas recomendadas para ter a melhor experiência usando o serviço spot.

Melhores práticas do Spot

- Preparar instâncias individuais para interrupções
- Ser flexível sobre tipos de instância e zonas de disponibilidade
- Usando a seleção de tipo de instância baseada em atributos
- Usar pontuações de posicionamento spot para identificar regiões e zonas de disponibilidade ideais
- Usar grupos do Auto Scaling ou a Frota do EC2 para gerenciar a capacidade agregada
- Usar a estratégia de alocação otimizada para preço e capacidade
- Use serviços integrados da AWS para gerenciar as instâncias spot
- Qual é o melhor método de solicitação spot para usar?

Preparar instâncias individuais para interrupções

A melhor maneira de lidar com interrupções de instâncias spot com tranquilidade é arquitetar a aplicação para que ela seja tolerante a falhas. Para fazer isso, é possível aproveitar as recomendações de rebalanceamento de instâncias do EC2 e avisos de interrupção de instâncias spot.

Uma recomendação de rebalanceamento de uma instância do EC2 é um sinal que notifica você quando uma instância spot corre grande risco de interrupção. O sinal oferece a oportunidade de gerenciar proativamente a instância spot antes do aviso de interrupção de dois minutos da instância spot. É possível decidir rebalancear sua workload em Instâncias spot novas ou existentes que não tenham risco elevado de interrupção. Tornamos mais fácil para você usar esse sinal por meio do atributo de rebalanceamento de capacidade nos grupos do Auto Scaling e na Frota do EC2.

Um aviso de interrupção da instância spot é um aviso emitido dois minutos antes de o Amazon EC2 interromper uma instância spot. Se a workload tiver “flexibilidade de tempo”, também é possível configurar as instâncias Spot para serem interrompidas ou para hibernarem, em vez de serem encerradas, quando forem interrompidas. O Amazon EC2 interrompe ou hiberna automaticamente suas instâncias spot durante a interrupção e retoma automaticamente as instâncias quando tivermos capacidade disponível.

Recomendamos que você crie uma regra no Amazon EventBridge que capture as recomendações de rebalanceamento e os avisos de interrupção e acione um ponto de verificação para o andamento da workload ou lide tranquilamente com a interrupção. Para obter mais informações, consulte Monitorar os sinais de recomendação de rebalanceamento. Para obter um exemplo detalhado que orienta você sobre como criar e usar regras de evento, consulte Aproveitar os avisos de interrupção de instância spot do Amazon EC2.

Para obter mais informações, consulte Recomendações de rebalanceamento de instâncias do EC2 e Interrupções de instâncias spot.

Ser flexível sobre tipos de instância e zonas de disponibilidade

Um grupo de capacidade spot é um conjunto de instâncias do EC2 não utilizadas, com o mesmo tipo de instância (por exemplo, `m5.large`) e a zona de disponibilidade (por exemplo, us-east-1a). É necessário ser flexível sobre quais tipos de instância solicita e em quais zonas de disponibilidade pode implantar a workload. Isso dá ao Spot uma chance melhor de encontrar e alocar a quantidade necessária de capacidade computacional. Por exemplo, não peça apenas `c5.large` se você está disposto a usar grandes das famílias c4, m5 e m4.

Dependendo de suas necessidades específicas, é possível avaliar para quais tipos de instância é possível ter flexibilidade para atender aos requisitos de computação. Se uma workload puder ser dimensionada verticalmente, é necessário incluir tipos de instância maiores (mais vCPUs e memória) nas solicitações. Se você puder dimensionar somente horizontalmente, deverá incluir tipos de instância de geração mais antiga, pois eles têm menos demanda de clientes sob demanda.

Uma boa regra geral é ser flexível para pelo menos 10 tipos de instância para cada workload. Além disso, verifique se todas as zonas de disponibilidade estão configuradas para uso na VPC e selecionadas para a workload.

Usando a seleção de tipo de instância baseada em atributos

Com a seleção do tipo de instância baseada em atributos, você pode especificar atributos de instância, como vCPUs, memória e armazenamento, para a workload que você quer executar. O EC2 Auto Scaling ou a frota do EC2 automaticamente identificará e inicializará instâncias que correspondam aos atributos especificados. Isso elimina o esforço necessário para selecionar manualmente tipos de instância específicos, o que exige um entendimento profundo da oferta de cada tipo de instância.

Além disso, a seleção do tipo de instância baseada em atributos permite que você use automaticamente tipos de instância recém-inicializados à medida que eles se tornam disponíveis. Isso garante acesso contínuo a uma gama cada vez mais ampla de capacidade de instância spot.

A seleção de tipo de instância baseada em atributos é ideal para workloads e frameworks que podem ser flexíveis em relação aos tipos de instância que são executadas, como workloads de computação de alta performance (HPC) e de big data.

Para obter mais informações, consulte Create mixed instances group using attribute-based instance type selection no Guia do usuário do Amazon EC2 Auto Scaling e Especificar atributos para seleção de tipo de instância para frota do EC2 ou frota spot neste guia.

Usar pontuações de posicionamento spot para identificar regiões e zonas de disponibilidade ideais

As instâncias spot são a capacidade não utilizada do EC2, e essa capacidade flutua com base na oferta e na demanda do EC2. Como resultado, talvez você nem sempre obtenha a capacidade spot exata de que precisa em um local específico e em um horário específico. Para mitigar essa imprevisibilidade, você pode usar o recurso de pontuação de posicionamento spot. Esse recurso fornece recomendações para regiões ou zonas de disponibilidade com maior probabilidade de ter capacidade suficiente para atender às suas necessidades de capacidade spot sem exigir que você inicialize primeiro instâncias spot nestes locais.

A pontuação de posicionamento spot é mais bem usada para workloads que podem ser flexíveis quanto aos tipos de instância e à região ou zona de disponibilidade que elas podem usar. Tudo que você precisa fazer é especificar a capacidade spot necessária, seus requisitos de tipo de instância e se você quer recomendações para regiões ou zonas de disponibilidade. Em troca, você recebe uma pontuação que varia de 1 a 10 para cada região ou zona de disponibilidade, indicando a probabilidade do provisionamento com êxito da capacidade spot solicitada naquele local. Uma pontuação de 10 indica que a solicitação de spot tem alta probabilidade de êxito.

É importante observar que a pontuação de posicionamento spot é uma recomendação pontual, pois a capacidade pode variar com o tempo. Ela não garante capacidade disponível nem prevê o risco de interrupção.

É possível usar o recurso de pontuação de posicionamento spot no console do Amazon EC2, na AWS CLI ou em um SDK. Para obter mais informações, consulte Pontuação de posicionamento de spot.

Usar grupos do Auto Scaling ou a Frota do EC2 para gerenciar a capacidade agregada

O spot permite que você pense em termos de capacidade agregada, ou seja, em unidades que incluem vCPUs, memória, armazenamento ou throughput de rede, em vez de pensar em termos de instâncias individuais. Os grupos do Auto Scaling e a Frota do EC2 permitem iniciar e manter uma capacidade pretendida, e solicitar recursos para substituir automaticamente os que forem interrompidos ou encerrados manualmente. Ao configurar um grupo do Auto Scaling ou uma Frota do EC2, você só precisa especificar os tipos de instância e a capacidade pretendida de acordo com as necessidades da aplicação. Para obter mais informações, consulte Grupos de Auto Scaling no Guia do usuário do Amazon EC2 Auto Scaling e Criar uma Frota do EC2. neste guia do usuário.

Usar a estratégia de alocação otimizada para preço e capacidade

As estratégias de alocação nos grupos de Auto Scaling ajudam a provisionar a capacidade prevista sem a necessidade de procurar manualmente os grupos de capacidade spot com capacidade adicional. Recomendamos o uso da estratégia `price-capacity-optimized`, pois ela provisiona automaticamente as instâncias dos grupos de capacidade spot mais disponíveis que também têm o menor preço possível. Também é possível aproveitar a estratégia de alocação de `price-capacity-optimized` na Frota do EC2. Como a capacidade da instância spot é proveniente de grupos com capacidade ideal, isso diminui a possibilidade de que as instâncias spot sejam recuperadas. Para obter mais informações, consulte Estratégias de alocação para vários tipos de instâncias no Guia do usuário do Amazon EC2 Auto Scaling e Quando as workloads têm um alto custo de interrupção neste guia do usuário.

Use serviços integrados da AWS para gerenciar as instâncias spot

Outros serviços da AWS integram-se ao Spot para reduzir os custos gerais de computação sem a necessidade de gerenciar instâncias ou frotas individuais. Recomendamos considerar as soluções a seguir para suas workloads aplicáveis: Amazon EMR, Amazon Elastic Container Service, AWS Batch, Amazon Elastic Kubernetes Service, Amazon SageMaker AI, AWS Elastic Beanstalk e Amazon GameLift Servers. Para saber mais sobre as melhores práticas do Spot com esses serviços, consulte o Site de workshops de Instâncias spot do Amazon EC2.

Qual é o melhor método de solicitação spot para usar?

Use a tabela a seguir para determinar qual API usar ao solicitar instâncias spot.

solicitações de	Quando usar?	Caso de uso	Devo usar esta API?
			Sim

solicitações de	Quando usar?	Caso de uso	Devo usar esta API?
CreateAutoScalingGroup	• Você precisa de várias instâncias com uma só configuração ou uma configuração mista. • Você deseja automatizar o gerenciamento do ciclo de vida por meio de uma API configurável.	Crie um grupo do Auto Scaling que gerencie o ciclo de vida de suas instâncias enquanto mantém o número desejado de instâncias. Compatível com dimensionamento horizontal da escala (adição de mais instâncias) entre os limites mínimo e máximo especificados.	

solicitações de	Quando usar?	Caso de uso	Devo usar esta API?
CreateFleet	• Você precisa de várias instâncias com uma só configuração ou uma configuração mista. • Você deseja gerenciar por conta própria o ciclo de vida da instância. • Se não precisar de autoescalabilidade, recomendamos que use um tipo `instant` de frota.	Crie uma frota de instâncias sob demanda e instâncias spot em uma única solicitação, com várias especificações de execução, que variam de acordo com o tipo de instância, a AMI, a zona de disponibilidade ou a sub-rede. Por padrão, a estratégia de alocação de instância spot usa o `lowest-price` por unidade, mas é possível alterá-la para `price-capacity-optimized`, `capacity-optimized` ou `diversified`.	Sim. No modo `instant` se não houver necessidade de autoescalabilidade

solicitações de	Quando usar?	Caso de uso	Devo usar esta API?
RunInstances	• Você já está usando a API RunInstances para executar instâncias sob demanda e simplesmente deseja mudar para a execução de instâncias spot alterando um só parâmetro. • Você não precisa de várias instâncias com diferentes tipos de instância.	Execute um número especificado de instâncias usando uma AMI e um tipo de instância.	Não. Porque RunInstances não permite tipos de instâncias mistas em uma única solicitação

solicitações de	Quando usar?	Caso de uso	Devo usar esta API?
RequestSpotFleet	• Desencorajamos fortemente o uso da API RequestSpotFleet por ser uma API herdada e sem investimento planejado. • Se quiser gerenciar o ciclo de vida da sua instância, use a API CreateFleet. • Se não quiser gerenciar o ciclo de vida da sua instância, use a API CreateAutoScalingGroup.	NÃO USE. RequestSpotFleet é uma API herdada e sem investimento planejado.	Não
RequestSpotInstances	• Desencorajamos fortemente o uso da API RequestSpotInstances por ser uma API herdada e sem investimento planejado.	NÃO USE. RequestSpotInstances é uma API herdada e sem investimento planejado.	Não

Como as Instâncias spot funcionam

Para iniciar uma instância Spot, você cria uma solicitação de instância spot ou o Amazon EC2 cria uma solicitação de instância spot em seu nome. A instância spot é iniciada quando a solicitação de instância spot é atendida.

É possível iniciar uma instância spot usando vários serviços diferentes. Para obter mais informações, consulte Conceitos básicos das instâncias spot do Amazon EC2. Neste guia do usuário, descrevemos as seguintes maneiras de executar uma instância spot usando o EC2:

- É possível criar uma solicitação de instância spot usando o assistente de inicialização de instâncias no console do Amazon EC2 ou o comando run-instances. Para obter mais informações, consulte Gerenciar as instâncias spot.
- É possível criar uma EC2 Fleet e nela especificar o número desejado de instâncias spot. O Amazon EC2 cria uma solicitação de instância spot em seu nome para cada instância spot especificada na EC2 Fleet. Para obter mais informações, consulte Criar uma Frota do EC2..
- É possível criar uma frota spot e nela especificar o número desejado de instâncias spot. O Amazon EC2 cria uma solicitação de instância spot em seu nome para cada instância spot especificada na solicitação de frota spot. Para obter mais informações, consulte Criar uma Frota spot.

Sua instância spot será iniciada se houver capacidade disponível. Sua instância spot será executada até que você a interrompa ou a encerre, ou até que o Amazon EC2 a interrompa (processo conhecido como interrupção da instância spot). O Amazon EC2 pode parar, encerrar ou hibernar uma instância spot ao interrompê-la.

Quando você usa instâncias spot, deve estar preparado para interrupções. O Amazon EC2 poderá interromper a sua instância spot quando a demanda por instâncias spot aumentar ou quando o suprimento 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 instâncias spot.

Conteúdo

- Estados da solicitação de instância spot
- Executar Instâncias spot em um grupo de execução
- Executar Instâncias spot em um grupo de zonas de disponibilidade
- Executar Instâncias spot em uma VPC

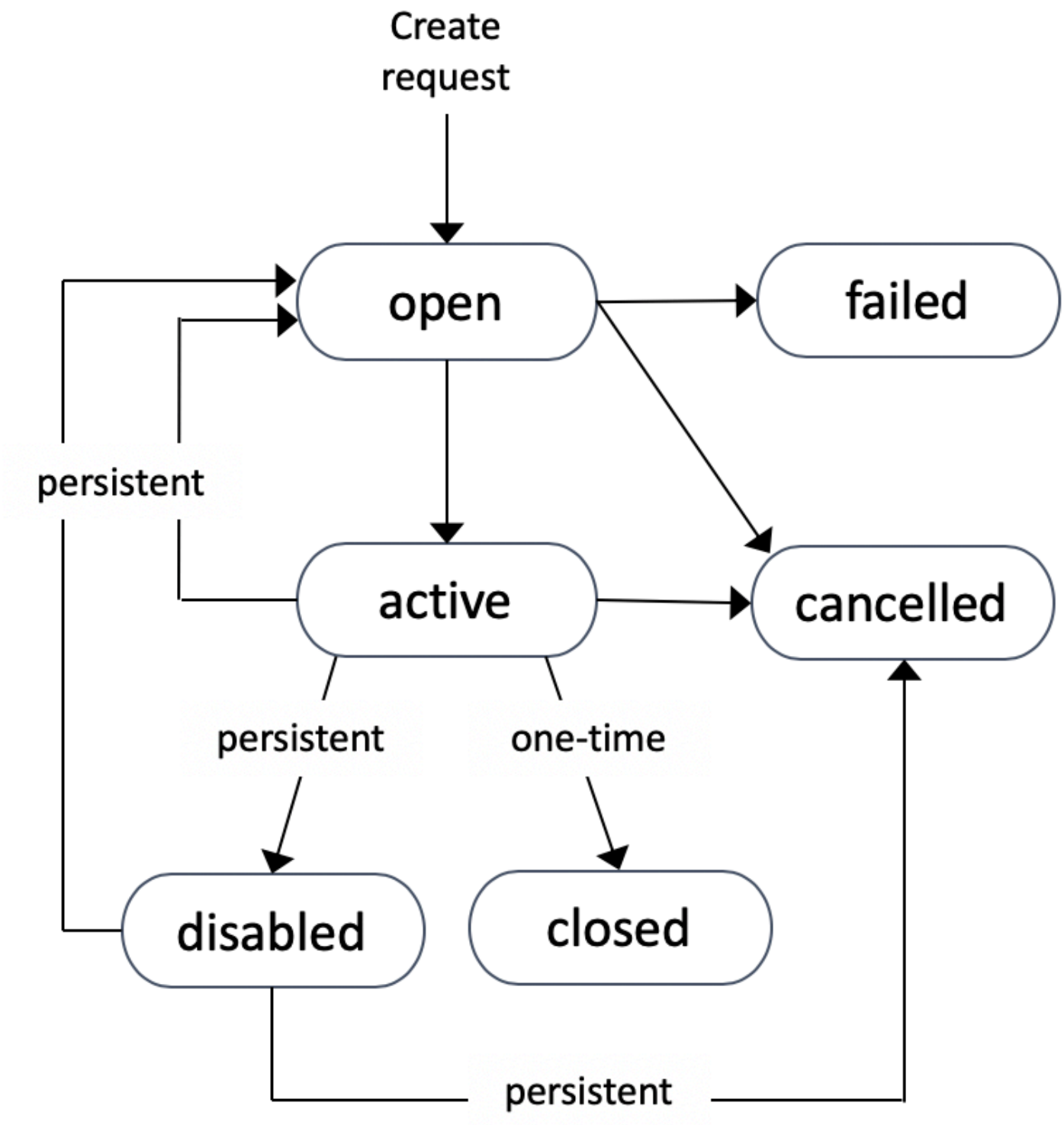
- Executar instâncias de desempenho expansível
- Executar no hardware de locatário único

Estados da solicitação de instância spot

Uma solicitação de instância spot pode estar em um dos seguintes estados:

- `open` – A solicitação está esperando para ser atendida.
- `active` – A solicitação foi atendida e tem uma instância spot associada.
- `failed` – A solicitação tem um ou mais parâmetros inválidos.
- `closed` – A instância spot foi interrompida ou encerrada.
- `disabled` – Você parou a instância spot.
- `cancelled` – Você cancelou a solicitação ou ela expirou.

A ilustração a seguir representa as transições entre os estados da solicitação. Observe que as transições dependem do tipo de solicitação (única ou persistente).



Uma solicitação de instância spot única permanece ativa até o Amazon EC2 executar a instância spot, a solicitação expirar ou você cancelar a solicitação. Se não houver capacidade 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 não houver capacidade disponível, sua instância spot será interrompida. Depois que a instância é interrompida, quando houver novamente capacidade disponível, a instância spot será iniciada (se estiver parada) ou retomada (se estiver hibernada). É possível parar uma instância spot e reiniciá-la quando houver capacidade disponível. Se a instância spot for encerrada (independentemente de estar parada ou em execução), a solicitação de instância spot será reaberta e o Amazon EC2 iniciará uma nova instância spot. Para mais informações, consulte Parar uma instância spot, Iniciar uma instância spot e Encerrar uma instância spot.

É possível acompanhar o status das solicitações de instância spot, bem como o status das instâncias spot executadas, pelo status. Para obter mais informações, consulte Obter o status de uma solicitação de instância spot.

Executar Instâncias spot em um grupo de execução

Especifique um grupo de execução na solicitação de instância spot para instruir o Amazon EC2 a executar um conjunto de instâncias spot somente se ele puder executar todas elas. Além disso, se o serviço spot precisar encerrar uma das instâncias em um grupo de execução, ele deverá encerrar todas elas. Contudo, se você encerrar uma ou mais instâncias em um grupo de execução, o Amazon EC2 não encerrará as instâncias restantes no grupo de execução.

Embora essa opção possa ser útil, adicionar essa restrição pode diminuir as chances de a sua solicitação de instância spot ser atendida e aumenta as chances de encerramento das instâncias spot. Por exemplo, seu grupo de execução inclui instâncias em várias zonas de disponibilidade. Se a capacidade em uma dessas zonas de disponibilidade diminuir e não estiver mais disponível, o Amazon EC2 encerrará todas as instâncias do grupo de execução.

Se você criar outra solicitação de instância spot bem-sucedida que especifique o mesmo grupo de execução (existente) de uma solicitação bem-sucedida anterior, as novas instâncias serão adicionadas ao grupo de execução. Subsequentemente, se uma instância nesse grupo de execução for encerrada, todas as instâncias no grupo de execução serão encerradas, o que inclui instâncias executadas pela primeira e a segunda solicitações.

Executar Instâncias spot em um grupo de zonas de disponibilidade

Especifique um grupo de zonas de disponibilidade na solicitação de instância spot para informar ao Amazon EC2 para iniciar um conjunto de instâncias spot na mesma zona de disponibilidade. O Amazon EC2 não precisa interromper todas as instâncias em um grupo de zonas de disponibilidade

ao mesmo tempo. Se o Amazon EC2 precisar interromper uma das instâncias em um grupo de zonas de disponibilidade, as outras permanecerão em execução.

Embora essa opção possa ser útil, a adição dessa restrição pode reduzir as possibilidades de sua solicitação de instância spot ser atendida.

Se você especificar um grupo de zonas de disponibilidade, mas não especificar uma zona de disponibilidade na solicitação de instância spot, o resultado dependerá da rede especificada.

VPC padrão

O Amazon EC2 usa a zona de disponibilidade para a sub-rede especificada. Se você não especificar uma sub-rede, ele selecionará uma zona de disponibilidade e sua sub-rede padrão, mas não necessariamente a zona de preço mais baixo. Se você excluir a sub-rede padrão de uma zona de disponibilidade, deverá especificar uma sub-rede diferente.

VPC não padrão

O Amazon EC2 usa a zona de disponibilidade para a sub-rede especificada.

Executar Instâncias spot em uma VPC

Especifique uma sub-rede para as Instâncias spot da mesma maneira que você especifica uma sub-rede para as Instâncias on-demand.

- [VPC padrão] Se você quiser que a instância spot seja executada em uma zona de disponibilidade de baixo preço, especifique 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] Especifique a sub-rede da instância spot.

Executar instâncias de desempenho expansível

Os tipos de instância T são instâncias de desempenho expansível. Se você executar as Instâncias spot usando um tipo de instância expansível e planejar usar as instâncias spot expansíveis imediatamente e por um breve período, sem tempo ocioso para acumular créditos de CPU, recomendamos iniciá-las no modo padrão para evitar pagar custos mais elevados. Se executar as Instâncias spot expansíveis no modo ilimitado e esgotar a CPU imediatamente, você gastará os créditos excedentes por isso. Se a instância for usada por um curto período, não haverá tempo para

acumular créditos de CPU para pagamento dos créditos excedentes, e você precisará pagar os créditos excedentes ao encerrar a instância.

O modo ilimitado será adequado para instâncias spot expansíveis somente se a instância for executada por tempo suficiente para acumular créditos de CPU para expansão. Caso contrário, pagar por créditos excedentes torna a as instâncias spot expansíveis mais caras do que o uso de outras instâncias. Para obter mais informações, consulte Quando usar o modo ilimitado versus CPU fixa.

As instâncias T2, quando configuradas no modo Padrão, recebem créditos de inicialização. As instâncias T2 são as únicas instâncias de performance expansível que recebem créditos de inicialização. Os créditos de lançamento são feitos para fornecer uma experiência de lançamento inicial produtiva para instâncias T2 fornecendo recursos computacionais suficientes para configurar a instância. Lançamentos repetidos de instâncias T2 para acessar novos créditos de lançamento não são permitidos. Se você precisar de uma CPU sustentada, poderá obter créditos (ficando inativo durante um período), usar o modo Ilimitado para T2 Instâncias spot ou usar um tipo de instância com CPU dedicada.

Executar no hardware de locatário único

É possível executar uma instância spot no hardware de ocupante único. As instâncias spot dedicadas são fisicamente isoladas de instâncias que pertencem a outras contas da AWS. Para obter mais informações, consulte Instâncias dedicadas do Amazon EC2 e as 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 Gerenciar as instâncias spot.
- Solicite uma solicitação spot em uma VPC com uma locação de instância `dedicated`. Para obter mais informações, consulte Iniciar Instâncias dedicadas em uma VPC com a locação padrão. Você não poderá solicitar uma instância spot com uma locação `default` se solicitá-la em uma VPC com uma locação de instância `dedicated`.

Todas as famílias de instâncias são compatíveis com Instâncias spot dedicadas, exceto instâncias T. Para cada família de instâncias compatíveis, apenas o maior tamanho de instância ou tamanho de metal é compatível com Instâncias spot dedicadas.

Visualizar o histórico de preços de instância spot

Os preços de instâncias spot são definidos pelo Amazon EC2 e ajustados gradualmente de acordo com tendências de longo prazo da oferta e da demanda de capacidade de instâncias spot.

Quando sua solicitação de spot for atendida, as instâncias spot serão iniciadas pelo preço spot atual, não excedendo o preço sob demanda. É possível visualizar o histórico de preços spot dos últimos 90 dias, filtrando por tipo de instância, sistema operacional e zona de disponibilidade.

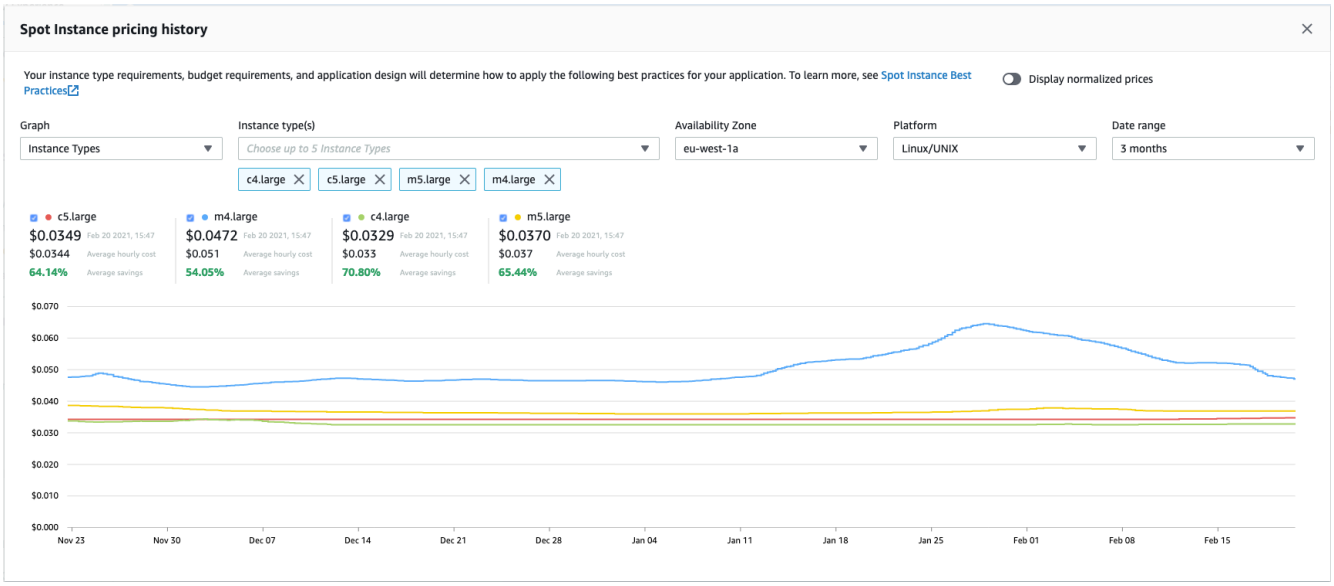
Para obter os preços de instâncias spot atuais, consulte a definição de preço de instâncias spot do Amazon EC2.

Console

Para visualizar o histórico de preços de spot

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Solicitações spot.
3. Escolha Histórico de definição de preço.
4. Em Graph (Gráfico), escolha comparar o histórico de preços por Availability Zones (Zonas de disponibilidade) ou por Instances Types (Tipos de Instância).
   - Se escolher Zonas de disponibilidade, escolha o Tipo de instância, o sistema operacional (Plataforma e o Intervalo de datas para os quais deseja visualizar o histórico de preços.
   - Se escolher Tipos de instância, escolha até cinco Tipos de instância, a Zona de disponibilidade, o sistema operacional (Plataforma) e o Intervalo de datas para os quais deseja visualizar o histórico de preços.

   A captura de tela a seguir mostra uma comparação de preços para diferentes tipos de instância.



5. Mova o ponteiro do mouse sobre o gráfico para exibir os preços em horas específicas no intervalo de datas selecionado. Os preços são exibidos nos blocos de informações acima do gráfico. O preço exibido na linha superior mostra o preço em uma data específica. O preço exibido na segunda linha mostra o preço médio durante o intervalo de datas selecionado.
6. Para exibir o preço por vCPU, ative a opção Display normalized prices (Exibir preços normalizados). Para exibir o preço do tipo de instância, desative Display normalized prices (Exibir preços normalizados).

AWS CLI

Para visualizar o histórico de preços de spot

Use o seguinte comando describe-spot-price-history.

```
aws ec2 describe-spot-price-history \
    --instance-types c6i.xlarge \
    --product-descriptions "Linux/UNIX" \
    --start-time 2025-04-01T00:00:00 \
    --end-time 2025-04-02T00:00:0
```

PowerShell

Para visualizar o histórico de preços de spot

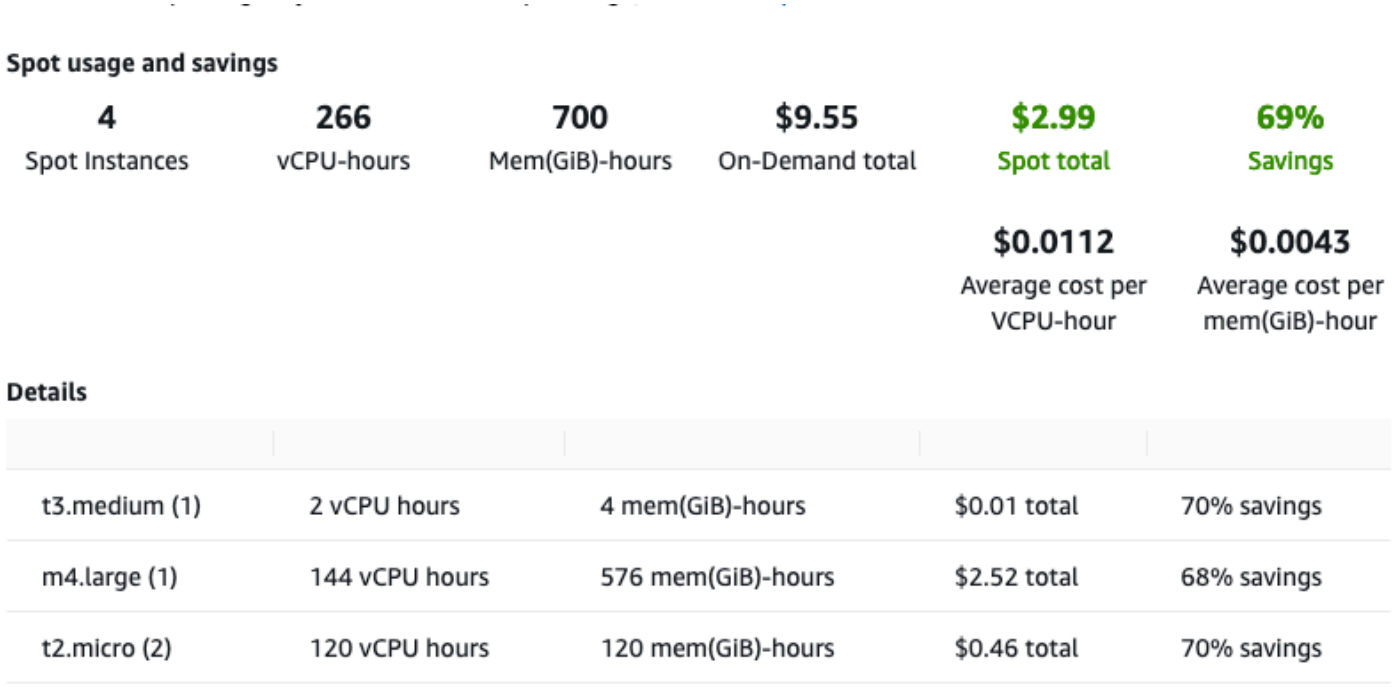
Use o cmdlet Get-EC2SpotPriceHistory.

```
Get-EC2SpotPriceHistory `
    -InstanceType c6i.xlarge `
    -ProductDescription "Linux/UNIX" `
    -UtcStartTime 2025-04-01T00:00:00 `
    -UtcEndTime 2025-04-02T00:00:0
```

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. É possível visualizar essas informações da última hora ou dos últimos três dias.

A captura de tela a seguir da seção Savings (Economia) mostra as informações de uso e de economia spot de uma frota spot.



É possível visualizar as seguintes informações de uso e de economia:

- Spot Instances (Instâncias spot): o número de instâncias spot executadas e encerradas pela frota spot. Ao visualizar o resumo de economias, o número representa todas as Instâncias spot em execução.

- vCPU-hours (Horas de vCPU) – o número de horas de vCPU usadas entre todas as Instâncias spot no período selecionado.
- Mem(GiB)-hours (Horas de mem(GiB)) – o número de horas de GiB usadas entre todas as Instâncias spot no período selecionado.
- On-Demand total (Total sob demanda) – a quantidade total que você pagaria pelo período de tempo selecionado se tivesse executado essas instâncias como Instâncias on-demand.
- Spot total (Total de Spot) – a quantidade total a ser paga para o período selecionado.
- Savings (Economias) – a porcentagem economizada por não pagar o preço sob demanda.
- Average cost per vCPU-hour (Custo médio por hora de vCPU) – o custo médio por hora de uso das vCPUs entre todas as Instâncias spot para o período selecionado, calculado da seguinte forma: Average cost per vCPU-hour (Custo médio por hora de vCPU) = Spot total (Total de Spot) / vCPU-hours (Horas de vCPU).
- Average cost per mem(GiB)-hour (Custo médio por hora de mem(GiB)) – o custo médio por hora de uso de GiBs entre todas as Instâncias spot para o período selecionado, calculado da seguinte forma: Average cost per mem(GiB)-hour (Custo médio por hora de mem(GiB)) = Spot total (Total de Spot) / mem(GiB)-hours (Horas de mem(GiB)).
- Tabela Details (Detalhes): os diferentes tipos de instância (o número de instâncias por tipo de instância está entre parênteses) que compõem a frota spot. Ao visualizar o resumo de economias, isso representa todas as Instâncias spot em execução.

As informações de economias podem ser visualizadas apenas usando o console do Amazon EC2.

Para visualizar as informações de economia de uma frota spot

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Solicitações spot.
3. Selecione o ID de uma frota spot e role até seção Savings (Economia).

   Se preferir, marque a caixa de seleção ao lado do ID de solicitação de frota spot e escolha a guia Economia.
4. Por padrão, a página exibe as informações de uso e de economia dos últimos três dias. É possível 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 economia de todas as instâncias spot em execução

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).

Criar uma solicitação de instância spot

Para usar instâncias spot, crie uma solicitação de instância spot que inclua o número de instâncias desejado, o tipo de instância e a zona de disponibilidade. Se houver capacidade disponível, o Amazon EC2 atenderá à solicitação imediatamente. Caso contrário, o Amazon EC2 esperará até a sua solicitação puder ser atendida ou até você cancelar a solicitação.

É possível usar o assistente de inicialização de instâncias no console do Amazon EC2 ou o comando run-instances para solicitar uma instância spot da mesma forma que é possível executar uma instância sob demanda. Este método é recomendado apenas pelos seguintes motivos:

- Você já está usando o assistente de execução de instância ou o comando run-instances para executar instâncias sob demanda e quer mudar para a execução de instâncias spot alterando um único parâmetro.
- Você não precisa de várias instâncias com diferentes tipos de instância.

Esse método geralmente não é recomendado para executar instâncias spot porque você não pode especificar vários tipos de instância e não é possível executar instâncias spot e instâncias sob demanda na mesma solicitação. Para os métodos preferidos de execução de instâncias spot, que incluem a execução de uma frota que inclui instâncias spot e instâncias sob demanda com vários tipos de instância, consulte Qual é o melhor método de solicitação spot para usar?

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 monitorar solicitações de instâncias spot, consulte Obter o status de uma solicitação de instância spot.

Console

Para criar uma solicitação de instância spot

As etapas de 1 a 9 são as mesmas que você usaria para executar uma instância sob demanda. Na Etapa 10, você configura a solicitação da instância spot.

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Na barra de navegação na parte superior da tela, selecione uma região.
3. No painel do console do Amazon EC2, selecione Launch instance (Executar instância).
4. (Opcional) Em Name and tags (Nome e etiquetas), é possível nomear a instância e marcar a solicitação de instância spot, a instância, os volumes e os gráficos elásticos. Para obter mais informações sobre tags, consulte Marcar com tag os recursos do Amazon EC2.

   a. Em Name (Nome), insira um nome descritivo para a instância.

      O nome da instância é uma tag em que a chave é Name (Nome) e o valor é o nome que você especificar. Se você não especificar um nome, a instância poderá ser identificada por seu ID, que é gerado automaticamente quando você inicia a instância.

   b. Para marcar a solicitação de instância spot, a instância, os volumes e os elementos gráficos elásticos, escolha Add additional tags (Adicionar outras etiquetas). Escolha Add tag (Adicionar tag), insira uma chave e um valor, e selecione o tipo de recurso a aplicar a tag. Escolha Add tag (Adicionar tag) para cada tag adicional a acrescentar.
5. Em Application and OS Images (Amazon Machine Image), (Imagens de aplicações e sistemas operacionais (imagem de máquina da Amazon), escolha o sistema operacional da instância e selecione uma AMI. Para obter mais informações, consulte Imagens de aplicações e sistemas operacionais (imagem de máquina da Amazon).
6. Em Instance type (Tipo de instância), selecione o tipo de instância que atende aos requisitos para a configuração do hardware e o tamanho da instância. Para obter mais informações, consulte Tipo de instância.
7. Em Key pair (login) (Par de chaves: login) escolha um par de chaves existente ou selecione Create new key pair (Criar um novo par de chaves) para criar um novo. Para obter mais informações, consulte Pares de chaves do Amazon EC2 e instâncias do Amazon EC2.

> **Important**
>
> Se você escolher a opção Proceed without key pair (Not recommended) (Prosseguir sem par de chaves, não recomendado), não conseguirá se conectar à instância a menos que escolha uma AMI configurada para permitir que os usuários façam login de outro modo.

8. Em Network settings (Configurações de rede), use as configurações padrão ou escolha Edit (Editar) para definir as configurações de rede, conforme necessário.

   Os grupos de segurança fazem parte das configurações de rede e definem regras de firewall para a instância. Essas regras especificam qual tráfego de rede de entrada será fornecido para sua instância.

   Para obter mais informações, consulte Configurações de rede.

9. A AMI que você selecionou inclui um ou mais volumes de armazenamento, incluindo o volume de dispositivo raiz. Na página Configure storage (Configurar armazenamento), especifique os volumes adicionais para anexar à instância escolhendo Add New Volume (Adicionar novo volume). Para obter mais informações, consulte Configurar armazenamento.

10. Em Advanced details (Detalhes avançados), configure a solicitação de instância spot da seguinte maneira:

    a. Em Opção de compra, marque a caixa de seleção Solicitar instâncias spot.

    b. É possível manter a configuração padrão para a solicitação de instância spot ou escolher Customize (Personalizar), à direita, para especificar configurações personalizadas para a solicitação da instância spot.

       Ao escolher a opção Customize (Personalizar), os campos a seguir serão exibidos.

       i. Preço máximo: e possível solicitar instâncias spot pelo preço spot, limitado ao preço sob demanda ou especificar o valor máximo que você está disposto a pagar.

          > **Warning**
          >
          > Se você especificar um preço máximo, as instâncias serão interrompidas com mais frequência do que se você escolher No maximum price (Sem preço máximo).

Se você especificar um preço máximo, ele deverá ser superior a USD 0,001. Especificar um valor abaixo de USD 0,001 resultará em uma falha na inicialização.

- Sem preço máximo: a instância spot será executada pelo preço spot atual. O preço nunca excederá o preço sob demanda. (Recomendado)
- Defina seu preço máximo (por instância/hora): você pode especificar o valor máximo que estiver disposto a pagar.
  - Se você especificar um preço máximo inferior ao preço spot atual, a instância spot não será executada.
  - Se você especificar um preço máximo superior ao preço spot atual, a instância spot será executada e cobrada de acordo com o preço spot atual. Depois que a instância spot estiver em execução, se o preço spot subir acima do preço máximo, o Amazon EC2 interromperá a instância spot.
  - Independentemente do preço máximo especificado, você sempre será cobrado o preço Spot atual.

  Para analisar as tendências de preços spot, consulte Visualizar o histórico de preços de instância spot.

ii. Tipos de solicitação: o tipo de solicitação de instância spot escolhido determina o que acontece se a instância spot for interrompida.

- Única: o Amazon EC2 faz uma solicitação única para a instância spot. Se a instância spot for interrompida, a solicitação não será reenviada.
- Solicitação persistente: o Amazon EC2 faz uma solicitação persistente para a instância spot. Se a instância spot for interrompida, a solicitação será reenviada para reabastecer a instância spot interrompida.

Se você não especificar um valor, o padrão é uma solicitação única.

iii. Valid to (Válido para): a data de expiração de uma solicitação de instância spot persistente.

Esse campo não é compatível com solicitações únicas. Uma solicitação única permanece ativa até que todas as instâncias da solicitação expirem ou você cancele a solicitação.

- Nenhuma data de expiração da solicitação: a solicitação permanecerá ativa até você cancelá-la.
- Defina a data de validade da solicitação: a solicitação persistente permanece ativa até a data especificada ou até que você a cancele.

iv. Comportamento de interrupção: o comportamento escolhido determina o que acontece quando uma instância spot é interrompida.

- Em solicitações persistentes, os valores válidos são Parar e Hibernar. Quando uma instância é parada ocorrem cobranças pelo armazenamento do volume EBS.

> **Note**
>
> As instâncias spot agora usam a mesma funcionalidade de hibernação que as instâncias sob demanda. Para habilitar a hibernação, você pode escolher Hibernar aqui ou Habilitar no campo Comportamento de parar - hibernar, que aparece mais abaixo no assistente de inicialização de instância. Para conhecer os pré-requisitos de hibernação, consulte Pré-requisitos para a hibernação de instância do EC2.

- Para as solicitações únicas, somente Terminate (Encerrar) é válido.

Se você não especificar um valor, o padrão é Terminate (Encerrar) que não é válido para uma solicitação de instância spot persistente. Se você mantiver o padrão e tentar executar uma solicitação de instância spot persistente, receberá um erro.

Para obter mais informações, consulte Comportamento das interrupções de instâncias spot.

11. No painel Summary (Resumo), para Number of instances (Número de instâncias), insira o número de instâncias a serem executadas.

> **Note**
>
> O Amazon EC2 cria uma solicitação distinta para cada instância spot.

12. No painel Summary (Resumo), revise os detalhes da instância e faça as alterações necessárias. Depois de enviar sua solicitação de instância spot, não é possível alterar os

parâmetros da solicitação. É possível navegar diretamente para uma seção no assistente de execução de instância, escolhendo seu link no painel Summary (Resumo). Para obter mais informações, consulte Resumo.

13. Quando estiver pronto para iniciar a instância, escolha Launch instance (Iniciar instância).

    Se a instância não executar ou o estado passar imediatamente para `terminated`, em vez de `running`, consulte Solucionar problemas de inicialização de instâncias do Amazon EC2.

AWS CLI

Para criar uma solicitação de instância spot usando run-instances

Use o comando run-instances e especifique as opções da instância spot no parâmetro `--instance-market-options` como segue.

```
--instance-market-options file://spot-options.json
```

Veja a seguir a estrutura de dados a ser especificada no arquivo JSON. Também é possível especificar `ValidUntil` e `InstanceInterruptionBehavior`. Se você não especificar um campo na estrutura de dados, será usado o valor padrão.

O exemplo a seguir cria uma solicitação `persistent`.

```
{
  "MarketType": "spot",
  "SpotOptions": {
    "SpotInstanceType": "persistent"
  }
}
```

Para criar uma solicitação de instância spot usando request-spot-instances

> **Note**
>
> Não recomendamos o uso do comando request-spot-instances por ser uma API herdada e sem investimento planejado. Para obter mais informações, consulte Qual é o melhor método de solicitação spot para usar?

Use o comando request-spot-instances para criar uma solicitação única:

```
aws ec2 request-spot-instances \
    --instance-count 5 \
    --type "one-time" \
    --launch-specification file://specification.json
```

Use o comando request-spot-instances para criar uma requisição persistente:

```
aws ec2 request-spot-instances \
    --instance-count 5 \
    --type "persistent" \
    --launch-specification file://specification.json
```

Para que os arquivos de especificação de execução de exemplo sejam usados com esses comandos, consulte Exemplo de especificações de execução de solicitações de instância spot. Se você baixar um arquivo de especificação de execução no console de solicitações de spot, use o comando request-spot-fleet (o console de solicitações spot especifica uma solicitação de instância spot usando uma frota spot).

PowerShell

Para criar uma solicitação de instância spot

Use o cmdlet New-EC2Instance e especifique as opções da instância spot usando o parâmetro `-InstanceMarketOption`.

```
-InstanceMarketOptions $marketOptions
```

Crie a estrutura de dados para as opções de instância spot da seguinte forma.

```
$spotOptions = New-Object Amazon.EC2.Model.SpotMarketOptions
$spotOptions.SpotInstanceType="persistent"
$marketOptions = New-Object Amazon.EC2.Model.InstanceMarketOptionsRequest
$marketOptions.MarketType = "spot"
$marketOptions.SpotOptions = $spotOptions
```

Exemplo de especificações de execução de solicitações de instância spot

Os exemplos a seguir mostram configurações de execução que é possível usar com o comando request-spot-instances para criar uma solicitação de instância spot. Para obter mais informações, consulte Gerenciar as instâncias spot.

> **Important**
>
> Não recomendamos o uso do comando request-spot-instances por ser uma API herdada e sem investimento planejado. Para obter mais informações, consulte Qual é o melhor método de solicitação spot para usar?.

Exemplos

- Exemplo 1: Executar Instâncias spot
- Exemplo 2: executar Instâncias spot na zona de disponibilidade especificada
- Exemplo 3: executar Instâncias spot na sub-rede especificada
- Exemplo 4: executar uma instância spot dedicada

Exemplo 1: Executar Instâncias spot

O exemplo a seguir não inclui uma zona de disponibilidade nem sub-rede. O Amazon EC2 seleciona uma zona de disponibilidade para você. O Amazon EC2 executa as instâncias na sub-rede padrão da zona de disponibilidade selecionada.

```
{
  "ImageId": "ami-0abcdef1234567890",
  "KeyName": "my-key-pair",
  "SecurityGroupIds": [ "sg-1a2b3c4d5e6f7g8h9" ],
  "InstanceType": "m5.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-0abcdef1234567890",
  "KeyName": "my-key-pair",
  "SecurityGroupIds": [ "sg-1a2b3c4d5e6f7g8h9" ],
```

```
  "InstanceType": "m5.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-0abcdef1234567890",
  "SecurityGroupIds": [ "sg-1a2b3c4d5e6f7g8h9" ],
  "InstanceType": "m5.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, é necessário incluir o ID da sub-rede e o ID do grupo de segurança usando a interface de rede, em vez de usar os campos `SubnetId` e `SecurityGroupIds` mostrados no bloco de código anterior.

```
{
  "ImageId": "ami-0abcdef1234567890",
  "KeyName": "my-key-pair",
  "InstanceType": "m5.medium",
  "NetworkInterfaces": [
    {
      "DeviceIndex": 0,
      "SubnetId": "subnet-1a2b3c4d5e6f7g8h9",
      "Groups": [ "sg-1a2b3c4d5e6f7g8h9" ],
      "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.

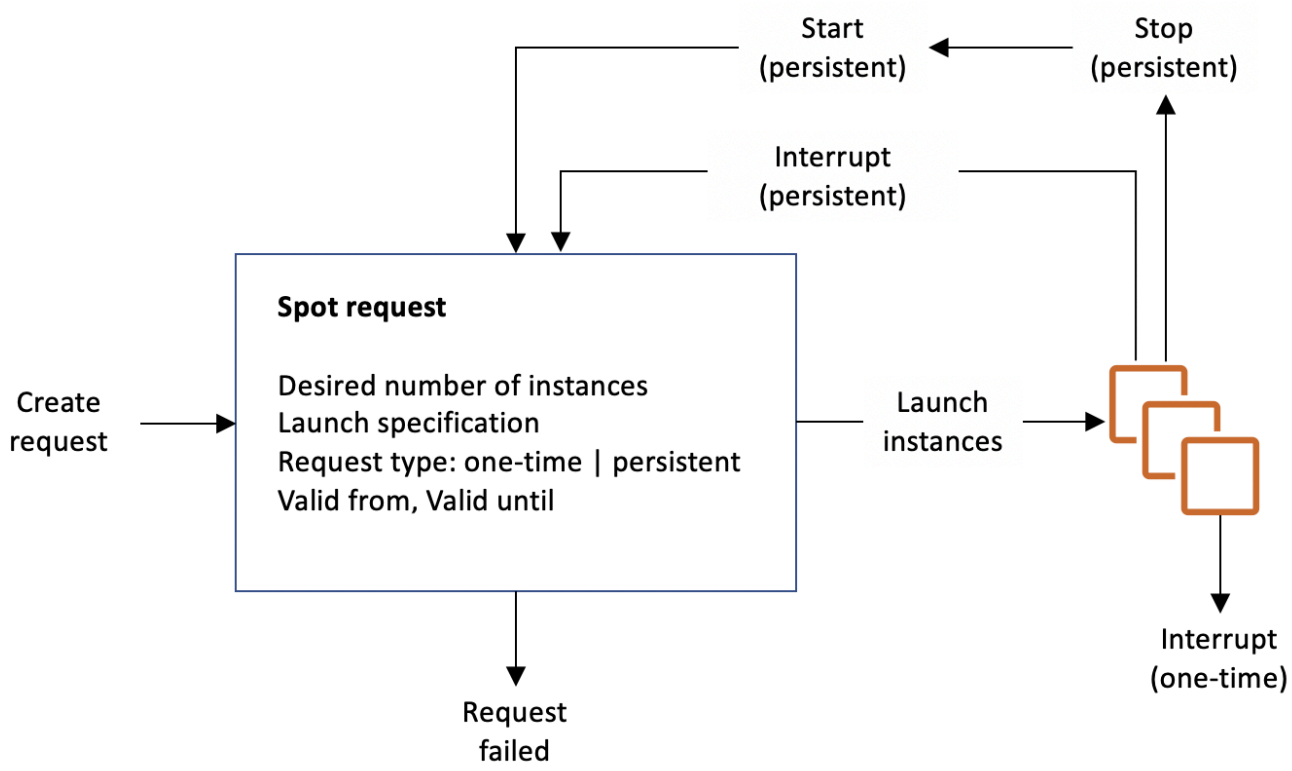
```
{
  "ImageId": "ami-0abcdef1234567890",
  "KeyName": "my-key-pair",
  "SecurityGroupIds": [ "sg-1a2b3c4d5e6f7g8h9" ],
  "InstanceType": "c5.8xlarge",
  "SubnetId": "subnet-1a2b3c4d5e6f7g8h9",
  "Placement": {
    "Tenancy": "dedicated"
  }
}
```

Obter o status de uma solicitação de instância 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.

A ilustração a seguir mostra como as solicitações de instância spot funcionam. Observe que o tipo de solicitação (única ou persistente) determina se a solicitação será reaberta ou quando o Amazon EC2 interromper uma instância spot, ou você parar uma instância spot. Se a requisição for persistente, ela será aberta novamente depois que a instância spot for interrompida. Se a solicitação for persistente e você parar a instância spot, a solicitação só será reaberta depois que você reiniciar a instância spot.



Conteúdo

- Obter informações do status da solicitação
- Códigos de status das solicitações spot
- Evento de atendimento de solicitação de instância spot do EC2
- Mudanças de estado para uma solicitação spot

Obter informações do status da solicitação

É possível obter informações de status para sua solicitação de instância spot.

Console

Para obter informações de status da solicitação

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Spot Requests (Solicitações spot) e selecione a solicitação spot.

3. Para verificar o status, na guia Descrição, marque o campo Status .

AWS CLI

Para obter informações de status da solicitação

Use o seguinte comando describe-spot-instance-requests.

```
aws ec2 describe-spot-instance-requests --spot-instance-request-
ids sir-0e54a519c9EXAMPLE
```

PowerShell

Para obter informações de status da solicitação

Use o cmdlet Get-EC2SpotInstanceRequest.

```
Get-EC2SpotInstanceRequest -SpotInstanceRequestId sir-0e54a519c9EXAMPLE
```

Códigos de status das solicitações spot

As informações de status da solicitação spot são compostas de um código de status da solicitação, o tempo de atualização e uma mensagem de status. Juntas, essas informações ajudam a determinar a disposição de sua solicitação spot.

Veja a seguir os códigos de status de solicitação spot:

`az-group-constraint`

O Amazon EC2 não pode executar todas as instâncias que você solicitou na mesma zona de disponibilidade.

`bad-parameters`

Um ou mais parâmetros para sua solicitação spot são inválidos (por exemplo, a AMI que você especificou não existe). A mensagem de status de solicitação indica qual parâmetro é inválido.

`canceled-before-fulfillment`

O usuário cancelou a solicitação spot antes de ser atendida.

`capacity-not-available`

Não há capacidade suficiente disponível para as instâncias solicitadas.

`constraint-not-fulfillable`

A solicitação spot não pode ser atendida porque uma ou mais restrições são inválidas (por exemplo, a zona de disponibilidade não existe). A mensagem de status de solicitação indica qual restrição é inválida.

`fulfilled`

A solicitação spot é `active` e Amazon EC2 está executando seu Instâncias spot.

`instance-stopped-by-price`

Sua instância foi interrompida porque o preço spot excedeu seu preço máximo.

`instance-stopped-by-user`

A instância foi interrompida porque um usuário interrompeu a instância ou executou o comando de desligamento a partir da instância.

`instance-stopped-no-capacity`

Sua instância foi interrompida devido às necessidades de gerenciamento de capacidade do EC2.

`instance-terminated-by-price`

Sua instância foi encerrada porque o preço spot excedeu seu preço máximo. Se sua solicitação for uma sugestão de preço persistente, o processo será reiniciado, portanto, sua solicitação está com a avaliação pendente.

`instance-terminated-by-schedule`

Sua instância spot foi encerrada no final da duração prevista.

`instance-terminated-by-service`

A instância foi encerrada em um estado interrompido.

`instance-terminated-by-user` ou `spot-instance-terminated-by-user`

Você encerrou uma instância spot que tinha sido atendida, portanto, o estado da solicitação é `closed` (a menos que se trate de uma requisição persistente) e o estado da instância é `terminated` .

`instance-terminated-launch-group-constraint`

Uma ou mais instâncias no grupo de execução foram encerradas, portanto, a restrição do grupo de execução deixou de ser atendida.

`instance-terminated-no-capacity`

Sua instância foi encerrada devido aos processos padrão de gerenciamento de capacidade.

`launch-group-constraint`

O Amazon EC2 não pode executar todas as instâncias que você solicitou ao mesmo tempo. Todas as instâncias em um grupo de execução são iniciadas e encerradas juntas.

`limit-exceeded`

O limite no número de volumes EBS ou de armazenamento de volume total foi excedido. Para obter mais informações, consulte Quotas for Amazon EBS no Guia do usuário do Amazon EBS.

`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 grupo de posicionamento 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.

Evento de atendimento de solicitação de instância spot do EC2

Quando uma solicitação de instância spot é atendida, o Amazon EC2 envia um evento de atendimento de solicitação de instância spot do EC2 ao Amazon EventBridge. É possível criar uma regra para realizar uma ação sempre que esse evento ocorrer, como invocar uma função Lambda ou notificar um tópico do Amazon SNS.

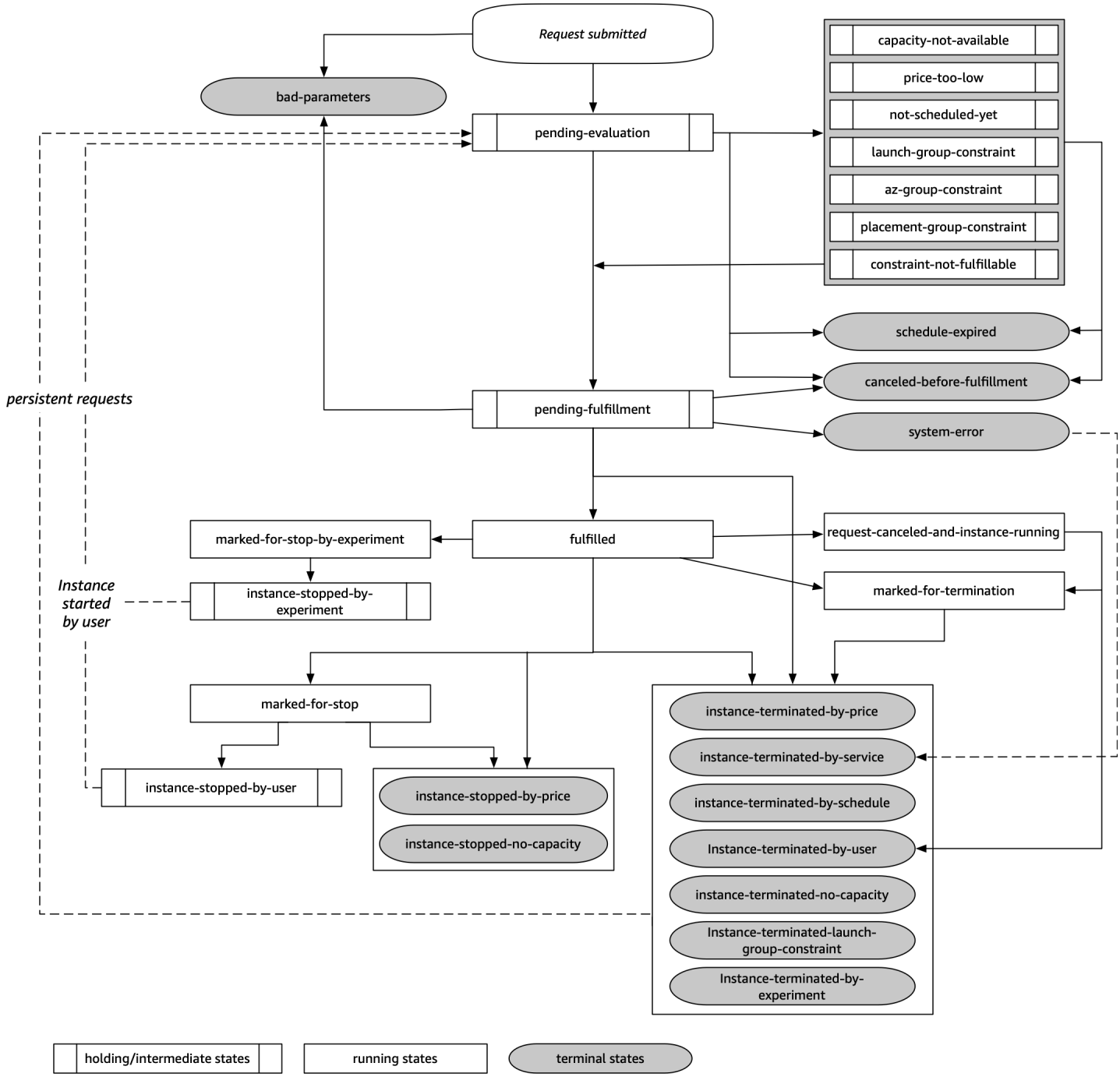
A seguir estão dados de exemplo para esse evento.

```
{
    "version": "0",
    "id": "01234567-1234-0123-1234-012345678901",
    "detail-type": "EC2 Spot Instance Request Fulfillment",
    "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": {
        "spot-instance-request-id": "sir-0e54a519c9EXAMPLE",
        "instance-id": "i-1234567890abcdef0"
    }
}
```

Para saber mais, consulte o Guia do Usuário do Amazon EventBridge.

Mudanças de estado para uma solicitação spot

O diagrama a seguir mostra os caminhos que a solicitação spot pode seguir durante todo o ciclo de vida, do envio ao encerramento. Cada etapa é representada como um nó, e o código de status de cada nó descreve o status da solicitação spot e da instância spot.



Avaliação pendente

Assim que você cria uma solicitação de instância spot, ela entra no estado `pending-evaluation`, a menos que um ou mais parâmetros da solicitação não sejam válidos (`bad-parameters`).

Código de status	Estado da solicitação	Estado da instância
`pending-evaluation`	`open`	Não aplicável
`bad-parameters`	`closed`	Não aplicável

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 não houver capacidade, sua solicitação permanecerá no estado de hibernação até que haja capacidade disponível. 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`	Não aplicável
`price-too-low`	`open`	Não aplicável
`not-scheduled-yet`	`open`	Não aplicável
`launch-group-constraint`	`open`	Não aplicável
`az-group-constraint`	`open`	Não aplicável
`placement-group-constraint`	`open`	Não aplicável

Código de status	Estado da solicitação	Estado da instância
`constraint-not-ful fillable`	`open`	Não aplicável

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`	Não aplicável
32	`cancelled`	Não aplicável
`bad-parameters`	`failed`	Não aplicável
`system-error`	`closed`	Não aplicável

[1] Se a solicitação for cancelada.

Atendimento pendente

Quando as restrições especificadas (se houver) forem atendidas, sua solicitação spot entrará no 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`	Não aplicável

Atendido

Quando todas as especificações das instâncias spot forem atendidas, sua solicitação spot será atendida. O Amazon EC2 executa as instâncias spot, o que pode levar alguns minutos. Se uma instância spot ficar em estado de hibernação, ela permanecerá nesse estado até que a solicitação possa ser atendida novamente ou seja cancelada.

Código de status	Estado da solicitação	Estado da instância
`fulfilled`	`active`	`pending` → `running`
`fulfilled`	`active`	`stopped` → `running`

Se você interromper uma instância spot, a solicitação spot entrará no estado `marked-for-stop` ou `instance-stopped-by-user` até que ela possa ser iniciada novamente ou até que a solicitação seja cancelada.

Código de status	Estado da solicitação	Estado da instância
`marked-for-stop`	`active`	`stopping`
32	`disabled` ou `cancelled` [2]	`stopped`

[1] Uma instância spot entrará no estado `instance-stopped-by-user` se você interromper a instância ou executar o comando de desligamento na própria instância. Depois de interromper a instância, é possível iniciá-la novamente. Na reinicialização, a solicitação de instância spot retornará para o estado `pending-evaluation` e o Amazon EC2 iniciará uma nova instância spot quando as restrições forem atendidas.

² O estado da solicitação spot será `disabled` se você interromper a instância spot, mas não cancelar a solicitação. O estado da solicitação será `cancelled` se a instância spot for interrompida e a solicitação expirar.

Atendido - terminal

As instâncias spot continuarão em execução, contanto que haja capacidade disponível para o tipo de instância e você não encerre a instância. Se o Amazon EC2 precisar encerrar as instâncias spot, a solicitação spot assumirá um estado terminal. Uma solicitação também entrará no estado terminal se você cancelar a solicitação spot ou encerrar as Instâncias spot.

Código de status	Estado da solicitação	Estado da instância
`request-canceled-and-instance-running`	`cancelled`	`running`
`marked-for-stop`	`active`	`running`
`marked-for-termination`	`active`	`running`
`instance-stopped-by-price`	`disabled`	`stopped`
`instance-stopped-by-user`	`disabled`	`stopped`
`instance-stopped-no-capacity`	`disabled`	`stopped`
`instance-terminated-by-price`	`closed` (única), `open` (persistente)	`terminated`
`instance-terminated-by-schedule`	`closed`	`terminated`
`instance-terminated-by-service`	`cancelled`	`terminated`

Código de status	Estado da solicitação	Estado da instância
`instance-terminated-by-user`	`closed` ou `cancelled` [1]	`terminated`
`instance-terminated-no-capacity`	`closed` (única), `open` (persistente)	`running` †
`instance-terminated-no-capacity`	`closed` (única), `open` (persistente)	`terminated`
`instance-terminated-launch-group-constraint`	`closed` (única), `open` (persistente)	`terminated`

[1] 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 atrase a detecção de que a instância spot foi encerrada. Nesse caso, o estado da solicitação poderá ser `closed` ou `cancelled`.

† Quando o Amazon EC2 interrompe uma instância spot, se precisa da capacidade de volta e a instância está configurada para terminar na interrupção, o status é imediatamente definido como`instance-terminated-no-capacity` (não é definido como `marked-for-termination`). No entanto, a instância permanece no estado `running` por 2 minutos para refletir o período de 2 minutos quando a instância recebe o aviso de interrupção da instância spot. Após 2 minutos, o estado da instância é definido como `terminated`.

Experimentos de interrupção

É possível usar AWS Fault Injection Service para iniciar a interrupção de uma instância spot e poder testar como as aplicações nessas instâncias spot respondem. Se o AWS FIS interromper uma instância spot, sua solicitação de spot entrará no estado `marked-for-stop-by-experiment` e depois no estado `instance-stopped-by-experiment`. Se o AWS FIS encerrar uma instância spot, sua solicitação de spot entrará no estado `instance-terminated-by-experiment`. Para obter mais informações, consulte the section called “Iniciar uma interrupção”.

Código de status	Estado da solicitação	Estado da instância
`marked-for-stop-by-experiment`	`active`	`running`
`instance-stopped-by-experiment`	`disabled`	`stopped`
`instance-terminated-by-experiment`	`closed`	`terminated`

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 iniciar uma nova instância spot quando as restrições forem cumpridas.

Marcar solicitações de instância spot

Para categorizar e gerenciar as solicitações de instância spot, é possível marcá-las com metadados personalizados. É possível atribuir uma tag a uma solicitação de instância spot ao criá-la ou posteriormente. É possível atribuir tags usando o console do Amazon EC2 ou uma ferramenta da linha de comando.

Quando você marca uma solicitação de instância spot, as instâncias e os volumes executados pela solicitação de instância spot não são marcados automaticamente. É necessário marcar explicitamente as instâncias e os volumes executados pela solicitação de instância spot. É possível atribuir volumes e uma tag a uma instância spot durante a execução ou posteriormente.

Para obter mais informações sobre como as tags funcionam, consulte Marcar com tag os recursos do Amazon EC2.

Conteúdos

- Pré-requisitos
- Marcar uma nova solicitação de instância spot
- Marcar uma solicitação de instância spot existente
- Exibir tags de solicitação de instância spot

Pré-requisitos

Conceda ao usuário permissão para marcar recursos. Para obter mais informações sobre políticas do IAM e políticas de exemplo, consulte Exemplo: marcar recursos.

A política do IAM criada é determinada pelo método usado para criação de uma solicitação de instância spot.

- Se você usar o assistente de execução de instâncias ou `run-instances` para solicitar uma Instâncias spot, consulte To grant a user the permission to tag resources when using the launch instance wizard or run-instances.
- Se você utiliza o comando `request-spot-instances` para solicitar instâncias spot, consulte To grant a user the permission to tag resources when using request-spot-instances.

Para conceder a um usuário do IAM permissão para marcar recursos ao usar o assistente de inicialização ou run-instances

Crie uma política do IAM que inclua o seguinte:

- A ação `ec2:RunInstances`. Essa ação concede ao usuário permissão para iniciar uma instância.
- Para `Resource`, especifique `spot-instances-request`. Essa ação permite que os usuários criem solicitações de instância spot, que solicitam instâncias spot.
- A ação `ec2:CreateTags`. Essa ação concede ao usuário permissão para criar tags.
- Para `Resource`, especifique `*`. Isso permite que os usuários marquem todos os recursos criados durante a execução da instância.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowLaunchInstances",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
```

```
                "arn:aws:ec2:us-east-1::image/*",
                "arn:aws:ec2:us-east-1:*:subnet/*",
                "arn:aws:ec2:us-east-1:*:network-interface/*",
                "arn:aws:ec2:us-east-1:*:security-group/*",
                "arn:aws:ec2:us-east-1:*:key-pair/*",
                "arn:aws:ec2:us-east-1:*:volume/*",
                "arn:aws:ec2:us-east-1:*:instance/*",
                "arn:aws:ec2:us-east-1:*:spot-instances-request/*"
            ]
        },
        {
            "Sid": "TagSpotInstanceRequests",
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "*"
        }
    ]
}
```

Quando você usa a ação RunInstances para criar solicitações de instância spot e marcar as solicitações de instância spot ao criá-las, deve estar ciente de que o Amazon EC2 avalia o recurso `spot-instances-request` na instrução RunInstances segundo a política do IAM, como se segue:

- Se você não marcar uma solicitação de instância spot na criação, o Amazon EC2 não avaliará o recurso `spot-instances-request` na instrução RunInstances.
- Se você marcar uma solicitação de instância spot na criação, o Amazon EC2 avaliará o recurso `spot-instances-request` na instrução RunInstances.

Portanto, para o recurso `spot-instances-request`, as seguintes regras se aplicam à diretiva do IAM:

- Caso você use RunInstances para criar uma solicitação de instância spot e não pretenda marcar a solicitação de instância spot na criação, não será necessário permitir explicitamente o recurso `spot-instances-request`. A chamada terá êxito.
- Caso use RunInstances para criar uma solicitação de instância spot e pretenda marcar a solicitação de instância spot na criação, você deverá incluir o recurso `spot-instances-request` na instrução de permissão RunInstances, caso contrário, a chamada falhará.

- Caso você use RunInstances para criar uma solicitação de instância spot e pretenda marcar a solicitação de instância spot na criação, especifique o recurso `spot-instances-request` ou inclua um curinga * na instrução de permissão CreateTags, caso contrário, a chamada falhará.

Por exemplo, políticas do IAM, incluindo políticas que não são compatíveis com solicitações de instância spot, consulte Trabalhar com Instâncias spot.

Para conceder a um usuário permissão para marcar recursos ao usar request-spot-instances

Crie uma política do IAM que inclua o seguinte:

- A ação `ec2:RequestSpotInstances`. Isso concede ao usuário permissão para criar uma solicitação de instância spot.
- A ação `ec2:CreateTags`. Essa ação concede ao usuário permissão para criar tags.
- Para `Resource`, especifique `spot-instances-request`. Isso permite que os usuários marquem somente a solicitação de instância spot.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "TagSpotInstanceRequest",
            "Effect": "Allow",
            "Action": [
                "ec2:RequestSpotInstances",
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:us-east-1:111122223333:spot-instances-
request/*"
        }
    ]
}
```

Marcar uma nova solicitação de instância spot

Nos exemplos AWS CLI e do PowerShell, configure a solicitação de instância spot da seguinte forma:

- Para `ResourceType`, especifique `spot-instances-request`. Se você especificar outro valor, ocorrerá falha na solicitação de instância spot.
- Em `Tags`, especifique o par de chave/valor. É possível especificar mais de um par de chave/valor.

Console

Para marcar uma nova solicitação de instância spot

1. Siga o procedimento do Gerenciar as instâncias spot.
2. Para adicionar uma tag, na página Adicionar tags, escolha Adicionar tag e insira a chave e o valor da tag. Escolha Adicionar outra tag para cada tag adicional.

   Para cada tag, é possível marcar a solicitação de instância spot, as instâncias spot e os volumes com a mesma tag. Para marcar os três, verifique se as opções Instances (Instâncias), Volumes e Spot Instance Requests (Solicitações de instâncias spot) estão selecionadas. Para marcar apenas um ou dois, verifique se os recursos que deseja marcar estão selecionados e os outros recursos estão limpos.
3. Preencha os campos obrigatórios para criar uma solicitação de instância spot e escolha Launch (Executar). Para obter mais informações, consulte Gerenciar as instâncias spot.

AWS CLI

Para marcar uma nova solicitação de instância spot

Use o comando request-spot-instances com a opção `--tag-specification`.

A especificação da tag adiciona duas tags à solicitação da instância spot: `Environment=Production` e `Cost-Center=123`.

```
aws ec2 request-spot-instances \
    --instance-count 5 \
    --type "one-time" \
    --launch-specification file://specification.json \
```

```
    --tag-specification 'ResourceType=spot-instances-
request,Tags=[{Key=Environment,Value=Production},{Key=Cost-Center,Value=123}]'
```

PowerShell

Para marcar uma nova solicitação de instância spot

Use o cmdlet Request-EC2SpotInstance com o parâmetro `-TagSpecification`.

```
-TagSpecification $tagspec
```

A especificação da tag é definida conforme a seguir. Ela adiciona duas tags à solicitação da instância spot: `Environment=Production` e `Cost-Center=123`.

```
$tag1 = @{Key="Environment"; Value="Production"}
$tag2 = @{Key="Cost-Center"; Value="123"}
$tagspec = New-Object Amazon.EC2.Model.TagSpecification
$tagspec.ResourceType = "spot-instances-request"
$tagspec.Tags = @($tag1,$tag2)
```

Marcar uma solicitação de instância spot existente

Console

Para marcar uma solicitação existente de instância spot

Depois de criar uma solicitação de instância spot, é possível adicionar tags à solicitação de instância spot usando o console.

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Solicitações spot.
3. Selecione sua solicitação de instância spot.
4. Escolha a guia Tags e Create Tag (Criar tag).

Para marcar uma solicitação de instância spot existente usando o console

Depois que sua solicitação de instância spot tiver executado a instância spot, será possível adicionar tags à instância usando o console. Para obter mais informações, consulte Adicionar tags usando o console.

AWS CLI

Para marcar uma solicitação de instância spot ou instância spot existente com uma tag

Use o comando create-tags para marcar os recursos existentes. No exemplo a seguir, a solicitação de instância spot e a instância spot existentes são marcadas com `purpose=test`.

```
aws ec2 create-tags \
    --resources sir-0e54a519c9EXAMPLE i-1234567890abcdef0 \
    --tags Key=purpose,Value=test
```

PowerShell

Para marcar uma solicitação de instância spot ou instância spot existente com uma tag

Use o cmdlet New-EC2Tag. O exemplo a seguir adiciona a tag `purpose=test` à solicitação de instância spot e à instância spot existentes.

```
New-EC2Tag `
    -Resource sir-0e54a519c9EXAMPLE, i-1234567890abcdef0 `
    -Tag @{Key="purpose"; Value="test"}
```

Exibir tags de solicitação de instância spot

Console

Para visualizar tags de solicitação de instância spot

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Solicitações spot.
3. Selecione sua solicitação de instância spot e escolha a guia Tags.

AWS CLI

Para descrever as tags de solicitação de instância spot

Use o comando describe-spot-instance-requests para visualizar a configuração da solicitação de instância spot especificada, que inclui todas as tags especificadas para a solicitação.

```
aws ec2 describe-spot-instance-requests \
    --spot-instance-request-ids sir-0e54a519c9EXAMPLE \
    --query "SpotInstanceRequests[*].Tags"
```

O seguinte é um exemplo de saída.

```
[
    [
        {
            "Key": "Environment",
            "Value": "Production"
        },
        {
            "Key": "Department",
            "Value": "101"
        }
    ]
]
```

PowerShell

Para descrever as tags de solicitação de instância spot

Use o cmdlet Get-EC2SpotInstanceRequest.

```
(Get-EC2SpotInstanceRequest `
    -SpotInstanceRequestId sir-0e54a519c9EXAMPLE).Tags
```

O seguinte é um exemplo de saída.

```
Key         Value
---         -----
Environment Production
Department  101
```

Cancelar uma solicitação de instância spot

Se você não quiser mais sua solicitação de instância spot, poderá cancelá-la. Você só pode cancelar solicitações de instância spot que estão `open`, `active` ou `disabled`.

- A solicitação de instância spot é `open` quando sua requisição não ainda não foi atendida e nenhuma instância foi iniciada.
- A solicitação de instância spot é `active` quando ela foi atendida e as instâncias spot foram inicializadas como resultado.
- Sua solicitação de instância spot consta como `disabled` quando você para a instância spot.

Se a solicitação de instância spot estiver `active` e tiver uma instância spot associada em execução, o cancelamento da solicitação não encerrará a instância. Para obter mais informações sobre como encerrar uma instância spot, consulte Encerrar uma instância spot.

Console

Para cancelar uma solicitação de instância spot

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 instância spot.
4. Escolha Ações, Cancelar solicitação.
5. (Opcional) Ao terminar de trabalhar com as Instâncias spot associadas, será possível encerrá-las. Na caixa de diálogo Cancelar solicitação spot, selecione Encerrar instâncias e escolha Confirmar.

AWS CLI

Para cancelar uma solicitação de instância spot

Use o seguinte comando cancel-spot-instance-requests.

```
aws ec2 cancel-spot-instance-requests --spot-instance-request-
ids sir-0e54a519c9EXAMPLE
```

PowerShell

Para cancelar uma solicitação de instância spot

Use o cmdlet Stop-EC2SpotInstanceRequest.

```
Stop-EC2SpotInstanceRequest -SpotInstanceRequestId sir-0e54a519c9EXAMPLE
```

Gerenciar as instâncias spot

O Amazon EC2 inicia uma instância spot quando há capacidade disponível. A instância spot será executada até ser interrompida ou até você a encerrar.

Conteúdo

- Encontrar as instâncias spot
- Encontre instâncias iniciadas por uma solicitação específica
- Parar uma instância spot
- Iniciar uma instância spot
- Encerrar uma instância spot

Encontrar as instâncias spot

Uma instância spot aparece na página Instâncias no console junto com as instâncias sob demanda. Use o procedimento a seguir para encontrar as instâncias spot.

Console

Para encontrar suas instâncias spot

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Para encontrar todas as instâncias spot, no painel de pesquisa, escolha Ciclo de vida da instância = spot.
4. Para confirmar que uma instância é uma instância spot, selecione a instância, escolha a guia Detalhes e verifique o valor de Ciclo de vida. O valor de uma instância spot é `spot` e o valor de uma instância sob demanda é `normal`.

AWS CLI

Para encontrar suas instâncias spot

Use o seguinte comando describe-instances.

```
aws ec2 describe-instances --filters "Name=instance-lifecycle,Values=spot"
```

Para determinar se uma instância é uma instância spot

Use o seguinte comando describe-instances.

```
aws ec2 describe-instances \
    --instance-ids i-1234567890abcdef0 \
    --query "Reservations[*].Instances[*].InstanceLifecycle" \
    --output text
```

Se a saída for `spot`, a instância será uma instância spot. Se não houver saída, a instância será uma instância sob demanda.

PowerShell

Para encontrar suas instâncias spot

Use o cmdlet Get-EC2Instance.

```
Get-EC2Instance -Filter @{Name="instance-lifecycle"; Values="spot"}
```

Para determinar se uma instância é uma instância spot

Use o cmdlet Get-EC2Instance.

```
(Get-EC2Instance -InstanceId i-1234567890abcdef0).Instances.InstanceLifecycle
```

Se a saída for `Spot`, a instância será uma instância spot. Se não houver saída, a instância será uma instância sob demanda.

Encontre instâncias iniciadas por uma solicitação específica

Use o procedimento a seguir para encontrar as instâncias spot iniciadas por uma solicitação específica de instância spot ou frota spot.

Console

Para encontrar as instâncias spot para uma solicitação

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Solicitações spot. A lista contém tanto as solicitações de instância spot quanto as solicitações de frota spot.

3. Se uma solicitação de instância spot for atendida, Capacidade será o ID da instância spot. Em uma frota spot, a Capacity (Capacidade) indica quanto da capacidade solicitada foi atendida. Para visualizar os IDs das instâncias em uma frota spot, escolha a seta de expansão ou selecione a frota e escolha Instances (Instâncias).
4. Em uma frota spot, Capacidade indica quanto da capacidade solicitada foi fornecida. Para visualizar os IDs das instâncias em uma frota spot, escolha o ID da frota para abrir sua página de detalhes e localize o painel Instâncias.

AWS CLI

Para encontrar as instâncias spot para uma solicitação

Use o seguinte comando describe-spot-instance-requests.

```
aws ec2 describe-spot-instance-requests \
    --spot-instance-request-ids sir-0e54a519c9EXAMPLE \
    --query "SpotInstanceRequests[*].{ID:InstanceId}"
```

A seguir está um exemplo de saída:

```
[
    {
        "ID": "i-1234567890abcdef0"
    },
    {
        "ID": "i-0598c7d356eba48d7"
    }
]
```

PowerShell

Para encontrar as instâncias spot para uma solicitação

Use o cmdlet Get-EC2SpotInstanceRequest.

```
(Get-EC2SpotInstanceRequest -SpotInstanceRequestId sir-0e54a519c9EXAMPLE).InstanceId
```

Parar uma instância spot

Caso não precise das instâncias spot na ocasião, mas quiser reiniciá-las posteriormente sem perder os dados persistentes no volume do Amazon EBS, é possível interrompê-las. As etapas para parar uma instância spot são semelhantes às etapas para parar uma instância sob demanda.

> **Note**
>
> Ao parar uma instância spot, será possível modificar alguns atributos da instância, mas não o tipo dela.
> Não cobramos pelo uso de uma instância spot parada nem por taxas de transferência de dados, mas cobramos pelo armazenamento nos volumes do Amazon EBS.

Limitações

- Você só pode parar uma instância spot se ela foi iniciada a partir de uma solicitação de instância spot `persistent`.
- Não é possível parar uma instância spot se a solicitação de instância spot associada foi cancelada. Quando a solicitação de instância spot é cancelada, você só pode encerrar a instância spot.
- Também não é possível parar as instâncias spot em um grupo de frota, grupo de lançamento ou grupo de zonas de disponibilidade.

Console

Para interromper uma instância spot

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 spot. Se você não salvou o ID da instância spot, consulte the section called “Encontrar as instâncias spot”.
4. Escolha Estado da instância e Parar instância.
5. Quando a confirmação for solicitada, escolha Parar.

AWS CLI

Para interromper uma instância spot

Use o comando stop-instances para interromper manualmente as Instâncias spot.

```
aws ec2 stop-instances --instance-ids i-1234567890abcdef0
```

PowerShell

Para interromper uma instância spot

Use o cmdlet Stop-EC2Instance.

```
Stop-EC2Instance -InstanceId i-1234567890abcdef0
```

Iniciar uma instância spot

É possível iniciar uma instância spot que havia parado.

Pré-requisitos

É possível iniciar uma instância spot somente se:

- Você parou manualmente a instância spot.
- A instância spot é uma instância com EBS.
- A capacidade da instância spot está disponível.
- O preço spot é inferior ao preço máximo.

Limitações

- Não é possível iniciar uma instância spot se ela fizer parte da frota ou do grupo de inicialização ou grupo de zona de disponibilidade.

As etapas para iniciar uma instância spot são semelhantes às etapas para iniciar uma instância sob demanda.

Console

Para iniciar uma instância spot

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 spot. Se você não salvou o ID da instância spot, consulte the section called “Encontrar as instâncias spot”.
4. Escolha Instance state (Estado da instância) e Start instance (Iniciar instância).

AWS CLI

Para iniciar uma instância spot

Use o comando start-instances para iniciar manualmente as Instâncias spot.

```
aws ec2 start-instances --instance-ids i-1234567890abcdef0
```

PowerShell

Para iniciar uma instância spot

Use o cmdlet Start-EC2Instance.

```
Start-EC2Instance -InstanceId i-1234567890abcdef0
```

Encerrar uma instância spot

> **Warning**
>
> O encerramento de uma instância é permanente e irreversível.
> Depois de encerrar uma instância, não será mais possível se conectar a ela e ela não poderá ser recuperada. Todos os volumes anexados do Amazon EBS configurados para serem excluídos no encerramento também serão excluídos permanentemente e não poderão ser recuperados. Todos os dados armazenados em volumes de armazenamento de instância serão perdidos permanentemente. Para obter mais informações, consulte Como funciona o encerramento de uma instância.
> Antes de encerrar uma instância, certifique-se de ter feito backup de todos os dados que você precise reter após o encerramento no armazenamento persistente.

Se você encerrar uma instância spot em execução ou parada que foi iniciada por uma solicitação de instância spot persistente, a solicitação de instância spot fará a transição para o estado open para

que a nova instância spot seja iniciada. Para garantir que nenhuma instância spot nova seja iniciada, primeiro é necessário cancelar a solicitação de instância spot.

Se você cancelar uma solicitação de instância spot `active` com uma instância spot em execução, a instância spot em execução não será automaticamente terminada, e você deverá terminá-la manualmente.

Se você cancelar uma solicitação de instância spot `disabled` com uma instância spot parada, a instância spot parada será automaticamente encerrada pelo serviço spot do Amazon EC2. Pode haver um pequeno atraso entre o momento em que você cancelar a solicitação de instância spot e o momento em que o serviço spot terminar a instância spot.

Para obter mais informações, consulte Cancelar uma solicitação de instância spot.

Console

Para encerrar manualmente uma instância spot

1. Antes de encerrar a instância, confirme que não perderá dados verificando se seus volumes do Amazon EBS não serão excluídos no encerramento e se você copiou todos os dados de que precisa dos volumes de armazenamento persistente de instância, como o Amazon EBS ou o Amazon S3.
2. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
3. No painel de navegação, escolha Instances (Instâncias).
4. Selecione a instância spot. Se você não salvou o ID da instância spot, consulte the section called “Encontrar as instâncias spot”.
5. Escolha Estado da instância e Encerrar instância.
6. Quando a confirmação for solicitada, escolha Encerrar (excluir).

AWS CLI

Para encerrar manualmente uma instância spot

Use o comando terminate-instances para encerrar manualmente as Instâncias spot.

```
aws ec2 terminate-instances --instance-ids i-1234567890abcdef0 i-0598c7d356eba48d7
```

PowerShell

Para encerrar manualmente uma instância spot

Use o cmdlet Remove-EC2Instance.

```
Remove-EC2Instance -InstanceId i-1234567890abcdef0
```

Interrupções de instâncias spot

É possível executar Instâncias spot na capacidade adicional do EC2 para obter grandes descontos em troca de devolvê-los quando o Amazon EC2 precisar da capacidade de volta. Quando o Amazon EC2 recupera uma instância spot, chamamos esse evento de interrupção de instância spot.

A demanda por Instâncias spot pode variar significativamente de um momento para outro, e a disponibilidade das Instâncias spot também pode variar significativamente dependendo de quantas instâncias do EC2 não utilizadas estão disponíveis. É sempre possível que sua instância spot seja interrompida. Veja a seguir os possíveis motivos pelos quais o Amazon EC2 pode interromper Instâncias spot:

Capacidade

O Amazon EC2 pode interromper sua instância spot quando ele precisar dela de volta. O EC2 recupera sua instância principalmente para redirecionar a capacidade, mas também pode ocorrer por outros motivos, como manutenção de host ou descomissionamento de hardware

Preço

O preço spot é superior ao preço máximo.

É possível especificar o preço máximo em sua solicitação spot. No entanto, se você especificar um preço máximo, as instâncias serão interrompidas com mais frequência do que se você não especificar esse parâmetro.

Restrições

Se a solicitação de spot 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.

Quando o Amazon EC2 interrompe uma instância spot, ele encerra, para ou hiberna a instância, dependendo do comportamento da interrupção que você especificou ao criar a solicitação spot.

Conteúdo

- Comportamento das interrupções de instâncias spot
- Preparar para interrupções de instâncias spot
- Iniciar a interrupção de uma instância spot
- Avisos de interrupção de instância spot
- Encontrar Instâncias spot interrompidas
- Determinar se o Amazon EC2 terminou uma instância spot
- Faturamento para Instâncias spot interrompidas

Comportamento das interrupções de instâncias spot

Ao criar uma solicitação spot, você pode especificar o comportamento de interrupção. Os possíveis comportamentos de interrupção são os seguintes:

- Interromper
- Hibernar
- Encerrar

O comportamento padrão será que o Amazon EC2 encerre as instâncias spot quando elas forem interrompidas.

Parar Instâncias spot interrompida

É possível especificar que o Amazon EC2 pare suas instâncias spot quando elas são interrompidas. O tipo de solicitação da instância spot deve ser `persistent`. Não é possível especificar um grupo de execução na solicitação de instância spot. Para EC2 Fleet ou frota spot, o tipo de solicitação deve ser `maintain`.

Considerações

- Somente o Amazon EC2 pode reiniciar uma instância spot interrompida parada.
- Para uma instância spot iniciada por uma solicitação de instância spot `persistent`: o Amazon EC2 reinicia a instância parada quando a capacidade está disponível na mesma zona de

disponibilidade e para o mesmo tipo de instância que a instância parada (a mesma especificação de início deve ser usada).

- Ao parar uma instância spot, será possível modificar alguns atributos da instância, mas não o tipo dela. Se você desanexar ou excluir um volume do EBS, ele não será anexado quando a instância spot for iniciada. Se você desvincular o volume raiz e o Amazon EC2 tentar iniciar a instância spot, a instância falhará ao iniciar e o Amazon EC2 terminará a instância interrompida.
- É possível encerrar uma instância spot enquanto ela está interrompida.
- Se você cancelar uma solicitação de instância spot, uma EC2 Fleet ou uma frota spot, o Amazon EC2 terminará todas as instâncias spot associadas que estiverem paradas.
- Enquanto uma instância spot estiver parada, você será cobrado apenas pelos volumes do EBS, que são preservados. Com a EC2 Fleet e a frota spot, se houver muitas instâncias interrompidas, será possível exceder o limite de número de volumes do EBS na sua conta. Para obter mais informações sobre como você é cobrado quando uma instância spot é interrompida, consulte Faturamento para Instâncias spot interrompidas.
- Certifique-se de estar familiarizado com as implicações de parar uma instância. Para obter informações sobre o que acontece quando uma instância está parada, consulte Diferenças entre os estados de instâncias.

Hibernar Instâncias spot interrompida

É possível especificar que o Amazon EC2 hiberne suas instâncias spot quando elas estão interrompidas. Para obter mais informações, consulte Hibernar sua instância do Amazon EC2.

O Amazon EC2 agora oferece a mesma experiência de hibernação para as instâncias spot que está disponível atualmente para as instâncias sob demanda. Ele oferece um suporte mais amplo, sendo compatível com o seguinte para hibernação de instâncias spot:

- Mais AMIs compatíveis
- Mais famílias de instâncias compatíveis
- Hibernação iniciada pelo usuário

Terminar instâncias spot interrompidas

Quando o Amazon EC2 interrompe uma instância spot, ele termina a instância por padrão, a menos que você especifique um comportamento de interrupção diferente, como parar ou hibernar. Para obter mais informações, consulte Encerramento de instâncias do Amazon EC2.

Preparar para interrupções de instâncias spot

A demanda por Instâncias spot pode variar significativamente de um momento para outro, e a disponibilidade das Instâncias spot também pode variar significativamente dependendo de quantas instâncias do EC2 não utilizadas estão disponíveis. É sempre possível que sua instância spot seja interrompida. Portanto, é necessário garantir que a aplicação esteja preparada para uma interrupção de instância spot.

Recomendamos que você siga essas práticas recomendadas para estar preparado para uma interrupção da instância spot.

- Crie sua solicitação de spot usando um grupo do Auto Scaling. Se suas Instâncias spot forem interrompidas, o grupo do Auto Scaling iniciará automaticamente as instâncias de substituição. Para obter mais informações, consulte Grupos de Auto Scaling com vários tipos de instância e opções de compra no Manual do usuário do Amazon EC2 Auto Scaling.
- 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. Também é possível usar dados de usuário para executar comandos no startup.
- Os dados nos volumes de armazenamento de instância são perdidos quando a instância é interrompida ou encerrada. Faça backup de todos os dados importantes em volumes de armazenamento de instância para um armazenamento mais persistente, como o Amazon S3, o Amazon EBS ou o Amazon DynamoDB.
- Armazene regularmente os dados importantes em um lugar em que eles não sejam afetados se a instância spot for terminada. Por exemplo, é possível usar o Amazon S3, o Amazon EBS ou o DynamoDB.
- Divida o trabalho em tarefas pequenas (usando uma grade, um Hadoop ou uma arquitetura baseada em fila) ou use pontos de verificação para que você possa salvar seu trabalho com frequência.
- O Amazon EC2 emite um sinal de recomendação de rebalanceamento para a instância spot quando a instância apresenta risco elevado de interrupção. É possível confiar na recomendação de rebalanceamento para gerenciar proativamente as interrupções de instância spot sem precisar aguardar o aviso de interrupção de dois minutos da instância spot. Para obter mais informações, consulte Recomendações de rebalanceamento de instâncias do EC2.
- Use os avisos de interrupção de instância spot para monitorar o status das instâncias spot. Para obter mais informações, consulte Avisos de interrupção de instância spot.

- Embora nos esforcemos ao máximo para fornecer esse aviso o mais rápido possível, pode ser que a instância spot seja interrompida antes que o aviso seja disponibilizado. Teste sua aplicação para garantir que ele lide tranquilamente com a interrupção inesperada de uma instância, mesmo que você esteja monitorando sinais de recomendação de rebalanceamento e avisos de interrupção. É possível fazer isso executando a aplicação com uma instância sob demanda e, em seguida, terminando a instância sob demanda por conta própria.
- Execute um experimento de injeção de falhas controlado com AWS Fault Injection Service para testar como sua aplicação responde quando sua instância spot é interrompida. Para obter mais informações, consulte o Tutorial: Teste interrupções de instância spot usando o AWS FIS no Guia do usuário do AWS Fault Injection Service.

Iniciar a interrupção de uma instância spot

É possível selecionar uma solicitação de instância spot ou uma solicitação de frota spot no console do Amazon EC2 e iniciar uma interrupção de instância spot para poder testar como as aplicações nessas instâncias spot lidam com interrupções. Quando você inicia a interrupção de uma instância spot, o Amazon EC2 avisa que a instância spot será interrompida em dois minutos e, passados os dois minutos, o Amazon EC2 interrompe a instância spot.

O serviço subjacente que realiza a interrupção da instância spot é o AWS Fault Injection Service (AWS FIS). Para obter mais informações sobre as AWS FIS, consulte AWS Fault Injection Service.

> **Note**
>
> Os comportamentos de interrupção são `terminate`, `stop` e `hibernate`. Se o comportamento de interrupção for definido como `hibernate`, quando você iniciar a interrupção de uma instância spot, o processo de hibernação começará imediatamente.

Iniciar uma interrupção de insitância spot é compatível com todas as Regiões da AWS, exceto Ásia-Pacífico (Jacarta), Ásia-Pacífico (Osaka), China (Pequim), China (Ningxia) e Oriente Médio (EAU).

Conteúdo

- Iniciar a interrupção de uma instância spot
- Verificar a interrupção da instância spot
- Cotas

Iniciar a interrupção de uma instância spot

É possível usar o console do EC2 para iniciar rapidamente a interrupção de uma instância spot. Ao selecionar uma solicitação de Instância Spot, você pode iniciar a interrupção de uma Instância Spot. Ao selecionar uma solicitação de frota spot, você pode iniciar a interrupção de várias instâncias spot de uma só vez.

Para fazer experimentos mais avançados para testar interrupções de instâncias spot, você pode criar seus próprios experimentos usando o console do AWS FIS.

Para iniciar a interrupção de uma instância spot usando o console do EC2

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Spot Requests (Solicitações de spot).
3. Selecione uma solicitação de instância spot e escolha Actions (Ações), Initiate interruption (Iniciar interrupção). Você não pode selecionar várias solicitações de instância spot para iniciar uma interrupção.
4. Na caixa de diálogo Initiate Spot Instance interruption (Iniciar interrupção de instância spot), em Service access (Acesso ao serviço), use o perfil padrão ou escolha um perfil existente. Para escolher uma função existente, escolha Usar uma função de serviço existente e, em seguida, para Função do IAM}, selecione a função a ser usada.
5. Quando estiver pronto para iniciar a interrupção da instância spot, escolha Initiate interruption (Iniciar interrupção).

Para iniciar a interrupção de uma ou mais instâncias spot em uma solicitação de frota spot usando o console EC2

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Spot Requests (Solicitações de spot).
3. Selecione uma solicitação de instância spot e escolha Actions (Ações), Initiate interruption (Iniciar interrupção). Você não pode selecionar várias solicitações do Spot Fleet para iniciar uma interrupção.
4. Na caixa de diálogo Especificar número de instâncias spot, em Número de instâncias a serem interrompidas, insira o número de instâncias spot a serem interrompidas e escolha Confirmar.

> **Note**
>
> O número não pode exceder o número de instâncias spot na frota ou sua cota para o número de instâncias spot que AWS FIS podem ser interrompidas por experimento.

5. Na caixa de diálogo Initiate Spot Instance interruption (Iniciar interrupção de instância spot), em Service access (Acesso ao serviço), use o perfil padrão ou escolha um perfil existente. Para escolher uma função existente, escolha Usar uma função de serviço existente e, em seguida, para Função do IAM}, selecione a função a ser usada.
6. Quando estiver pronto para iniciar a interrupção da instância spot, escolha Initiate interruption (Iniciar interrupção).

Para fazer experimentos mais avançados para testar interrupções de instâncias spot usando o console do AWS FIS

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Spot Requests (Solicitações de spot).
3. Escolha Actions (Ações), Create advanced experiments (Criar experimentos avançados).

   O console do AWS FIS será aberto. Para obter mais informações, consulte o Tutorial: testar interrupções de instância spot usando o AWS FIS no Guia do usuário do AWS Fault Injection Service.

Verificar a interrupção da instância spot

Depois que você inicia a interrupção, ocorre o seguinte:

- A instância spot recebe uma recomendação de rebalanceamento da instância.
- Um aviso de interrupção de instância spot é emitido dois minutos antes de AWS FIS interromper sua instância.
- Passados os dois minutos, a instância spot é interrompida.
- Uma instância spot que foi interrompida pelo AWS FIS permanece parada até ser reiniciada.

Para verificar se a instância foi interrompida depois que você iniciou a interrupção

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

2. No painel de navegação, abra Spot Requests (Solicitações de spot) e Instances (Instâncias) em guias ou janelas separadas do navegador.
3. Para Solicitações Spot, selecione a solicitação de Instância Spot ou a solicitação de Frota Spot. O status inicial é `fulfilled`. Depois que a instância é interrompida, o status se altera como se segue, dependendo do comportamento da interrupção:
   - `terminate`: o status se altera para `instance-terminated-by-experiment`.
   - `stop`: o status se altera para `marked-for-stop-by-experiment` e depois `instance-stopped-by-experiment`.
4. Em Instances (Instâncias), selecione a instância spot. O status inicial é `Running`. Dois minutos depois que você recebe o aviso de interrupção da instância spot, o status se altera como se segue, dependendo do comportamento da interrupção:
   - `stop`: o status se altera para `Stopping` e depois `Stopped`.
   - `terminate`: o status se altera para `Shutting-down` e depois `Terminated`.

Cotas

Você Conta da AWS tem a seguinte cota padrão para o número de instâncias spot que AWS FIS podem ser interrompidas por experimento.

Nome	Padrão	Ajustável	Descrição
Instâncias spot de destino para aws:ec2:send-spot-instance-interruptions	Cada região compatível: 5	Sim	O número máximo de instâncias spot que aws:ec2:send-spot-instance-interruptions pode atingir quando você identifica alvos usando tags, por experimento.

É possível solicitar um aumento da cota. Para obter mais informações, consulte Solicitar um aumento de cota no Guia do usuário do Service Quotas..

Para visualizar todas as cotas de AWS FIS, abra o console Service Quotas. No painel de navegação, escolha AWS services (Serviços da) e selecione AWS Fault Injection Service. Você também pode ver todas as cotas AWS Fault Injection Service no Guia do AWS Fault Injection Service usuário.

Avisos de interrupção de instância spot

Um aviso de interrupção da instância spot é um aviso emitido dois minutos antes de o Amazon EC2 parar ou encerrar uma instância spot. Se você especificar uma hibernação como o comportamento de interrupção, receberá um aviso de interrupção, mas não receberá o aviso dois minutos antes porque o processo de hibernação começará imediatamente.

A melhor maneira de lidar com interrupções de instâncias spot com tranquilidade é arquitetar a aplicação para que ela seja tolerante a falhas. Para fazer isso, é possível aproveitar os avisos de interrupção de instância spot. Recomendamos que você verifique esses avisos de interrupção a cada 5 segundos.

Os avisos de interrupção são disponibilizados como um evento do Eventbridge e como itens nos metadados de instância da instância spot. Avisos de interrupção são emitidos de acordo com o melhor esforço.

EC2 Spot Instance Interruption WarningEvento

Quando o Amazon EC2 vai interromper a instância spot, ele emite um evento dois minutos antes da interrupção real (exceto para a hibernação, que recebe o aviso de interrupção, mas não dois minutos antes, porque a hibernação começa imediatamente). Este evento pode ser detectado pelo Amazon EventBridge. Para obter mais informações sobre eventos no EventBridge, consulte o Guia do usuário do Amazon EventBridge. Para obter um exemplo detalhado que orienta você sobre como criar e usar regras de evento, consulte Aproveitar os avisos de interrupção de instância spot do Amazon EC2.

Este é um exemplo do evento de interrupção da instância spot. Os valores possíveis para `instance-action` são `hibernate`, `stop` ou `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-2a:instance/i-1234567890abcdef0"],
```

```
    "detail": {
        "instance-id": "i-1234567890abcdef0",
        "instance-action": "action"
    }
}
```

> **Note**
>
> O formato de ARN do evento de interrupção da instância spot é `arn:aws:ec2:`*`availability-zone`*`:instance/`*`instance-id`*. Esse formato é diferente do formato de ARN de recurso do EC2.

instance-action

O item `instance-action` especifica a ação e o tempo aproximado (em UTC) em que a ação ocorrerá.

Se a instância spot estiver marcada para ser parada ou terminada pelo Amazon EC2, o item `instance-action` estará presente nos seus metadados de instância. Caso contrário, não estará presente. É possível recuperar `instance-action` usando o Instance Metadata Service versão 2 (IMDSv2) da seguinte forma.

Linux

```
TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
    && curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/spot/instance-action
```

Windows

```
[string]$token = Invoke-RestMethod `
    -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} `
    -Method PUT -Uri http://169.254.169.254/latest/meta-data/spot/instance-action
```

A saída do exemplo a seguir indica o momento em que essa instância será parada.

```
{"action": "stop", "time": "2017-09-18T08:22:00Z"}
```

A saída do exemplo a seguir indica o momento em que essa instância será terminada.

```
{"action": "terminate", "time": "2017-09-18T08:22:00Z"}
```

Se o Amazon EC2 não estiver se preparando para parar ou terminar a instância, ou se você mesmo terminar a instância, `instance-action` não estará presente nos metadados da instância e você receberá um erro HTTP 404 ao tentar recuperá-la.

termination-time

O item `termination-time` especifica o horário aproximado em UTC em que a instância receberá a sinalização de desligamento.

> **Note**
>
> Este item é mantido para compatibilidade com versões anteriores. Use `instance-action` em seu lugar.

Se a instância spot estiver marcada para ser encerrada pelo Amazon EC2 (devido a uma interrupção da instância spot em que o comportamento de interrupção está definido como `terminate` ou devido ao cancelamento de uma solicitação de instância spot persistente), o item `termination-time` estará presente nos metadados da instância. Caso contrário, não estará presente. É possível recuperar `termination-time` usando o IMDSv2 da seguinte maneira.

Linux

```
TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"`
if curl -H "X-aws-ec2-metadata-token: $TOKEN" -s http://169.254.169.254/latest/meta-data/spot/termination-time | grep -q .*T.*Z; then echo termination_scheduled; fi
```

Windows

```
[string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/meta-data/spot/termination-time
```

O seguinte é um exemplo de saída.

```
2015-01-05T18:02:00Z
```

Se o Amazon EC2 não estiver se preparando para encerrar a instância (seja porque não há interrupção da instância spot, seja porque o comportamento de interrupção está definido como `stop` ou `hibernate`), ou se você tiver encerrado a instância spot por conta própria, o item `termination-time` não estará presente nos metadados da instância (portanto, você receberá um erro HTTP 404) ou conterá um valor que não corresponde a um valor de tempo.

Se o Amazon EC2 não encerrar a instância, o status da solicitação será definido como `fulfilled`. O valor de `termination-time` permanece nos metadados da instância com o tempo aproximado original, que agora está no passado.

Encontrar Instâncias spot interrompidas

Quando você descreve suas instâncias do EC2, os resultados incluem suas instâncias spot. O ciclo de vida da instância de uma instância spot é `spot`. O estado da instância de uma instância spot é `stopped` `outerminated`, dependendo do comportamento de interrupção que foi configurado. Para uma instância spot hibernada, o estado da instância é `stopped`.

Para obter detalhes adicionais sobre o motivo da interrupção, verifique o código de status da solicitação spot. Para obter mais informações, consulte the section called “Obter o status de uma solicitação de instância spot”.

Console

Para encontrar uma instância spot interrompida

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Aplique o seguinte filtro: Instance lifecycle=spot.
4. Aplique o filtro Instance state=stoped ou Instance state=terminated, dependendo do comportamento de interrupção configurado.
5. Para cada instância spot, na guia Detalhes, em Detalhes da instância, localize a Mensagem de transição de estado. Os códigos a seguir indicam que a instância spot foi interrompida.
   - `Server.SpotInstanceShutdown`
   - `Server.SpotInstanceTermination`

AWS CLI

Para encontrar instâncias spot interrompidas

Use o comando describe-instante com a opção `--filters`. Para listar apenas os IDs das instâncias na saída, inclua a opção `--query`.

Se o comportamento da interrupção for encerrar as instâncias spot, use o seguinte exemplo:

```
aws ec2 describe-instances \
    --filters Name=instance-lifecycle,Values=spot \
              Name=instance-state-name,Values=terminated \
              Name=state-reason-code,Values=Server.SpotInstanceTermination \
    --query "Reservations[*].Instances[*].InstanceId"
```

Se o comportamento da interrupção for parar as instâncias spot, use o seguinte exemplo:

```
aws ec2 describe-instances \
    --filters Name=instance-lifecycle,Values=spot \
              Name=instance-state-name,Values=stopped \
              Name=state-reason-code,Values=Server.SpotInstanceShutdown \
    --query "Reservations[*].Instances[*].InstanceId"
```

PowerShell

Para encontrar instâncias spot interrompidas

Use o cmdlet Get-EC2Instance.

Se o comportamento da interrupção for encerrar as instâncias spot, use o seguinte exemplo:

```
(Get-EC2Instance `
    -Filter @{Key="instance-lifecycle"; Values="spot"} `
            @{Key="instance-state-name"; Values="terminated"} `
            @{Key="state-reason-code";
 Values="Server.SpotInstanceTermination"}).Instances.InstanceId
```

Se o comportamento da interrupção for parar as instâncias spot, use o seguinte exemplo:

```
(Get-EC2Instance `
    -Filter @{Key="instance-lifecycle"; Values="spot"} `
            @{Key="instance-state-name"; Values="stopped"} `
```

```
            @{Key="state-reason-code";
Values="Server.SpotInstanceTermination"}).Instances.InstanceId
```

Determinar se o Amazon EC2 terminou uma instância spot

Uma instância spot é executada até que o Amazon EC2 a encerre em resposta a uma interrupção da instância spot, ou até que você mesmo a encerre. Para obter mais informações, consulte the section called “Comportamento de interrupção”.

Após uma instância spot ser encerrada, você pode usar o AWS CloudTrail para ver se o Amazon EC2 a encerrou. Se o log do CloudTrail incluir um `BidEvictedEvent`, isso indica que o Amazon EC2 encerrou a instância spot. Se, em vez disso, você vir um evento `TerminateInstances`, isso indica que um usuário encerrou a instância spot.

Como alternativa, se você quiser receber uma notificação de que o Amazon EC2 interromperá sua instância spot, use o Amazon EventBridge para responder ao evento de Aviso de interrupção da instância spot do EC2.

Para visualizar eventos BidEvictedEvent no CloudTrail

1. Abra o console do CloudTrail em https://console.aws.amazon.com/cloudtrail/.
2. No painel de navegação, selecione Event history (Histórico de eventos).
3. Na lista de filtros, escolha Nome do evento e, em seguida, no campo de filtro à direita, insira **`BidEvictedEvent`**.
4. (Opcional) Selecione um intervalo de tempo.
5. Se a lista não estiver vazia, escolha BidEvictedEvent na entrada resultante para abrir a página de detalhes. É possível encontrar informações sobre a instância spot no painel Registro de eventos, incluindo o ID da instância spot. Veja abaixo um exemplo do registro de evento.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "accountId": "123456789012",
        "invokedBy": "ec2.amazonaws.com"
    },
    "eventTime": "2016-08-16T22:30:00Z",
    "eventSource": "ec2.amazonaws.com",
    "userAgent": "ec2.amazonaws.com",
    "sourceIPAddress": "ec2.amazonaws.com",
```

```
    "eventName": "BidEvictedEvent",
    "awsRegion": "us-east-2",
    "eventID": "d27a6096-807b-4bd0-8c20-a33a83375054",
    "eventType": "AwsServiceEvent",
    "recipientAccountId": "123456789012",
    "RequestParameters": null,
    "ResponseElements": null,
    "serviceEventDetails": {
        "instanceIdSet": [
          "i-1eb2ac8eEXAMPLE"
        ]
    }
}
```

6. Se você não encontrou uma entrada para o evento `BidEvictedEvent`, insira **`TerminateInstances`** como o nome do evento. Para obter mais informações sobre o registro de evento para `TerminateInstances`, consulte the section called “Exemplos de eventos da API do Amazon EC2”.

Faturamento para Instâncias spot interrompidas

Quando uma instância spot é interrompida, você é cobrado pelo uso da instância e do volume do EBS, podendo incorrer em outras cobranças, conforme indicado a seguir.

Uso da instância

Quem interrompe a instância spot	Sistema operacional	Interrompida na primeira hora	Interrompida em qualquer hora após a primeira
Se você interromper ou encerrar a instância spot	Windows e Linux (com exceção de SUSE)	Cobrança pelos segundos usados	Cobrança pelos segundos usados
	SUSE	Cobrança pela hora completa, mesmo se você usou somente uma parte da hora	Cobrança pelas horas completas usadas e cobrança por uma hora completa pela hora parcial interrompida

Quem interrompe a instância spot	Sistema operacional	Interrompida na primeira hora	Interrompida em qualquer hora após a primeira
Se o Amazon EC2 interromper a instância spot	Windows e Linux (com exceção de SUSE)	Sem cobrança	Cobrança pelos segundos usados
	SUSE	Sem cobrança	Cobrança pelas horas completas usadas, mas sem cobrança pela hora parcial interrompida

Uso do volume do EBS

Enquanto uma instância spot estiver parada, você será cobrado apenas pelos volumes do EBS, que são preservados.

Com a EC2 Fleet e a frota spot, se houver muitas instâncias interrompidas, será possível exceder o limite de número de volumes do EBS na sua conta.

Recomendações de rebalanceamento de instâncias do EC2

Uma recomendação de rebalanceamento de instância do EC2 é um sinal que envia uma notificação quando uma instância Spot tem risco elevado de interrupção. O sinal pode chegar antes do aviso de interrupção da instância Spot de dois minutos, dando a você a oportunidade de gerenciar proativamente a instância spot. É possível decidir rebalancear sua workload em Instâncias spot novas ou existentes que não tenham risco elevado de interrupção.

Nem sempre é possível para o Amazon EC2 enviar o sinal de recomendação de rebalanceamento antes do aviso de interrupção da instância spot de dois minutos. Portanto, o sinal de recomendação de rebalanceamento pode chegar junto com o aviso de interrupção de dois minutos.

As recomendações de rebalanceamento são disponibilizadas como um evento do EventBridge e como um item nos metadados de instância na instância spot. Os eventos são emitidos com base no melhor esforço.

> **Note**
>
> As recomendações de rebalanceamento só são aceitas para Instâncias spot que sejam executadas depois de 5 de novembro de 2020, 0h (UTC).

Conteúdo

- Rebalancear ações que é possível executar
- Monitorar os sinais de recomendação de rebalanceamento
- Serviços que usam o sinal de recomendação de rebalanceamento

Rebalancear ações que é possível executar

Estas são algumas das possíveis ações de rebalanceamento que é possível executar:

Desligamento normal

Quando você receber o sinal de recomendação de rebalanceamento para uma instância spot, poderá iniciar os procedimentos de desligamento da instância, o que pode incluir a garantia de que os processos sejam concluídos antes de serem interrompidos. Por exemplo, é possível fazer upload de logs de sistema ou de aplicações para o Amazon Simple Storage Service (Amazon S3), desligar operadores do Amazon SQS ou concluir o cancelamento do registro do Sistema de Nomes de Domínio (DNS). Também é possível salvar seu trabalho em armazenamento externo e retomá-lo mais tarde.

Impedir que novos trabalhos sejam programados

Quando você recebe o sinal de recomendação de rebalanceamento para uma instância spot, pode impedir que novos trabalhos sejam programados na instância enquanto ela continuar a ser usada até o trabalho programado ser concluído.

Executar proativamente novas instâncias de substituição

É possível configurar grupos do Auto Scaling, EC2 Fleet ou frota spot para iniciar automaticamente as instâncias spot de substituição quando um sinal de recomendação de rebalanceamento é emitido. Para obter mais informações, consulte Use Capacity Rebalancing to handle Amazon EC2 Spot interruptions no Guia do usuário do Amazon EC2 Auto Scaling e Use o rebalanceamento de capacidade na frota do EC2 e na frota spot para substituir instâncias spot em risco neste guia do usuário.

Monitorar os sinais de recomendação de rebalanceamento

É possível monitorar o sinal de recomendação de rebalanceamento de modo que, quando ele for emitido, você possa executar as ações especificadas na seção anterior. O sinal de recomendação de rebalanceamento é disponibilizado como um evento que é enviado para o Amazon EventBridge (anteriormente conhecido como Amazon CloudWatch Events) e como metadados de instância na instância spot.

Monitorar sinais de recomendação de rebalanceamento:

- Usar o Amazon EventBridge
- Usar metadados da instância

Usar o Amazon EventBridge

Quando o sinal de recomendação de rebalanceamento é emitido para uma instância spot, o evento para o sinal é enviado para o Amazon EventBridge. Se o EventBridge detectar um padrão de evento que corresponda a um padrão definido em uma regra, o EventBridge invocará um destino (ou destinos) especificado(s) na regra.

Veja a seguir um exemplo de evento para o sinal de recomendação de rebalanceamento.

```
{
    "version": "0",
    "id": "12345678-1234-1234-1234-123456789012",
    "detail-type": "EC2 Instance Rebalance Recommendation",
    "source": "aws.ec2",
    "account": "123456789012",
    "time": "yyyy-mm-ddThh:mm:ssZ",
    "region": "us-east-2",
    "resources": ["arn:aws:ec2:us-east-2:123456789012:instance/i-1234567890abcdef0"],
    "detail": {
        "instance-id": "i-1234567890abcdef0"
    }
}
```

Os campos a seguir formam o padrão de evento definido na regra:

`"detail-type": "EC2 Instance Rebalance Recommendation"`

Identifica que o evento é um evento de recomendação de rebalanceamento

`"source": "aws.ec2"`

Identifica que o evento é de Amazon EC2

Criar uma regra de EventBridge

É possível escrever uma regra de EventBridge e automatizar quais ações tomar quando o padrão de evento corresponder à regra.

O exemplo a seguir cria uma regra de EventBridge para enviar um e-mail, mensagem de texto ou notificação por push para dispositivos móveis sempre que Amazon EC2 emite um sinal de recomendação de rebalanceamento. O sinal é emitido como um evento de `EC2 Instance Rebalance Recommendation`, que aciona a ação definida pela regra.

Antes de criar a regra EventBridge, você deve criar o tópico do Amazon SNS para e-mail, mensagem de texto ou notificação por push móvel.

Para criar uma regra de EventBridge para um evento de recomendação de rebalanceamento

1. Abra o console do Amazon EventBridge em https://console.aws.amazon.com/events/.
2. Selecione Criar regra.
3. Em Define rule detail (Definir detalhe da regra), faça o seguinte:
   a. Informe um Name (Nome) para a regra e, opcionalmente, uma descrição.

      Uma regra não pode ter o mesmo nome que outra regra na mesma região e no mesmo barramento de eventos.
   b. Em Event Bus (Barramento de eventos), escolha default (padrão). Quando um serviço da AWS em sua conta gerar um evento, ele sempre irá para o barramento de eventos padrão da sua conta.
   c. Em Rule type (Tipo de regra), escolha Rule with an event pattern (Regra com um padrão de evento).
   d. Escolha Próximo.
4. Em Build event pattern (Criar padrão de evento), faça o seguinte:
   a. Em Event source (Origem do evento), escolha Eventos da AWS ou eventos de parceiro do EventBridge.

b. Em Event pattern (Padrão de evento), neste exemplo você especificará o seguinte padrão de evento para corresponder ao evento `EC2 Instance Rebalance Recommendation` e, em seguida, escolherá Save (Salvar).

```
{
 "source": ["aws.ec2"],
 "detail-type": ["EC2 Instance Rebalance Recommendation"]
}
```

Para adicionar o padrão de evento, é possível usar um modelo escolhendo Event pattern form (Formulário de padrão de evento), ou especifique seu próprio padrão escolhendo Custom pattern (JSON editor) (Padrão personalizado (editor JSON)), como segue:

i. Para usar um modelo para criar o padrão de evento, faça o seguinte:

A. Escolha Event pattern form (Formulário de evento).

B. Em Event source (Origem do evento), escolha AWS services (Serviços da).

C. Em AWS Service (Produto da), escolha EC2 Spot Fleet (Frota spot do EC2).

D. Em Event type (Tipo de evento), escolha EC2 Instance Rebalance Recommendation (Recomendação de rebalanceamento da instância do EC2).

E. Para personalizar o modelo, escolha Edit pattern (Editar padrão) e faça as alterações para corresponder ao padrão de evento de exemplo.

ii. (Alternativa) Para especificar um padrão de evento personalizado, faça o seguinte:

A. Escolha Custom pattern (JSON editor) (Padrão personalizado (editor JSON)).

B. Na caixa Event pattern (Padrão de evento), adicione o padrão de evento para este exemplo.

c. Escolha Próximo.

5. Em Select target(s) (Selecionar destino(s)), faça o seguinte:

a. Em Tipos de destino, escolha Serviço da AWS.

b. Em Select a target (Selecione um destino), escolha SNS topic (Tópico do SNS) para enviar um email, mensagem de texto ou notificação por push móvel quando o evento ocorrer.

c. Em Topic (Tópico), escolha um tópico existente. Para fazer isso, você precisa criar um tópico do Amazon SNS usando o console do Amazon SNS. Para obter mais informações,

consulte Usar o Amazon SNS para mensagens de aplicação para pessoa (A2P) no Guia do desenvolvedor do Amazon Simple Notification Service.

d. (Opcional) Em Additional settings (Configurações adicionais), é possível, opcionalmente, definir configurações adicionais. Para obter mais informações, consulte Criar regras do Amazon EventBridge que reajam a eventos (etapa 16) no Guia do usuário do Amazon EventBridge.

e. Escolha Próximo.

6. (Opcional) Em Tags (Etiquetas), é possível atribuir, opcionalmente, uma ou mais etiquetas à sua regra e, em seguida, escolher Next (Próximo).
7. Em Review and create (Revisar e criar), faça o seguinte:

a. Revise os detalhes da regra e modifique-os conforme necessário.

b. Escolha Criar regra.

Para obter mais informações, consulte Amazon EventBridge rules (Regras do Amazon EventBridge) e Amazon EventBridge event patterns (Padrões de eventos do Amazon EventBridge) no Amazon EventBridge User Guide (Manual do usuário do Amazon EventBridge).

Usar metadados da instância

A categoria de metadados da instância `events/recommendations/rebalance` fornece o horário aproximado, em UTC, quando o sinal de recomendação de rebalanceamento foi emitido para uma instância spot.

Recomendamos que você verifique se há sinais de recomendação de rebalanceamento a cada 5 segundos para que você não perca a oportunidade de agir de acordo com a recomendação de rebalanceamento.

Se uma instância spot receber uma recomendação de rebalanceamento, o horário em que o sinal foi emitido estará presente nos metadados da instância. É possível recuperar o horário em que o sinal foi emitido da seguinte forma.

IMDSv2

Linux

Execute o seguinte comando em sua instância Linux.

IMDSv2

```
TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
    && curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/events/recommendations/rebalance
```

Windows

Execute o seguinte cmdlet na sua instância Windows.

```
[string]$token = Invoke-RestMethod `
    -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} `
    -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
Invoke-RestMethod `
    -Headers @{"X-aws-ec2-metadata-token" = $token} `
    -Method GET -Uri http://169.254.169.254/latest/meta-data/events/recommendations/rebalance
```

IMDSv1

Linux

Execute o seguinte comando em sua instância Linux.

```
curl http://169.254.169.254/latest/meta-data/events/recommendations/rebalance
```

Windows

Execute o seguinte cmdlet na sua instância Windows.

```
Invoke-RestMethod -Uri http://169.254.169.254/latest/meta-data/events/recommendations/rebalance
```

A seguir, é mostrado um exemplo de saída, que indica o horário, em UTC, em que o sinal de recomendação de rebalanceamento foi emitido para a instância spot.

```
{"noticeTime": "2020-10-27T08:22:00Z"}
```

Se o sinal não tiver sido emitido para a instância, o `events/recommendations/rebalance` não estará presente e você receberá uma mensagem de erro HTTP 404 quando tentar recuperá-lo.

Serviços que usam o sinal de recomendação de rebalanceamento

O Amazon EC2 Auto Scaling, a EC2 Fleet e a frota spot usam o sinal de recomendação de rebalanceamento para facilitar a manutenção da disponibilidade da workload, aumentando proativamente a frota com uma nova instância spot antes que uma instância em execução receba o aviso de interrupção da instância spot de dois minutos. É possível fazer com que esses serviços monitorem e respondam proativamente às alterações que afetam a disponibilidade da suas Instâncias spot. Para saber mais, consulte:

- Usar o rebalanceamento de capacidade para lidar com interrupções spot do Amazon EC2 no Guia do usuário do Amazon EC2 Auto Scaling.
- Use o rebalanceamento de capacidade na frota do EC2 e na frota spot para substituir instâncias spot em risco no tópico frota do EC2 e frota spot neste guia do usuário

Pontuação de posicionamento de spot

O recurso de pontuação de posicionamento de spot recomenda uma região ou zona de disponibilidade da AWS com base nos requisitos de capacidade spot. A capacidade de spot flutua e você não pode ter certeza de que sempre obterá a capacidade de que precisa. Uma pontuação de posicionamento de spot indica a probabilidade de uma solicitação de spot ter êxito em uma região ou zona de disponibilidade.

> **Note**
>
> Uma pontuação de posicionamento de spot não oferece nenhuma garantia em termos de capacidade disponível ou risco de interrupção. Uma pontuação de posicionamento de spot serve apenas como uma recomendação.

Casos de uso

É possível usar o recurso de pontuação de posicionamento de spot para o seguinte:

- Para realocar e escalar a capacidade computacional de spot em uma região diferente, conforme necessário, em resposta ao aumento das necessidades de capacidade ou diminuição da capacidade disponível na região atual.
- Para identificar a zona de disponibilidade ideal para executar workloads de zona de disponibilidade única.

- Para simular futuras necessidades de capacidade spot para que você possa escolher uma região ideal para a expansão de suas workloads baseadas em spot.
- Para encontrar uma combinação ideal de tipos de instância para atender às suas necessidades de capacidade spot.

Conteúdo

- Limitações
- Custos
- Como funciona a pontuação de posicionamento de spot
- Permissões necessárias para pontuação de posicionamento spot
- Calcular a pontuação de posicionamento spot

Limitações

- Limite da capacidade-alvo: o limite de capacidade-alvo da pontuação de posicionamento de spot é baseado em seu uso recente de spot, levando em conta um potencial aumento de uso. Se você não fez uso de spot recentemente, fornecemos para você um limite padrão baixo, alinhado com seu limite de solicitação de spot.
- Limite de configurações de solicitação: podemos limitar o número de novas configurações de solicitação dentro de um período de 24 horas se detectarmos padrões não associados ao uso pretendido do recurso de pontuação de posicionamento de spot. Se você atingir o limite, poderá repetir as configurações de solicitação que já usou, mas não poderá especificar novas configurações de solicitação até o próximo período de 24 horas.
- Número mínimo de tipos de instância: se especificar tipos de instância, você deverá especificar pelo menos três tipos de instância diferentes, caso contrário, o Amazon EC2 retornará uma baixa pontuação de posicionamento de spot. Da mesma forma, se você especificar atributos de instância, eles deverão ser resolvidos como, pelo menos, três tipos de instância diferentes. Tipos de instância são considerados diferentes se tiverem nomes diferentes. Por exemplo, m5.8xlarge, m5a.8xlarge, and m5.12xlarge são todos considerados diferentes.

Custos

Não há cobrança adicional pelo uso do recurso de pontuação de posicionamento de spot.

Como funciona a pontuação de posicionamento de spot

Ao usar o recurso de pontuação de posicionamento de spot, primeiramente você especifica os requisitos de computação para suas instâncias spot e, em seguida, o Amazon EC2 retorna as 10 principais regiões ou zonas de disponibilidade nas quais sua solicitação de spot provavelmente vai obter êxito. Cada região ou zona de disponibilidade é pontuada em uma escala de 1 a 10, com 10 indicando que é altamente provável que sua solicitação de spot tenha êxito e 1 indicando que sua solicitação de spot provavelmente não terá êxito.

Para usar o recurso de pontuação de posicionamento de spot, siga estas etapas:

- Etapa 1: especificar seus requisitos de spot
- Etapa 2: filtrar a resposta da pontuação de posicionamento de spot
- Etapa 3: revisar as recomendações
- Etapa 4: usar as recomendações

Etapa 1: especificar seus requisitos de spot

Primeiro, você especifica a capacidade-alvo de spot desejada e seus requisitos de computação, da seguinte forma:

1. Especifique a capacidade-alvo de spot e, opcionalmente, a unidade da capacidade-alvo.

   É possível especificar a capacidade-alvo de spot desejada em termos do número de instâncias ou vCPUs, ou em termos de quantidade de memória em MiB. Para especificar a capacidade-alvo em número de vCPUs ou quantidade de memória, especifique a unidade de capacidade-alvo como `vcpu` ou `memory-mib`. Caso contrário, o padrão é o número de instâncias.

   Ao especificar a capacidade-alvo em termos de número de vCPUs ou quantidade de memória, é possível usar essas unidades ao calcular a capacidade total. Por exemplo, se você quiser usar uma combinação de instâncias de tamanhos diferentes, é possível especificar a capacidade-alvo como um número total de vCPUs. O recurso de pontuação de posicionamento de spot considera cada tipo de instância na solicitação pelo número de vCPUs e conta o número total de vCPUs em vez do número total de instâncias ao totalizar a capacidade-alvo.

   Por exemplo, digamos que você especifique uma capacidade-alvo total de 30 vCPUs e sua lista de tipos de instância consista em c5.xlarge (4 vCPUs), m5.2xlarge (8 vCPUs) e r5.large (2 vCPUs). Para atingir um total de 30 vCPUs, é possívelria obter uma combinação de 2 c5.xlarge (2*4 vCPUs), 2 m5.2xlarge (2*8 vCPUs) e 3 r5.large (3*2 vCPUs).

2. Especifique tipos de instância ou atributos de instância.

   É possível especificar os tipos de instância a serem usados ou especificar os atributos de instância necessários para seus requisitos de computação e deixar o Amazon EC2 identificar os tipos de instância que têm esses atributos. Isso é conhecido como seleção de tipo de instância baseada em atributos.

   Você não pode especificar os tipos de instância e os atributos de instância na mesma solicitação de pontuação de posicionamento de spot.

   Se especificar tipos de instância, você deverá especificar pelo menos três tipos de instância diferentes, caso contrário, o Amazon EC2 retornará uma baixa pontuação de posicionamento de spot. Da mesma forma, se você especificar atributos de instância, eles deverão ser resolvidos como, pelo menos, três tipos de instância diferentes.

Para obter exemplos de maneiras diferentes de especificar seus requisitos de spot, consulte Exemplos de configuração.

Etapa 2: filtrar a resposta da pontuação de posicionamento de spot

O Amazon EC2 calcula a pontuação de posicionamento de spot para cada região ou zona de disponibilidade e retorna as 10 principais regiões ou as 10 principais zonas de disponibilidade nas quais sua solicitação de spot provavelmente terá êxito. O padrão é retornar uma lista de regiões pontuadas. Se você planeja iniciar toda a sua capacidade spot em uma única zona de disponibilidade, será útil solicitar uma lista de zonas de disponibilidade pontuadas.

É possível especificar um filtro de região para restringir as regiões que serão retornadas na resposta.

É possível combinar o filtro de região e uma solicitação de zonas de disponibilidade pontuadas. Dessa forma, as zonas de disponibilidade pontuadas serão restringidas às regiões para filtradas. Para encontrar a zona de disponibilidade com a maior pontuação em uma região, especifique somente essa região, e a resposta retornará uma lista com as pontuações de todas as zonas de disponibilidade na região.

Etapa 3: revisar as recomendações

A pontuação de posicionamento de spot para cada região ou zona de disponibilidade é calculada com base na capacidade-alvo, na composição dos tipos de instância, nas tendências de uso histórico e atual de spot e na hora em que a solicitação é feita. Como a capacidade spot está

constantemente flutuando, a mesma solicitação de pontuação de posicionamento de spot pode produzir pontuações diferentes quando calculada em horas diferentes.

Regiões e zonas de disponibilidade são pontuadas em uma escala de 1 a 10. Uma pontuação de 10 indica que sua solicitação de spot tem alta probabilidade, mas não garantia, de ter êxito. Uma pontuação de 1 indica que sua solicitação de spot tem muito pouca probabilidade de ter êxito. A mesma pontuação pode ser retornada para diferentes regiões ou zonas de disponibilidade.

Se pontuações baixas forem retornadas, será possível editar seus requisitos de computação e recalcular a pontuação. Também é possível solicitar recomendações de pontuação de posicionamento de spot para os mesmos requisitos de computação em diferentes horas do dia.

Etapa 4: usar as recomendações

Uma pontuação de posicionamento de spot só é relevante se a solicitação de spot tiver exatamente a mesma configuração que a configuração de pontuação de posicionamento de spot (capacidade-alvo, unidade de capacidade-alvo e tipos de instância ou atributos de instância) e estiver configurada para usar a estratégia de alocação de `capacity-optimized`. Caso contrário, a probabilidade de obter a capacidade de spot disponível não será alinhada com a pontuação.

Embora uma pontuação de posicionamento de spot sirva como diretriz e nenhuma pontuação garanta que sua solicitação de spot será atendida total ou parcialmente, é possível usar as seguintes informações para obter os melhores resultados:

- Usar a mesma configuração: a pontuação de posicionamento de spot é relevante somente se a configuração da solicitação de spot (capacidade-alvo, unidade da capacidade-alvo e tipos de instância ou atributos de instância) no seu grupo do Auto Scaling, frota do EC2 ou frota spot for a mesma que você inseriu para obter a pontuação de posicionamento de spot.

  Se você usou a seleção de tipo de instância baseada em atributo na solicitação de pontuação de posicionamento de spot, poderá usar a seleção de tipo de instância baseada em atributo para configurar seu grupo do Auto Scaling, frota do EC2 ou frota spot. Para obter mais informações, consulte Create mixed instances group using attribute-based instance type selection e Especificar atributos para seleção de tipo de instância para frota do EC2 ou frota spot.

  > **Note**
  >
  > Se você especificou sua capacidade-alvo em termos do número de vCPUs ou da quantidade de memória e tiver especificado tipos de instância na configuração de pontuação de posicionamento de spot, observe que não é possível criar essa configuração

no grupo do Auto Scaling, frota do EC2 ou frota spot. Em vez disso, é necessário definir manualmente a ponderação de instâncias usando o parâmetro `WeightedCapacity`.

- Usar a estratégia de alocação **`capacity-optimized`**: qualquer pontuação pressupõe que sua solicitação de frota será configurada para usar todas as zonas de disponibilidade (para solicitação de capacidade entre regiões) ou uma só zona de disponibilidade (se estiver solicitando capacidade em uma zona de disponibilidade) e a estratégia `capacity-optimized` de alocação de spot para que sua solicitação de capacidade de spot tenha êxito. Se você usar outras estratégias de alocação, como `lowest-price`, a probabilidade de obter a capacidade de spot disponível não será alinhada com a pontuação.
- Agir assim que tiver uma pontuação: a recomendação de pontuação de posicionamento de spot reflete a capacidade de spot disponível no momento da solicitação, e a mesma configuração pode produzir pontuações diferentes quando calculada em momentos diferentes devido a flutuações na capacidade de spot. Embora uma pontuação de 10 signifique que sua solicitação de capacidade de spot tem alta probabilidade, mas não garantia, de ter êxito, para obter os melhores resultados, recomendamos que você aja assim que tiver a pontuação, imediatamente. Também recomendamos que obtenha uma nova pontuação toda vez que tentar fazer uma solicitação de capacidade.

Permissões necessárias para pontuação de posicionamento spot

Por padrão, as identidades do IAM (usuários, perfis ou grupos) não têm permissão para usar the section called “Pontuação de posicionamento de spot”. Para permitir que as identidades do IAM usem a pontuação de posicionamento spot, crie uma política do IAM que conceda permissão para usar ação `ec2:GetSpotPlacementScores` da API do EC2. Depois, anexe a política às identidades do IAM que requeiram essa permissão.

O exemplo de política do IAM a seguir concede permissão para usar a ação `ec2:GetSpotPlacementScores` da API do EC2.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
```

```
            "Action": "ec2:GetSpotPlacementScores",
            "Resource": "*"
        }
    ]
}
```

Para obter mais informações sobre como editar uma política do IAM, consulte Edição de políticas do IAM no Guia do usuário do IAM.

Para conceder acesso, adicione as permissões aos seus usuários, grupos ou perfis:

- Usuários e grupos no Centro de Identidade do AWS IAM:

  Crie um conjunto de permissões. Siga as instruções em Criação de um conjunto de permissões no Guia do usuário do Centro de Identidade do AWS IAM.
- Usuários gerenciados no IAM com provedor de identidades:

  Crie um perfil para a federação de identidades. Siga as instruções em Criando um perfil para um provedor de identidades de terceiros (federação) no Guia do Usuário do IAM.
- Usuários do IAM:
  - Crie um perfil que seu usuário possa assumir. Siga as instruções em Criação de um perfil para um usuário do IAM no Guia do usuário do IAM.
  - (Não recomendado) Vincule uma política diretamente a um usuário ou adicione um usuário a um grupo de usuários. Siga as instruções em Adição de permissões a um usuário (console) no Guia do usuário do IAM.

Calcular a pontuação de posicionamento spot

É possível calcular uma pontuação de posicionamento spot com base na capacidade de destino e nos requisitos de computação. Para obter mais informações, consulte the section called “Como funciona a pontuação de posicionamento de spot”.

Permissões obrigatórias

Certifique-se de que você tenha as permissões necessárias. Para obter mais informações, consulte the section called “Permissões obrigatórias”.

Opções

- Calcular usando atributos de instância
- Calcular usando tipos de instância
- Calcular usando a AWS CLI

Deseja uma solução automatizada? Em vez de seguir as etapas manuais deste guia do usuário, você pode criar um painel de rastreamento de pontuação de posicionamento spot que captura e armazena automaticamente as pontuações no Amazon CloudWatch. Para obter mais informações, consulte Guidance for Building a Spot Placement Score Tracker Dashboard on AWS.

Calcular usando atributos de instância

Para calcular uma pontuação de posicionamento de spot especificando atributos de instância

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Solicitações spot.
3. Escolha a seta para baixo ao lado de Request Spot Instances e escolha Calculate Spot Placement Score.
4. Escolha Enter requirements (Inserir requisitos).
5. Em Target capacity (Capacidade-alvo), insira a capacidade desejada em termos do número de instances (instâncias) ou vCPUs, ou quantidade de memory (MiB) (memória).
6. Em Instance type requirements (Requisitos de tipo de instância), para especificar seus requisitos de computação e deixar que o Amazon EC2 identifique os tipos de instância ideais com esses requisitos, escolha Specify instance attributes that match your compute requirements (Especificar atributos de instância que correspondam aos requisitos de computação).
7. Em vCPUs, insira o número mínimo e máximo desejado de vCPUs. Para não especificar nenhum limite, selecione No minimum (Sem mínimo), No maximum (Sem máximo) ou ambos.
8. Em Memory (GiB) (Memória), insira a quantidade mínima e máxima de memória desejada. Para não especificar nenhum limite, selecione No minimum (Sem mínimo), No maximum (Sem máximo) ou ambos.
9. Em CPU architecture (Arquitetura da CPU), selecione a arquitetura de instância requisitada.
10. (Opcional) Em Additional instance attributes (Atributos de instância adicionais), é possível, opcionalmente, especificar um ou mais atributos para expressar seus requisitos de computação com mais detalhes. Cada atributo adicional inclui mais uma restrição à solicitação. É possível omitir os atributos adicionais; quando omitidos, os valores padrão são usados. Para obter uma descrição de cada atributo e seus valores padrão, consulte get-spot-placement-scores.

11. (Opcional) Para visualizar os tipos de instância com os atributos especificados, expanda Preview matching instance types (Previsualizar os tipos de instância correspondentes). Para excluir os tipos de instância de serem usados na avaliação do posicionamento, selecione as instâncias e escolha Exclude selected instance types (Excluir tipos de instância selecionados).
12. Escolha Load placement scores (Carregar pontuações de posicionamento) e analise os resultados.
13. (Opcional) Para exibir a pontuação de posicionamento de spot para regiões específicas, em Regions to evaluate (Regiões a serem avaliadas), selecione as regiões a serem avaliadas e, em seguida, escolha Calculate placement scores (Calcular pontuações de posicionamento).
14. (Opcional) Para exibir a pontuação de posicionamento de spot para as zonas de disponibilidade nas regiões que a ferramenta exibe, marque a caixa de seleção Fornecer pontuações de posicionamento por zona de disponibilidade. Uma lista de zonas de disponibilidade pontuadas é útil se você quiser iniciar toda a sua capacidade de spot em uma única zona de disponibilidade.
15. (Opcional) Para editar seus requisitos de computação e obter uma nova pontuação de posicionamento, escolha Edit (Editar), faça os ajustes necessários e, em seguida, escolha Calculate placement scores (Calcular pontuações de posicionamento).

Calcular usando tipos de instância

Para calcule uma pontuação de posicionamento de spot especificando tipos de instância

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Solicitações spot.
3. Escolha a seta para baixo ao lado de Request Spot Instances e escolha Calculate Spot Placement Score.
4. Escolha Enter requirements (Inserir requisitos).
5. Em Target capacity (Capacidade-alvo), insira a capacidade desejada em termos do número de instances (instâncias) ou vCPUs, ou quantidade de memory (MiB) (memória).
6. Em Instance type requirements (Requisitos de tipo de instância), para especificar os tipos de instância a serem usados, escolha Manually select instance types (Selecionar manualmente os tipos de instância).
7. Escolha Select instance types (Selecionar tipos de instância), selecione os tipos de instância a serem usados e escolha Select (Selecionar). Para localizar rapidamente tipos de instância, é possível usar a barra de filtro para filtrar os tipos de instância por diferentes propriedades.

8. Escolha Load placement scores (Carregar pontuações de posicionamento) e analise os resultados.
9. (Opcional) Para exibir a pontuação de posicionamento de spot para regiões específicas, em Regions to evaluate (Regiões a serem avaliadas), selecione as regiões a serem avaliadas e, em seguida, escolha Calculate placement scores (Calcular pontuações de posicionamento).
10. (Opcional) Para exibir a pontuação de posicionamento de spot para as zonas de disponibilidade nas regiões que a ferramenta exibe, marque a caixa de seleção Fornecer pontuações de posicionamento por zona de disponibilidade. Uma lista de zonas de disponibilidade pontuadas é útil se você quiser iniciar toda a sua capacidade de spot em uma única zona de disponibilidade.
11. (Opcional) Para editar a lista de tipos de instância e obter uma nova pontuação de posicionamento, escolha Edit (Editar), faça os ajustes necessários e, em seguida, escolha Calculate placement scores (Calcular pontuações de posicionamento).

Calcular usando a AWS CLI

Para calcular uma pontuação de posicionamento de spot

1. (Opcional) Para gerar todos os parâmetros possíveis que podem ser especificados para a configuração de pontuação de posicionamento de spot, use o comando get-spot-placement-scores e o parâmetro `--generate-cli-skeleton`.

```
aws ec2 get-spot-placement-scores \
    --region us-east-1 \
    --generate-cli-skeleton
```

O seguinte é um exemplo de saída.

```
{
    "InstanceTypes": [
        ""
    ],
    "TargetCapacity": 0,
    "TargetCapacityUnitType": "vcpu",
    "SingleAvailabilityZone": true,
    "RegionNames": [
        ""
    ],
    "InstanceRequirementsWithMetadata": {
        "ArchitectureTypes": [
```

```
            "x86_64_mac"
        ],
        "VirtualizationTypes": [
            "hvm"
        ],
        "InstanceRequirements": {
            "VCpuCount": {
                "Min": 0,
                "Max": 0
            },
            "MemoryMiB": {
                "Min": 0,
                "Max": 0
            },
            "CpuManufacturers": [
                "amd"
            ],
            "MemoryGiBPerVCpu": {
                "Min": 0.0,
                "Max": 0.0
            },
            "ExcludedInstanceTypes": [
                ""
            ],
            "InstanceGenerations": [
                "previous"
            ],
            "SpotMaxPricePercentageOverLowestPrice": 0,
            "OnDemandMaxPricePercentageOverLowestPrice": 0,
            "BareMetal": "excluded",
            "BurstablePerformance": "excluded",
            "RequireHibernateSupport": true,
            "NetworkInterfaceCount": {
                "Min": 0,
                "Max": 0
            },
            "LocalStorage": "included",
            "LocalStorageTypes": [
                "hdd"
            ],
            "TotalLocalStorageGB": {
                "Min": 0.0,
                "Max": 0.0
            },
```

```
            "BaselineEbsBandwidthMbps": {
                "Min": 0,
                "Max": 0
            },
            "AcceleratorTypes": [
                "fpga"
            ],
            "AcceleratorCount": {
                "Min": 0,
                "Max": 0
            },
            "AcceleratorManufacturers": [
                "amd"
            ],
            "AcceleratorNames": [
                "vu9p"
            ],
            "AcceleratorTotalMemoryMiB": {
                "Min": 0,
                "Max": 0
            }
        }
    },
    "DryRun": true,
    "MaxResults": 0,
    "NextToken": ""
}
```

2. Crie um arquivo de configuração JSON usando a saída da etapa anterior e configure-o da seguinte forma:

   a. Em `TargetCapacity`, insira a capacidade desejada em termos do número de instâncias ou vCPUs, ou quantidade de memória (MiB).

   b. Em `TargetCapacityUnitType`, insira a unidade para a capacidade-alvo. Se você omitir esse parâmetro, ele assumirá o padrão `units`.

      Valores válidos: `units` (o que se traduz em número de instâncias) | `vcpu` | `memory-mib`

   c. Em `SingleAvailabilityZone`, especifique `true` para uma resposta que retorna uma lista de zonas de disponibilidade pontuadas. Uma lista de zonas de disponibilidade pontuadas é útil se você quiser iniciar toda a sua capacidade de spot em uma única zona de disponibilidade. Se você omitir esse parâmetro, ele assumirá o padrão `false`, e a resposta retornará uma lista de regiões pontuadas.

d. (Opcional) Em `RegionNames`, especifique as regiões que deseja usar como filtro. É necessário especificar o código de região, por exemplo, `us-east-1`.

   Com um filtro de região, a resposta retorna apenas as regiões que você especificou. Se tiver especificado `true` para `SingleAvailabilityZone`, a resposta retornará apenas as zonas de disponibilidade nas regiões que você especificou.

e. É possível incluir um `InstanceTypes` ou `InstanceRequirements`, mas não ambos na mesma configuração.

   Especifique uma das seguintes opções na configuração de JSON:

   - Para especificar uma lista de tipos de instância, especifique os tipos de instância no parâmetro `InstanceTypes`. Especifique pelo menos três tipos de instância diferentes. Se você especificar apenas um ou dois tipos de instância, a pontuação de posicionamento de spot retornará uma pontuação baixa. Para obter uma lista dos tipos de instância , consulte Tipos de instância do Amazon EC2.
   - Para especificar os atributos da instância para que o Amazon EC2 identifique os tipos de instância que correspondem a esses atributos, especifique os atributos localizados na estrutura `InstanceRequirements`.

     É necessário fornecer valores para `VCpuCount`, `MemoryMiB` e `CpuManufacturers`. É possível omitir os outros atributos; quando omitidos, os valores padrão são usados. Para obter uma descrição de cada atributo e seus valores padrão, consulte get-spot-placement-scores.

   Para obter configurações de exemplo, consulte Exemplos de configuração.

3. Para obter a pontuação de posicionamento de spot para os requisitos especificados no arquivo JSON, use o comando get-spot-placement-scores e especifique o nome e o caminho do arquivo JSON usando o parâmetro `--cli-input-json`.

```
aws ec2 get-spot-placement-scores \
    --region us-east-1 \
    --cli-input-json file://file_name.json
```

Exemplo de saída se `SingleAvailabilityZone` for definido como `false` ou omitido (se omitido, o padrão `false` será usado); uma lista classificada de regiões será retornada.

```
"SpotPlacementScores": [
    {
        "Region": "us-east-1",
        "Score": 7
    },
    {
        "Region": "us-west-1",
        "Score": 5
    },
   ...
```

Exemplo de saída se `SingleAvailabilityZone` for definido como `true`; uma lista pontuada de zonas de disponibilidade será retornada.

```
"SpotPlacementScores": [
    {
        "Region": "us-east-1",
        "AvailabilityZoneId": "use1-az1",
        "Score": 8
    },
    {
        "Region": "us-east-1",
        "AvailabilityZoneId": "usw2-az3",
        "Score": 6
    },
   ...
```

Exemplos de configuração

Quando usar a AWS CLI, será possível usar os exemplos de configurações as seguir.

Exemplos de configuração

- Exemplo: especificar tipos de instância e capacidade-alvo
- Exemplo: especificar tipos de instância e capacidade-alvo em termos de memória
- Exemplo: especificar atributos para seleção de tipo de instância baseada em atributos
- Exemplo: especificar atributos para seleção de tipo de instância baseada em atributos e retornar uma lista pontuada de zonas de disponibilidade

Exemplo: especificar tipos de instância e capacidade-alvo

O exemplo de configuração a seguir especifica três tipos de instância diferentes e uma capacidade-alvo de spot de 500 instâncias spot.

```
{
    "InstanceTypes": [
        "m5.4xlarge",
        "r5.2xlarge",
        "m4.4xlarge"
    ],
    "TargetCapacity": 500
}
```

Exemplo: especificar tipos de instância e capacidade-alvo em termos de memória

O exemplo de configuração a seguir especifica três tipos de instância diferentes e uma capacidade-alvo de spot de 500.000 MiB de memória, em que o número de Instâncias spot a serem iniciadas deve fornecer um total de 500.000 MiB de memória.

```
{
    "InstanceTypes": [
        "m5.4xlarge",
        "r5.2xlarge",
        "m4.4xlarge"
    ],
    "TargetCapacity": 500000,
    "TargetCapacityUnitType": "memory-mib"
}
```

Exemplo: especificar atributos para seleção de tipo de instância baseada em atributos

O exemplo de configuração a seguir é configurado para seleção de tipo de instância baseada em atributos e é seguido de um texto explicativo do exemplo de configuração.

```
{
    "TargetCapacity": 5000,
    "TargetCapacityUnitType": "vcpu",
    "InstanceRequirementsWithMetadata": {
        "ArchitectureTypes": ["arm64"],
        "VirtualizationTypes": ["hvm"],
```

```
        "InstanceRequirements": {
            "VCpuCount": {
                "Min": 1,
                "Max": 12
            },
            "MemoryMiB": {
                "Min": 512
            }
        }
    }
}
```

`InstanceRequirementsWithMetadata`

Para usar a seleção do tipo de instância baseada em atributo, é necessário incluir a estrutura `InstanceRequirementsWithMetadata` na configuração e especificar os atributos desejados para as Instâncias spot.

No exemplo anterior, os seguintes atributos de instância necessários são especificados:

- `ArchitectureTypes` – o tipo de arquitetura dos tipos de instância deve ser `arm64`.
- `VirtualizationTypes` – o tipo de virtualização dos tipos de instância deve ser `hvm`.
- `VCpuCount`: os tipos de instância devem ter no mínimo 1 e no máximo 12 vCPUs.
- `MemoryMiB`: os tipos de instância devem ter no mínimo 512 MiB de memória. Omitindo o parâmetro `Max`, você está indicando que não há limite máximo.

Observe que existem vários outros atributos opcionais que é possível especificar. Para obter a lista de atributos, consulte get-spot-placement-scores.

`TargetCapacityUnitType`

O parâmetro `TargetCapacityUnitType` especifica a unidade da capacidade-alvo. No exemplo, a capacidade-alvo é `5000` e o tipo de unidade de capacidade-alvo é `vcpu`, que juntos especificam uma capacidade-alvo desejada de 5000 vCPUs, em que o número de instâncias spot a serem iniciadas deve fornecer um total de 5000 vCPUs.

Exemplo: especificar atributos para seleção de tipo de instância baseada em atributos e retornar uma lista pontuada de zonas de disponibilidade

O exemplo de configuração a seguir é configurado para seleção de tipo de instância baseada em atributos. Especificando `"SingleAvailabilityZone": true`, a resposta retornará uma lista de zonas de disponibilidade pontuadas.

```
{
    "TargetCapacity": 1000,
    "TargetCapacityUnitType": "vcpu",
    "SingleAvailabilityZone": true,
    "InstanceRequirementsWithMetadata": {
        "ArchitectureTypes": ["arm64"],
        "VirtualizationTypes": ["hvm"],
        "InstanceRequirements": {
            "VCpuCount": {
                "Min": 1,
                "Max": 12
            },
            "MemoryMiB": {
                "Min": 512
            }
        }
    }
}
```

Rastrear os custos das instâncias spot usando o feed de dados da instância spot

Para compreender as cobranças relativas às suas instâncias spot, o Amazon EC2 fornece um feed de dados que descreve o uso que você faz de sua instância spot e a definição de preços. Esse feed de dados é enviado a um bucket do Amazon S3 que você especifica ao assinar um feed de dados.

O feed de dados normalmente chega em seu bucket uma vez por hora. Se você não tiver uma instância spot em execução em uma hora específica, não receberá um arquivo de feed de dados nessa hora.

Cada hora de uso de uma instância spot é coberto em um único arquivo de dados. Esses arquivos são compactados (gzip) antes de serem entregues ao seu bucket. O Amazon EC2 pode gravar vários arquivos em uma determinada hora de uso quando os arquivos estiverem muito grandes (por exemplo, quando o conteúdo dos arquivos para a hora ultrapassar 50 MB antes da compactação).

> **Note**
>
> Você só pode criar um feed de dados de instância spot para cada Conta da AWS.

O feed de dados da instância spot é compatível em todas as regiões AWS, exceto China (Pequim), China (Ningxia), AWS GovCloud (EUA) e as regiões que estão desabilitadas por padrão.

Conteúdo

- Nome e formato de arquivo do feed de dados
- Requisitos do bucket do Amazon S3
- Assinar seu feed de dados da instância spot
- Visualização dos dados no feed de dados
- Excluir seu feed de dados de instância spot

Nome e formato de arquivo do feed de dados

O nome de arquivo do feed de dados de instância spot usa o seguinte formato (com a data e a hora em UTC):

```
bucket-name.s3.amazonaws.com/optional-prefix/aws-account-id.YYYY-MM-DD-HH.n.unique-id.gz
```

Por exemplo, se o nome do bucket for **amzn-s3-demo-bucket** e o prefixo for **my-prefix**, os nomes dos arquivos serão semelhantes ao seguinte:

```
amzn-s3-demo-bucket.s3.amazonaws.com/my-prefix/111122223333.2023-12-09-07.001.b959dbc6.gz
```

Para obter mais informações sobre os nomes de bucket, consulte Regras de nomeação de bucket no Guia do usuário do Amazon S3.

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

Campo	Descrição
`Timestamp`	O time stamp usado para determinar o preço cobrado pelo uso dessa instância.
`UsageType`	O tipo de uso e instância que está sendo cobrado. Para `m1.small` Instâncias spot, este campo está definido como `SpotUsage` . Para todos os outros tipos de instância, esse campo é definido como `SpotUsage:` {instance-type}. Por exemplo, `SpotUsage:c1.medium` .
`Operation`	O produto que está sendo cobrado. Nas Instâncias spot do Linux, este campo é definido como `RunInstances` . Nas Instâncias spot do Windows, este campo é definido como `RunInstances:0002` . O uso de spot é agrupado de acordo com a zona de disponibilidade.
`InstanceID`	O ID da instância spot que gerou este uso de instância.
`MyBidID`	O ID da solicitação de instância spot que gerou este uso de instância.
`MyMaxPrice`	O preço máximo especificado para essa solicitação de spot.
`MarketPrice`	O preço spot na hora especificada no campo `Timestamp` .
`Charge`	O preço cobrado por este uso de instância.
`Version`	A versão do feed de dados. A versão possível é a 1.0.

Requisitos do bucket do Amazon S3

Ao assinar o feed de dados, especifique 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:

- É necessário ter a permissão `FULL_CONTROL` para o bucket. Se você for o proprietário do bucket, terá essa permissão por padrão. Caso contrário, o proprietário do bucket deve conceder essa permissão à sua Conta da AWS.
- Quando você assina um feed de dados, essas permissões são usadas para atualizar o ACL do bucket a fim de fornecer à conta de feed de dados da AWS a permissão `FULL_CONTROL`. A conta de feed de dados da AWS grava arquivos de feed de dados no bucket. Se sua conta não tiver as permissões necessárias, os arquivos de feed de dados não poderão ser gravados no bucket. Para obter mais informações, consulte Logs enviados ao Amazon S3 no Guia do usuário do Amazon CloudWatch Logs.

  Se você atualizar o ACL e eliminar as permissões para a conta do feed de dados da AWS, os arquivos de feed de dados não poderão ser gravados no bucket. É necessário 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.
- Caso criptografe o bucket do Amazon S3 usando criptografia no lado do servidor com uma chave do AWS KMS armazenada no AWS Key Management Service (SSE-KMS), você deverá usar uma chave gerenciada pelo cliente. Para obter mais informações, consulte Criptografia no lado do servidor de bucket do Amazon S3 no Guia do usuário do Amazon CloudWatch Logs.

Assinar seu feed de dados da instância spot

É possível se inscrever para receber o feed de dados da instância spot a qualquer momento. Não é possível realizar essa tarefa usando o console do Amazon EC2.

Se você receber um erro informando que o bucket não tem permissões suficientes, consulte o seguinte artigo para obter informações sobre solução de problemas: Troubleshoot the data feed for Spot Instances.

AWS CLI

Para assinar seu feed de dados

Use o comando create-spot-datafeed-subscription.

Para especificar um bucket com um prefixo, use o seguinte exemplo:

```
aws ec2 create-spot-datafeed-subscription \
    --bucket amzn-s3-demo-bucket \
    --prefix my-prefix
```

Para especificar um bucket sem um prefixo, use o seguinte exemplo:

```
aws ec2 create-spot-datafeed-subscription \
    --bucket amzn-s3-demo-bucket
```

PowerShell

Para assinar seu feed de dados

Use o cmdlet New-EC2SpotDatafeedSubscription.

Para especificar um bucket com um prefixo, use o seguinte exemplo:

```
New-EC2SpotDatafeedSubscription `
    -Bucket amzn-s3-demo-bucket `
    -Prefix my-prefix
```

Para especificar um bucket sem um prefixo, use o seguinte exemplo:

```
New-EC2SpotDatafeedSubscription `
    -Bucket amzn-s3-demo-bucket
```

Visualização dos dados no feed de dados

No Console de gerenciamento da AWS, abra o AWS CloudShell. Use o comando s3 sync a seguir para obter os arquivos .gz do bucket do S3 para o feed de dados e armazená-los na pasta que você especificar.

```
aws s3 sync s3://amzn-s3-demo-bucket ./data-feed
```

Para exibir o conteúdo de um arquivo .gz, acesse a pasta em que você armazenou o conteúdo do bucket do S3.

```
cd data-feed
```

Use o comando ls para visualizar os nomes dos arquivos. Use o comando zcat com o nome do arquivo para exibir o conteúdo do arquivo compactado. O comando a seguir é um exemplo.

```
zcat  111122223333.2023-12-09-07.001.b959dbc6.gz
```

O seguinte é um exemplo de saída.

```
#Version: 1.0
#Fields: Timestamp UsageType Operation InstanceID MyBidID MyMaxPrice MarketPrice Charge
 Version
2023-12-09 07:13:47 UTC USE2-SpotUsage:c7a.medium       RunInstances:SV050
 i-0c3e0c0b046e050df     sir-pwq6nmfp    0.0510000000 USD        0.0142000000 USD
  0.0142000000 USD        1
```

Excluir seu feed de dados de instância spot

Após terminar de usar o feed de dados da instância spot, será possível excluí-lo.

AWS CLI

Para excluir seu feed de dados

Use o comando delete-spot-datafeed-subscription.

```
aws ec2 delete-spot-datafeed-subscription
```

PowerShell

Para excluir seu feed de dados

Use o cmdlet Remove-EC2SpotDatafeedSubscription.

```
Remove-EC2SpotDatafeedSubscription
```

Função vinculada ao serviço para solicitações de instâncias spot

O Amazon EC2 usa funções vinculadas ao serviço para as permissões necessárias para chamar outros produtos da AWS em seu nome. O perfil vinculado ao serviço é um tipo exclusivo de perfil

do IAM vinculado diretamente ao AWS service (Serviço da AWS). Os perfis vinculados a serviços oferecem uma maneira segura de delegar permissões a outros Serviços da AWS, pois somente o serviço vinculado pode assumir uma função vinculada ao serviço. Para obter mais informações, consulte Perfis vinculados ao serviço no Guia do usuário do IAM.

O Amazon EC2 usa a função vinculada ao serviço denominada AWSServiceRoleForEC2Spot para executar e gerenciar Instâncias spot em seu nome.

Permissões concedidas pelo AWSServiceRoleForEC2Spot

O Amazon EC2 usa AWSServiceRoleForEC2Spot para concluir as ações a seguir:

- `ec2:DescribeInstances` – Descrever instâncias spot
- `ec2:StopInstances` – Parar instâncias spot
- `ec2:StartInstances` – Iniciar instâncias spot

Criar a função vinculada ao serviço

Na maioria das circunstâncias, você não precisa criar manualmente uma função vinculada ao serviço. O Amazon EC2 cria a função AWSServiceRoleForEC2Spot vinculada ao serviço na primeira vez que você solicita uma instância spot usando o console.

Se você tinha uma solicitação de instância spot ativa antes de outubro de 2017, quando o Amazon EC2 começou a oferecer suporte a essa função vinculada ao serviço, o Amazon EC2 criou a função AWSServiceRoleForEC2Spot em sua conta da AWS. Para obter mais informações, consulte Uma nova função apareceu na minha conta no Guia do usuário do IAM.

Se você usar a AWS CLI ou uma API para solicitar uma instância spot, deverá assegurar que essa função existe.

Para criar AWSServiceRoleForEC2Spot usando o console

1. Abra o console do IAM em https://console.aws.amazon.com/iam/.
2. No painel de navegação, escolha Perfis.
3. Selecione Create role.
4. Na página Select type of trusted entity (Selecionar tipo de entidade confiável), escolha EC2, EC2 - Spot Instances (EC2 - instâncias spot), Next: Permissions (Próximo: permissões).
5. Na próxima página, escolha Next:Review (Próximo: revisar).

6. Na página Review (Revisar), selecione Create role (Criar função).

Para criar AWSServiceRoleForEC2Spot usando a AWS CLI

Use o comando create-service-linked-role da seguinte forma.

```
aws iam create-service-linked-role --aws-service-name spot.amazonaws.com
```

Se você não precisar mais usar Instâncias spot, é recomendável excluir a função AWSServiceRoleForEC2Spot. Depois que essa função for excluída da sua conta, o Amazon EC2 criará a função novamente se você solicitar Instâncias spot.

Conceder acesso às chaves gerenciadas pelo cliente para uso com AMIs criptografadas e snapshots do EBS

Se você especificar uma AMI criptografada ou um snapshot do Amazon EBS criptografado para suas instâncias spot e usar uma chave gerenciada pelo cliente para criptografia, deverá conceder à função AWSServiceRoleForEC2Spot permissão para usar a chave gerenciada pelo cliente de forma que o Amazon EC2 consiga executar instâncias spot em seu nome. Para isso, adicione uma concessão à chave gerenciada pelo cliente, conforme exibido no procedimento a seguir.

Durante a definição de permissões, as concessões são uma alternativa às políticas de chave. Para obter mais informações, consulte Uso de concessões e Uso de políticas de chave no AWS KMS, no Guia do desenvolvedor do AWS Key Management Service.

Para conceder as permissões para a função AWSServiceRoleForEC2Spot para usar a chave gerenciada pelo cliente

- Use o comando create-grant para adicionar uma concessão à chave gerenciada pelo cliente e especificar a entidade principal (a função vinculada ao serviço AWSServiceRoleForEC2) que recebe permissão para executar as operações permitidas pela concessão. A chave gerenciada pelo cliente é especificada pelo parâmetro `key-id` e o ARN da chave gerenciada pelo cliente. A entidade principal é especificada pelo parâmetro `grantee-principal` e pelo ARN da função vinculada ao serviço AWSServiceRoleForEC2Spot.

```
aws kms create-grant \
    --region us-east-1 \
    --key-id arn:aws:kms:us-
east-1:444455556666:key/1234abcd-12ab-34cd-56ef-1234567890ab \
```

```
    --grantee-principal arn:aws:iam::111122223333:role/aws-service-role/
spot.amazonaws.com/AWSServiceRoleForEC2Spot \
    --operations "Decrypt" "Encrypt" "GenerateDataKey"
 "GenerateDataKeyWithoutPlaintext" "CreateGrant" "DescribeKey" "ReEncryptFrom"
 "ReEncryptTo"
```

Cotas de instâncias spot

Há cotas para o número de instâncias spot em execução e as solicitações de instâncias spot pendentes por Conta da AWS por região. Depois que uma solicitação de instância spot pendente é atendida, a solicitação não é mais contabilizada na cota porque a instância em execução é contabilizada na cota.

As cotas de instância spot são gerenciadas em termos do número de unidades de processamento central virtuais (vCPUs) que as instâncias spot em execução estão usando ou usarão até o atendimento de solicitações de instância spot abertas. Se você encerrar as instâncias spot, mas não cancelar as solicitações de instância spot, as solicitações serão contabilizadas em relação à cota de vCPU da instância spot até que o Amazon EC2 detecte os encerramentos de instância spot e feche as solicitações.

Fornecemos os tipos de cota a seguir para instâncias spot.

Nome	Padrão	Ajustável
Todas as solicitações de instância spot DL	0	Sim
Todas as solicitações de instância spot F	0	Sim
Todas as solicitações de instância spot G e VT	0	Sim
Todas as solicitações de instância spot Inf	0	Sim
Todas as solicitações de instância spot P	0	Sim
Todas as solicitações de instância spot padrão (A, C, D, H, I, M, R, T, Z)	5	Sim
Todas as solicitações de instância spot Trn	0	Sim
Todas as solicitações de instância spot X	0	Sim

Mesmo que o Amazon EC2 ajuste automaticamente suas cotas de instância spot com base em seu uso, é possível solicitar um aumento de cota, se for o caso. Por exemplo, se você pretende lançar mais Instâncias spot do que a cota atual permite, solicite um aumento de cota. Também é possível solicitar um aumento de cota se você enviar uma solicitação de instância spot e receber uma mensagem de erro `Max spot instance count exceeded`. Para solicitar aumento de cota, use o console do Service Quotas descrito em Service Quotas do Amazon EC2.

É possível iniciar qualquer combinação de tipos de instância que atenda às necessidades em constante mudança da sua aplicação. Por exemplo: com uma cota de solicitações de todas instâncias spotpadrão de 256 vCPUs, é possível solicitar 32 instâncias spot `m5.2xlarge` (32 x 8 vCPUs) ou 16 instâncias spot `c5.4xlarge` (16 x 16 vCPUs).

Com a integração de métricas do Amazon CloudWatch, é possível monitorar o uso do EC2 em relação às suas cotas. Também é possível configurar alarmes para alertar quando estiver chegando próximo da cota. Para obter mais informações, consulte Alarmes do Service Quotas e do Amazon CloudWatch no Guia do usuário do Service Quotas.

Hosts dedicados do Amazon EC2

Um host dedicado do Amazon EC2 é um servidor físico totalmente dedicado para seu uso. Como opção, você pode compartilhar a capacidade da instância com outras contas da AWS. Para obter mais informações, consulte Compartilhamento de host dedicado do Amazon EC2 entre contas.

Os hosts dedicados fornecem visibilidade e controle sobre o posicionamento de instância, além de compatibilidade com afinidade ao host. Isso significa que você pode iniciar e executar instâncias em hosts específicos e garantir que as instâncias sejam executadas somente em hosts específicos. Para obter mais informações, consulte Posicionamento automático e afinidade de host dedicado do Amazon EC2.

O hosts dedicados fornecem compatibilidade abrangente com o modelo traga a sua própria licença (BYOL). Eles permitem que você use suas licenças de software existentes por soquete, por núcleo ou por VM, incluindo o Windows Server, o SQL Server, o SUSE Linux Enterprise Server, o Red Hat Enterprise Linux ou outras licenças de software vinculadas a VMs, soquetes ou núcleos físicos, de acordo com os termos de sua licença.

Se você precisar que suas instâncias sejam executadas em hardware dedicado, mas não precisar de visibilidade ou controle sobre o posicionamento das instâncias e não precisar usar licenças de software por soquete ou por núcleo, avalie a possibilidade de usar instâncias dedicadas. É possível usar instâncias dedicadas e hosts dedicados para iniciar instâncias do Amazon EC2 em servidores

físicos dedicados. Não há diferenças físicas de performance ou de segurança entre Instâncias dedicadas e instâncias em Hosts dedicados. No entanto, há algumas diferenças básicas entre os dois. A tabela a seguir destaca algumas das principais diferenças entre Hosts dedicados e Instâncias dedicadas:

	Dedicated Host	Dedicated Instance
Servidor físico dedicado	Servidor físico com capacidade de instância totalmente dedicada para seu uso.	Um servidor físico dedicado a uma única conta de cliente.
Compartilhamento de capacidade de instância	Pode compartilhar a capacidade de instância com outras contas.	Não compatível
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	Sem suporte
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	Compatível. Para obter mais informações, consulte Recuperação de um host dedicado do Amazon EC2.	Compatível
Traga sua própria	Compatível	Suporte parcial *

	Dedicated Host	Dedicated Instance
licença (BYOL)		
Capacity Reservations	Não compatível	Compatível

* O Microsoft SQL Server com Mobilidade de Licenças por meio do Software Assurance e as licenças do Windows Virtual Desktop Access (VDA) podem ser usadas com Instância dedicada.

Para obter mais informações sobre as instâncias dedicadas, consulte Instâncias dedicadas do Amazon EC2.

Restrições do Hosts dedicados

Antes de alocar Hosts dedicados, observe as seguintes limitações e restrições:

- Para executar RHEL E SUSE Linux nos Hosts dedicados, é necessário trazer suas próprias AMIs. Você não pode executar as AMIs do RHEL e SUSE Linux que são oferecidas pela AWS ou disponíveis no AWS Marketplace com os hosts dedicados. Para obter mais informações sobre como criar sua própria AMI, consulte Traga suas próprias licenças de software para os hosts dedicados do Amazon EC2.

  Essa restrição não se aplica a hosts alocados para instâncias de alta memória (`u-6tb1.metal`, `u-9tb1.metal`, `u-12tb1.metal`, `u-18tb1.metal` e `u-24tb1.metal`). As AMIs do RHEL e do SUSE Linux oferecidas pela AWS ou disponíveis no AWS Marketplace podem ser usadas com esses hosts.
- Há um limite para o número de hosts dedicados em execução por família de instâncias por conta da AWS por região. As cotas se aplicam somente às instâncias em execução. Se a sua instância estiver pendente, sendo interrompida ou tiver sido interrompida, ela não será contabilizada para a sua cota. Para ver as cotas da sua conta ou solicitar aumento da cota, use o console do Service Quotas.
- Grupos de Auto Scaling são compatíveis ao usar um modelo de execução que especifica um grupo de recursos de host. Para obter mais informações, consulte Criar um modelo de execução usando configurações avançadas no Guia do usuário do Amazon EC2 Auto Scaling.
- Não há suporte para instâncias do Amazon RDS.

- O nível de uso gratuito da AWS não está disponível para hosts dedicados.
- O controle de posicionamento de instância se refere ao gerenciamento de execuções de instâncias em Hosts dedicados. Não é possível iniciar hosts dedicados em grupos de posicionamento.
- Se você alocar um host para um tipo de instância virtualizada, não poderá modificar o tipo de instância para um tipo de instância `.metal` depois que o host for alocado. Por exemplo, se você alocar um host para o tipo de instância `m5.large`, não poderá modificar o tipo de instância para `m5.metal`.

  Da mesma forma, se você alocar um host para um tipo de instância `.metal`, não poderá modificar o tipo de instância para um tipo de instância virtualizada depois que o host for alocado. Por exemplo, se você alocar um host para o tipo de instância `m5.metal`, não poderá modificar o tipo de instância para `m5.large`.

Conteúdo

- Preços e faturamento de hosts dedicados do Amazon EC2
- Configurações de capacidade de instância de host dedicado do Amazon EC2
- Instâncias T3 expansíveis em hosts dedicados do Amazon EC2
- Traga suas próprias licenças de software para os hosts dedicados do Amazon EC2
- Posicionamento automático e afinidade de host dedicado do Amazon EC2
- Alocar um host dedicado do Amazon EC2 para uso em sua conta
- Iniciar instâncias do Amazon EC2 em um host dedicado do Amazon EC2
- Iniciar instâncias do Amazon EC2 em um grupo de recursos de host
- Modificar a configuração de posicionamento automático para um host dedicado existente do Amazon EC2
- Modificar os tipos de instância compatíveis para um host dedicado existente do Amazon EC2
- Modificar a locação e a afinidade de host dedicado do Amazon EC2 para uma instância do Amazon EC2
- Liberar um host dedicado do Amazon EC2
- Migre para hosts dedicados do Amazon EC2 baseadas em Nitro
- Comprar reservas de host dedicado para obter descontos na fatura
- Compartilhamento de host dedicado do Amazon EC2 entre contas
- Hosts dedicados do Amazon EC2 no AWS Outposts
- Recuperação de um host dedicado do Amazon EC2

- Manutenção de host dedicado do Amazon EC2
- Monitorar o estado dos hosts dedicados do Amazon EC2
- Monitorar as alterações da configuração de host dedicado do Amazon EC2 usando o AWS Config

Preços e faturamento de hosts dedicados do Amazon EC2

O preço de um Host dedicado varia de acordo com a opção de pagamento.

Opções de pagamento

- Hosts dedicados sob demanda
- Dedicated Host Reservations
- Savings Plans
- Definição de preço para o Windows Server no Hosts dedicados

Hosts dedicados sob demanda

O faturamento sob demanda é automaticamente ativado quando você aloca um Host dedicado à sua conta.

O preço sob demanda para um Host dedicado varia por família de instância e por região. É cobrado por segundo (com mínimo de 60 segundos) por Host dedicado ativo, independentemente da quantidade ou do tamanho das instâncias que você optar por executar nele. Para obter mais informações sobre a definição de preço sob demanda, consulte Amazon EC2 Hosts dedicados On-Demand Pricing (Definição de preço sob demanda).

É possível liberar um Host dedicado sob demanda a qualquer momento para parar de acumular cobranças para ele. Para obter informações sobre como liberar um Host dedicado, consulte Liberar um host dedicado do Amazon EC2.

Dedicated Host Reservations

Os Reservas de hosts dedicados fornecem um desconto de faturamento em comparação com a execução de Hosts dedicados sob demanda. Há três opções de pagamento disponíveis para as reservas:

- Sem pagamento adiantado — as reservas sem pagamento adiantado fornecem um desconto no uso do Host dedicado durante um período de vigência e não requerem pagamento adiantado.

Disponível para períodos de vigência de um e três anos. Apenas algumas famílias de instâncias oferecem suporte para o período de vigência de três anos para a opção Sem reservas antecipadas.

- Pagamento adiantado parcial — deve ser feito o pagamento adiantado de uma parte da reserva, e as horas restantes do período de vigência são cobradas com uma taxa com desconto. Disponível para períodos de vigência de um e três anos.
- Pagamento integral adiantado — fornece o menor preço. Disponível para períodos de vigência de um e três anos e abrange todo o custo do período antecipadamente, sem nenhuma outra cobrança futura.

É necessário ter Hosts dedicados ativos em sua conta para poder comprar reservas. Cada reserva pode cobrir um ou mais hosts que oferecem suporte para a mesma família de instâncias em uma única zona de disponibilidade. As reservas são aplicadas à família da instância do host e não ao tamanho da instância. Se você tiver três Hosts dedicados com diferentes tamanhos de instâncias (`m4.xlarge`, `m4.medium` e `m4.large`), poderá associar uma única reserva `m4` a todos esses Hosts dedicados. A família de instâncias e a zona de disponibilidade da reserva devem corresponder aos hosts dedicados aos quais você quer se associar.

Quando uma reserva for associada a um Host dedicado, o Host dedicado não poderá ser liberado até que o prazo da reserva termine.

Para obter mais informações sobre a definição de preço de reservas, consulte Definição de preço de Hosts dedicados do Amazon EC2.

Savings Plans

Savings Plans são um modelo de definição de preço flexível que oferece economias significativas em Instâncias on-demand. Com o Savings Plans, você se compromete com uma quantidade consistente de uso, em USD por hora, por um período de vigência de um ou de três anos. Isso oferece a flexibilidade de usar Hosts dedicados que melhor atendam às suas necessidades e continuar economizando dinheiro, em vez de se comprometer com um Host dedicado específico. Para obter mais informações, consulte o Guia do usuário do AWS Savings Plans.

> **Note**
>
> Savings Plans não são compatíveis com hosts dedicados `u-6tb1.metal`, `u-9tb1.metal`, `u-12tb1.metal`, `u-18tb1.metal`, e `u-24tb1.metal`.

Definição de preço para o Windows Server no Hosts dedicados

Conforme os termos de licenciamento da Microsoft, é possível trazer suas licenças de Windows Server e SQL Server para o Hosts dedicados. Não há cobrança adicional para uso de software caso você opte por trazer as próprias licenças.

Além disso, também é possível usar as AMIs do Windows Server fornecidas pela Amazon para executar as versões mais recentes do Windows Server no Hosts dedicados. Isso é comum para cenários nos quais você tem licenças do SQL Server qualificadas para execução no Hosts dedicados, mas precisa do Windows Server para executar a workload do SQL Server. As AMIs do Windows Server fornecidas pela Amazon são compatíveis somente com os tipos de instância da geração atual. Para obter mais informações, consulte Amazon EC2 Dedicated Hosts Pricing (Definição de preço de hosts dedicados do Amazon EC2).

Configurações de capacidade de instância de host dedicado do Amazon EC2

Os hosts dedicados oferecem suporte a diferentes configurações (núcleos físicos, sockets e vCPUs) que permitem executar instâncias de famílias e tamanhos diferentes.

Ao alocar um host dedicado em sua conta, será possível escolher uma configuração que ofereça suporte a um tipo de instância único ou a vários tipos de instância dentro da mesma família de instâncias. O número de instâncias podem ser executadas em um host depende da configuração escolhida.

Conteúdo

- Suporte a um tipo de instância único
- Suporte a vários tipos de instância

Suporte a um tipo de instância único

É possível alocar um host dedicado que ofereça suporte somente um tipo de instância. Com essa configuração, todas as instâncias executadas no host dedicado devem ser do mesmo tipo da instância especificada no momento da alocação do host.

Por exemplo, é possível alocar um host que ofereça suporte somente ao tipo de instância `m5.4xlarge`. Nesse caso, somente instâncias `m5.4xlarge` poderão ser executadas nesse host.

O número de instâncias que é possível iniciar no host depende do número de núcleos físicos fornecidos pelo host e do número de núcleos consumidos pelo tipo de instância especificado. Por

exemplo, ao alocar um host para instâncias `m5.4xlarge`, tenha em mente que o host fornece 48 núcleos físicos e cada instância `m5.4xlarge` consome 8 núcleos físicos. Isso significa que é possível iniciar até 6 instâncias nesse host (48 núcleos físicos/8 núcleos por instância = 6 instâncias).

Suporte a vários tipos de instância

É possível alocar um host dedicado que ofereça suporte a vários tipos de instância da mesma família de instâncias. Isso permite que executar diferentes tipos de instância no mesmo host, desde que elas sejam da mesma família de instâncias e o host tenha capacidade de instância suficiente.

Por exemplo, é possível alocar um host que ofereça suporte a diferentes tipos de instância dentro da família de instâncias R5. Nesse caso, será possível iniciar determinadas combinações de tipos de instância R5, como `r5.large`, `r5.xlarge`, `r5.2xlarge` e`r5.4xlarge`, nesse host dentro da capacidade do núcleo físico do host.

As seguintes famílias de instâncias são compatíveis com hosts dedicados com suporte a vários tipos de instância:

- Uso geral: A1 | M5 | M5n | M6i | M7i | T3
- Otimizadas para computação: C5 | C5n | C6i | C7i
- Otimizadas para memória: R5 | R5n | R6i | R7i

O número de instâncias que é possível executar no host depende do número de núcleos físicos fornecidos pelo host e do número de núcleos consumidos por cada tipo de instância executado no host. Por exemplo, se você alocar um host R5, que fornece 48 núcleos físicos, e executar duas instâncias `r5.2xlarge` (4 núcleos x 2 instâncias) e três instâncias `r5.4xlarge` (8 núcleos x 3 instâncias), essas instâncias consumirão um total de 32 núcleos. Assim, talvez seja possível executar certas combinações de instâncias R5, desde que estejam dentro dos 16 núcleos restantes.

No entanto, para cada família de instâncias, há um limite no número de instâncias que podem ser executadas para cada tipo de instância. Por exemplo, um host dedicado R5 oferece suporte a até 2 instâncias `r5.8xlarge`, as quais usam 32 dos núcleos físicos. Nesse caso, instâncias R5 adicionais de tipos menores podem ser usadas para preencher o host até a capacidade do núcleo ser atingida. Para obter o número de tipos de instância válidos para cada família de instâncias, consulte a Tabela de configuração de hosts dedicados.

A tabela a seguir mostra exemplos de combinações de tipos de instâncias.

Família de instâncias	Combinações de exemplo de tipos de instância
R5	• Exemplo 1: 4 x `r5.4xlarge` + 4 x `r5.2xlarge` • Exemplo 2: 1 x `r5.12xlarge` + 1 x `r5.4xlarge` + 1 x `r5.2xlarge` + 5 x `r5.xlarge` + 2 x `r5.large`
C5	• Exemplo 1: 1 x `c5.9xlarge` + 2 x `c5.4xlarge` + 1 x `c5.xlarge` • Exemplo 2: 4 x `c5.4xlarge` + 1 x `c5.xlarge` + 2 x `c5.large`
M5	• Exemplo 1: 4 x `m5.4xlarge` + 4 x `m5.2xlarge` • Exemplo 2: 1 x `m5.12xlarge` + 1 x `m5.4xlarge` + 1 x `m5.2xlarge` + 5 x `m5.xlarge` + 2 x `m5.large`

Considerações

Lembre-se do seguinte ao trabalhar com hosts dedicados que oferecem suporte a vários tipos de instâncias:

- É possível usar vários tipos de instâncias no mesmo host apenas dentro da mesma família de instâncias.
- Ao combinar tipos de instância, para maximizar a utilização do host, convém iniciar primeiro os tipos de instância maiores, seguidos pelos tipos de instância menores.
  - Dependendo da combinação e da ordem de lançamento dos tipos de instâncias em um host dedicado, talvez não seja fisicamente possível maximizar a utilização do host. Ao combinar tipos de instâncias em um host, uma certa capacidade pode estar disponível no host, mas não ser utilizável. Por exemplo, você pode ver 16 vCPUs disponíveis em um host r5n, mas talvez não

consiga iniciar uma instância 4xlarge no host, mesmo que r5n.4xlarge seja executada em 16 vCPUs.

> **Note**
>
> Se você habilitar um host dedicado A1 para vários tipos de instância, poderá executar apenas uma combinação de instâncias `a1.xlarge` e `a1.2xlarge` nesse host. Se você executar uma instância `a1.medium` ou `a1.large` nesse host, ficará restrito a executar somente mais do mesmo tipo de instância no host. Uma única instância `a1.4xlarge` consome toda a capacidade do host. Se você precisar de um host para instâncias `a1.medium` ou `a1.large`, recomendamos alocar hosts separados para esses tipos de instância.

Instâncias T3 expansíveis em hosts dedicados do Amazon EC2

Hosts dedicados são compatíveis com instâncias expansíveis T3. As instâncias T3 apresentam um bom custo-benefício para usar seu software de licença BYOL elegível em hardware dedicado. O menor espaço de vCPU das instâncias T3 permite consolidar seus workloads em menos hosts e maximizar a utilização da licença por núcleo.

Os hosts dedicados T3 são mais adequados para executar o software BYOL com utilização de CPU baixa a moderada. Isso inclui licenças de software qualificadas por soquete, por núcleo ou por VM, como Windows Server, Windows Desktop, SQL Server, SUSE Enterprise Linux Server, Red Hat Enterprise Linux e Oracle Database. Exemplos de workloads adequados a hosts dedicados T3 são bancos de dados pequenos e médios, desktops virtuais, ambientes de desenvolvimento e teste, repositórios de código e protótipos de produtos. Os hosts dedicados T3 não são recomendados para workloads com alta utilização sustentada da CPU ou para workloads que apresentem expansãos de CPU correlacionadas simultaneamente.

As instâncias T3 em hosts dedicados usam o mesmo modelo de crédito que as instâncias T3 em hardware de locação compartilhada. No entanto, eles são compatíveis apenas com o modo de crédito `standard`, não com o modo de crédito `unlimited`. No modo `standard`, as instâncias T3 em hosts dedicados recebem, gastam e acumulam créditos da mesma maneira que as instâncias expansíveis em hardware de locação compartilhada. Elas fornecem performance de CPU de linha de base com capacidade de expansão acima do nível da linha de base. Para expansãos acima da linha de base, a instância gasta os créditos acumulados no seu saldo de créditos de CPU. Quando

os créditos acumulados estão esgotados, a utilização da CPU é reduzida para o nível de linha de base. Para mais informações sobre o modo `standard`, consulte Como funcionam as instâncias expansíveis padrão.

Os hosts dedicados T3 oferecem suporte a todos os recursos oferecidos pelos hosts dedicados do Amazon EC2, incluindo vários tamanhos de instância em um único host, grupos de recursos de host e BYOL.

Tamanhos e configurações de instância T3 compatíveis

Os hosts dedicados T3 executam instâncias T3 expansíveis de uso geral que compartilham recursos de CPU do host, fornecendo uma performance de CPU de linha de base e a capacidade de expansão para um nível mais alto quando necessário. Isso permite que os hosts dedicados T3, que têm 48 núcleos, suportem até no máximo 192 instâncias por host. Para utilizar os recursos do host de forma eficiente e fornecer a melhor performance de instância, o algoritmo de posicionamento de instância do Amazon EC2 calcula automaticamente o número de instâncias e combinações de tamanho de instância compatíveis que podem ser iniciadas no host.

Os hosts dedicados T3 oferecem suporte a vários tipos de instância no mesmo host. Todos os tamanhos de instâncias T3 são compatíveis em um host dedicado. É possível executar diferentes combinações de instâncias T3 até o limite de CPU do host.

A tabela a seguir lista os tipos de instância compatíveis, resume a performance de cada tipo de instância e indica o número máximo de instâncias de cada tamanho que pode ser lançado.

Tipo de instâ	vCPUs	Memória (GiB)	Utilização da linha de base de CPU por vCPU	Expansão da largura de banda da rede (Gbps)	Expansão da largura de banda da Amazon EBS (Mbps)	Número máximo de instâncias por host dedicado
t3.na	2	0,5	5%	5	Até 2.085	192
t3.m	2	1	10%	5	Até 2.085	192
t3.sn	2	2	20%	5	Até 2.085	192
t3.m	2	4	20%	5	Até 2.085	192

Tipo de instâ	vCPUs	Memória (GiB)	Utilização da linha de base de CPU por vCPU	Expansão da largura de banda da rede (Gbps)	Expansão da largura de banda da Amazon EBS (Mbps)	Número máximo de instâncias por host dedicado
t3.la	2	8	30%	5	2.780	96
t3.xl	4	16	40%	5	2.780	48
t3.2x e	8	32	40%	5	2.780	24

Monitorar a utilização da CPU para hosts dedicados T3

É possível usar a métrica `DedicatedHostCPUUtilization` do Amazon CloudWatch para monitorar a utilização da vCPU de um host dedicado. A métrica está disponível no namespace `EC2` e na dimensão `Per-Host-Metrics`. Para obter mais informações, consulte Métricas de host dedicado.

Traga suas próprias licenças de software para os hosts dedicados do Amazon EC2

O Hosts dedicados permite usar suas licenças de software por VM, por núcleo e por soquete existentes. Quando você leva sua própria licença, é responsável por gerenciar as próprias licenças. No entanto, o Amazon EC2 tem recursos que ajudam você a manter a conformidade com a licença, como afinidade de instâncias e posicionamento direcionado.

Estas são as etapas gerais para trazer sua própria imagem de máquina com licença por volume para o Amazon EC2.

1. Verifique se os termos de licença que regem o uso de suas imagens de máquina permitem o uso de um ambiente de nuvem virtualizado. Para obter mais informações sobre o Licenciamento da Microsoft, consulte Amazon Web Services e Licenciamento da Microsoft.
2. Depois de verificar se sua imagem de máquina pode ser usada no Amazon EC2, importe-a com o VM Import/Export. Para obter informações sobre como importar sua imagem de máquina, consulte o Manual do usuário do VM Import/Export.
3. Depois de importar a imagem de máquina, será possível executar instâncias dela no Hosts dedicados ativo na sua conta.

4. Ao executar essas instâncias, dependendo do sistema operacional, talvez seja necessário ativar essas instâncias em seu próprio servidor KMS (por exemplo, Windows Server ou Windows SQL Server). Não é possível ativar a AMI do Windows importada no servidor Amazon Windows KMS.

> **Note**
>
> Para controlar como as imagens são usadas na AWS, ative a gravação de host no AWS Config. É possível usar o AWS Config para gravar alterações de configuração em um host dedicado e usar a saída como fonte de dados para geração de relatórios de licenças. Para obter mais informações, consulte Monitorar as alterações da configuração de host dedicado do Amazon EC2 usando o AWS Config.

Posicionamento automático e afinidade de host dedicado do Amazon EC2

O controle de posicionamento do Hosts dedicados ocorre em nível de instância e de host.

Posicionamento automático

O posicionamento automático é configurado no nível do host. Ele permite que você gerencie se as instâncias são executadas em um host específico ou em qualquer host disponível com as configurações correspondentes.

Quando o posicionamento automático de um Host dedicado está desabilitado, ele só aceita execuções de instâncias de locação de host que especificam seu ID exclusivo de host. Trata-se da configuração padrão para novos Hosts dedicados.

Quando o posicionamento automático de um Host dedicado está habilitado, ele aceita todas as execuções de instâncias de locação de host 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 `Default` 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).

Alocar um host dedicado do Amazon EC2 para uso em sua conta

Para começar a usar um host dedicado, é necessário primeiro alocá-lo para uso em sua conta. Depois da alocação do Host dedicado, a capacidade do Host dedicado é imediatamente disponibilizada em sua conta, e é possível começar a executar instâncias no Host dedicado.

Ao alocar um host dedicado em sua conta, será possível escolher uma configuração que ofereça suporte a um tipo de instância único ou a vários tipos de instância dentro da mesma família de instâncias. O número de instâncias podem ser executadas no host depende da configuração escolhida. Para obter mais informações, consulte Configurações de capacidade de instância de host dedicado do Amazon EC2.

Console

Como alocar um Host dedicado

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Hosts dedicados e Allocate Host dedicado (Alocar Host dedicado).
3. Em Instance family (Família de instâncias), escolha a família de instâncias do Host dedicado.
4. Especifique se o Host dedicado oferece suporte a vários tipos de instância na família de instâncias selecionada ou a um único tipo específico de instância. Faça uma das coisas a seguir.

   - Para configurar o Host dedicado para oferecer suporte a vários de tipos de instância na família de instâncias selecionada, em Support multiple instance types (Oferecer suporte a vários tipos de instância), escolha Enable (Habilitar) Isso permitirá executar diferentes tipos de instância da família de instâncias selecionada no Host dedicado. Por exemplo, se você escolher a família de instâncias `m5` e escolher essa opção, poderá executar instâncias `m5.xlarge` e `m5.4xlarge` no Host dedicado.

- Para configurar o Host dedicado a fim de oferecer suporte a um tipo de instância na família de instâncias selecionada, desmarque Support multiple instance types (Oferecer suporte a vários tipos de instância) e, em Instance type (Tipo de instância), escolha o tipo de instância ao qual oferecer suporte. Isso permite que você execute um único tipo de instância no Host dedicado. Por exemplo, se você escolher essa opção e especificar `m5.4xlarge` como o tipo de instância compatível, poderá executar apenas instâncias `m5.4xlarge` no Host dedicado.

5. Em Availability Zone (Zona de disponibilidade), escolha a zona de disponibilidade na qual o Host dedicado será alocado.
6. Para permitir que o Host dedicado aceite lançamentos de instância não direcionada compatíveis com o tipo de instância, para Instance auto-placement (Autoposicionamento da instância), selecione Enable (Habilitar). Para obter mais informações sobre posicionamento automático, consulte Posicionamento automático e afinidade de host dedicado do Amazon EC2.
7. Para habilitar a recuperação do host para o Host dedicado, em Host recovery (Recuperação do host), selecione Enable (Habilitar). Para obter mais informações, consulte Recuperação de um host dedicado do Amazon EC2.
8. Em Quantity (Quantidade), insira o número de Hosts dedicados a ser alocado.
9. (Opcional) Escolha Adicionar nova tag e digite uma chave de tag e um valor de tag.
10. Escolha Allocate.

AWS CLI

Como alocar um Host dedicado

Use o comando allocate-hosts. O exemplo a seguir aloca um host dedicado que oferece suporte a vários tipos de instância da família de instâncias `m5` na zona de disponibilidade `us-east-1a`. Ele também permite a recuperação do host e desabilita o posicionamento automático.

```
aws ec2 allocate-hosts \
    --instance-family "m5" \
    --availability-zone "us-east-1a" \
    --auto-placement "off" \
    --host-recovery "on" \
    --quantity 1
```

O exemplo a seguir aloca um host dedicado que oferece suporte a inicializações de instâncias não direcionadas na zona de disponibilidade especificada, habilita recuperação do host e habilita o posicionamento automático.

```
aws ec2 allocate-hosts \
    --instance-type "m5.large" \
    --availability-zone "eu-west-1a" \
    --auto-placement "on" \
    --host-recovery "on" \
    --quantity 1
```

PowerShell

Como alocar um Host dedicado

Use o cmdlet New-EC2Host. O exemplo a seguir aloca um host dedicado que oferece suporte a vários tipos de instância da família de instâncias `m5` na zona de disponibilidade `us-east-1a`. O host também tem a recuperação do host habilitada e o posicionamento automático desabilitado.

```
New-EC2Host `
    -InstanceFamily m5 `
    -AvailabilityZone us-east-1a `
    -AutoPlacement Off `
    -HostRecovery On `
    -Quantity 1
```

O exemplo a seguir aloca um host dedicado que oferece suporte a inicializações de instâncias não direcionadas na zona de disponibilidade especificada e habilita recuperação do host.

```
New-EC2Host `
    -InstanceType m5.large `
    -AvailabilityZone eu-west-1a `
    -AutoPlacement On `
    -HostRecovery On `
    -Quantity 1
```

Iniciar instâncias do Amazon EC2 em um host dedicado do Amazon EC2

Depois de alocar um Host dedicado, é possível executar instâncias nele. Você não pode executar instâncias com locação de `host` se não tiver Hosts dedicados ativos com capacidade suficiente disponível para o tipo de instância que está executando.

Considerações

- AMIs do SQL Server, do SUSE e do RHEL fornecidas pelo Amazon EC2 não podem ser usadas com Hosts dedicados.
- Para hosts dedicados compatíveis com vários tamanhos de instâncias, recomendamos executar primeiro os tamanhos de instância maiores e preencher a capacidade de instâncias restante com os tamanhos de instância menores, conforme necessário.
- Antes de executar as instâncias, observe as limitações. Para obter mais informações, consulte Restrições do Hosts dedicados.

Console

Para executar uma instância em um Host dedicado específico na página de Hosts dedicados

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Escolha Hosts dedicados no painel de navegação.
3. Na página Dedicated Hosts (Hosts dedicados), selecione um host e escolha Actions (Ações), Launch Instance(s) onto Host (Iniciar instâncias no host).
4. Na seção Application and OS Images (Imagens de aplicações e do sistema operacional), selecione uma AMI na lista.
5. Na seção Instance type (Tipo de instância), selecione o tipo de instância a ser iniciada.

> **Note**
>
> Se o Host dedicado oferecer suporte a um único tipo de instância, o tipo de instância com suporte será selecionado por padrão e não poderá ser alterado.
> Se o Host dedicado oferecer suporte a vários tipos de instância, será necessário selecionar um tipo de instância na família de instâncias com suporte de acordo com a capacidade de instância disponível do Host dedicado. Recomendamos que

você execute primeiro os tamanhos de instância maiores e preencha a capacidade restante da instância com os tamanhos de instância menores, conforme necessário.

6. Na seção Key pair (Par de chaves), selecione o par de chaves a ser associado à instância.
7. Na seção Detalhes avançados, em finidade de locação, escolha uma das seguintes opções:
   - Desativada: afinidade de host desabilitada. A instância é iniciada no host especificado, mas não há garantia de que ela será reiniciada no mesmo host dedicado se for interrompida.
   - ID de um host dedicado: afinidade de host habilitada. Se for interrompida, a instância sempre será reiniciada nesse host específico, desde que ele tenha capacidade. Se o host não tiver capacidade, a instância não poderá ser reiniciada, e você deverá estabelecer afinidade com outro host.

   Para obter mais informações sobre afinidade, consulte Posicionamento automático e afinidade de host dedicado do Amazon EC2.

   > **Note**
   >
   > As opções Tenancy (Locação) e Host são pré-configuradas com base no host selecionado.

8. Configure as demais opções da instância conforme necessário. Para obter mais informações, consulte Referência para parâmetros de configuração de instâncias do Amazon EC2.
9. Escolha Iniciar instância.

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 (Iniciar instância).
3. Na seção Application and OS Images (Imagens de aplicações e do sistema operacional), selecione uma AMI na lista.
4. Na seção Instance type (Tipo de instância), selecione o tipo de instância a ser iniciada.
5. Na seção Key pair (Par de chaves), selecione o par de chaves a ser associado à instância.

6. Na seção Advanced details (Detalhes avançados), faça o seguinte:

   a. Em Tenancy (Locação), escolha Dedicated Host (Host dedicado).
   b. Em Target host by (Visar host por), selecione Host ID (ID do host).
   c. Em Host ID (ID do host), selecione o host no qual a instância será iniciada.
   d. Em Afinidade de locação, escolha uma das seguintes opções:

      - Desativada: afinidade de host desabilitada. A instância é iniciada no host especificado, mas não há garantia de que ela será reiniciada no mesmo host dedicado se for interrompida.
      - ID de um host dedicado: afinidade de host habilitada. Se for interrompida, a instância sempre será reiniciada nesse host específico, desde que ele tenha capacidade. Se o host não tiver capacidade, a instância não poderá ser reiniciada, e você deverá estabelecer afinidade com outro host.

      Para obter mais informações sobre afinidade, consulte Posicionamento automático e afinidade de host dedicado do Amazon EC2.
7. Configure as demais opções da instância conforme necessário. Para obter mais informações, consulte Referência para parâmetros de configuração de instâncias do Amazon EC2.
8. Escolha Iniciar instância.

AWS CLI

Como iniciar uma instância em um Host dedicado

Use o comando run-instances e especifique a afinidade, a locação e o host da instância na opção `--placement`.

Executar em um Host Dedicado específico com afinidade de host (a instância sempre é reiniciada no mesmo host se for interrompida):

```
--placement Affinity=host,Tenancy=host,HostId=h-07879acf49EXAMPLE
```

Executar em um Host Dedicado específico sem afinidade com o host (a instância pode ser reiniciada em qualquer host disponível):

```
--placement Tenancy=host,HostId=h-07879acf49EXAMPLE
```

Executar em qualquer Host Dedicado com posicionamento automático ativado e tipo de instância correspondente:

```
--placement Tenancy=host
```

PowerShell

Como iniciar uma instância em um Host dedicado

Use o cmdlet New-EC2Instance e especifique a afinidade, a locação e o host da instância no parâmetro `-Placement`.

Executar em um Host Dedicado específico com afinidade de host (a instância sempre é reiniciada no mesmo host se for interrompida):

```
-Placement_Affinity host `
-Placement_Tenancy host `
-Placement_HostId h-07879acf49EXAMPLE
```

Executar em um Host Dedicado específico sem afinidade com o host (a instância pode ser reiniciada em qualquer host disponível):

```
-Placement_Tenancy host `
-Placement_HostId h-07879acf49EXAMPLE
```

Executar em qualquer Host Dedicado com posicionamento automático ativado e tipo de instância correspondente:

```
-Placement_Tenancy host
```

Iniciar instâncias do Amazon EC2 em um grupo de recursos de host

Hosts dedicados também estão integrados ao AWS License Manager. Com o License Manager, é possível criar um grupo de recursos de host, que é uma coleção de Hosts dedicados gerenciados como uma única entidade. Ao criar um grupo de recursos de host, especifique as preferências de gerenciamento de host, como alocação automática e liberação automática, para os Hosts dedicados. Isso permite que você execute instâncias em Hosts dedicados sem alocar e gerenciar manualmente

esses hosts. Para obter mais informações, consulte Grupos de recursos de host no Guia do usuário do AWS License Manager.

Quando você executa uma instância em um grupo de recursos de host que tem um Host dedicado com capacidade de instância disponível, o Amazon EC2 executa a instância nesse host. Se o grupo de recursos de host não tiver um host com capacidade de instância disponível, o Amazon EC2 alocará automaticamente um novo host no grupo de recursos de host e, depois, executará a instância nesse host. Para obter mais informações, consulte Grupos de recursos de host no Guia do usuário do AWS License Manager.

Requisitos e limites

- É necessário associar uma configuração de licença baseada em núcleo ou soquete à AMI.
- Não é possível usar as AMIs do SQL Server, do SUSE ou do RHEL fornecidas pelo Amazon EC2 com o Hosts dedicados.
- Você não pode segmentar um host específico escolhendo um ID de host e não é possível habilitar a afinidade de instâncias ao executar uma instância em um grupo de recursos de host.

Console

Como executar uma instância em um grupo de recursos de host

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias), Launch Instance (Iniciar instância).
3. Na seção Application and OS Images (Imagens de aplicações e do sistema operacional), selecione uma AMI na lista.
4. Na seção Instance type (Tipo de instância), selecione o tipo de instância a ser iniciada.
5. Na seção Key pair (Par de chaves), selecione o par de chaves a ser associado à instância.
6. Na seção Advanced details (Detalhes avançados), faça o seguinte:
    a. Em Tenancy (Locação), escolha Dedicated Host (Host dedicado).
    b. Em Target host by (Visar host por), selecione Host resource group (Grupo de recursos do host).
    c. Em Tenancy host resource group name (Nome do grupo de recursos do host de locação), escolha o grupo de recursos de host no qual a instância será iniciada.
    d. Em Tenancy affinity (Afinidade de locação), faça uma destas opções:

- Selecione Off (Desativar): a instância será iniciada no host especificado, mas não é garantido que seja iniciada no mesmo host dedicado se for interrompida.
- Selecione o ID do host dedicado: se for interrompida, a instância sempre será reiniciada nesse host específico.

Para obter mais informações sobre afinidade, consulte Posicionamento automático e afinidade de host dedicado do Amazon EC2.

7. Configure as demais opções da instância conforme necessário. Para obter mais informações, consulte Referência para parâmetros de configuração de instâncias do Amazon EC2.
8. Escolha Iniciar instância.

AWS CLI

Como executar uma instância em um grupo de recursos de host

Use o comando run-instances. Na opção `--placement`, omita a locação e especifique o ARN do grupo de recursos de host.

```
--placement HostResourceGroupArn=arn:aws:resource-groups:us-
east-2:123456789012:group/my-resource-group
```

PowerShell

Como executar uma instância em um grupo de recursos de host

Use o cmdlet New-EC2Instance. No parâmetro `-Placement`, omita a locação e especifique o ARN do grupo de recursos de host.

```
-Placement_HostResourceGroupArn arn:aws:resource-groups:us-
east-2:123456789012:group/my-resource-group
```

Modificar a configuração de posicionamento automático para um host dedicado existente do Amazon EC2

É possível modificar as configurações de posicionamento automático de um host dedicado após alocá-lo à sua conta da AWS.

Console

Como modificar o posicionamento automático de um Host dedicado

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Hosts dedicados.
3. Selecione um host e escolha Actions (Ações), Modify host (Modificar host).
4. Em Instance auto-placement (Posicionamento automático da instância), escolha Enable (Habilitar) para habilitar o posicionamento automático ou desmarque Enable (Habilitar) para desabilitar o posicionamento automático. Para obter mais informações, consulte Posicionamento automático e afinidade de host dedicado do Amazon EC2.
5. Escolha Save (Salvar).

AWS CLI

Como modificar o posicionamento automático de um Host dedicado

Use o comando modify-hosts.

```
aws ec2 modify-hosts \
    --auto-placement on \
    --host-ids h-012a3456b7890cdef
```

PowerShell

Como modificar o posicionamento automático de um Host dedicado

Use o cmdlet Edit-EC2Host.

```
Edit-EC2Host `
    -AutoPlacement 1 `
    -HostId h-012a3456b7890cdef
```

Modificar os tipos de instância compatíveis para um host dedicado existente do Amazon EC2

É possível modificar um Host dedicado para alterar os tipos de instância aos quais ele oferece suporte Se ele oferecer suporte a um único tipo de instância no momento, será possível modificá-

lo para oferecer suporte a vários tipos de instância dentro dessa família de instâncias. De forma semelhante, se ele oferecer suporte a vários tipos de instância, será possível modificá-lo para oferecer suporte somente a um tipo específico de instância.

Para modificar o Host dedicado para oferecer suporte a vários tipos de instância, primeiro interrompa todas as instâncias em execução no host. Essa modificação leva aproximadamente 10 minutos para ser concluída. O Host dedicado faz a transição para o estado `pending` enquanto as modificações estão em andamento. Não é possível iniciar instâncias interrompidas ou executar novas instâncias no Host dedicado enquanto ele estiver no estado `pending`.

Para modificar um Host dedicado compatível com vários tipos de instância para que ofereça suporte a um tipo específico de instância, o host não deve ter nenhuma instância em execução, ou as instâncias em execução devem ser do tipo ao qual você deseja que o host ofereça suporte. Por exemplo, para modificar um host que oferece suporte a vários tipos de instância na família de instâncias `m5` para oferecer suporte apenas a instâncias `m5.large`, o Host dedicado não deve ter nenhuma instância em execução ou ter apenas instâncias `m5.large` em execução.

Se você alocar um host para um tipo de instância virtualizada, não poderá modificar o tipo de instância para um tipo de instância `.metal` depois que o host for alocado. Por exemplo, se você alocar um host para o tipo de instância `m5.large`, não poderá modificar o tipo de instância para `m5.metal`. Da mesma forma, se você alocar um host para um tipo de instância `.metal`, não poderá modificar o tipo de instância para um tipo de instância virtualizada depois que o host for alocado. Por exemplo, se você alocar um host para o tipo de instância `m5.metal`, não poderá modificar o tipo de instância para `m5.large`.

Console

Como modificar os tipos de instância compatíveis de um Host dedicado

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Dedicated Host (Host dedicado).
3. Selecione o Host dedicado a ser modificado e escolha Actions (Ações), Modify host (Modificar host).
4. Dependendo da configuração atual do Host dedicado, siga um destes procedimentos:

   - Atualmente, se o Host dedicado oferecer suporte a um tipo de instância específico, o Support multiple instance types (Oferecer suporte a vários tipos de instância) não será habilitado e o Instance type (Tipo de instância) listará o tipo de instância compatível. Para

modificar o host para oferecer suporte a vários tipos na família de instâncias atual, em Support multiple instance types (Oferecer suporte a vários tipos de instância), escolha Enable (Habilitar).

Primeiro é necessário interromper todas as instâncias em execução no host antes de modificá-lo para oferecer suporte a vários tipos de instância.

- Atualmente, se o Host dedicado oferecer suporte a vários tipos de instância em uma família de instâncias, Enabled (Habilitado) estará selecionado em Support multiple instance types (Oferecer suporte a vários tipos de instância). Para modificar o host para oferecer suporte a um tipo específico de instância, em Support multiple instance types (Oferecer suporte a vários tipos de instância), desmarque Enable (Habilitar) e, em Instance type (Tipo de instância), selecione o tipo de instância específico ao qual oferecer suporte.

  Não é possível alterar a família de instâncias compatível do Host dedicado.

5. Escolha Save (Salvar).

AWS CLI

Como modificar os tipos de instância compatíveis de um Host dedicado

Use o comando modify-hosts.

O comando a seguir modifica um host dedicado para oferecer suporte a vários tipos de instância na família de instâncias `m5`.

```
aws ec2 modify-hosts \
    --instance-family m5 \
    --host-ids h-012a3456b7890cdef
```

O exemplo a seguir modifica um host dedicado para oferecer suporte apenas a instâncias `m5.xlarge`.

```
aws ec2 modify-hosts \
    --instance-type m5.xlarge \
    --instance-family --host-ids h-012a3456b7890cdef
```

PowerShell

Como modificar os tipos de instância compatíveis de um Host dedicado

Use o cmdlet Edit-EC2Host.

O comando a seguir modifica um host dedicado para oferecer suporte a vários tipos de instância na família de instâncias `m5`.

```
Edit-EC2Host `
    -InstanceFamily m5 `
    -HostId h-012a3456b7890cdef
```

O exemplo a seguir modifica um host dedicado para oferecer suporte apenas a instâncias `m5.xlarge`.

```
Edit-EC2Host `
    -InstanceType m5.xlarge `
    -HostId h-012a3456b7890cdef
```

Modificar a locação e a afinidade de host dedicado do Amazon EC2 para uma instância do Amazon EC2

É possível alterar a locação de uma instância depois de tê-la iniciado. Você também pode modificar a afinidade da instância para atingir um host específico ou permitir que ela seja iniciada em qualquer host dedicado disponível com atributos correspondentes em sua conta. Para modificar a locação ou a afinidade da instância, a instância deve estar no estado `stopped`.

Os detalhes do sistema operacional da instância, e se o SQL Server está ou não instalado, afetam quais conversões são compatíveis. Para obter mais informações sobre os caminhos de conversão de locação disponíveis para a sua instância, consulte Tenancy conversion no License Manager User Guide.

> **Note**
>
> Para instâncias T3, você deve iniciar a instância em um host dedicado para usar uma locação de `host`. Para instâncias T3, você não pode alterar a locação de `host` para `dedicated` ou `default`. Tentar fazer uma dessas alterações de locação não compatíveis gera um código de erro de `InvalidRequest`.

Console

Como modificar a locação ou a afinidade da instância

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Escolha Instances (Instâncias) e selecione a instância a ser modificada.
3. Escolha Instance state (Estado da instância), Stop (Interromper).
4. Com a instância selecionada, escolha Ações, Configurações de instância, Modificar posicionamento de instância).
5. Na página 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 do Amazon EC2.
     - 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 Posicionamento automático e afinidade de host dedicado do Amazon EC2.
6. Escolha Save (Salvar).

AWS CLI

Como modificar a locação ou a afinidade da instância

Use o comando modify-instance-placement. O exemplo a seguir altera a afinidade da instância especificada de `default` para `host` e especifica o Host dedicado com o qual a instância tem afinidade.

```
aws ec2 modify-instance-placement \
    --instance-id i-1234567890abcdef0 \
    --affinity host \
    --tenancy host \
    --host-id h-012a3456b7890cdef
```

PowerShell

Como modificar a locação ou a afinidade da instância

Use o cmdlet Edit-EC2InstancePlacement. O exemplo a seguir altera a afinidade da instância especificada de `default` para `host` e especifica o Host dedicado com o qual a instância tem afinidade.

```
Edit-EC2InstancePlacement `
    -InstanceId i-1234567890abcdef0 `
    -Affinity host `
    -Tenancy host `
    -HostId h-012a3456b7890cdef
```

Liberar um host dedicado do Amazon EC2

Se você não precisar mais de um host dedicado, poderá interromper as instâncias em execução no host, direcioná-las para serem iniciadas em outro host e liberar o host.

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.

Console

Como liberar um Host dedicado

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

3. Na página Hosts dedicados, selecione o Host dedicado a ser liberado.
4. Escolha Actions (Ações), Release host (Liberar host).
5. Para confirmar, escolha Release (Liberar).

AWS CLI

Como liberar um Host dedicado

Use o comando release-hosts.

```
aws ec2 release-hosts --host-ids h-012a3456b7890cdef
```

PowerShell

Como liberar um Host dedicado

Use o cmdlet Remove-EC2Host.

```
Remove-EC2Host -HostId h-012a3456b7890cdef
```

Depois de liberar um Host dedicado, você não pode reutilizar o mesmo host ou ID de host, e não terá mais taxas de faturamento sob demanda cobradas para ele. O estado do Host dedicado será alterado para `released` e não será mais possível executar nenhuma instância nesse host.

> **Note**
>
> Se você tiver liberado o Hosts dedicados recentemente, poderá levar um tempo para que eles parem de contar para seu limite. Durante esse tempo, é possível 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`.

Migre para hosts dedicados do Amazon EC2 baseadas em Nitro

O Sistema Nitro é uma coleção de hardware e componentes de software desenvolvidos pela AWS que permitem alta performance, alta disponibilidade e alta segurança. Os hosts dedicados baseados

em Nitro oferecem melhor performance de preço em comparação aos hosts dedicados baseados em Xen. Se você tiver algum host dedicado baseado em Xen em sua conta, recomendamos que você migre suas workloads para hosts dedicados baseados em Nitro. Para obter mais informações, consulte AWS Nitro System.

Para migrar de um host dedicado baseado em Xen para um host dedicado baseado em Nitro, é preciso migrar as instâncias baseadas em Xen em seu host dedicado para tipos de instância baseados em Nitro, alocar um novo host dedicado baseado em Nitro e, em seguida, mover suas instâncias baseadas em Nitro migradas para seu novo host dedicado baseado em Nitro.

Este tópico fornece etapas detalhadas para migrar de hosts dedicados baseados em Xen para hosts dedicados baseados em Nitro.

Etapas da migração

- Etapa 1: identificar os hosts dedicados baseadas em Xen
- Etapa 2: migrar instâncias baseadas em Xen para tipos de instância baseadas em Nitro
- Etapa 3: alocar um host dedicado baseado em Nitro
- Etapa 4: mover as instâncias migradas para o novo host dedicado baseado em Nitro
- Etapa 5: Liberar Host dedicado baseado em Xen não utilizado

Etapa 1: identificar os hosts dedicados baseadas em Xen

Os hosts dedicados a seguir são baseados em Xen e podem ser migrados para hosts dedicados baseados em Nitro.

- Uso geral: M3 | M4
- Otimizadas para computação: C3 | C4
- Otimizadas para memória: R3 | R4 | X1 | X1e
- Otimizadas para armazenamento: D2 | H1 | I2 | I3
- Computação acelerada: F1 | G3 | P2 | P3

Para verificar se você tem hosts dedicados baseados em Xen em sua conta

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

3. No campo Pesquisar, use o filtro de Família de instâncias para pesquisar os hosts dedicados baseados em Xen acima. Por exemplo, Família de instâncias = m3.

Etapa 2: migrar instâncias baseadas em Xen para tipos de instância baseadas em Nitro

As instâncias executadas em hosts dedicados baseados em Xen também são baseadas em Xen. Você deve migrar essas instâncias para tipos de instância baseados em Nitro antes de poder movê-las para hosts dedicados baseados em Nitro.

> **Important**
>
> Antes de começar a migrar as instâncias, recomendamos que você faça um backup dos dados. Para obter mais informações, consulte Criação de snapshots de vários volumes do Amazon EBS de uma instância do Amazon EC2.

Para encontrar instâncias em execução em seus hosts dedicados baseados em Xen

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Hosts dedicados.
3. Selecione o host baseado em Xen que você pretende migrar e, em seguida, selecione a guia Instâncias em execução. A guia lista todas as instâncias em execução do host selecionado.

Para migrar instâncias de Linux, consulte Alterações no tipo de instância do Amazon EC2.

Para migrar instâncias do Windows, consulte Migrar uma instância do EC2 Windows para um tipo de instância baseada em Nitro.

> **Note**
>
> Certifique-se de migrar suas instâncias para um tipo de instância que corresponda ao host dedicado baseado em Nitro para o qual você pretende migrar. Por exemplo, se você pretende migrar para um host dedicado M7i, certifique-se de migrar suas instâncias para um tipo de instância M7i.

Etapa 3: alocar um host dedicado baseado em Nitro

Para encontrar hosts dedicados baseados em Nitro compatíveis

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Tipos de instâncias.
3. Aplique os filtros a seguir:
   - Hipervisor = nitro
   - Suporte de host dedicado = true

Depois de encontrar um tipo de instância adequado baseado em Nitro, aloque um novo host dedicado.

Etapa 4: mover as instâncias migradas para o novo host dedicado baseado em Nitro

Depois de alocar o host dedicado baseado em Nitro e ele atingir o estado `available`, será possível mover as instâncias que você migrou anteriormente para os tipos de instância baseados em Nitro para o novo host dedicado.

Para mover suas instâncias para seu novo Host dedicado baseado em Nitro

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instâncias.
3. Selecione a instância migrada e escolha Ações, Configurações de instância, Modificar posicionamento de instância).
4. Em Host dedicado de destino, selecione o novo Host dedicado baseado em Nitro e, em seguida, escolha Salvar.
5. Reinicie a instância. Selecione a instância e escolha Estado da instância e Iniciar instância.

Etapa 5: Liberar Host dedicado baseado em Xen não utilizado

Depois de migrar suas workloads do host dedicado baseado em Xen para o novo host dedicado baseado em Nitro, é possível liberar o host dedicado baseado em Xen se não precisar mais dele.

Comprar reservas de host dedicado para obter descontos na fatura

As reservas de host dedicado oferecem um desconto de até 70% em comparação com os preços de host dedicado sob demanda. É necessário ter hosts dedicados ativos alocados em sua conta para poder comprar reservas de host dedicado. Para obter mais informações, consulte Dedicated Host Reservations.

Console

Como comprar reservas

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Selecione Hosts dedicados, Reservas de hosts dedicados, Purchase Reserva de hosts dedicados (Comprar Reserva de hosts dedicados).
3. Na tela Encontrar ofertas, faça o seguinte:
   a. Em Família de instâncias, selecione a família de instâncias do host dedicado para a qual deseja adquirir a reserva de host dedicado.
   b. Em Opção de pagamento, selecione e configure a opção de pagamento de sua preferência.
4. Escolha Próximo.
5. Selecione os hosts dedicados aos quais deseja associar a reserva de host dedicado e, em seguida, escolha Próximo.
6. (Opcional) Atribua etiquetas à reserva de host dedicado.
7. Analise o pedido e escolha Adquirir.

AWS CLI

Como comprar reservas

1. Use o comando describe-host-reservation-offerings para listar as ofertas disponíveis que atendam às suas necessidades. O exemplo a seguir lista as ofertas compatíveis com instâncias na família de instâncias `m4` e tem período de vigência de um ano.

   O prazo é especificado em segundos. Um período de vigência de um ano inclui 31.536.000 segundos, e um período de vigência de três anos inclui 94.608.000 segundos.

```
aws ec2 describe-host-reservation-offerings \
```

```
    --filter Name=instance-family,Values=m4 \
    --max-duration 31536000
```

O comando retorna uma lista de ofertas que correspondem aos seus critérios. Anote o ID da oferta a ser adquirida.

2. Use o comando purchase-host-reservation para comprar a oferta e fornecer o `offeringId` indicado na etapa anterior. O exemplo a seguir compra a reserva especificada e ela é associada a um host dedicado específico já atribuído à conta da AWS, e uma etiqueta é aplicada com uma chave de `purpose` e um valor de `production`.

```
aws ec2 purchase-host-reservation \
    --offering-id hro-03f707bf363b6b324 \
    --host-id-set h-013abcd2a00cbd123 \
    --tag-specifications 'ResourceType=host-
reservation,Tags={Key=purpose,Value=production}'
```

PowerShell

Como comprar reservas

1. Use o cmdlet Get-EC2HostReservationOffering para listar as ofertas disponíveis que atendem às suas necessidades. Os seguintes exemplos listam as ofertas compatíveis com instâncias na família de instâncias `m5` e têm prazo de um ano.

   O prazo é especificado em segundos. Um período de vigência de um ano inclui 31.536.000 segundos, e um período de vigência de três anos inclui 94.608.000 segundos.

```
$filter = @{Name="instance-family"; Values="m5"}
Get-EC2HostReservationOffering `
    -Filter $filter `
    -MaxDuration 31536000
```

   O comando retorna uma lista de ofertas que correspondem aos seus critérios. Anote o ID da oferta a ser adquirida.

2. Use o cmdlet New-EC2HostReservation para comprar a oferta e forneça o ID de oferta anotado na etapa anterior. O exemplo a seguir compra a reserva especificada e ela é associada a um host dedicado específico já atribuído à conta da AWS.

```
New-EC2HostReservation `
    -OfferingId hro-03f707bf363b6b324 `
    -HostIdSet h-013abcd2a00cbd123
```

Compartilhamento de host dedicado do Amazon EC2 entre contas

O compartilhamento de host dedicado permite que proprietários de hosts dedicados os compartilhem com outras contas da AWS ou em uma organização da AWS. Isso permite criar e gerenciar os hosts dedicados centralmente, e compartilhar o host dedicado entre várias contas da AWS ou em sua organização da AWS.

Nesse modelo, a conta da AWS que possui o host dedicado (proprietária) compartilha-a com outras contas da AWS (consumidores). Os consumidores podem executar instâncias nos Hosts dedicados que são compartilhadas com eles da mesma maneira que executam instâncias em Hosts dedicados alocados em sua própria conta. O proprietário é responsável pelo gerenciamento do Host dedicado e pelas instâncias executadas nele. Os proprietários não podem modificar instâncias que os consumidores executam em Hosts dedicados compartilhados. Os consumidores são responsáveis por gerenciar as instâncias que executam em Hosts dedicados compartilhados com eles. Os consumidores não podem visualizar ou modificar instâncias de propriedade de outros consumidores ou do proprietário do Host dedicado, e não podem modificar os Hosts dedicados que são compartilhados com eles.

Um proprietário de Host dedicado pode compartilhar um Host dedicado com:

- Contas específicas da AWS dentro ou fora de sua organização na AWS
- Uma unidade organizacional dentro de sua organização da AWS
- Toda a sua organização da AWS

Tópicos

- Pré-requisitos para compartilhar Hosts dedicados
- Limitações para compartilhamento de Host dedicado
- Serviços relacionados
- Compartilhamento entre zonas de disponibilidade
- Permissões de Host dedicado compartilhado

- Faturamento e medição
- Limites de Host dedicado
- Recuperação de host e compartilhamento do Host dedicado
- Compartilhar um host dedicado do Amazon EC2 entre várias contas da AWS
- Cancelar o compartilhamento de um host dedicado com outras contas da AWS
- Visualizar os hosts dedicados do Amazon EC2 compartilhados em sua conta da AWS

Pré-requisitos para compartilhar Hosts dedicados

- Para compartilhar um host dedicado, é necessário ser o proprietário dele em sua conta da AWS. Não é possível compartilhar um Host dedicado que tenha sido compartilhado com você.
- Para compartilhar um host dedicado com a sua organização da AWS ou com uma unidade organizacional de sua organização da AWS, é necessário habilitar o compartilhamento com o AWS Organizations. Para obter mais informações, consulte Habilitar o compartilhamento com o AWS Organizations no Guia do usuário do AWS RAM.

Limitações para compartilhamento de Host dedicado

Não é possível compartilhar Hosts dedicados que foram alocados para os seguintes tipos de instância: `u-6tb1.metal`, `u-9tb1.metal`, `u-12tb1.metal`, `u-18tb1.metal` e `u-24tb1.metal`.

Serviços relacionados

AWS Resource Access Manager

O compartilhamento de host dedicado integra-se ao AWS Resource Access Manager (AWS RAM). O AWS RAM é um serviço que permite compartilhar seus recursos da AWS com qualquer conta da AWS ou por meio do AWS Organizations. Com o AWS RAM, você compartilha recursos que possui criando um compartilhamento de recursos. Um compartilhamento de recursos especifica os recursos a serem compartilhados, e os consumidores com os quais compartilhá-los. Os consumidores podem ser contas individuais da AWS, unidades organizacionais ou toda uma organização do AWS Organizations.

Para obter mais informações sobre o AWS RAM, consulte o Manual do usuário do AWS RAM.

Compartilhamento entre zonas de disponibilidade

Para garantir a distribuição de recursos entre as zonas de disponibilidade de uma região, mapeamos as zonas de disponibilidade de forma independente para os nomes de cada conta. Isso pode resultar em diferenças na nomenclatura de zonas de disponibilidade entre contas. Por exemplo, a zona de disponibilidade `us-east-1a` de sua conta da AWS pode não ter o mesmo local que a `us-east-1a` de outra conta da AWS.

Para identificar o local de seus Hosts dedicados relativo a suas contas, use o ID da zona de disponibilidade (ID da AZ). O ID da zona de disponibilidade é um identificador exclusivo e consistente de uma zona de disponibilidade em todas as contas da AWS. Por exemplo, `use1-az1` é um ID de zona de disponibilidade da região `us-east-1` e é o mesmo local em cada conta da AWS.

Como visualizar os IDs de zona de disponibilidade para as zonas de disponibilidade em sua conta

1. Abra o console do AWS RAM em https://console.aws.amazon.com/ram/home.
2. Os IDs de zona de disponibilidade da região atual são exibidos no painel Your AZ ID (Seu ID de AZ) no lado direito da tela.

Permissões de Host dedicado compartilhado

Permissões para proprietários

Os proprietários são responsáveis pelo gerenciamento de seus Hosts dedicados compartilhados e das instâncias executadas neles. Os proprietários podem visualizar todas as instâncias em execução no Host dedicado compartilhado, incluindo aquelas executadas pelos consumidores. No entanto, os proprietários não podem realizar ações nas instâncias que foram executadas pelos consumidores.

Permissões para consumidores

Os consumidores são responsáveis por gerenciar as instâncias que executam em um Host dedicado compartilhado. Os consumidores não podem modificar o Host dedicado compartilhado de nenhuma forma e não podem visualizar nem modificar instâncias que foram executadas por outros consumidores ou pelo proprietário do Host dedicado.

Faturamento e medição

Não há cobranças adicionais pelo compartilhamento de Hosts dedicados.

Os proprietários são cobrados por Hosts dedicados compartilhado. Os consumidores não são cobrados pelas instâncias que executam no Hosts dedicados compartilhado.

Reservas de hosts dedicados continuam a oferecer descontos de cobrança por Hosts dedicados compartilhados. Somente proprietários de Host dedicado podem comprar Reservas de hosts dedicados para Hosts dedicados compartilhados que possuem.

Limites de Host dedicado

Hosts dedicados compartilhados são contabilizados somente para os limites de Hosts dedicados do proprietário. Os limites de Hosts dedicados do consumidor não são afetados por Hosts dedicados que foram compartilhados com eles. Da mesma forma, as instâncias executadas pelos consumidores em Hosts dedicados compartilhados não são contabilizadas para seus limites de instâncias.

Recuperação de host e compartilhamento do Host dedicado

A recuperação de host recupera instâncias executadas pelo proprietário do Host dedicado e pelos consumidores com os quais ele foi compartilhado. O Host dedicado de reposição é alocado na conta do proprietário. É adicionado aos mesmos compartilhamentos de recursos que o Host dedicado original e é compartilhado com os mesmos consumidores.

Para obter mais informações, consulte Recuperação de um host dedicado do Amazon EC2.

Compartilhar um host dedicado do Amazon EC2 entre várias contas da AWS

Quando um proprietário compartilha um Host dedicado, ele permite que os consumidores executem instâncias no host. Os consumidores podem executar tantas instâncias no host compartilhado quanto sua capacidade disponível permitir.

> **Important**
>
> Observe que você é responsável por garantir que possui direitos de licença apropriados para compartilhar qualquer licença BYOL no Hosts dedicados.

Se você compartilhar um Host dedicado com o posicionamento automático habilitado, lembre-se do seguinte, pois isso pode gerar uso não intencional do Host dedicado:

- Se os consumidores executarem instâncias com locação de Host dedicado e não tiverem capacidade em um Host dedicado que possuam na conta, a instância será executada automaticamente no Host dedicado compartilhado.

Para compartilhar um Host dedicado, é necessário adicioná-lo a um compartilhamento de recursos. Um compartilhamento de recursos é um recurso do AWS RAM que permite que você compartilhe seus recursos entre contas da AWS. Um compartilhamento de recursos especifica os recursos a serem compartilhados, e os consumidores com os quais compartilhá-los. É possível adicionar o Host dedicado a um recurso existente ou adicioná-lo a um novo compartilhamento de recursos.

Se você fizer parte de uma organização no AWS Organizations e o compartilhamento estiver habilitado na organização, os consumidores da organização receberão acesso automaticamente ao host dedicado compartilhado. Caso contrário, os consumidores receberão um convite para participar do compartilhamento de recursos e acesso ao Host dedicado compartilhado depois de aceitar o convite.

> **Note**
>
> Depois de compartilhar um Host dedicado, pode levar alguns minutos para que os consumidores tenham acesso a ele.

Console

Como compartilhar um Host dedicado de sua propriedade usando o console do Amazon EC2

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Hosts dedicados.
3. Escolha o Host dedicado a ser compartilhado e selecione Ações, Compartilhar host.
4. Selecione o compartilhamento de recursos ao qual adicionar o Host dedicado e escolha Compartilhar host.

   Pode levar alguns minutos para que os consumidores obtenham acesso ao host compartilhado.

Para compartilhar um host dedicado de sua propriedade usando o console do AWS RAM

Consulte Create a resource share no AWS RAM User Guide.

AWS CLI

Para compartilhar um host dedicado do qual você é o proprietário

Use o comando create-resource-share.

```
aws ram create-resource-share \
    --name my-resource-share \
    --resource-arns arn:aws:ec2:us-east-2:123456789012:dedicated-
host/h-07879acf49EXAMPLE
```

PowerShell

Para compartilhar um host dedicado do qual você é o proprietário

Use o cmdlet New-RAMResourceShare.

```
New-RAMResourceShare `
    -Name my-resource-share `
    -ResourceArn arn:aws:ec2:us-east-2:123456789012:dedicated-
host/h-07879acf49EXAMPLE
```

Cancelar o compartilhamento de um host dedicado com outras contas da AWS

O proprietário do Host dedicado pode cancelar o compartilhamento de um Host dedicado compartilhado a qualquer momento. Ao cancelar o compartilhamento de um Host dedicado compartilhado, as seguintes regras são aplicadas:

- Os consumidores com os quais o Host dedicado foi compartilhado não podem mais executar novas instâncias nele.
- As instâncias de propriedade de consumidores que estavam em execução no Host dedicado no momento do cancelamento do compartilhamento continuam a ser executadas, mas são programadas para desativação. Os consumidores recebem notificações de desativação para as instâncias e têm duas semanas para agir sobre as notificações. No entanto, se o Host dedicado for compartilhado novamente com o consumidor durante o período de aviso de desativação, as desativações de instância serão canceladas.

Para cancelar o compartilhamento de um Host dedicado compartilhado de sua propriedade, é necessário removê-lo do compartilhamento de recursos.

Console

Para cancelar o compartilhamento de um host dedicado compartilhado do qual você é o proprietário

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Hosts dedicados.
3. Escolha o Host dedicado do qual cancelar o compartilhamento e escolha a guia Compartilhamento.
4. A guia Compartilhamento lista os compartilhamentos de recursos aos quais o Host dedicado foi adicionado. Selecione o compartilhamento de recursos do qual remover o Host dedicado e escolha Remover do compartilhamento de recursos.

Para cancelar o compartilhamento de um host dedicado compartilhado de sua propriedade usando o console do AWS RAM

Consulte Atualizar um compartilhamento de recursos no Guia do usuário do AWS RAM.

AWS CLI

Para cancelar o compartilhamento de um host dedicado compartilhado do qual você é o proprietário

Use o comando disassociate-resource-share.

```
aws ram disassociate-resource-share \
    --resource-share-arn arn:aws:ram:us-east-2:123456789012:resource-share/7ab63972-b505-7e2a-420d-6f5d3EXAMPLE \
 --resource-arns arn:aws:ec2:us-east-2:123456789012:dedicated-host/h-07879acf49EXAMPLE
```

PowerShell

Para cancelar o compartilhamento de um host dedicado compartilhado do qual você é o proprietário

Use o cmdlet Disconnect-RAMResourceShare.

```
Disconnect-RAMResourceShare `
    -ResourceShareArn "arn:aws:ram:us-east-2:123456789012:resource-share/7ab63972-b505-7e2a-420d-6f5d3EXAMPLE" `
```

```
    -ResourceArn "arn:aws:ec2:us-east-2:123456789012:dedicated-
host/h-07879acf49EXAMPLE"
```

Visualizar os hosts dedicados do Amazon EC2 compartilhados em sua conta da AWS

É possível visualizar os hosts dedicados que você compartilha com outras contas e os hosts dedicados que são compartilhados com você. Se você for o proprietário do host dedicado, poderá ver todas as instâncias em execução no host, incluindo as instâncias iniciadas pelos consumidores. Se o host dedicado for compartilhado com você, você só poderá ver as instâncias que iniciou no host compartilhado, e não as iniciadas por outros consumidores.

Proprietários e consumidores podem identificar Hosts dedicados compartilhados usando um dos seguintes métodos.

Console

Para identificar um host dedicado compartilhado

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Hosts dedicados. A tela lista Hosts dedicados de sua propriedade e Hosts dedicados compartilhados com você.
3. A coluna Owner (Proprietário) mostra o ID de conta da AWS do proprietário do host dedicado.
4. Para visualizar as instâncias em execução nos hosts, selecione a guia Instâncias.

AWS CLI

Para identificar um host dedicado compartilhado

Use o comando describe-hosts. O comando retorna os Hosts dedicados de sua propriedade e os Hosts dedicados compartilhados com você. O valor de `Owner` é o ID da conta do proprietário do Host dedicado. A lista `Instances` descreve as instâncias em execução no host.

```
aws ec2 describe-hosts --filter "Name=state,Values=available"
```

PowerShell

Para identificar um host dedicado compartilhado

Use o cmdlet Get-EC2host. O cmdlet retorna os hosts dedicados dos quais você é o proprietário e os hosts dedicados compartilhados com você. O valor de `Owner` na resposta é o ID da conta do proprietário do host dedicado. A lista `Instances` descreve as instâncias em execução no host.

```
Get-EC2Host -Filter @{Name="state"; Values="available"}
```

Hosts dedicados do Amazon EC2 no AWS Outposts

O AWS Outposts é um serviço totalmente gerenciado que estende a infraestrutura, os serviços, as APIs e as ferramentas da AWS para o local. Ao fornecer acesso local à infraestrutura gerenciada pela AWS, o AWS Outposts permite que você crie e execute aplicações on-premises usando as mesmas interfaces de programação que nas regiões da AWS, usando recursos locais de computação e armazenamento para menor latência e necessidades de processamento de dados locais.

Um Outpost é um grupo de capacidade de computação e armazenamento da AWS implantado em um local do cliente. A AWS opera, monitora e gerencia essa capacidade como parte de uma região da AWS.

É possível alocar hosts dedicados nos Outposts que você tiver em sua conta. Isso torna mais fácil para você trazer suas licenças de software e workloads existentes que exigem um servidor físico dedicado para AWS Outposts. Você também pode direcionar ativos de hardware específicos em um Outpost para ajudar a minimizar a latência entre as workloads.

Os hosts dedicados permitem que você use suas licenças de software qualificadas no Amazon EC2 para obter a flexibilidade e a economia de usar suas próprias licenças. Outras licenças de software vinculadas a máquinas virtuais, soquetes ou núcleos físicos também podem ser usadas em hosts dedicados, sujeitos aos termos de licença. Embora o Outposts sempre tenha sido um ambiente de locatário único qualificado para workloads BYOL, os hosts dedicados permitem limitar as licenças necessárias a um único host, e não a toda a implantação do Outpost.

Além disso, o uso de hosts dedicados em um Outpost oferece maior flexibilidade na implantação do tipo de instância e um controle mais granular sobre o posicionamento da instância. É possível segmentar um host específico para execuções de instância e usar a afinidade do host para garantir que a instância sempre seja executada nesse host, ou é possível usar o posicionamento automático para executar uma instância em qualquer host disponível que tenha configurações correspondentes e capacidade disponível.

Sumário

- Pré-requisitos
- Recursos compatíveis
- Considerações
- Alocar um Host dedicado do Amazon EC2 no AWS Outposts

Pré-requisitos

É necessário ter um Outpost instalado em seu local. Para obter mais informações, consulte Criar um Outpost e solicitar capacidade do Outpost no Manual do usuário do AWS Outposts.

Recursos compatíveis

- Há suporte para as seguintes famílias de instâncias: `C5`, `M5`, `R5`, `C5d`, `M5d`, `R5d`, `G4dn` e `i3en`.
- Os hosts dedicados no Outposts podem ser configurados para serem compatíveis com vários tamanhos de instância. A compatibilidade com vários tamanhos de instância está disponível para as seguintes famílias de instâncias: `C5`, `M5`, `R5`, `C5d`, `M5d` e `R5d`. Para obter mais informações, consulte Configurações de capacidade de instância de host dedicado do Amazon EC2.
- Hosts dedicados no Outposts são compatíveis com o posicionamento automático e as execuções de instâncias direcionadas. Para obter mais informações, consulte Posicionamento automático e afinidade de host dedicado do Amazon EC2.
- Hosts dedicados no Outposts são compatíveis com a afinidade do host. Para obter mais informações, consulte Posicionamento automático e afinidade de host dedicado do Amazon EC2.
- Hosts dedicados no Outposts são compatíveis o compartilhamento com AWS RAM. Para obter mais informações, consulte Compartilhamento de host dedicado do Amazon EC2 entre contas.

Considerações

- Reservas do host dedicado não são compatíveis com o Outposts.
- Grupos de recursos de host e AWS License Manager não são compatíveis com o Outposts.
- Hosts dedicados no Outposts não são compatíveis com a instâncias T3 intermitentes.
- Hosts dedicados no Outposts não são compatíveis com a recuperação do host.
- Não há compatibilidade da recuperação automática simplificada em instâncias com locação de hosts dedicados em Outposts.

Alocar um Host dedicado do Amazon EC2 no AWS Outposts

Você aloca e usa hosts dedicados em Outposts da mesma forma que faria com hosts dedicados em uma região da AWS.

Pré-requisitos

Crie uma sub-rede no Outpost. Para obter mais informações, consulte Criar uma sub-rede no Manual do usuário do AWS Outposts.

Para alocar um host dedicado a um Outpost, use um destes métodos:

Console

Para alocar um host dedicado usando o Outpost usando o console do AWS Outposts

1. Abra o console do AWS Outposts em https://console.aws.amazon.com/outposts/.
2. No painel de navegação, escolha Outposts. Selecione o Outpost e, em seguida, escolha Actions (Ações), Allocate Dedicated Host (Alocar host dedicado).
3. Configure o host dedicado, conforme necessário. Para obter mais informações, consulte Alocar um host dedicado do Amazon EC2 para uso em sua conta.

   > **Note**
   >
   > Availability Zone (Zona de disponibilidade) e Outpost ARN (ARN do Outpost) devem ser preenchidos previamente com a zona de disponibilidade e o ARN do Outpost selecionado.

4. Escolha Allocate.

Para alocar um host dedicado usando o Outpost 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 Dedicated Hosts (Hosts dedicados) e Allocate Host dedicado (Alocar host dedicado).
3. Em Availability Zone (Zona de disponibilidade), selecione a zona de disponibilidade associada ao Outpost.
4. Em Outpost ARN (ARN do Outpost), insira o ARN do Outpost.

5. Para direcionar ativos de hardware específicos no Outpost, em Segmente ativos de hardware específicos no Outpost, selecione Habilitar. Para cada ativo de hardware de destino, escolha Adicionar ID do ativo e, em seguida, insira o ID do ativo de hardware.

> **Note**
>
> O valor especificado para Quantidade deve ser igual ao número de IDs de ativos que você especifica. Por exemplo, se você especificar três IDs de ativos, a Quantidade também deverá ser 3.

6. Defina as configurações restantes do host dedicado, conforme necessário. Para obter mais informações, consulte Alocar um host dedicado do Amazon EC2 para uso em sua conta.
7. Escolha Allocate.

AWS CLI

Para alocar um host dedicado em um Outpost

Use o comando allocate-hosts. Em `--availability-zone`, especifique a zona de disponibilidade associada ao Outpost. Em `--outpost-arn`, especifique o ARN do Outpost. Opcionalmente, para `--asset-ids`, especifique os IDs dos ativos de hardware do Outpost de destino.

```
aws ec2 allocate-hosts \
    --availability-zone "us-east-1a" \
    --outpost-arn "arn:aws:outposts:us-east-1a:111122223333:outpost/
op-4fe3dc21baEXAMPLE" \
    --asset-ids asset_id \
    --instance-family "m5" \
    --auto-placement "off" \
    --quantity 1
```

PowerShell

Para alocar um host dedicado em um Outpost

Use o cmdlet New-EC2Host. Especifique a zona de disponibilidade associada ao Outpost. Opcionalmente, para `-AssetId`, especifique os IDs dos ativos de hardware do Outpost de destino.

```
New-EC2Host `
    -AvailabilityZone "us-east-1a" `
    -OutpostArn "arn:aws:outposts:us-east-1a:111122223333:outpost/
op-4fe3dc21baEXAMPLE" `
    -AssetId asset_id `
    -InstanceFamily "m5" `
    -AutoPlacement "off" `
    -Quantity 1
```

Como iniciar uma instância em um host dedicado em um Outpost

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Hosts dedicados. Selecione o host dedicado que você alocou na etapa anterior e escolha Actions (Ações), Launch instance onto host (Executar instância no host).
3. Defina a instância conforme necessário e, em seguida, inicie a instância. Para obter mais informações, consulte Iniciar instâncias do Amazon EC2 em um host dedicado do Amazon EC2.

Recuperação de um host dedicado do Amazon EC2

A recuperação automática do host dedicado reinicia as instâncias em um novo host substituto quando certas condições problemática são detectadas no host dedicado. A recuperação do host reduz a necessidade de intervenção manual e diminui a carga operacional em caso de falhas inesperadas no host dedicado relativas a eventos de alimentação do host ou conectividade da rede. Outros problemas do host dedicado exigirão intervenção manual para recuperação.

Conteúdo

- Como um host dedicado do Amazon EC2 recupera trabalhos
- Tipos de instâncias compatíveis
- Preços
- Gerenciar recuperação de um host dedicado do Amazon EC2
- Visualizar a configuração de recuperação de host do host dedicado do Amazon EC2
- Recuperar manualmente as instâncias que não são compatíveis com a recuperação de host dedicado do Amazon EC2

Como um host dedicado do Amazon EC2 recupera trabalhos

O processo de recuperação do host e dos grupos de recursos do host usa verificações de integridade no nível do host para avaliar a disponibilidade do host dedicado e detectar falhas nos sistemas subjacentes. O tipo de falha do host dedicado determina se a recuperação automática do host dedicado é possível. Os exemplos de problemas que podem causar falha nas verificações de integridade no nível do host incluem:

- Perda de conectividade de rede
- Perda de energia do sistema
- Problemas de hardware ou software no host físico

> **Important**
>
> A recuperação automática do host dedicado não ocorre quando o host está programado para ser desativado.

Recuperação automática de host dedicado

Quando uma falha de alimentação do sistema ou de conectividade de rede é detectada no seu host dedicado, a recuperação automática do host dedicado é iniciada, e o Amazon EC2 aloca automaticamente um host dedicado substituto na mesma zona de disponibilidade do host dedicado original. O Host dedicado em substituição recebe um novo ID do host, mas retém os mesmos atributos que o Host dedicado original, como:

- Availability Zone
- Tipo de instância
- Tags
- Configurações de autoposicionamento
- Reserva

Quando o host dedicado substituto é alocado, as instâncias são recuperadas para o host dedicado substituto. As instâncias recuperadas retêm os mesmos atributos que as instâncias originais, como:

- ID da instância

- Endereços IP privados
- Endereços IP elásticos
- Anexos de volume do EBS
- Todos os metadados da instância

Além disso, a integração incorporada com o AWS License Manager automatiza o monitoramento e o gerenciamento das licenças.

> **Note**
>
> A integração com o AWS License Manager é compatível somente nas regiões em que o AWS License Manager está disponível.

Se as instâncias tiverem um relacionamento de afinidade de host com o host dedicado prejudicado, as instâncias recuperadas estabelecem afinidade do host com o host dedicado de substituição.

Quando todas as instâncias tiverem sido recuperadas para o Host dedicado de substituição, o Host dedicado prejudicado será liberado e o Host dedicado de substituição ficará disponível para uso.

Quando a recuperação do host for iniciada, o proprietário da conta da AWS será notificado por e-mail e por um evento AWS Health Dashboard. A segunda notificação é enviada após a recuperação do host ser concluída com sucesso.

Se você estiver usando o AWS License Manager para acompanhar suas licenças, o AWS License Manager alocará novas licenças para o host dedicado de substituição conforme os limites de configuração da licença. Se a configuração da licença tiver limites rígidos que serão violados em resultado da recuperação do host, o processo de recuperação não será permitido e você será notificado da falha de recuperação do host por meio de uma notificação do Amazon SNS (se as configurações de notificação foram definidas no AWS License Manager). Se a configuração da licença tiver limites suaves que serão violados como resultado da recuperação do host, a recuperação poderá continuar e você será notificado acerca da violação do limite por meio de uma notificação do Amazon SNS. Para obter mais informações, consulte Uso de configurações de licença e Configurações no License Manager no Guia do usuário do AWS License Manager.

Estados de recuperação do host

Quando a falha do Host dedicado for detectada, o Host dedicado prejudicado entra no estado `under-assessment` e todas as instâncias entram no estado `impaired`. Não é possível executar instâncias no Host dedicado prejudicado enquanto estiver no estado `under-assessment`.

Depois de o Host dedicado de substituição ser alocado, ele entra no estado `pending`. Ele continua nesse estado até que o processo de recuperação do host esteja concluído. Não é possível executar instâncias no Host dedicado de substituição enquanto ele estiver no estado `pending`. As instâncias recuperadas no Host dedicado de substituição continuam no estado `impaired` durante o processo de recuperação.

Depois de a recuperação do host ser concluída, o Host dedicado de substituição entrará no estado `available` e as instâncias recuperadas retornarão ao estado `running`. É possível abrir instâncias no Host dedicado de substituição depois de entrar no estado `available`. O Host dedicado prejudicado original é liberado permanentemente e entra no estado `released-permanent-failure`.

Quando um host dedicado comprometido tiver instâncias que não oferecem suporte à recuperação do host, por exemplo, instâncias com volume raiz de armazenamento de instância, o host dedicado não é liberado. Em vez disso, é marcado para aposentadora e entra no estado `permanent-failure`.

Cenários sem recuperação automática de host dedicado

A recuperação automática do host dedicado não ocorre quando o host está programado para ser desativado. Você receberá uma notificação de retirada no AWS Health Dashboard, um evento do Amazon CloudWatch e o endereço de email do proprietário da conta da AWS recebe uma mensagem sobre a falha do host dedicado. Siga as etapas de remedição descritas na notificação de desativação dentro do prazo especificado para recuperar manualmente as instâncias restantes no host que está sendo desativado.

As instâncias interrompidas não são recuperadas para o Host dedicado de substituição. Se você tentar iniciar uma instância interrompida que mire no Host dedicado prejudicado, o início da instância falhará. Recomendamos que você modifique a instância interrompida para mirar em um a host dedicado diferente ou abrir em qualquer host dedicado disponível, com configurações correspondentes e autoposicionamento habilitado.

As instâncias com armazenamento de instâncias não são recuperadas para o Host dedicado de substituição. Como medida de remediação, o Host dedicado prejudicado será marcado para

desativação e você receberá tal notificação depois de a recuperação do host ser concluída. Siga as etapas de remedição descritas na notificação de desativação dentro do prazo especificado para recuperar manualmente as instâncias restantes no Host dedicado prejudicado.

Tipos de instâncias compatíveis

A recuperação do host é compatível com as seguintes famílias de instâncias:

- Uso geral: A1 | M3 | M4 | M5 | M5n | M5zn | M6a | M6g | M6i | T3 | Mac1 | Mac2 | Mac2-m1ultra | Mac2-m2 | Mac2-m2pro
- Otimizadas para computação: C3 | C4 | C5 | C5n | C6a | C6g | C6i
- Otimizadas para memória: R3 | R4 | R5 | R5b | R5n | R6g | R6i | U-6tb1 | U-9tb1 | U-12tb1 | U-18tb1 | U-24tb1 | X1 | X1e | X2iezn
- Computação acelerada: Inf1 | G3 | G5g | P2 | P3

Para recuperar instâncias não compatíveis, consulte Recuperar manualmente as instâncias que não são compatíveis com a recuperação de host dedicado do Amazon EC2.

> **Note**
>
> A recuperação automática de host dedicado de tipos de instância metal levará mais tempo para detectar e recuperar do que os tipos de instância não metal.

Preços

Não há cobranças adicionais para usar a recuperação do host; aplicam-se as cobranças usuais do Host dedicado. Para obter mais informações, consulte Definição de preço de hosts dedicados do Amazon EC2.

Assim que a recuperação for iniciada, você não será mais cobrado pelo Host dedicado prejudicado. A cobrança pelo host dedicado começa somente depois de entrar no estado `available`.

Se o Host dedicado prejudicado tiver sido cobrado usando a taxa sob demanda, o Host dedicado de substituição também são cobrados usando essa taxa. Se o Host dedicado prejudicado tiver um Reserva de hosts dedicados ativo, ele será transferido para o Host dedicado de substituição.

Gerenciar recuperação de um host dedicado do Amazon EC2

A recuperação automática do host dedicado reinicia as instâncias em um novo host substituto quando certas condições problemática são detectadas no host dedicado. É possível habilitar a recuperação do host no momento da alocação do host dedicado ou após a alocação.

Use os procedimentos a seguir para habilitar a recuperação do host ao alocá-lo.

Console

Para habilitar a recuperação do host na alocação

Ao alocar um host dedicado usando o console do Amazon EC2, para Recuperação do host, escolha Habilitar. Para obter mais informações, consulte Alocar um host dedicado do Amazon EC2 para uso em sua conta.

AWS CLI

Para habilitar a recuperação do host na alocação

Use o comando allocate-hosts.

```
aws ec2 allocate-hosts \
    --instance-type m5.large \
    --availability-zone eu-west-1a \
    --auto-placement on \
    --host-recovery on \
    --quantity 1
```

PowerShell

Para habilitar a recuperação do host na alocação

Use o cmdlet New-EC2Host.

```
New-EC2Host `
    -InstanceType m5.large `
    -AvailabilityZone eu-west-1a `
    -AutoPlacement on `
    -HostRecovery on `
    -Quantity 1
```

Use os procedimentos a seguir para gerenciar a recuperação de host para um host dedicado.

Console

Para gerenciar a recuperação do host após a alocação

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Hosts dedicados.
3. Selecione o host dedicado.
4. Selecione Ações, Modificar host.
5. Em Recuperação do host, selecione ou desmarque Habilitar.
6. Escolha Salvar.

AWS CLI

Para habilitar a recuperação do host após a alocação

Use o comando modify-hosts.

```
aws ec2 modify-hosts \
    --host-recovery on \
    --host-ids h-012a3456b7890cdef
```

Para desabilitar a recuperação do host após a alocação

Use o comando modify-hosts e especifique o parâmetro `host-recovery` com um valor de `off`.

```
aws ec2 modify-hosts \
    --host-recovery off \
    --host-ids h-012a3456b7890cdef
```

PowerShell

Para habilitar a recuperação do host após a alocação

Use o cmdlet Edit-host.

```
Edit-EC2Host `
    -HostRecovery on `
    -HostId h-012a3456b7890cdef
```

Para desabilitar a recuperação do host após a alocação

Use o cmdlet Edit-EC2Host.

```
Edit-EC2Host `
    -HostRecovery off `
    -HostId h-012a3456b7890cdef
```

Visualizar a configuração de recuperação de host do host dedicado do Amazon EC2

É possível ver a configuração de recuperação do host para o Host dedicado a qualquer momento.

Console

Para visualizar a configuração de recuperação do host para um host dedicado

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Hosts dedicados.
3. Selecione o Host dedicado e, na aba Description (Descrição), confira o campo Host Recovery (Recuperação do host).

AWS CLI

Para visualizar a configuração de recuperação do host para um host dedicado

Use o comando describe-hosts.

```
aws ec2 describe-hosts \
    --host-ids h-012a3456b7890cdef \
    --query Hosts[].HostRecovery
```

O seguinte é um exemplo de saída.

```
on
```

PowerShell

Para visualizar a configuração de recuperação do host para um host dedicado

Use o cmdlet Get-EC2Host.

```
(Get-EC2Host -HostId h-012a3456b7890cdef).Hosts | Select HostRecovery
```

O seguinte é um exemplo de saída.

```
HostRecovery
------------
on
```

Recuperar manualmente as instâncias que não são compatíveis com a recuperação de host dedicado do Amazon EC2

A recuperação do host não é compatível com a recuperação de instâncias que usam volumes do armazenamento de instâncias. Siga as instruções abaixo para recuperar à mão todas as instâncias que não puderem ser recuperadas automaticamente.

> **Warning**
>
> Os dados nos volumes de armazenamento de instâncias serão perdidos quando a instância for interrompida, hibernada ou encerrada. Isso inclui volumes de armazenamento de instância que estão anexados a uma instância com volume raiz do EBS. Para proteger os dados dos volumes de armazenamento de instâncias, faça backup no armazenamento persistente antes de a instância ser interrompida ou encerrada.

Recuperar manualmente instâncias compatíveis com EBS

Para instâncias compatíveis com EBS que não possam ser recuperadas automaticamente, recomendamos pará-las e iniciá-las automaticamente para recuperá-las a um novo Host dedicado. Para obter mais informações sobre como interromper a instância, além de informações sobre as mudanças em sua configuração de instância quando ela estiver interrompida, consulte Início e interrupção de instâncias do Amazon EC2.

Recuperação manual de instâncias com volume raiz de armazenamento de instância

Para instâncias com volume raiz de armazenamento de instância que não puderam ser recuperadas automaticamente, recomendamos realizar o seguinte:

1. Abrir a instância de substituição em um novo Host dedicado a partir da AMI mais recente.
2. Migrar todos os dados necessários para a instância de substituição.

3. Encerrar a instância original no Host dedicado prejudicado.

Manutenção de host dedicado do Amazon EC2

Com a manutenção do host, na eventualidade de um host dedicado ficar degradado, migraremos automaticamente as instâncias em execução nele para um host dedicado substituto íntegro. Isso ajuda a minimizar o tempo de inatividade da sua workload e a simplificar o gerenciamento dos hosts dedicados. A manutenção de host também é realizada para a manutenção planejada e rotineira do Amazon EC2.

O Amazon EC2 é compatível com dois tipos de manutenção de host:

- Manutenção de host de migração em tempo real: as instâncias são migradas automaticamente para o host de substituição em até 24 horas, sem interrompê-las e reiniciá-las.
- Manutenção de host baseada em reinicialização: as instâncias são agendadas para eventos programados de reinicialização da instância, durante os quais elas são automaticamente interrompidas e reiniciadas no host de substituição.

Conteúdo

- Comparação entre manutenção de host e recuperação de host
- Considerações
- Serviços relacionados
- Preços
- Como a manutenção de host funciona para os hosts dedicados do Amazon EC2
- Configurar a manutenção de host para um host dedicado do Amazon EC2

Comparação entre manutenção de host e recuperação de host

A seguinte tabela mostra as principais diferenças entre recuperação de host e manutenção de host.

	Recuperação do host	Manutenção de host
Acessibilidade de instâncias	Inacessível	Acessível
Estado de um host dedicado	`under-assessment`	`permanent-failure`

	Recuperação do host	Manutenção de host
Grupo de recursos de host	Compatível	Não compatível

Para obter mais informações sobre a recuperação de host, consulte Recuperação de host.

Considerações

- A manutenção de host está disponível em todas as Regiões da AWS, exceto nas regiões da China e AWS GovCloud (US) Regions.
- A manutenção de host não é compatível com o AWS Outposts, com o AWS Local Zones e com o AWS Wavelength Zones.
- A manutenção do host não pode ser ativada nem desativada para hosts que já estejam em um grupo de recursos de host. Os hosts adicionados a um grupo de recursos de host retêm sua configuração de manutenção de host. Para obter mais informações, consulte Grupos de recursos de host.
- A manutenção do host não é compatível com os seguintes tipos de instância, pois esses tipos têm volume raiz de armazenamento de instância: C1, C3, D2, I2, M1, M2, M3, R3 e X1.

Serviços relacionados

Host dedicado se integra com o AWS License Manager: rastreia licenças em todos os hosts dedicados do Amazon EC2 (disponível apenas nas regiões em que o AWS License Manager está disponível). Para obter mais informações, consulte o Manual do usuário do AWS License Manager.

Você deve ter licenças suficientes na Conta da AWS para o novo host dedicado. As licenças associadas ao host degradado são liberadas quando o host é liberado após a conclusão do evento programado.

Preços

Não há cobranças adicionais para usar a manutenção de host, mas as cobranças usuais do host dedicado se aplicam. Para obter mais informações, consulte Definição de preço de hosts dedicados do Amazon EC2.

Assim que a recuperação é iniciada, você deixa de ser mais cobrado pelo host dedicado degradado. A cobrança pelo host dedicado começa somente depois de entrar no estado `available`.

Se a cobrança do host dedicado degradado fosse realizada com base na taxa de sob demanda, o host dedicado substituto também será cobrado usando essa taxa. Se o host dedicado degradado tinha uma reserva de host dedicado ativa, ela será transferida para o host dedicado de substituição.

Como a manutenção de host funciona para os hosts dedicados do Amazon EC2

Após detectar a degradação em um host dedicado que esteja habiltado para manutenção de host, alocamos automaticamente um host dedicado de substituição para a conta. O Host dedicado em substituição recebe um novo ID do host, mas retém os mesmos atributos que o Host dedicado original, como:

- Configurações de autoposicionamento
- Zona de disponibilidade
- Associação de reserva de host dedicado
- Afinidade de host
- Configurações de manutenção de host
- Configurações de recuperação de host
- Tipo de instância
- Tags

Após a alocação do host de substituição, migramos as instâncias usando a manutenção de host de migração em tempo real ou a manutenção do host baseada em reinicialização, dependendo da instância.

Depois que o host degradado não tiver mais instâncias em execução, ele será liberado permanentemente da conta.

Manutenção de host de migração em tempo real

As instâncias que precisarem da manutenção de host de migração em tempo real serão migradas automaticamente para o host de substituição em até 24 horas, sem interrompê-las e reiniciá-las. As instâncias migradas mantêm seus atributos existentes, incluindo:

- ID da instância
- Metadados da instância
- Anexos de volume do Amazon EBS

- Endereços IP elásticos e endereço IP privado
- Memória, CPU e estados de rede

Alguns tamanhos de instância maiores podem sofrer uma pequena diminuição na performance durante a migração.

Depois que as instâncias forem migradas automaticamente para o host substituto, enviaremos notificações por e-mail e pelo painel do AWS Health. As notificações incluem os IDs dos hosts degradados e dos hosts de substituição, informações sobre as instâncias que foram migradas automaticamente usando a manutenção de host de migração em tempo real e informações sobre as instâncias restantes.

Manutenção de host baseada em reinicialização

As instâncias que exigem manutenção de host baseada em reinicialização são programadas para eventos programados de reinicialização da instância por 14 dias a partir da data da notificação. É possível continuar a acessar as instâncias no host dedicado degradado antes do evento programado.

É possível reprogramar eventos de reinicialização para uma data que esteja dentro do prazo de 7 dias da data e hora do evento original. Para obter mais informações, consulte Reagendar um evento programado para uma instância do EC2.

O Amazon EC2 reserva automaticamente a capacidade no host de substituição para essas instâncias. Não é possível executar instâncias nessa capacidade reservada.

O console do Amazon EC2 mostra a capacidade reservada como capacidade usada. Pode parecer que as instâncias estão sendo executadas tanto no host degradado quanto no host substituto. No entanto, as instâncias continuarão sendo executadas somente no host degradado até que sejam interrompidas ou migradas para a capacidade reservada no host substituto.

Na data e hora do evento programado, as instâncias são automaticamente interrompidas e reiniciadas na capacidade reservada no host de substituição. As instâncias migradas mantêm seus atributos existentes, incluindo:

- ID da instância
- Metadados da instância
- Anexos de volume do Amazon EBS

- Endereços IP elásticos e endereço IP privado

No entanto, como as instâncias são interrompidas e reiniciadas durante a migração, elas não retêm seus estados de memória, CPU e rede.

Você também pode interromper e reiniciar manualmente essas instâncias a qualquer momento antes do evento programado para migrá-las para o host de substuição ou para um host diferente. Talvez seja necessário modificar a afinidade de host da instância para reiniciá-la em um host diferente. Caso interrompa uma instância antes do evento programado, a capacidade reservada no host de substituição será liberada e ficará disponível para uso.

Estados de manutenção de host

Quando um host se degrada, ele entra no estado `permanent-failure`. Você não pode executar instâncias em um host dedicado no estado `permanent-failure`.

Depois que o host de substituição for alocado, ele permanecerá no estado `pending` até que as instâncias compatíveis com a manutenção de host de migração em tempo real sejam migradas automaticamente do host degradado e até que os eventos programados estejam agendados para as instâncias restantes. Após a conclusão dessas tarefas, o host de substituição entrará no estado `available`.

Depois que o host de substituição entrar no estado `available`, você poderá usá-lo como usa qualquer outro host na conta. No entanto, parte da capacidade de instância no host de substituição será reservada para as instâncias que precisarem ser migradas do host degradado. Não é possível executar novas instâncias nessa capacidade reservada.

Quando o host degradado não tem mais instâncias em execução, ele entra no estado `released, permanent-failure` e é liberado permanentemente da conta. Observe que o host e seus recursos permanecem visíveis no console por um curto período.

Migração automática

Algumas instâncias não podem ser migradas automaticamente para o host de substituição.

Instâncias com volumes raiz baseados no EBS

Para essas instâncias, programamos eventos de interrupção da instância por 28 dias a partir da data da notificação. Na data e hora do evento programado, as instâncias são interrompidas. Recomendamos que você interrompa manualmente ao reiniciar a instância no host de substituição

ou em outro host. Talvez seja necessário modificar a afinidade de host da instância para reiniciá-la em um host diferente.

Instâncias com um volume raiz de armazenamento de instância

Para essas instâncias, programamos eventos de desativação de instâncias para 28 dias a partir da data da notificação. Na data e hora do evento programado, as instâncias são encerradas permanentemente. Recomendamos que você execute manualmente as instâncias de substituição no host de substituição e depois migre os dados necessários para as instâncias de substituição antes do evento programado.

As seguintes instâncias têm volume raiz do tipo armazenamento de instância: C1, C3, D2, I2, M1, M2, M3, R3 e X1.

É possível continuar a acessar as instâncias no host dedicado degradado antes do evento programado.

Configurar a manutenção de host para um host dedicado do Amazon EC2

Habilite a manutenção de host para garantir que as instâncias em execução em um host dedicado sejam recuperadas automaticamente em um novo host dedicado durante um evento de manutenção programado.

Se você desabilitar a manutenção de host, receberá uma notificação por e-mail para remover o host degradado e migrar manualmente as instâncias para outro host dentro de 28 dias. Um host substituto será alocado se você tiver uma reserva de host dedicado. Após 28 dias, as instâncias em execução no host degradado são encerradas e o host é liberado automaticamente.

Console

Para habilitar a manutenção do host para o seu host dedicado

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Hosts dedicados.
3. Selecione Host dedicado Ações > Modificar host.
4. Selecione ativado no campo Manutenção de host.

Para desabilitar a manutenção do host para o seu host dedicado

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

2. No painel de navegação, selecione Hosts dedicados.
3. Selecione Host dedicado Ações > Modificar host.
4. Selecione Desativado no campo Manutenção de host.

AWS CLI

Para habilitar a manutenção do host para o seu host dedicado

Use o comando modify-hosts.

```
aws ec2 modify-hosts \
    --host-maintenance on \
    --host-ids h-0d123456bbf78910d
```

Para desabilitar a manutenção do host para o seu host dedicado

Use o comando modify-hosts.

```
aws ec2 modify-hosts \
    --host-maintenance off \
    --host-ids h-0d123456bbf78910d
```

PowerShell

Para habilitar a manutenção do host para o seu host dedicado

Use o cmdlet Edit-EC2Host.

```
Edit-EC2Host `
    -HostMaintenance on `
    -HostId h-0d123456bbf78910d
```

Para desabilitar a manutenção do host para o seu host dedicado

Use o cmdlet Edit-EC2Host.

```
Edit-EC2Host `
    -HostMaintenance off `
    -HostId h-0d123456bbf78910d
```

Monitorar o estado dos hosts dedicados do Amazon EC2

O Amazon EC2 monitora constantemente o estado do seu Hosts dedicados. As atualizações são comunicadas no console do Amazon EC2. É possível visualizar informações sobre um Host dedicado usando os métodos a seguir.

Console

Como visualizar o estado de um Host dedicado

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Hosts dedicados.
3. Localize o Host dedicado na lista e revise o valor na coluna State (Estado).

AWS CLI

Como visualizar o estado de um Host dedicado

Use o comando describe-hosts.

```
aws ec2 describe-hosts --host-id h-012a3456b7890cdef
```

PowerShell

Como visualizar o estado de um Host dedicado

Use o cmdlet Get-EC2Host.

```
Get-EC2Host -HostId h-012a3456b7890cdef
```

A tabela a seguir explica os possíveis estados de um Host dedicado.

Estado	Descrição
`available`	AWSA não detectou nenhum problema com o host dedicado. Não estão programados manutenções ou reparos. As instâncias podem ser executadas neste host dedicado.

Estado	Descrição
`released`	O Host dedicado foi liberado. O ID do host não está mais uso. Os hosts liberados não podem ser reutilizados.
`under-assessment`	AWSA 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.
`pending`	O host dedicado não pode ser usado para inicializações de novas instâncias. Ele está sendo modificado para oferecer suporte a vários tipos de instância, ou uma recuperação de host está em andamento.
`permanent-failure`	Uma falha irrecuperável foi detectada. Você receberá um aviso de remoção por meio de suas instâncias e por e-mail. Suas instâncias podem continuar a ser executadas. Se você interromper ou encerrar todas as instâncias de um host dedicado neste estado, a AWS desativará o host. A AWS não reinicia instâncias nesse estado. As instâncias não podem ser executadas no Hosts dedicados neste estado.
`released-permanent-failure`	AWSA liberará permanentemente os hosts dedicados que falharem e não tiverem mais instâncias em execução. O ID do Host dedicado não está mais disponível para uso.

Monitorar as alterações da configuração de host dedicado do Amazon EC2 usando o AWS Config

É possível usar o AWS Config para gravar as alterações de configuração de hosts dedicados e de instâncias que são iniciadas, interrompidas ou encerradas neles. Em seguida, use as informações capturadas pelo AWS Config como fonte de dados para geração de relatórios de licenças.

AWS ConfigO grava individualmente as informações de configuração dos hosts dedicados e das instâncias e emparelha essas informações por meio de relacionamentos. Há três condições de geração de relatórios:

- Status de gravação do AWS Config: quando On (Ativado), o AWS Config está gravando um ou mais tipos de recursos da AWS que podem incluir hosts dedicados e instâncias dedicadas. Para

capturar as informações necessárias para geração de relatórios de licenças, verifique se os hosts e as instâncias estão sendo gravados com os campos a seguir.

- Status de gravação do host — quando está Enabled (Habilitado), as informações de configuração de Hosts dedicados são gravadas.
- Instance recording status (Status de gravação da instância) — quando Enabled (Habilitado), as informações de configuração de Instâncias dedicadas são gravadas.

Se qualquer uma das três condições estiver desabilitada, o ícone do botão Edit Config Recording (Editar gravação de configuração) ficará vermelho. Para aproveitar todos os benefícios dessa ferramenta, verifique se os três métodos de gravação estão ativados. Quando os três estão ativados, o ícone fica verde. Para editar as configurações, escolha Edit Config Recording (Editar gravação de configuração). Você será direcionado à pagina Set up AWS Config (Configurar CC) no console do AWS Config, onde poderá configurar o AWS Config e começar a gravar em seus hosts, instâncias e outros tipos de recursos com suporte. Para obter mais informações, consulte Configuração do AWS Config para uso do console no Guia do desenvolvedor do AWS Config.

> **Note**
>
> AWS ConfigO 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, é possível pesquisar quantas instâncias são executadas nesse host, juntamente com o número de soquetes e núcleos no host. Para qualquer uma dessas instâncias, também é possível procurar o ID de sua imagem de máquina da Amazon (AMI). É possível 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, é possível 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, é possível usar o comando list-discovered-resources para obter uma lista de todos os hosts e instâncias. Depois, é possível usar o comando get-resource-config-history para obter detalhes de configuração de um host ou instância para um intervalo de tempo específico.
- Usando a API do AWS Config em suas aplicações. Primeiro, é possível usar a ação ListDiscoveredResources para obter uma lista de todos os hosts e instâncias. Depois, é possível 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 o a seguir.

```
aws configservice get-resource-config-history \
    --resource-type AWS::EC2::Instance \
    --resource-id i-1234567890abcdef0
```

Para gerenciar as configurações do AWS Config usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Na página Hosts dedicados, escolha Edit Config Recording (Editar gravação de configuração).
3. No console do AWS Config, siga as etapas fornecidas para ativar a gravação. Para obter mais informações, consulte Configuração do AWS Config usando o console.

Para obter mais informações, consulte Visualização de detalhes de configuração no console do AWS Config.

Como ativar o AWS Config usando a linha de comando ou a API

- CLI da AWS: Visualizar detalhes da configuração (AWS CLI) no Guia do desenvolvedor do AWS Config.
- API do Amazon EC2: GetResourceConfigHistory.

Instâncias dedicadas do Amazon EC2

Por padrão, as instâncias EC2 são executadas em hardware de locação compartilhada. Isso significa que várias contas da AWS podem compartilhar o mesmo hardware físico.

As instâncias dedicadas são instâncias EC2 executadas em hardware dedicado a uma única conta da AWS. Isso significa que as instâncias dedicadas são isoladas fisicamente no nível de hardware do host em relação às instâncias pertencentes a outras Contas da AWS, mesmo que essas contas estejam vinculadas a uma única conta pagante. No entanto, as instâncias dedicadas podem compartilhar o hardware com outras instâncias da mesma Conta da AWS que não sejam instâncias dedicadas.

As instâncias dedicadas não oferecem visibilidade nem controle sobre o posicionamento das instâncias, além de não serem compatíveis com afinidade ao host. Se você parar e iniciar uma instância dedicada, talvez ela não seja executada no mesmo host. Da mesma forma, você não pode direcionar um host específico no qual iniciar ou executar uma instância. Além disso, as instâncias dedicadas oferecem um suporte limitado para o modelo traga a sua própria licença (BYOL).

Se você precisar de visibilidade e controle sobre o posicionamento da instância, além de compatibilidade mais abrangente com o modelo BYOL, avalie a possibilidade de usar um host dedicado. É possível usar instâncias dedicadas e hosts dedicados para iniciar instâncias do Amazon EC2 em servidores físicos dedicados. Não há diferenças físicas de performance ou de segurança entre Instâncias dedicadas e instâncias em Hosts dedicados. No entanto, há algumas diferenças básicas entre os dois. A tabela a seguir destaca algumas das principais diferenças entre Hosts dedicados e Instâncias dedicadas:

	Dedicated Host	Dedicated Instance
Servidor físico dedicado	Servidor físico com capacidade de instância totalmente dedicada para seu uso.	Um servidor físico dedicado a uma única conta de cliente.
Compartilhamento de capacidade de instância	Pode compartilhar a capacidade de instância com outras contas.	Não compatível
Faturamento	faturamento por host	Faturamento por instância

	Dedicated Host	Dedicated Instance
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 consisten te suas instâncias no mesmo servidor físico com o momento	Sem suporte
Posiciona mento direcionado de instâncias	Proporciona visibilidade e controle adicionais sobre como as instâncias são colocadas em um servidor físico	Não suportado
Recuperação automática de instâncias	Compatível. Para obter mais informaçõ es, consulte Recuperação de um host dedicado do Amazon EC2.	Compatível
Traga sua própria licença (BYOL)	Compatível	Suporte parcial *
Reservas de capacidade	Não compatível	Compatível

* O Microsoft SQL Server com Mobilidade de Licenças por meio do Software Assurance e as licenças do Windows Virtual Desktop Access (VDA) podem ser usadas com Instância dedicada.

Para obter mais informações, consulte Hosts dedicados do Amazon EC2.

Conteúdo

- Conceitos básicos da Instâncias dedicadas
- Recursos compatíveis
- Limitações da Instâncias dedicadas

- Definição de preço para Instâncias dedicadas
- Iniciar Instâncias dedicadas em uma VPC com a locação padrão
- Alterar a locação de uma instância do EC2
- Alterar a locação da instância de uma VPC

Conceitos básicos da Instâncias dedicadas

Uma VPC pode ter uma locação de `default` ou `dedicated`. Por padrão, suas VPCs têm locação `default` e as instâncias lançadas em uma VPC de locação `default` têm locação `default`. Para iniciar instâncias dedicadas, faça o seguinte:

- Crie uma VPC com uma locação de `dedicated`, para que todas as instâncias na VPC sejam executadas como instâncias dedicadas. Para obter mais informações, consulte Iniciar Instâncias dedicadas em uma VPC com a locação padrão.
- Crie uma VPC com uma locação de `default` e especifique manualmente uma locação de `dedicated` para as instâncias que serão executadas como instâncias dedicadas. Para obter mais informações, consulte Iniciar Instâncias dedicadas em uma VPC com a locação padrão.

Recursos compatíveis

Instâncias dedicadas são compatíveis com os seguintes recursos e integrações de serviço da AWS:

Atributos

- Instâncias reservadas
- Ajuste de escala automático
- Recuperação automática
- Instâncias spot dedicadas
- Instâncias expansíveis

Instâncias reservadas

Para reservar capacidade para suas instâncias dedicadas, é possível comprar instâncias reservadas dedicadas ou reservas de capacidade. Para obter mais informações, consulte Visão geral de instâncias reservadas para o Amazon EC2 e Reservar capacidade computacional com reservas de capacidade sob demanda do EC2.

Ao adquirir uma Instância reservada dedicada, você está comprando a capacidade de iniciar uma instância dedicada por uma taxa de uso muito reduzida. A redução do preço de uso se aplica apenas quando você inicia uma instância com locação dedicada. Quando você compra uma Instância reservada com locação padrão, ela se aplica somente a uma instância em execução com locação `default`. Ela não é aplicada a uma instância em execução com locação `dedicated`.

Você não pode usar o processo de modificação para alterar a locação de uma Instância reservada depois de adquiri-la. No entanto, é possível trocar uma Instância reservada convertível por uma nova Instância reservada convertível com uma locação diferente.

Ajuste de escala automático

É possível usar o Amazon EC2 Auto Scaling para executar Instâncias dedicadas. Para obter mais informações, consulte Criar um modelo de execução usando configurações avançadas no Guia do usuário do Amazon EC2 Auto Scaling.

Recuperação automática

É possível configurar a recuperação automática para uma instância dedicada se ela ficar impedida devido a uma falha de hardware subjacente ou a um problema que exija o envolvimento da AWS para ser reparado. Para obter mais informações, consulte Recuperação automática de instâncias.

Instâncias spot dedicadas

É possível executar uma instância spot dedicada especificando uma locação de `dedicated` ao criar uma solicitação de instâncias spot. Para obter mais informações, consulte Executar no hardware de locatário único.

Instâncias expansíveis

É possível aproveitar os benefícios da execução em hardware de locação dedicada com the section called “Instâncias expansíveis”. As instâncias dedicadas T3 são executadas no modo ilimitado por padrão, e elas fornecem um nível de linha de base de performance da CPU com a capacidade de expansão para um nível de CPU mais alto quando exigido por sua workload. A performance basal da T3 e a capacidade de expansão são regidas por créditos de CPU. Devido à natureza expansível dos tipos de instância T3, recomendamos monitorar como suas instâncias T3 usam os recursos de CPU do hardware dedicado para obter a melhor performance. As instâncias dedicadas T3 destinam-se a clientes com workloads diversas que exibem comportamento aleatório da CPU, mas que, preferencialmente, têm o uso médio da CPU em ou abaixo dos usos da linha de base. Para obter mais informações, consulte the section called “Principais conceitos”.

O Amazon EC2 tem sistemas para identificar e corrigir a variabilidade na performance. No entanto, ainda é possível passar por variabilidade de curto prazo se você iniciar várias instâncias dedicadas T3 que tenham padrões correlacionados de uso da CPU. Para essas workloads mais exigentes ou correlacionadas, recomendamos o uso de instâncias dedicadas M5 ou M5a em vez de instâncias dedicadas T3.

Limitações da Instâncias dedicadas

Tenha o seguinte em mente ao usar instâncias dedicadas:

- Alguns serviços da AWS ou seus recursos não são compatíveis com uma VPC com a locação de instância definida como `dedicated`. Verifique a documentação do serviço para confirmar se há alguma limitação.
- Alguns tipos de instância não podem ser iniciados em uma VPC com a locação da instância definida como `dedicated`. Para obter mais informações sobre os tipos de instância compatíveis, consulte Instâncias dedicadas do Amazon EC2.
- Quando você iniciar uma instância dedicada compatível com o Amazon EBS, o volume do EBS não é executado em hardware de ocupante único.

Definição de preço para Instâncias dedicadas

A definição de preço de Instâncias dedicadas é diferente da definição de preço de Instâncias sob demanda. Para obter mais informações, consulte Instâncias dedicadas do Amazon EC2.

Iniciar Instâncias dedicadas em uma VPC com a locação padrão

Ao criar uma VPC, você tem a opção de especificar sua locação de instância. Se você iniciar uma instância em uma VPC que tenha uma locação de instância `dedicated`, ela será executada como uma instância dedicada em hardware dedicado ao seu uso.

Para obter mais informações sobre a execução de uma instância com uma locação de `host`, consulte Iniciar instâncias do Amazon EC2 em um host dedicado do Amazon EC2.

Para obter mais informações sobre as opções de locação de VPC, consulte Crie uma VPC no Manual do usuário da Amazon VPC.

Requisitos

- Escolha um tipo de instância compatível. Para obter mais informações, consulte Instâncias dedicadas do Amazon EC2.

Console

Para executar uma instância dedicada em uma VPC de locação padrão

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias), Launch Instance (Iniciar instância).
3. Na seção Application and OS Images (Imagens de aplicações e do sistema operacional), selecione uma AMI na lista.
4. Na seção Instance type (Tipo de instância), selecione o tipo de instância a ser iniciada.
5. Na seção Key pair (Par de chaves), selecione o par de chaves a ser associado à instância.
6. Na seção Advanced details (Detalhes avançados), em Tenancy (Locação), selecione Dedicated (Dedicada).
7. Configure as demais opções da instância conforme necessário. Para obter mais informações, consulte Referência para parâmetros de configuração de instâncias do Amazon EC2.
8. Escolha Iniciar instância.

AWS CLI

Para configurar a opção de locação para uma instância durante a execução

Use a o comando run-instances e inclua a `Tenancy` com a opção de `--placement`.

```
--placement Tenancy=dedicated
```

PowerShell

Para configurar a opção de locação para uma instância durante a execução

Use o cmdlet New-EC2Instance com o parâmetro `-Placement_Tenancy`.

```
-Placement_Tenancy dedicated
```

Alterar a locação de uma instância do EC2

É possível alterar a locação de uma instância interrompida depois de iniciá-la. As alterações que você fizer entrarão em vigor na próxima vez que a instância for iniciada.

Como alternativa, você pode alterar a locação da sua nuvem privada virtual (VPC). Para obter mais informações, consulte the section called “Alterar a locação de uma VPC”.

Limitações

- Você não pode alterar a locação de uma instância usando o Console de gerenciamento da AWS.
- A instância deve estar no estado `stopped`.
- Os detalhes do sistema operacional da instância, e se o SQL Server está ou não instalado, afetam quais conversões são compatíveis. Para obter mais informações sobre os caminhos de conversão de locação disponíveis para a sua instância, consulte Tenancy conversion no License Manager User Guide.
- Para instâncias T3, você deve iniciar a instância em um host dedicado para usar uma locação de `host`. Você não pode alterar a locação de `host` para `dedicated` ou `default`. Tentar fazer uma dessas alterações de locação não compatíveis gera um código de erro de `InvalidRequest`.

AWS CLI

Para modificar o valor da locação de uma instância

Use o comando modify-instance-placement.

```
aws ec2 modify-instance-placement \
    --instance-id i-1234567890abcdef0 \
    --tenancy dedicated
```

PowerShell

Para modificar o valor da locação de uma instância

Use o cmdlet Edit-EC2InstancePlacement.

```
Edit-EC2InstancePlacement `
    -InstanceId i-1234567890abcdef0 `
    -Tenancy Dedicated
```

Alterar a locação da instância de uma VPC

Você pode alterar a locação da instância de uma nuvem privada virtual (VPC) de `dedicated` para `default` depois de criá-la. Modificar a locação da instância de uma 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 de outra forma durante a execução.

Como alternativa, você pode alterar a locação de instâncias específicas. Para obter mais informações, consulte the section called “Altere a locação de uma instância”.

Limitações

- Você não pode alterar a locação da instância de uma VPC de `default` para `dedicated` depois de criá-la.
- Você não pode modificar a locação de instâncias de uma VPC usando o Console de gerenciamento da AWS.

AWS CLI

Para modificar o atributo de locação da instância de uma VPC

Use o comando modify-vpc-tenancy. O único valor de locação compatível é `default`.

```
aws ec2 modify-vpc-tenancy \
    --vpc-id vpc-1234567890abcdef0 \
    --instance-tenancy default
```

PowerShell

Para modificar o atributo de locação da instância de uma VPC

Use o cmdlet Edit-EC2VpcTenancy. O único valor de locação compatível é `Default`.

```
Edit-EC2VpcTenancy `
    -VpcId vpc-1234567890abcdef0 `
    -InstanceTenancy Default
```

Reservas de capacidade sob demanda e blocos de capacidade para ML

As reservas de capacidade permitem que você reserve capacidade computacional para as instâncias do Amazon EC2 em uma determinada zona de disponibilidade. Há dois tipos de reserva de capacidade, que atendem a casos de uso diferentes.

Tipos de reserva de capacidade

- Reservas de capacidade sob demanda
- Blocos de capacidade para ML

Estes são alguns casos de uso comuns de reservas de capacidade sob demanda:

- Eventos de escalação: você pode criar reservas de capacidade sob demanda antes de eventos críticos para os negócios de modo a garantir que possa escalar quando necessário.
- Requisitos regulamentares e recuperação de desastres: use reservas de capacidade sob demanda para atender aos requisitos regulamentares de alta disponibilidade e reserve capacidade para recuperação de desastres em uma outra zona ou região de disponibilidade.
- Compartilhamento de capacidade não utilizada — Use reservas de capacidade interruptível para disponibilizar a capacidade não utilizada para outras workloads em sua conta, mantendo o controle para recuperá-la quando necessário.

Estes são alguns casos de uso comuns de reservas de capacidade:

- Treinamento e ajuste fino de modelo de machine learning (ML): tenha acesso ininterrupto às instâncias de GPU que você reservou para concluir o treinamento e o ajuste fino do modelo de ML.
- Experimentos e protótipos de ML: executar experimentos e desenvolver protótipos que exigem instâncias de GPU por períodos curtos.

Quando usar reserva de capacidade sob demanda

Use reservas de capacidade sob demanda se você tiver requisitos rígidos de capacidade e se suas workloads essenciais para os negócios, atuais ou futuras, exigirem garantia de capacidade. Com as reservas de capacidade sob demanda, você garante que sempre terá acesso à capacidade do Amazon EC2 que reservou, pelo tempo que precisar.

Quando usar blocos de capacidade para ML

Use blocos de capacidade para ML quando precisar garantir acesso ininterrupto às instâncias de GPU por um período de tempo definido, a partir de uma data futura. Os blocos de capacidade são ideais para treinar e ajustar modelos de ML, fazer pequenas execuções experimentais e lidar com picos temporários de demanda inferida no futuro. Com blocos de capacidade, você pode garantir que terá acesso aos recursos de GPU em uma data específica para executar as workloads de ML.

Reservar capacidade computacional com reservas de capacidade sob demanda do EC2

As reservas de capacidade do Amazon EC2 permitem que você reserve capacidade computacional para instâncias do Amazon EC2 em uma determinada zona de disponibilidade por qualquer duração. Caso tenha requisitos rígidos de capacidade para workloads essenciais aos negócios, atuais ou futuras, que exijam um determinado nível de garantia de capacidade de longo ou curto prazo, recomendamos criar uma reserva de capacidade para ajudar a garantir que você sempre tenha acesso à capacidade do Amazon EC2 quando precisar, pelo tempo que precisar.

É possível criar uma reserva de capacidade a qualquer momento e escolher quando ela começa. É possível solicitar uma reserva de capacidade para uso imediato ou para uma data futura.

- Caso solicite uma reserva de capacidade para uso imediato, a reserva de capacidade ficará disponível para uso imediato e não haverá compromisso de prazo. É possível modificar e cancelar a reserva de capacidade a qualquer momento para liberar a capacidade reservada e interromper as cobranças recorrentes.
- Ao solicitar uma reserva de capacidade com data futura, especifique a data futura desejada para que a reserva de capacidade fique disponível para uso. Você também deve especificar uma duração de compromisso pela qual se compromete a manter a capacidade solicitada em sua conta após a data especificada. Na data e hora solicitadas, a reserva de capacidade fica disponível para uso e a duração do compromisso é iniciada. Durante o compromisso, você não pode diminuir a contagem de instâncias ou a duração do compromisso abaixo do compromisso inicial, nem cancelar a reserva de capacidade. Após o término da duração do compromisso, será possível modificar a reserva de capacidade da forma como desejar ou cancelá-la se não precisar mais dela.

Reservas de Capacidade só podem ser usadas por instâncias que correspondam aos seus atributos. Por padrão, as reservas de capacidade correspondem automaticamente às novas instâncias e às instâncias em execução que têm atributos correspondentes (por exemplo: tipo de instância, plataforma, zona de disponibilidade e locação). Isso significa que qualquer instância com atributos correspondentes são automaticamente executadas na Reserva de capacidade. No entanto, também é possível destinar uma Reserva de capacidade para workloads específicas. Isso permite que você controle explicitamente quais instâncias têm permissão de execução na capacidade reservada. Você também pode especificar que as instâncias serão executadas somente em uma reserva de capacidade ou um grupo de recursos de reserva de capacidade.

> **Important**
>
> As reservas de capacidade com data futura servem para ajudar você a iniciar e cobrir instâncias incrementais e não para cobrir instâncias em execução existentes. Caso precise cobrir as instâncias em execução existentes, use as reservas de capacidade com início imediato.

Todas as instâncias do Amazon EC2 compatíveis que têm os atributos exigidos, ou seja, tipo de instância, plataforma, zona de disponibilidade e locação, são elegíveis para execução em uma reserva de capacidade. A instância do Amazon EC2 pode ser iniciada por você (instâncias não gerenciadas) ou em seu nome por um serviço da AWS (instâncias gerenciadas). Isso é particularmente válido para Reservas de capacidade abertas, que correspondem automaticamente a qualquer instância em execução que tenha atributos correspondentes. Por exemplo, instâncias gerenciadas lançadas em seu nome pelos serviços a seguir estão qualificadas para execução em Reservas de capacidade que você cria e gerencia.

- Amazon EC2 Auto Scaling
- Amazon ECS
- Amazon EKS
- Amazon EMR
- Amazon SageMaker AI
- AWS Batch
- AWS Elastic Beanstalk
- AWS ParallelCluster
- Serviço de Computação Paralela da AWS (AWS PCS)

Conteúdo

- Conceitos das reservas de capacidade do Amazon EC2
- Diferenças entre Reservas de Capacidade, Instâncias reservadas e Savings Plans
- Plataformas compatíveis
- Cotas
- Limitações
- Definição de preços e faturamento da Reserva de capacidade

- Criar uma Reserva de capacidade
- Visualizar o estado de uma reserva de capacidade
- Iniciar instâncias em uma Reserva de capacidade existente
- Modificar uma reserva de capacidade ativa
- Modificar as configurações de reserva de capacidade da instância
- Mover a capacidade entre reservas de capacidade
- Dividir a capacidade de uma reserva de capacidade existente
- Cancelar uma Reserva de capacidade
- Usar reservas de capacidade em grupos de posicionamento de cluster
- Grupos de Reserva de capacidade
- Reservas de Capacidade em zonas locais
- Reservas de Capacidade em zonas Wavelength
- Reservas de Capacidade no AWS Outposts
- Reservas de capacidade compartilhadas
- Frotas de reserva de capacidade
- Monitorar o uso de reservas de capacidade com métricas do CloudWatch
- Monitorar a subutilização da Reserva de capacidade
- Monitorar alterações de estado para Reservas de capacidade com data no futuro
- Reservas de capacidade

Conceitos das reservas de capacidade do Amazon EC2

Os conceitos-chave a seguir se aplicam às reservas de capacidade.

Tópicos

- Data e hora de início
- Data e hora de encerramento
- Duração do compromisso
- Avaliação da reserva de capacidade com data futura
- Atributos da reserva de capacidade
- Critérios de correspondência de instâncias

Data e hora de início

A data e a hora de início definem quando a reserva de capacidade fica disponível para uso. Uma reserva de capacidade pode começar imediatamente ou em uma data futura.

- Se você optar por iniciar uma reserva de capacidade imediatamente, a capacidade reservada já ficará disponível para uso após sua criação, e o faturamento será iniciado assim que a reserva de capacidade entrar no estado ativo. Não há necessidade de assumir nenhum compromisso de prazo. É possível modificar a reserva de capacidade conforme necessário a qualquer momento para atender às suas necessidades, bem como cancelá-la para liberar a capacidade e interromper as cobranças.
- Caso opte por iniciar uma reserva de capacidade em uma data futura, especifique uma data e hora futuras nas quais precisará da capacidade reservada e uma duração de compromisso, que é a duração mínima pela qual você se compromete a manter a reserva de capacidade solicitada em sua conta após o provisionamento. Na data futura especificada, a reserva de capacidade fica disponível para uso e o faturamento começa nesse momento, quando a reserva de capacidade entra no estado ativo. A duração do compromisso começa assim que a reserva de capacidade é provisionada na conta. Durante esse período, você não pode diminuir a contagem de instâncias abaixo da contagem de instâncias confirmadas, escolher uma data de término anterior à duração do compromisso ou cancelar a reserva de capacidade. No entanto, após o término da duração do compromisso, será possível modificar a reserva de capacidade da forma como desejar ou cancelá-la para liberar a capacidade reservada e interromper as cobranças.

Data e hora de encerramento

A data e a hora de término definem quando a reserva de capacidade termina e a capacidade reservada é liberada da sua conta. É possível configurar uma reserva de capacidade para terminar automaticamente em uma data e hora específicas ou para permanecer ativa indefinidamente até que você a cancele manualmente.

Se você configurar uma reserva de capacidade para terminar automaticamente, a reserva de capacidade vai expirar dentro de 1 hora após o horário especificado. Por exemplo, se você especificar `5/31/2019, 13:30:55`, é garantido que a reserva de capacidade termine entre `13:30:55` e `14:30:55` em `5/31/2019`.

Após o término da reserva, a capacidade reservada é liberada da conta, e você não pode mais destinar instâncias à reserva de capacidade. Instâncias em execução na capacidade reservada continuam a executar sem interrupção. Se as instâncias que estão destinando uma reserva de

capacidade forem interrompidas, não será possível 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. Para obter mais informações, consulte Modificar as configurações de reserva de capacidade da instância.

Duração do compromisso

A duração do compromisso se aplica somente às reservas de capacidade com data futura.

A duração do compromisso é a duração mínima pela qual você se compromete a ter a reserva de capacidade com data futura no estado ativo em sua conta depois de provisionada. É possível manter uma reserva de capacidade com data futura por mais tempo do que a duração do compromisso, mas não por menos. As seguintes especificações se aplicam à duração do compromisso:

- Você não pode cancelar uma reserva de capacidade durante a vigência do compromisso.
- Você não pode diminuir a contagem de instâncias abaixo da contagem de instâncias confirmada, mas pode aumentá-la.
- Você não pode configurar uma reserva de capacidade para terminar automaticamente em uma data ou hora que esteja dentro da duração do compromisso. É possível estender a data e a hora de término durante o período de compromisso.

O Amazon EC2 usa a duração do compromisso especificada para avaliar se há suporte para a solicitação. A duração mínima do compromisso é 14 dias. Ao avaliar uma solicitação, o Amazon EC2 pode determinar que há suporte para uma duração de compromisso mais curta. Nesse caso, o Amazon EC2 agendará a reserva de capacidade com data futura com a duração do compromisso menor. Isso significa que você se compromete a manter a reserva de capacidade em sua conta por um período menor do que o solicitado inicialmente.

Avaliação da reserva de capacidade com data futura

Quando você solicita uma reserva de capacidade com data futura, o Amazon EC2 avalia a solicitação para determinar se há suporte para ela com base na disponibilidade da capacidade e na duração do compromisso que você especificar. A avaliação costuma ser concluída em cinco dias. O Amazon EC2 considera vários fatores ao avaliar uma solicitação, incluindo:

- Fornecimento de capacidade previsto
- A duração do compromisso
- Com que antecedência você solicita a reserva de capacidade em relação à data de início

- O tamanho da solicitação

É possível solicitar uma reserva de capacidade com data futura entre 5 e 120 dias de antecedência. Recomendamos que você faça a solicitação com pelo menos 56 dias (8 semanas) de antecedência para melhorar nossa capacidade de atendê-la. A duração mínima do compromisso é 14 dias, e a contagem mínima de instâncias é de 32 vCPUs.

A reserva de capacidade permanece no estado `assessing` enquanto a solicitação está sendo avaliada.

Se a solicitação puder ser atendida, a reserva de capacidade entrará no estado `scheduled` e será programada para entrega na data e hora solicitadas. A contagem total de instâncias permanece 0 enquanto a reserva de capacidade está no estado `scheduled`. Uma reserva de capacidade programada ficará `active` e será disponibilizada para uso na data solicitada.

Se uma solicitação não puder ser atendida, a reserva de capacidade entrará no estado `unsupported`. Reservas de capacidade sem suporte não são entregues.

É possível cancelar uma reserva de capacidade com data futura enquanto ela estiver no estado `assessing`.

Para obter mais informações, consulte Criar uma reserva de capacidade com data futura.

Atributos da reserva de capacidade

Ao criar uma reserva de capacidade, especifique os seguintes atributos:

- Zona de disponibilidade
- Tipo de instância
- Plataforma (tipo de sistema operacional)
- Locação (`default` ou `dedicated`)

Somente instâncias que correspondam a esses atributos podem ser iniciadas ou executadas na reserva de capacidade.

Critérios de correspondência de instâncias

Os critérios de correspondência de instâncias, ou a elegibilidade de instâncias, determinam quais delas podem ser iniciadas e executadas na reserva de capacidade. Uma reserva de capacidade pode ter um dos seguintes critérios de correspondência:

- Aberta: a reserva de capacidade corresponde automaticamente a todas as instâncias que têm atributos correspondentes (tipo de instância, plataforma e zona de disponibilidade). As instâncias novas e existentes que têm atributos correspondentes são executadas automaticamente na reserva de capacidade sem nenhuma configuração adicional.
- Destinada: a reserva de capacidade só aceita instâncias que tenham atributos correspondentes (tipo de instância, plataforma e zona de disponibilidade) e estejam explicitamente destinadas para a reserva de capacidade. A instância deve direcionar especificamente a reserva de capacidade para ser iniciada ou executada na capacidade reservada. Isso permite que você controle explicitamente quais instâncias têm permissão para serem executadas na capacidade reservada e ajuda a evitar o uso não intencional da capacidade reservada.

Ao solicitar uma reserva de capacidade com data futura, você pode especificar somente os critérios de correspondência direcionados. Isso garante que a capacidade fornecida pela reserva de capacidade seja incremental ou adicional a qualquer instância em execução ou capacidade reservada que você tenha no momento da entrega. Depois que a reserva de capacidade se tornar ativa em sua conta, será possível alterar os critérios de correspondência de instâncias para aberto, se necessário. No entanto, lembre-se de que todas as instâncias correspondentes serão executadas automaticamente na reserva de capacidade, o que pode levar ao uso não intencional da capacidade e impedir que você inicie novas instâncias na contagem total de instâncias solicitadas.

Diferenças entre Reservas de Capacidade, Instâncias reservadas e Savings Plans

A tabela a seguir destaca as principais diferenças entre Reservas de Capacidade, Instâncias reservadas e Savings Plans:

	Capacity Reservations	Instâncias reservadas zonais	Instâncias reservadas regionais	Savings Plans
Prazo	Não é necessário nenhum compromisso para reservas de capacidade de uso imediato. Elas podem ser criadas, modificad	Exige compromisso fixo de um ano ou de três anos		

	Capacity Reservations	Instâncias reservadas zonais	Instâncias reservadas regionais	Savings Plans
	as e cancelada s conforme necessário. Em reservas de capacidade com data futura, você especifica uma duração de compromisso pela qual se compromet e a manter a capacidade em sua conta. Após o término da duração do compromis so, será possível cancelar a reserva de capacidade a qualquer momento.			
Benefício da capacidac e	Capacidade reservada em uma zona de disponibilidade específica.		Nenhuma capacidade reservada.	
Desconto de faturamen to	Sem desconto de faturamento. †	Fornece um desconto de faturamento.		

	Capacity Reservations	Instâncias reservadas zonais	Instâncias reservadas regionais	Savings Plans
Limites de instâncias	Seus limites instância sob demanda por região se aplicam.	O padrão é 20 por zona de disponibilidade. É possível solicitar um aumento de limite.	O padrão é 20 por região. É possível solicitar um aumento de limite.	Sem limite.

† É possível combinar Reservas de Capacidade com Savings Plans ou instâncias reservadas regionais para receber um desconto.

Para obter mais informações, consulte:

- Visão geral de instâncias reservadas para o Amazon EC2
- Guia do usuário do Savings Plans

Plataformas compatíveis

É necessário criar a reserva de capacidade com a plataforma correta para garantir que ela corresponda corretamente às suas instâncias. As reservas de capacidade oferecem suporte aos seguintes valores para `platform`:

- Linux/UNIX
- Linux com SQL Server Standard
- Linux com SQL Server Web
- Linux com SQL Server Enterprise
- SUSE Linux
- Red Hat Enterprise Linux
- RHEL com SQL Server Standard
- RHEL com SQL Server Enterprise
- RHEL com SQL Server Web

- RHEL com HA
- RHEL com HA e SQL Server Standard
- RHEL com HA e SQL Server Enterprise
- Ubuntu Pro
- Windows
- Windows com SQL Server
- Windows com SQL Server Web
- Windows com SQL Server Standard
- Windows com SQL Server Enterprise

Para garantir que uma instância seja executada em uma reserva de capacidade específica, a plataforma da reserva de capacidade deve corresponder à plataforma da AMI utilizada para iniciar a instância. Para AMIs do Linux, é importante verificar se a plataforma da AMI usa o valor geral Linux/UNIX ou um valor mais específico, como SUSE Linux.

Console

Para verificar a plataforma da AMI

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione AMIs.
3. Selecione a AMI.
4. Na guia Detalhes, anote o valor de Detalhes da plataforma.

AWS CLI

Para verificar a plataforma da AMI

Utilize o comando describe-images e verifique o valor de `PlatformDetails`.

```
aws ec2 describe-images \
    --image-ids ami-0abcdef1234567890 \
    --query Images[*].PlatformDetails
```

O seguinte é um exemplo de saída.

```
[
    "Linux/UNIX"
]
```

PowerShell

Para verificar a plataforma da AMI

Use o cmdlet Get-EC2Image e verifique o valor de `PlatformDetails`.

```
Get-EC2Image `
    -ImageId ami-0abcdef1234567890 | `
    Select PlatformDetails
```

O seguinte é um exemplo de saída.

```
PlatformDetails
---------------
Linux/UNIX
```

Cotas

O número de instâncias para as quais você tem permissão para reservar capacidade é baseado na cota de instâncias sob demanda de sua conta. É possível reservar capacidade para todas as instâncias permitidas pela cota, menos o número de instâncias que já estão em execução.

As reservas de capacidade nos estados `assessing`, `scheduled`, `pending`, `active` e `delayed` contam para a cota de instâncias sob demanda.

Limitações

Antes de criar Reservas de Capacidade, observe as seguintes limitações e restrições.

- Reservas de Capacidade ativas e não utilizadas entram na contagem dos limites de instância sob demanda.
- As Reservas de Capacidade não são transferíveis de uma conta da AWS para outra. Entretanto, é possível compartilhar reservas de capacidade com outras contas da AWS. Para obter mais informações, consulte Reservas de capacidade compartilhadas.

- Os descontos de faturamento Instância reservada de zona não se aplicam às Reservas de Capacidade.
- É possível criar reservas de capacidade em grupos de posicionamento de cluster. Não há suporte para grupos de posicionamento disseminados e de partição.
- As Reservas de Capacidade não podem ser usadas com Hosts dedicados. As reservas de capacidade não podem ser usadas com instâncias dedicadas.
- [Instâncias do Windows] Não é possível usar as reservas de capacidade com o modelo de licenciamento traga a sua própria licença (BYOL).
- [Instâncias Red Hat] É possível usar as reservas de capacidade com o modelo de licenciamento traga a sua própria licença (BYOL).
- O Reservas de Capacidade não garante que uma instância hibernada possa retomar depois de tentar iniciá-la.
- É possível solicitar reservas de capacidade com data futura para uma contagem de instâncias com um mínimo de 32 vCPUs. Por exemplo, se você solicitar uma reserva de capacidade com data futura para instâncias `m5.xlarge`, deverá solicitar pelo menos 8 instâncias (8 * m5.xlarge = 32 vCPUs).
- É possível solicitar reservas de capacidade com data futura somente para tipos de instância nestas séries: C, G, I, M, R e T.

Definição de preços e faturamento da Reserva de capacidade

Os tópicos desta seção fornecem uma visão geral do preço e do faturamento das reservas de capacidade.

Tópicos

- Preços
- Faturamento
- Descontos de faturamento
- Visualizar sua fatura

Preços

As Reservas de capacidade são cobradas pela taxa sob demanda equivalente independentemente de você executar instâncias na capacidade reservada ou não, incluindo qualquer sobretaxa regional aplicável para instâncias dedicadas. Se você não usar a reserva, ela será exibida como uma reserva

não utilizada em sua fatura do Amazon EC2. Quando executa uma instância que corresponde aos atributos de uma reserva, você paga apenas pela instância e nada pela reserva. Não há cobranças antecipadas ou adicionais.

Por exemplo, se criar uma Reserva de capacidade para 20 instâncias `m4.large` do Linux e executar 15 instâncias `m4.large` do Linux na mesma zona de disponibilidade, você será cobrado por 15 instâncias ativas e por 5 instâncias não usadas na reserva.

Descontos de faturamento para Savings Plans e instâncias reservadas regionais aplicam-se a reservas de capacidade. Para obter mais informações, consulte Descontos de faturamento.

Para obter mais informações, consulte Definição de preço Amazon EC2.

Faturamento

O faturamento começa assim que a Reserva de capacidade for provisionada na conta. Ele prosseguirá enquanto a Reserva de capacidade permanecer provisionada na conta. Para reservas de capacidade com data futura, isso significa que o faturamento começa somente quando a reserva de capacidade é provisionada em sua conta na data futura solicitada.

As Reservas de Capacidade são cobradas por granularidade por segundo. Isso significa que você é cobrado por horas parciais. Por exemplo, se uma reserva de capacidade permanecer provisionada em sua conta por 24 horas e 15 minutos, você será cobrado por `24.25` horas de reserva.

O exemplo a seguir mostra como uma Reserva de capacidade é cobrada. A Reserva de capacidade é criada para uma instância `m4.large` do Linux, que tem uma taxa sob demanda de 0,10 USD por hora de uso. Neste exemplo, a Reserva de capacidade está provisionada 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	Total cost
Unused Capacity Reservation	$0.10	$0.00	$0.00	$0.00	$0.00	$0.00	**$0.10**
On-demand Instance Usage	$0.00	$0.10	$0.10	$0.10	$0.10	$0.10	**$0.50**
Hourly cost	**$0.10**	**$0.10**	**$0.10**	**$0.10**	**$0.10**	**$0.10**	**$0.60**

Descontos de faturamento

Os descontos de faturamento para Savings Plans e instâncias reservadas regionais aplicam-se a reservas de capacidade. A AWS aplica automaticamente esses descontos às reservas de capacidade que têm atributos correspondentes. Quando uma Reserva de capacidade é usada por uma instância, o desconto é aplicado à instância. Os descontos são preferencialmente aplicados ao uso de instâncias antes de cobrir Reservas de Capacidade não utilizadas.

Os descontos de faturamento de Instâncias reservadas zonais não se aplicam às Reservas de Capacidade.

Para obter mais informações, consulte:

- Visão geral de instâncias reservadas para o Amazon EC2
- Guia do usuário do Savings Plans
- Opções de faturamento e compra

Visualizar sua fatura

É possível revisar as cobranças e taxas da sua conta no console do AWS Billing and Cost Management.

- O Painel exibe um resumo de gastos da sua conta.
- Na página Bills (Faturas), em Details (Detalhes), expanda a seção Elastic Compute Cloud e a região para obter informações de faturamento sobre suas Reservas de Capacidade.

É possível visualizar as cobranças online ou baixar um arquivo CSV. Para obter mais informações, consulte Itens de linha de reserva de capacidade.

Criar uma Reserva de capacidade

É possível criar uma reserva de capacidade a qualquer momento para garantir que tenha capacidade computacional disponível em uma zona de disponibilidade específica. Uma reserva de capacidade pode começar imediatamente ou em uma data futura. A capacidade fica disponível para uso somente quando a reserva de capacidade entra no estado `active`.

> **Note**
>
> Se você criar uma reserva de capacidade com critérios de correspondência de instâncias `open` e tiver instâncias em execução com atributos correspondentes no momento em que a reserva de capacidade se tornar ativa, essas instâncias serão executadas automaticamente na capacidade reservada. Para evitar isso, use critérios de correspondência de instâncias `targeted`. Para obter mais informações, consulte Critérios de correspondência de instâncias.

Sua solicitação de criação de uma Reserva de capacidade poderá falhar se uma das seguintes opções for verdadeira:

- O Amazon EC2 não tem capacidade suficiente para realizar a solicitação. Tente novamente mais tarde, tente uma zona de disponibilidade diferente ou tente uma solicitação menor. Se a sua aplicação for flexível entre tipos e tamanhos de instâncias, tente diferentes atributos de instância.
- A quantidade solicitada excede o limite de instância sob demanda para a família de instâncias selecionada. Aumente o limite de instância sob demanda para a família de instâncias e tente novamente. Para obter mais informações, consulte Cotas de instância sob demanda.

Tópicos

- Criar uma reserva de capacidade para uso imediato
- Criar uma reserva de capacidade com data futura

Criar uma reserva de capacidade para uso imediato

Você cria uma reserva de capacidade para uso imediato.

Console

Para criar uma reserva de capacidade

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Selecione Reservas de Capacidade e Create Reserva de capacidade (Criar Reserva de capacidade).
3. Defina as configurações a seguir na seção Detalhes da instância.

a. Tipo de instância: o tipo de instância para o qual reservar capacidade.

b. Plataforma: o sistema operacional das suas instâncias. Para obter mais informações, consulte Plataformas compatíveis.

c. Zona de disponibilidade a zona de disponibilidade na qual reservar a capacidade.

d. Locação: o tipo de locação a ser usada na capacidade reservada. Escolha Padrão para reservar capacidade em hardware compartilhado ou Dedicado para reservar capacidade em hardware dedicado a sua conta.

e. (Opcional) ARN do grupo de posicionamento: o ARN do grupo de posicionamento de cluster no qual criar a reserva de capacidade. Para obter mais informações, consulte Usar reservas de capacidade em grupos de posicionamento de cluster.

f. Contagem total de instâncias: o número de instâncias para as quais reservar capacidade. Se você especificar uma quantidade que exceda sua cota de instâncias sob demanda restante para o tipo de instância selecionada, a solicitação falhará.

4. Defina as seguintes configurações na seção Reservation details (Detalhes da reserva):

a. A reserva de capacidade começa: escolha Imediatamente.

b. Término da reserva de capacidade: escolha uma das seguintes opções:

- Manualmente: reserve a capacidade até que você a cancele explicitamente.
- Horário específico: cancele a reserva de capacidade automaticamente na data e na hora especificadas.

c. Elegibilidade de instância: escolha uma das seguintes opções:

- aberto: (padrão) a reserva de capacidade corresponde a qualquer instância que tenha atributos correspondentes (tipo de instância, plataforma, zona de disponibilidade e locação). Se você executar uma instância com atributos correspondentes, ela será colocada na capacidade reservada automaticamente.
- Direcionada: a reserva de capacidade aceita somente instâncias que tenham atributos correspondentes (tipo de instância, plataforma, zona de disponibilidade e locação) e estejam explicitamente destinadas para a reserva.

5. Escolha Criar.

AWS CLI

Para criar uma reserva de capacidade

Use o comando create-capacity-reservation.

```
aws ec2 create-capacity-reservation \
    --availability-zone az_name \
    --instance-type instance_type \
    --instance-count number_of_instances \
    --instance-platform operating_system \
    --instance-match-criteria open|targeted
```

PowerShell

Para criar uma reserva de capacidade

Use o cmdlet Add-EC2CapacityReservation.

```
Add-EC2CapacityReservation `
    -AvailabilityZone az_name `
    -InstanceType instance_type `
    -InstanceCount number_of_instances `
    -InstancePlatform operating_system `
    -InstanceMatchCriterion open|targeted
```

Criar uma reserva de capacidade com data futura

Solicite uma reserva de capacidade com data futura se precisar que a capacidade reservada fique disponível em uma data e hora futuras.

Depois de solicitar uma reserva de capacidade com data futura, a solicitação passa por uma avaliação para determinar se ela pode ser atendida. Para obter mais informações, consulte Avaliação da reserva de capacidade com data futura.

Considerações

- É possível solicitar reservas de capacidade com data futura para tipos de instância nestas séries: C, G, I, M, R e T.
- É possível solicitar reservas de capacidade com data futura para uma contagem de instâncias com um mínimo de 32 vCPUs. Por exemplo, se você solicitar uma reserva de capacidade com data futura para instâncias `m5.xlarge`, deverá solicitar capacidade pelo menos para 8 instâncias (8 * m5.xlarge = 32 vCPUs).

- É possível solicitar uma reserva de capacidade com data futura entre 5 e 120 dias de antecedência. No entanto, recomendamos solicitar com pelo menos 56 dias (oito semanas) de antecedência para melhorar a capacidade de atendimento.
- A duração mínima do compromisso é 14 dias.

Console

Para criar uma reserva de capacidade

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Selecione Reservas de Capacidade e Create Reserva de capacidade (Criar Reserva de capacidade).
3. Defina as configurações a seguir na seção Detalhes da instância.
   a. Tipo de instância: o tipo de instância para o qual reservar capacidade.
   b. Plataforma: o sistema operacional das suas instâncias. Para obter mais informações, consulte Plataformas compatíveis.
   c. Zona de disponibilidade a zona de disponibilidade na qual reservar a capacidade.
   d. Locação: o tipo de locação a ser usada na capacidade reservada. Escolha Padrão para reservar capacidade em hardware compartilhado ou Dedicado para reservar capacidade em hardware dedicado a sua conta.
   e. Contagem total de instâncias: o número de instâncias para as quais reservar capacidade. Se você especificar uma quantidade que exceda sua cota de instâncias sob demanda restante para o tipo de instância selecionada, a solicitação falhará.
4. Defina as seguintes configurações na seção Reservation details (Detalhes da reserva):
   a. A reserva de capacidade começa: escolha Em um horário específico.
   b. Data de início: especifique a data e a hora em que a reserva de capacidade deve ficar disponível para uso. Para obter mais informações, consulte Data e hora de início.
   c. Duração do compromisso: especifique a duração mínima pela qual você se compromete a manter a reserva de capacidade após a entrega. Para obter mais informações, consulte Duração do compromisso.
   d. Término da reserva de capacidade: escolha uma das seguintes opções:
      - Quando eu cancelar: reserve a capacidade até que você a cancele explicitamente.

- Horário específico: cancele a reserva de capacidade automaticamente na data e na hora especificadas.

5. Escolha Criar.

AWS CLI

Para criar uma reserva de capacidade

Use o comando create-capacity-reservation.

```
aws ec2 create-capacity-reservation \
    --availability-zone az_name \
    --instance-type instance_type \
    --instance-count number_of_instances \
    --instance-platform operating_system \
    --instance-match-criteria targeted \
    --delivery-preference incremental \
    --commitment-duration commitment_in_seconds \
    --start-date YYYY-MMDDThh:mm:ss.sssZ
```

PowerShell

Para criar uma reserva de capacidade

Use o cmdlet Add-EC2CapacityReservation.

```
Add-EC2CapacityReservation `
    -AvailabilityZone az_name `
    -InstanceType instance_type `
    -InstanceCount number_of_instances `
    -InstancePlatform operating_system `
    -InstanceMatchCriterion targeted `
    -DeliveryPreference incremental `
    -CommitmentDuration commitment_in_seconds `
    -StartDate  YYYY-MMDDThh:mm:ss.sssZ
```

Visualizar o estado de uma reserva de capacidade

O Amazon EC2 monitora constantemente o estado das reservas de capacidade.

Devido ao modelo de consistência eventual seguido pela API do Amazon EC2, depois de criar uma reserva de capacidade, até cinco minutos poderão ser necessários para o estado da reserva de capacidade refletir que é `active`. Durante esse período, a reserva de capacidade pode permanecer no estado `pending`. No entanto, ela já pode estar disponível para uso. Nesse caso, as tentativas de iniciar instâncias na reserva de capacidade seriam bem-sucedidas.

Console

Para visualizar suas reservas de capacidade

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Reservas de Capacidade.
3. Selecione a reserva de capacidade.

AWS CLI

Para descrever suas reservas de capacidade

Use o comando describe-capacity-reservations.

Por exemplo, o comando a seguir descreve todas as Reservas de Capacidade.

```
aws ec2 describe-capacity-reservations
```

O seguinte é um exemplo de saída.

```
{
    "CapacityReservations": [
        {
            "CapacityReservationId": "cr-1234abcd56EXAMPLE",
            "EndDateType": "unlimited",
            "AvailabilityZone": "eu-west-1a",
            "InstanceMatchCriteria": "open",
            "Tags": [],
            "EphemeralStorage": false,
            "CreateDate": "2019-08-16T09:03:18.000Z",
            "AvailableInstanceCount": 1,
            "InstancePlatform": "Linux/UNIX",
            "TotalInstanceCount": 1,
            "State": "active",
```

```
            "Tenancy": "default",
            "EbsOptimized": true,
            "InstanceType": "a1.medium",
            "PlacementGroupArn": "arn:aws:ec2:us-east-1:123456789012:placement-
group/MyPG"
        },
        {
            "CapacityReservationId": "cr-abcdEXAMPLE9876ef",
            "EndDateType": "unlimited",
            "AvailabilityZone": "eu-west-1a",
            "InstanceMatchCriteria": "open",
            "Tags": [],
            "EphemeralStorage": false,
            "CreateDate": "2019-08-07T11:34:19.000Z",
            "AvailableInstanceCount": 3,
            "InstancePlatform": "Linux/UNIX",
            "TotalInstanceCount": 3,
            "State": "cancelled",
            "Tenancy": "default",
            "EbsOptimized": true,
            "InstanceType": "m5.large"
        }
    ]
}
```

PowerShell

Para descrever uma reserva de capacidade

Use o cmdlet Get-EC2CapacityReservation.

```
Get-EC2CapacityReservation `
    -CapacityReservationId cr-1234abcd56EXAMPLE
```

Estados de reservas de capacidade

Os estados possíveis das reservas de capacidade são descritos a seguir.

Estado	Descrição
`active`	a capacidade está disponível para uso.

Estado	Descrição
`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. 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 que não são válidos, restrições da capacidade ou restrições de limite da instância. É possível visualizar uma solicitação com falha por 60 minutos.
`scheduled`	(Somente reservas de capacidade com data futura) A solicitação de reserva de capacidade com data futura foi aprovada e a reserva de capacidade está programada para entrega na data de início solicitada.
`assessing`	(Somente reservas de capacidade com data futura) O Amazon EC2 está avaliando sua solicitação de reserva de capacidade com data futura. Para obter mais informações, consulte Avaliação da reserva de capacidade com data futura.
`delayed`	(Somente reservas de capacidade com data futura) O Amazon EC2 encontrou um atraso no provisionamento da reserva de capacidade com data futura solicitada. O Amazon EC2 não consegue entregar a capacidade solicitada na data e hora de início solicitadas.
`unsupported`	(Somente reservas de capacidade com data futura) O Amazon EC2 não pode atender à solicitação de reserva de capacidade com data futura devido a restrições de capacidade. É possível visualizar as solicitações não atendidas por 30 dias. A reserva de capacidade não será entregue.

Iniciar instâncias em uma Reserva de capacidade existente

Só é possível iniciar uma instância em uma reserva de capacidade que:

- Tenha atributos correspondentes (tipo de instância, plataforma, zona de disponibilidade e locação)
- Tenha capacidade disponível suficiente
- Esteja no estado `active`

Ao executar uma instância, é possível especificar se deseja executá-la em qualquer Reserva de capacidade `open`, em uma Reserva de capacidade específica ou em um grupo de Reservas de Capacidade.

Se preferir, configure a instância para evitar a execução em um Reserva de capacidade, mesmo que você tenha uma Reserva de capacidade `open` com atributos correspondentes e capacidade disponível.

A execução de uma instância em uma Reserva de capacidade reduz a capacidade disponível pelo número de instâncias executadas. Por exemplo, se você executar três instâncias, a capacidade disponível da Reserva de capacidade será reduzida em três.

Console

Para iniciar instâncias em uma reserva de capacidade existente

1. Siga o procedimento para executar uma instância, mas não execute a instância até concluir as etapas a seguir para especificar as configurações para o grupo de posicionamento e a reserva de capacidade.
2. Expanda os Detalhes avançados e faça o seguinte:

   a. Em Grupo de posicionamento, selecione o grupo de posicionamento de cluster no qual deseja executar a instância.

   b. Em Capacity Reservation (Reserva de capacidade), escolha uma das seguintes opções dependendo da configuração da reserva de capacidade:

      - Nenhuma: impede que as instâncias sejam executadas em uma reserva de capacidade. As instâncias são executadas na capacidade sob demanda.
      - Aberta: executa as instâncias em qualquer reserva de capacidade que tenha atributos correspondentes e capacidade suficiente para o número de instâncias selecionadas.

Se você não tiver uma Reserva de capacidade correspondente com capacidade suficiente, a instância usará a capacidade sob demanda.

- Especificar reserva de capacidade: inicia as instâncias na reserva de capacidade selecionada. Se a Reserva de capacidade selecionada não tiver capacidade suficiente para o número de instâncias selecionadas, a execução da instância falhará.
- Especificar grupo de recursos de reserva de capacidade: inicia as instâncias em qualquer reserva de capacidade com atributos correspondentes e capacidade disponível no grupo de reserva de capacidade selecionado. Se o grupo selecionado não tiver uma Reserva de capacidade com atributos correspondentes e capacidade disponível, as instâncias serão executadas na capacidade sob demanda.
- Especificar somente reserva de capacidade: inicia as instâncias em uma reserva de capacidade. Se um ID de reserva de capacidade não for especificado, as instâncias serão iniciadas em uma reserva de capacidade aberta. Se a capacidade não estiver disponível, as instâncias falharão ao iniciar.
- Especificar somente grupo de recursos de reserva de capacidade: inicia as instâncias em uma reserva de capacidade em um grupo de recursos de reserva de capacidade. Se um ARN de grupo de recursos de reserva de capacidade não for especificado, as instâncias serão iniciadas em uma reserva de capacidade aberta. Se a capacidade não estiver disponível, as instâncias falharão ao iniciar.

3. No painel Resumo, analise a configuração da instância e selecione Iniciar instância.

AWS CLI

Para iniciar uma instância em uma reserva de capacidade existente

Use o comando run-instances e especifique a opção `--capacity-reservation-specification`.

O exemplo a seguir executa uma instância em qualquer reserva de capacidade aberta com atributos correspondentes e capacidade disponível:

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --count 1 \
    --instance-type t2.micro \
    --key-name my-key-pair \
    --subnet-id subnet-0abcdef1234567890 \
```

```
    --capacity-reservation-specification CapacityReservationPreference=open
```

O exemplo a seguir executa uma instância em uma reserva de capacidade `targeted`:

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --count 1 \
    --instance-type t2.micro \
    --key-name my-key-pair \
    --subnet-id subnet-0abcdef1234567890 \
    --capacity-reservation-specification \
        CapacityReservationTarget={CapacityReservationId=cr-1234abcd56EXAMPLE}
```

O exemplo a seguir executa uma instância no grupo de reserva de capacidade especificado:

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --count 1 \
    --instance-type t2.micro \
    --key-name my-key-pair \
    --subnet-id subnet-0abcdef1234567890 \
    --capacity-reservation-specification \

 CapacityReservationTarget={CapacityReservationResourceGroupArn=arn:aws:resource-
groups:us-west-2:123456789012:group/my-cr-group}
```

O exemplo a seguir inicia uma instância somente em uma reserva de capacidade. Como o ID da reserva de capacidade não é especificado, a instância é iniciada em qualquer reserva de capacidade aberta com atributos correspondentes e capacidade disponível:

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --count 1 \
    --instance-type t2.micro \
    --key-name my-key-pair \
    --subnet-id subnet-0abcdef1234567890 \
    --capacity-reservation-specification \
        CapacityReservationPreference=capacity-reservations-only
```

O exemplo a seguir inicia uma instância somente em uma reserva de capacidade específica. Se a capacidade não estiver disponível na reserva de capacidade especificada, a instância falhará ao iniciar.

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --count 1 \
    --instance-type t2.micro \
    --key-name my-key-pair \
    --subnet-id subnet-0abcdef1234567890 \
    --capacity-reservation-specification \
        CapacityReservationPreference=capacity-reservations-only \
        CapacityReservationTarget={CapacityReservationId=cr-1234abcd56EXAMPLE}
```

PowerShell

Para iniciar uma instância em uma reserva de capacidade existente

Use o cmdlet New-EC2Instance.

O exemplo a seguir executa uma instância em qualquer reserva de capacidade aberta com atributos correspondentes e capacidade disponível:

```
New-EC2Instance `
    -ImageId ami-0abcdef1234567890 `
    -InstanceType t2.micro `
    -KeyName "my-key-pair" `
    -SubnetId subnet-0abcdef1234567890 `
    -CapacityReservationSpecification_CapacityReservationPreference "open"
```

O exemplo a seguir executa uma instância em uma reserva de capacidade `targeted`:

```
New-EC2Instance `
    -ImageId ami-0abcdef1234567890 `
    -InstanceType t2.micro `
    -KeyName "my-key-pair" `
    -SubnetId subnet-0abcdef1234567890 `
    -CapacityReservationTarget_CapacityReservationId cr-1234abcd56EXAMPLE
```

O exemplo a seguir executa uma instância no grupo de reserva de capacidade especificado:

```
New-EC2Instance `
```

```
    -ImageId ami-0abcdef1234567890 `
    -InstanceType t2.micro `
    -KeyName "my-key-pair" `
    -SubnetId subnet-0abcdef1234567890 `
    -CapacityReservationTarget_CapacityReservationResourceGroupArn `
        "arn:aws:resource-groups:us-west-2:123456789012:group/my-cr-group"
```

O exemplo a seguir inicia uma instância somente em uma reserva de capacidade. Como o ID da reserva de capacidade não é especificado, a instância é iniciada em qualquer reserva de capacidade aberta com atributos correspondentes e capacidade disponível:

```
New-EC2Instance `
    -ImageId ami-0abcdef1234567890 `
    -InstanceType t2.micro `
    -KeyName "my-key-pair" `
    -SubnetId subnet-0abcdef1234567890 `
    -CapacityReservationSpecification_CapacityReservationPreference "capacity-
reservations-only"
```

O exemplo a seguir inicia uma instância somente em uma reserva de capacidade específica. Se a capacidade não estiver disponível na reserva de capacidade especificada, a instância falhará ao iniciar.

```
New-EC2Instance `
    -ImageId ami-0abcdef1234567890 `
    -InstanceType t2.micro `
    -KeyName "my-key-pair" `
    -SubnetId subnet-0abcdef1234567890 `
    -CapacityReservationSpecification_CapacityReservationPreference "capacity-
reservations-only" `
    -CapacityReservationTarget_CapacityReservationId cr-1234abcd56EXAMPLE
```

Modificar uma reserva de capacidade ativa

Se você tiver uma reserva de capacidade existente que não seja adequada para a workload que precisa da capacidade, você pode modificar a quantidade e a elegibilidade da instância (`open` ou `targeted`) e a hora de término (`At specific time` ou `Manually`). Se você especificar uma nova quantidade de instâncias que exceda seu limite de instância sob demanda restante para o tipo de instância selecionada, a atualização falhará.

As modificações permitidas dependem do estado da reserva de capacidade:

- Estado `assessing` ou `scheduled`: você pode modificar somente as tags.
- Estado `pending`: você não pode modificar a reserva de capacidade de forma alguma.
- Estado `active`, mas ainda dentro da duração do compromisso: você não pode diminuir a contagem de instâncias abaixo da contagem de instâncias confirmadas, nem definir uma data de término anterior à duração confirmada. Todas as outras modificações são permitidas.
- Estado `active` sem duração de compromisso ou duração de compromisso expirada: todas as modificações são permitidas.
- Estados `expired`, `cancelled`, `unsupported` ou `failed`: você não pode modificar a reserva de capacidade de forma alguma.

Considerações

- Não é possível alterar o tipo de instância, a plataforma, a zona de disponibilidade nem a locação após a criação. Se for necessário modificar qualquer um desses atributos, recomendamos cancelar a reserva e, em seguida, criar uma nova com os atributos necessários.
- Se você modificar uma reserva de capacidade existente ao alterar a elegibilidade da instância de `targeted` para `open`, todas as instâncias em execução que correspondam aos atributos da reserva de capacidade, que tenham o parâmetro `CapacityReservationPreference` definido como `open` e que ainda não estejam em execução na reserva de capacidade usarão a reserva de capacidade modificada automaticamente.
- Para alterar a elegibilidade da instância, a reserva de capacidade deve estar completamente ociosa (uso zero) porque o Amazon EC2 não pode modificar a elegibilidade de uma instância quando as instâncias estão sendo executadas dentro da reserva.

Console

Para modificar uma reserva de capacidade

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 a capacidade total, o fim da reserva de capacidade ou as opções de elegibilidade da instância, conforme necessário, e escolha Salvar.

AWS CLI

Para modificar uma reserva de capacidade

Use o comando modify-capacity-reservation. O exemplo a seguir modifica a reserva de capacidade especificada para reservar capacidade para oito instâncias.

```
aws ec2 modify-capacity-reservation \
    --capacity-reservation-id cr-1234567890abcdef0 \
    --instance-count 8
```

PowerShell

Para modificar uma reserva de capacidade

Use o cmdlet Edit-EC2CapacityReservation. O exemplo a seguir modifica a reserva de capacidade especificada para reservar capacidade para oito instâncias.

```
Edit-EC2CapacityReservation `
    -CapacityReservationId cr-1234567890abcdef0 `
    -InstanceCount 8
```

Modificar as configurações de reserva de capacidade da instância

É possível modificar as configurações da Reserva de capacidade a seguir para uma instância interrompida a qualquer momento:

- Inicie em qualquer reserva de capacidade que tenha atributos correspondentes (por exemplo, tipo de instância, plataforma, zona de disponibilidade e locação) e capacidade disponível.
- Execute a instância em uma Reserva de capacidade específica.
- Inicie em qualquer reserva de capacidade que tenha atributos correspondentes e capacidade disponível em um grupo de reserva de capacidade
- Impeça que a instância seja iniciada em uma Reserva de capacidade.

Console

Para modificar as configurações de reserva de capacidade de uma instância

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

2. Escolha Instances (Instâncias) e selecione a instância a ser modificada. Interrompa a instância se ela ainda não tiver sido interrompida.
3. Escolha Ações, Configurações da instância, Modificar configurações da reserva de capacidade.
4. Para Reserva de capacidade, selecione uma das seguintes opções:

   - Aberta: executa as instâncias em qualquer reserva de capacidade que tenha atributos correspondentes e capacidade suficiente para o número de instâncias selecionadas. Se você não tiver uma Reserva de capacidade correspondente com capacidade suficiente, a instância usará a capacidade sob demanda.
   - Nenhuma: impede que as instâncias sejam executadas em uma reserva de capacidade. As instâncias são executadas na capacidade sob demanda.
   - Especificar reserva de capacidade: inicia as instâncias na reserva de capacidade selecionada. Se a Reserva de capacidade selecionada não tiver capacidade suficiente para o número de instâncias selecionadas, a execução da instância falhará.
   - Especificar grupo de reserva de capacidade: executa as instâncias em qualquer reserva de capacidade com atributos correspondentes e capacidade disponível no grupo de reserva de capacidade selecionado. Se o grupo selecionado não tiver uma Reserva de capacidade com atributos correspondentes e capacidade disponível, as instâncias serão executadas na capacidade sob demanda.
   - Especificar somente reserva de capacidade: inicia as instâncias em uma reserva de capacidade. Se um ID de reserva de capacidade não for especificado, as instâncias serão iniciadas em uma reserva de capacidade aberta. Se a capacidade não estiver disponível, as instâncias falharão ao iniciar.
   - Especificar somente grupo de recursos de reserva de capacidade: inicia as instâncias em uma reserva de capacidade em um grupo de recursos de reserva de capacidade. Se um ARN de grupo de recursos de reserva de capacidade não for especificado, as instâncias serão iniciadas em uma reserva de capacidade aberta. Se a capacidade não estiver disponível, as instâncias falharão ao iniciar.

AWS CLI

Para modificar as configurações de reserva de capacidade de uma instância

Use o comando modify-instance-capacity-reservation-attributes.

O exemplo a seguir altera a preferência de reserva de capacidade para `none`.

```
aws ec2 modify-instance-capacity-reservation-attributes \
    --instance-id i-1234567890abcdef0 \
    --capacity-reservation-specification CapacityReservationPreference=none
```

O exemplo a seguir altera o destino para uma reserva de capacidade específica.

```
aws ec2 modify-instance-capacity-reservation-attributes \
    --instance-id i-1234567890abcdef0 \
    --capacity-reservation-specification \
    CapacityReservationTarget={CapacityReservationId=cr-1234567890abcdef0}
```

O exemplo a seguir altera o destino para um grupo de reserva de capacidade específico.

```
aws ec2 modify-instance-capacity-reservation-attributes \
    --instance-id i-1234567890abcdef0 \
    --capacity-reservation-specification \

 CapacityReservationTarget={CapacityReservationResourceGroupArn=arn:aws:resource-
groups:us-west-2:123456789012:group/my-cr-group}
```

O exemplo a seguir altera a preferência de reserva de capacidade para `capacity-reservation-only`. Como uma reserva de capacidade não é especificada, as instâncias são iniciadas em qualquer reserva de capacidade aberta com atributos correspondentes e capacidade disponível.

```
aws ec2 modify-instance-capacity-reservation-attributes \
    --instance-id i-1234567890abcdef0 \
    --capacity-reservation-specification CapacityReservationPreference=capacity-
reservation-only
```

O exemplo a seguir altera a preferência de reserva de capacidade para `capacity-reservation-only` e altera o destino para uma reserva de capacidade específica. Se a capacidade não estiver disponível na reserva de capacidade especificada, as instâncias falharão ao iniciar.

```
aws ec2 modify-instance-capacity-reservation-attributes \
    --instance-id i-1234567890abcdef0 \
    --capacity-reservation-specification \
```

```
        CapacityReservationPreference=capacity-reservation-only \
        CapacityReservationTarget={CapacityReservationId=cr-1234567890abcdef0}
```

PowerShell

Para modificar as configurações de reserva de capacidade de uma instância

Use o cmdlet Edit-EC2InstanceCapacityReservationAttribute.

O exemplo a seguir altera a preferência de reserva de capacidade para none.

```
Edit-EC2InstanceCapacityReservationAttribute `
    -InstanceId i-1234567890abcdef0 `
    -CapacityReservationSpecification_CapacityReservationPreference "none"
```

O exemplo a seguir altera o destino para uma reserva de capacidade específica.

```
Edit-EC2InstanceCapacityReservationAttribute `
    -InstanceId i-1234567890abcdef0 `
    -CapacityReservationTarget_CapacityReservationId cr-1234567890abcdef0
```

O exemplo a seguir altera o destino para um grupo de reserva de capacidade específico.

```
Edit-EC2InstanceCapacityReservationAttribute `
    -InstanceId i-1234567890abcdef0 `
    -CapacityReservationTarget_CapacityReservationResourceGroupArn `
        "arn:aws:resource-groups:us-west-2:123456789012:group/my-cr-group"
```

O exemplo a seguir altera a preferência de reserva de capacidade para `capacity-reservation-only`. Como uma reserva de capacidade não é especificada, as instâncias são iniciadas em qualquer reserva de capacidade aberta com atributos correspondentes e capacidade disponível.

```
Edit-EC2InstanceCapacityReservationAttribute `
    -InstanceId i-1234567890abcdef0 `
    -CapacityReservationSpecification_CapacityReservationPreference "capacity-
reservation-only"
```

O exemplo a seguir altera a preferência de reserva de capacidade para `capacity-reservation-only` e altera o destino para uma reserva de capacidade específica. Se a

capacidade não estiver disponível na reserva de capacidade especificada, as instâncias falharão ao iniciar.

```
Edit-EC2InstanceCapacityReservationAttribute `
    -InstanceId i-1234567890abcdef0 `
    -CapacityReservationSpecification_CapacityReservationPreference "capacity-
reservation-only" `
    -CapacityReservationTarget_CapacityReservationId cr-1234567890abcdef0
```

Mover a capacidade entre reservas de capacidade

É possível mover a capacidade de uma reserva de capacidade para outra a fim de redistribuir seus recursos de computação reservados conforme necessário. Por exemplo, se precisar de capacidade adicional em uma reserva com uso crescente e tiver capacidade disponível em outra reserva, poderá realocar essa capacidade entre as duas reservas.

Pré-requisitos para mover a capacidade

Como pré-requisito, as duas reservas de capacidade devem atender às seguintes condições:

- As duas reservas devem estar no estado ativo.
- As duas reservas devem ser de propriedade da sua Conta da AWS. Você não pode mover a capacidade entre reservas pertencentes a diferentes Contas da AWS.
- As duas reservas devem ser iguais em:
  - Tipo de instância
  - Plataforma
  - Zona de disponibilidade
  - Locação
  - Grupo de posicionamento
  - End Time

A elegibilidade da instância das reservas de capacidade de destino (`open` ou `targeted`) e as tags não precisam corresponder à reserva de origem. A configuração das duas reservas permanece a mesma, exceto que a reserva de origem reduziu a capacidade e a reserva de destino aumentou a capacidade.

Quando você especifica a quantidade de instâncias a serem movidas, por padrão, qualquer capacidade disponível é movida primeiro, seguida por qualquer instância em execução elegível (a capacidade usada na sua reserva). Por exemplo, se você mover quatro instâncias de uma reserva com cinco instâncias usadas e três instâncias disponíveis, as três instâncias disponíveis e uma instância usada serão movidas.

> **Note**
>
> Quando você move a capacidade usada de sua reserva especificando uma Quantidade a ser movida que seja maior do que a capacidade disponível, somente as instâncias que foram iniciadas com a Especificação de reserva de capacidade como `open` serão movidas.

Considerações

As seguintes considerações são aplicáveis ao mover a capacidade de uma reserva para outra:

- A capacidade usada só pode ser movida entre reservas de capacidade com elegibilidade de instância `open` compartilhadas com o mesmo conjunto de contas.
- Ao mover a capacidade usada, as instâncias elegíveis são selecionadas aleatoriamente. Não é possível especificar quais instâncias em execução serão movidas. Se não for encontrado um número suficiente de instâncias elegíveis para atender à quantidade a ser movida, a operação de movimentação falhará.
- Se você mover toda a capacidade da reserva de origem, a reserva de capacidade será automaticamente cancelada.
- Reservas de capacidade com data futura: não é possível mover a capacidade de uma reserva de capacidade com data futura durante o período de compromisso.

> **Note**
>
> Não há suporte para mover a capacidade de um bloco de capacidade.

mover capacidade

É possível mover capacidade de uma reserva de capacidade de origem para uma reserva de capacidade de destino.

Console

Para mover capacidade

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Reservas de capacidade.
3. Selecione um ID de reserva de capacidade sob demanda que tenha capacidade para movimentação.
4. Em Ações, Gerenciar capacidade, escolha Mover.
5. Na página Mover capacidade, em Reserva de capacidade de destino, selecione uma reserva na lista.
6. Em Quantidade a ser movida, use o controle deslizante ou digite o número de instâncias a serem movidas da reserva de capacidade de origem para a reserva de capacidade de destino.
7. Revise o resumo e, quando estiver pronto, escolha Mover.

AWS CLI

Para mover capacidade

Use o comando move-capacity-reservation-instances. O exemplo a seguir move dez instâncias da reserva de capacidade de origem especificada para a reserva de capacidade de destino especificada.

```
aws ec2 move-capacity-reservation-instances \
    --source-capacity-reservation-id cr-1234567890abcdef0 \
    --destination-capacity-reservation-id cr-021345abcdef56789 \
    --instance-count 10
```

PowerShell

Para mover capacidade

Use o cmdlet Move-EC2CapacityReservationInstance. O exemplo a seguir move dez instâncias da reserva de capacidade de origem especificada para a reserva de capacidade de destino especificada.

```
Move-EC2CapacityReservationInstance `
```

```
    -SourceCapacityReservationId cr-1234567890abcdef0 `
    -DestinationCapacityReservationId cr-021345abcdef56789 `
    -InstanceCount 10
```

Dividir a capacidade de uma reserva de capacidade existente

É possível dividir a capacidade de uma reserva de capacidade existente e criar uma nova. Ao dividir a capacidade, você aloca uma parte da reserva original para uma workload específica ou a compartilha com outra Conta da AWS. Por exemplo, para compartilhar parcialmente uma reserva de capacidade com outra conta, você pode dividir parte da capacidade para criar uma reserva de capacidade menor. A reserva de capacidade menor pode então ser compartilhada com a outra conta usando o AWS Resource Access Manager.

Ao separar a capacidade de uma reserva de capacidade existente, uma nova reserva de capacidade será criada automaticamente. A reserva existente permanecerá inalterada, exceto pela redução da capacidade total em relação ao número de instâncias divididas. As instâncias que estão em execução na reserva de capacidade existente não são afetadas. É possível dividir a reserva existente em apenas uma nova reserva de capacidade.

A nova reserva de capacidade terá a mesma configuração da reserva de capacidade existente, exceto pelas tags. Por padrão, a nova reserva de capacidade não tem nenhuma tag. É possível especificar novas tags durante a operação de divisão. A nova reserva de capacidade também pode ser modificada depois de criada, se necessário.

Quando você especifica a quantidade de instâncias a serem divididas, por padrão, qualquer capacidade disponível é dividida primeiro, seguida por qualquer instância em execução elegível (a capacidade usada na sua reserva). Por exemplo, se você dividir quatro instâncias de uma reserva de capacidade com cinco instâncias usadas e três instâncias disponíveis, as três instâncias disponíveis e uma instância usada serão divididas em uma nova reserva.

Pré-requisitos para dividir a capacidade

Como pré-requisito, sua reserva de capacidade deve atender às seguintes condições:

- A reserva de origem deve estar no estado ativo.
- A reserva de origem deve pertencer a sua Conta da AWS.

> **Note**
>
> Quando você divide a capacidade usada da sua reserva especificando uma Quantidade a ser dividida que seja maior do que a capacidade disponível, somente as instâncias que foram iniciadas com a Especificação de reserva de capacidade como `open` serão divididas.

Considerações

As seguintes considerações são aplicáveis ao dividir a capacidade de uma reserva para outra:

- A capacidade usada só pode ser dividida em reservas de capacidade com elegibilidade de instância "aberta" que não sejam compartilhadas com nenhuma conta.
- Ao dividir a capacidade usada, as instâncias elegíveis são selecionadas aleatoriamente. Não é possível especificar quais instâncias em execução serão divididas. Se não for encontrado um número suficiente de instâncias elegíveis para atender à quantidade a ser dividida, a operação de divisão falhará.
- A quantidade máxima de instâncias a serem divididas de uma reserva existente é o tamanho da reserva menos um. Por exemplo, se a capacidade total da sua reserva for de cinco instâncias, será possível dividir no máximo quatro instâncias em uma nova reserva.
- Reservas de capacidade com data futura: não é possível dividir a capacidade de uma reserva de capacidade com data futura durante o período de compromisso.
- Grupos de recursos: se a reserva de capacidade existente pertencer a um grupo de recursos, a nova reserva de capacidade não será adicionada automaticamente ao grupo de recursos. É possível adicionar a nova reserva de capacidade a um grupo de recursos após sua criação, se necessário.
- Compartilhamento: se a reserva de capacidade existente for compartilhada com uma conta de consumidor, a nova reserva de capacidade não será compartilhada automaticamente com a conta do consumidor. É possível compartilhar a nova reserva de capacidade depois de criada, se necessário.
- Grupo de posicionamento de cluster: se a reserva de capacidade existente fizer parte de um grupo de posicionamento de cluster, a nova reserva de capacidade será criada no mesmo grupo de posicionamento de cluster.

> **Note**
>
> A divisão da capacidade de um bloco de capacidade não é compatível.

Controlar o acesso para dividir reservas de capacidade usando tags

É possível usar tags para controlar o acesso aos recursos do Amazon EC2, incluindo dividir a capacidade de uma reserva de capacidade existente para criar uma reserva de capacidade. Para obter mais informações, consulte Controlar o acesso a recursos da AWS usando tags no Guia do usuário do IAM.

Para controlar o acesso para dividir uma reserva de capacidade usando tags, certifique-se de especificar as tags de recurso e de solicitação na instrução de política, pois as políticas do IAM são avaliadas em relação à reserva de capacidade de origem e à reserva de capacidade recém-criada. O exemplo de política a seguir inclui a chave de condição `ec2:ResourceTag` com a tag `Owner=ExampleDepartment1` para a reserva de capacidade de origem e a chave de condição `ec2:RequestTag` com a tag `stack=production` para a reserva de capacidade recém-criada.

```
{
  "Statement": [
    {
      "Sid": "AllowSourceCapacityReservation",
      "Effect": "Allow",
      "Action": "ec2:CreateCapacityReservationBySplitting",
      "Resource": "arn:aws:ec2:us-east-1:111122223333:capacity-reservation/
cr-1234567890abcdef0",
      "Condition": {
        "StringEquals": {
          "ec2:ResourceTag/Owner": "ExampleDepartment1"
        }
      }
    },
    {
      "Sid": "AllowNewlyCreatedCapacityReservation",
      "Effect": "Allow",
      "Action": ["ec2:CreateCapacityReservationBySplitting", "ec2:CreateTags"],
      "Resource": "arn:aws:ec2:us-east-1:111122223333:capacity-reservation/*",
      "Condition": {
        "StringEquals": {
```

```
          "aws:RequestTag/stack": "production"
        }
      }
    }
  ]
}
```

Dividir a capacidade

É possível dividir a capacidade de uma reserva de capacidade existente para criar uma nova.

Console

Para dividir a capacidade

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Reservas de capacidade.
3. Selecione um ID de reserva de capacidade sob demanda que tenha capacidade para divisão.
4. Em Ações, Gerenciar capacidade, escolha Dividir.
5. Na página Dividir reserva de capacidade, em Quantidade a ser dividida, use o controle deslizante ou digite o número de instâncias para dividir da reserva atual.
6. (Opcional) Adicione tags para a nova reserva de capacidade.
7. Revise o resumo e, quando estiver pronto, escolha Dividir.

AWS CLI

Para dividir a capacidade

Use o comando `create-capacity-reservation-by-splitting`. O exemplo a seguir cria uma nova reserva de capacidade dividindo dez instâncias da reserva de capacidade especificada.

```
aws ec2 create-capacity-reservation-by-splitting \
    --source-capacity-reservation-id cr-1234567890abdef0 \
    --instance-count 10
```

PowerShell

Para dividir a capacidade

Use o cmdlet New-EC2CapacityReservationBySplitting. O exemplo a seguir cria uma nova reserva de capacidade dividindo dez instâncias da reserva de capacidade especificada.

```
New-EC2CapacityReservationBySplitting `
    -SourceCapacityReservationId cr-1234567890abdef0 `
    -InstanceCount 10
```

Cancelar uma Reserva de capacidade

É possível cancelar uma reserva de capacidade que esteja em um dos estados a seguir:

- `assessing`
- `active` e não há duração de compromisso ou a duração do compromisso expirou. Você não pode cancelar uma reserva de capacidade com data futura durante a vigência do compromisso.

> **Note**
>
> Não é possível modificar nem cancelar um bloco de capacidade. Para obter mais informações, consulte Blocos de capacidade para ML.

Se uma reserva de capacidade com data futura entrar no estado `delayed`, a duração do compromisso será dispensada e será possível cancelá-la assim que ela entrar no estado `active`.

Quando você cancela uma Reserva de capacidade, a capacidade é liberada imediatamente e não é mais reservada para seu uso.

É possível 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 tarifas padrão de instância sob demanda ou em uma tarifa com desconto, se você tiver um Savings Plan ou uma instância reservada regional correspondente.

Depois que você cancela uma Reserva de capacidade, as instâncias que a usavam como destino não podem mais ser executadas. Modifique essas instâncias para que elas tenham outra Reserva de

capacidade como destino, sejam executadas em uma Reserva de capacidade aberta com atributos correspondentes e capacidade suficiente ou evitem a execução em uma Reserva de capacidade. Para obter mais informações, consulte Modificar as configurações de reserva de capacidade da instância.

Console

Para cancelar uma reserva de capacidade

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).

AWS CLI

Para cancelar uma reserva de capacidade

Use o comando cancel-capacity-reservation.

```
aws ec2 cancel-capacity-reservation \
    --capacity-reservation-id cr-1234567890abcdef0
```

PowerShell

Para cancelar uma reserva de capacidade

Use o cmdlet Remove-EC2CapacityReservation.

```
Remove-EC2CapacityReservation `
    -CapacityReservationId cr-1234567890abcdef0
```

Usar reservas de capacidade em grupos de posicionamento de cluster

É possível criar reservas de capacidade em um grupo de posicionamento de cluster para reservar a capacidade computacional do Amazon EC2 para suas workloads. Os grupos de posicionamento de cluster oferecem o benefício de baixa latência de rede e alta throughput de rede.

Criar uma reserva de capacidade em um grupo de posicionamento de cluster garante que você tenha acesso à capacidade de computação nos grupos de posicionamento de cluster quando

precisar dela, pelo tempo necessário. Isso é ideal para reservar capacidade para workloads de alta performance (HPC) que exigem escalabilidade computacional. Isso permite que você diminua a escala do cluster, garantindo que a capacidade permaneça disponível para seu uso, para que você possa escalar o backup quando necessário.

Depois de criar uma reserva de capacidade em um grupo de posicionamento de cluster, você pode compartilhá-la com outras contas da AWS. Para obter mais informações, consulte Compartilhar reservas de capacidade em grupos de posicionamento de cluster.

Tópicos

- Limitações
- Trabalhar com reservas de capacidade em grupos de posicionamento de cluster
- Compartilhar reservas de capacidade em grupos de posicionamento de cluster

Limitações

Lembre-se do seguinte ao criar reservas de capacidade em grupos de posicionamento de cluster:

- Se uma reserva de capacidade existente não estiver em um grupo de posicionamento, não será possível modificar a reserva de capacidade para reservar capacidade em um grupo de posicionamento. Para reservar capacidade em um grupo de posicionamento, crie a reserva de capacidade no grupo de posicionamento.
- Depois de criar uma reserva de capacidade em um grupo de posicionamento, você não poderá modificá-la para reservar capacidade fora do grupo de posicionamento.
- É possível aumentar sua capacidade reservada em um grupo de posicionamento modificando uma reserva de capacidade existente no grupo de posicionamento ou criando reservas de capacidade adicionais no grupo de posicionamento. No entanto, você aumenta suas chances de obter um erro de capacidade insuficiente.
- É possível compartilhar as reservas de capacidade somente a partir dos grupos de posicionamento de cluster de sua propriedade. Não é possível compartilhar as reservas de capacidade a partir de grupos de posicionamento de cluster que não sejam de sua propriedade.
- Não é possível excluir um grupo de posicionamento de cluster que tenha reservas de capacidade `active`. É necessário cancelar todas as reservas de capacidade no grupo de posicionamento de cluster antes de excluí-las.

Trabalhar com reservas de capacidade em grupos de posicionamento de cluster

Para começar a usar reservas de capacidade com grupos de posicionamento de cluster, execute as etapas a seguir.

> **Note**
>
> Se você quiser criar uma reserva de capacidade em um grupo de posicionamento de cluster existente, pule a Etapa 1. Em seguida, para as Etapas 2 e 3, especifique o ARN do grupo de posicionamento de cluster existente.

Tarefas

- Etapa 1: (condicional) crie um grupo de posicionamento de cluster para uso com uma reserva de capacidade
- Etapa 2: crie uma reserva de capacidade em um grupo de posicionamento de cluster
- Etapa 3: inicie instâncias em reservas de capacidade em um grupo de posicionamento de cluster

Etapa 1: (condicional) crie um grupo de posicionamento de cluster para uso com uma reserva de capacidade

Execute esta etapa somente se precisar criar um novo grupo de posicionamento de cluster. Para usar um grupo de posicionamento de cluster existente, ignore esta etapa e, em seguida, para as Etapas 2 e 3, use o ARN desse grupo de posicionamento de cluster.

Console

Para criar um grupo de posicionamento de cluster

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Placement Groups (Grupos de posicionamento) e Create placement group (Criar grupo de posicionamento).
3. Em Name (Nome), especifique um nome descritivo para o grupo de posicionamento.
4. Em Placement strategy (Estratégia de posicionamento), escolha Cluster.
5. Escolha Criar grupo.
6. Na tabela Grupos de posicionamento, na coluna ARN do grupo, anote o ARN do grupo de posicionamento em cluster que você criou. Você precisará dela para a próxima etapa.

AWS CLI

Para criar um grupo de posicionamento de cluster

Use o comando create-placement-group.

```
aws ec2 create-placement-group \
    --group-name MyPG \
    --strategy cluster
```

Tome nota do ARN do grupo de posicionamento retornado na saída, pois você precisará dele na próxima etapa.

PowerShell

Para criar um grupo de posicionamento de cluster

Use o cmdlet New-EC2PlacementGroup.

```
New-EC2PlacementGroup `
    -GroupName my-placement-group `
    -Strategy "cluster"
```

Tome nota do ARN do grupo de posicionamento retornado na saída, pois você precisará dele na próxima etapa.

Etapa 2: crie uma reserva de capacidade em um grupo de posicionamento de cluster

Você cria uma reserva de capacidade em um grupo de posicionamento de cluster da mesma forma que você cria qualquer reserva de capacidade. No entanto, você também deve especificar o ARN do grupo de posicionamento de cluster no qual criar a reserva de capacidade.

Considerações

- O grupo de posicionamento de cluster especificado deve estar no estado `available`. Se o grupo de posicionamento de cluster estiver no estado `pending`, `deleting` ou `deleted`, a solicitação falha.
- A reserva de capacidade e o grupo de posicionamento de cluster devem estar na mesma zona de disponibilidade. Se a solicitação para criar a reserva de capacidade especificar uma zona de disponibilidade diferente da do grupo de posicionamento de cluster, a solicitação falhará.

- É possível criar reservas de capacidade somente para tipos de instância com suporte para grupos de posicionamento de cluster. Se você especificar um tipo de instância sem suporte, a solicitação falhará.
- Se você criar uma reserva de capacidade `open` em um grupo de posicionamento de cluster e existirem instâncias em execução que tenham atributos correspondentes (ARN de grupo de posicionamento, tipo de instância, zona de disponibilidade, plataforma e locação), essas instâncias serão executadas automaticamente na reserva de capacidade.
- Sua solicitação de criação de uma Reserva de capacidade poderá falhar se uma das seguintes opções for verdadeira:
  - O Amazon EC2 não tem capacidade suficiente para realizar a solicitação. Tente novamente mais tarde, tente uma zona de disponibilidade diferente ou tente uma capacidade menor. Se a sua workload for flexível entre tipos e tamanhos de instâncias, tente diferentes atributos de instância.
  - A quantidade solicitada excede o limite de instância sob demanda para a família de instâncias selecionada. Aumente o limite de instância sob demanda para a família de instâncias e tente novamente. Para obter mais informações, consulte Cotas de instância sob demanda.

Console

Para criar uma reserva de capacidade

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Selecione Reservas de Capacidade e Create Reserva de capacidade (Criar Reserva de capacidade).
3. Na página Criar uma reserva de capacidade, especifique o tipo de instância, a plataforma, a zona de disponibilidade, a locação, a quantidade e a data de término conforme necessário.
4. Em Grupo de posicionamento, especifique o ARN do grupo de posicionamento de cluster no qual criar a reserva de capacidade.
5. Escolha Criar.

Para obter mais informações, consulte Criar uma Reserva de capacidade.

AWS CLI

Para criar uma reserva de capacidade

Use o comando create-capacity-reservation. Em `--placement-group-arn`, especifique o ARN do grupo de posicionamento de cluster no qual criar a reserva de capacidade.

```
aws ec2 create-capacity-reservation \
    --instance-type instance_type \
    --instance-platform platform \
    --availability-zone-id az_id \
    --instance-count quantity \
    --placement-group-arn "placement_group_arn"
```

PowerShell

Para criar uma reserva de capacidade

Use o cmdlet Add-EC2CapacityReservation. Em `-PlacementGroupArn`, especifique o ARN do grupo de posicionamento de cluster no qual criar a reserva de capacidade.

```
Add-EC2CapacityReservation `
    -InstanceType instance_type `
    -InstancePlatform platform `
    -AvailabilityZoneId az_id `
    -InstanceCount quantity `
    -PlacementGroupArn "placement_group_arn"
```

Etapa 3: inicie instâncias em reservas de capacidade em um grupo de posicionamento de cluster

É possível iniciar uma instância em uma reserva de capacidade em um grupo de posicionamento de cluster usando uma das opções a seguir:

- Especificar o ARN do grupo de posicionamento de cluster no qual iniciar a instância — Quando você fornece o ARN de um grupo de posicionamento de cluster, o Amazon EC2 lança a instância nesse grupo de posicionamento de cluster. É possível usar um dos seguintes métodos:
  - Especificar *open* — Você não precisa especificar a reserva de capacidade na solicitação de início da instância. Se a instância tiver atributos (ARN de grupo de posicionamento, tipo de instância, zona de disponibilidade, plataforma e locação) que correspondam a uma reserva de capacidade no grupo de posicionamento de cluster especificado, a instância será iniciada automaticamente na reserva de capacidade.

  - Especificar a reserva de capacidade — Se a reserva de capacidade aceitar somente iniciar instâncias-alvo, você deverá especificar a reserva de capacidade-alvo além do grupo de posicionamento de cluster na solicitação.
  - Especificar um grupo de reserva de capacidade — Para obter mais informações, consulte Usar reservas de capacidade em grupos de posicionamento de cluster com um grupo de reserva de capacidade.
- Especificar somente um grupo de reserva de capacidade — Para obter mais informações, consulte Usar reservas de capacidade em grupos de posicionamento de cluster com um grupo de reserva de capacidade.
- Especificar somente uma reserva de capacidade — Você pode iniciar instâncias em uma reserva de capacidade em um grupo de posicionamento de cluster.

> **Note**
>
> Quando você executa instâncias especificando somente uma reserva de capacidade ou apenas um grupo de reserva de capacidade, as instâncias são iniciadas nas reservas de capacidade criadas no grupo de posicionamento de cluster, mas as instâncias não são diretamente vinculadas ao grupo de posicionamento de cluster.

Console

Para iniciar instâncias em uma reserva de capacidade existente

1. Siga o procedimento para executar uma instância, mas não execute a instância até concluir as etapas a seguir para especificar as configurações para o grupo de posicionamento e a reserva de capacidade.
2. Expanda os Detalhes avançados e faça o seguinte:
   a. Em Grupo de posicionamento, selecione o grupo de posicionamento de cluster no qual deseja executar a instância.
   b. Em Capacity Reservation (Reserva de capacidade), escolha uma das seguintes opções dependendo da configuração da reserva de capacidade:
      - Aberta: para executar as instâncias em qualquer reserva de capacidade `open` no grupo com posicionamento em cluster que tenha atributos correspondentes e capacidade suficiente.

- Destino por ID: para executar as instâncias em uma reserva de capacidade que aceite somente execuções direcionadas de instância.
- Destino por grupo: para executar as instâncias em qualquer reserva de capacidade com atributos correspondentes e capacidade disponível no grupo de reserva de capacidade selecionado.

3. No painel Resumo, analise a configuração da instância e selecione Iniciar instância. Para obter mais informações, consulte Executar uma instância do EC2 usando o assistente de inicialização de instâncias no console.

AWS CLI

Para iniciar instâncias em uma reserva de capacidade existente

Use o comando run-instances. Se você precisar ter como alvo uma reserva de capacidade ou um grupo de reserva de capacidade especifico, especifique o parâmetro `--capacity-reservation-specification`. Em `--placement`, especifique o parâmetro `GroupName` e, em seguida, especifique o nome do grupo de posicionamento que você criou nas etapas anteriores.

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --count quantity \
    --instance-type instance_type \
    --key-name key_pair_name \
    --subnet-id subnet-0abcdef1234567890 \
    --capacity-reservation-specification
 CapacityReservationTarget={CapacityReservationId=capacity_reservation_id} \
    --placement "GroupName=cluster_placement_group_name"
```

PowerShell

Para iniciar instâncias em uma reserva de capacidade existente

Use o cmdlet New-EC2Instance. Em `-Placement`, especifique o parâmetro `GroupName` e, em seguida, especifique o nome do grupo de posicionamento que você criou nas etapas anteriores.

```
New-EC2Instance `
    -ImageId ami-0abcdef1234567890 `
    -InstanceType instance_type `
```

```
    -KeyName key_pair_name `
    -SubnetId subnet-0abcdef1234567890 `
    -CapacityReservationTarget_CapacityReservationId capacity_reservation_id `
    -Placement_GroupName cluster_placement_group_name
```

Compartilhar reservas de capacidade em grupos de posicionamento de cluster

Você pode compartilhar reservas de capacidade em grupos de posicionamento de cluster compartilhando somente as reservas de capacidade ou compartilhando as reservas de capacidade e o grupo de posicionamento de cluster no qual elas foram criadas.

Ao compartilhar somente a reserva de capacidade, você concede às contas de consumidores acesso somente a essa reserva de capacidade. As contas de consumidores não tem visibilidade ou acesso ao grupo de posicionamento de cluster no qual a reserva de capacidade foi criada. Isso fornece controle refinado sobre o acesso a contas de consumidores. As contas de consumidores não podem visualizar nenhuma informação sobre o grupo de posicionamento de cluster, incluindo seu ARN.

Quando você compartilha o grupo de posicionamento de cluster e a reserva de capacidade, o grupo de posicionamento do cluster fica visível e acessível às contas dos consumidores. Eles podem iniciar instâncias e criar suas próprias reservas de capacidade neles.

Para obter mais informações, consulte os recursos a seguir.

- Inicie instâncias em reservas de capacidade em um grupo de posicionamento de cluster
- Reservas de capacidade compartilhadas
- Grupos de posicionamento compartilhados

Grupos de Reserva de capacidade

É possível usar o AWS Resource Groups para criar coleções lógicas de Reservas de Capacidade, chamadas grupos de recursos. Um grupo de recursos é um agrupamento lógico de recursos da AWS que estão todos na mesma região da AWS. Para obter mais informações sobre grupos de recursos, consulte O que são grupos de recursos? no Guia do usuário do AWS Resource Groups.

É possível incluir reservas de capacidade de sua propriedade em sua conta e reservas de capacidade compartilhadas com você por outras contas da AWS em um único grupo de recursos. Além disso, é possível incluir reservas de capacidade com atributos diferentes (por exemplo, tipo de instância, plataforma, zona de disponibilidade e locação) em um único grupo de recursos.

Ao criar grupos de recursos para reservas de capacidade, é possível direcionar instâncias para um grupo de reservas de capacidade em vez de uma reserva de capacidade individual. As instâncias direcionadas a um grupo de reservas de capacidade correspondem a qualquer reserva de capacidade no grupo que tenha atributos correspondentes (por exemplo, tipo de instância, plataforma, zona de disponibilidade e locação) e capacidade disponível. Se o grupo não tiver uma Reserva de capacidade com atributos correspondentes e capacidade disponível, as instâncias serão executadas usando a capacidade sob demanda. Se uma Reserva de capacidade correspondente for adicionada ao grupo de destino em um estágio posterior, a correspondência da instância será automática e ela será movida para sua capacidade reservada.

Para evitar o uso não intencional de Reservas de Capacidade em um grupo, configure as Reservas de Capacidade no grupo para aceitar somente as instâncias que se dirigem explicitamente à reserva de capacidade. Para fazer isso, defina Instance eligibility como Only instances that specify this reservation ao criar a Reserva de capacidade usando o console do Amazon EC2. Ao usar a AWS CLI, especifique `--instance-match-criteria targeted` ao criar a reserva de capacidade. Isso garante que somente as instâncias explicitamente direcionadas ao grupo, ou a uma Reserva de capacidade no grupo, possam ser executadas no grupo.

Se uma Reserva de capacidade em um grupo for cancelada ou expirar enquanto tiver instâncias em execução, as instâncias serão automaticamente movidas para outra Reserva de capacidade no grupo que tenha atributos correspondentes e capacidade disponível. Se não houver Reservas de Capacidade restantes no grupo que tenham atributos correspondentes e capacidade disponível, as instâncias serão executadas na capacidade sob demanda. Se uma Reserva de capacidade correspondente for adicionada ao grupo de destino em um estágio posterior, a instância será automaticamente movida para sua capacidade reservada.

Tarefas

- Criar um grupo de reserva de capacidade
- Adicionar uma reserva de capacidade a um grupo
- Remover uma reserva de capacidade de um grupo
- Excluir um grupo de reserva de capacidade
- Usar reservas de capacidade em grupos de posicionamento de cluster com um grupo de reserva de capacidade

Criar um grupo de reserva de capacidade

Estes exemplos podem ser usados para criar um grupo de recursos para reservas de capacidade com os parâmetros de solicitação a seguir.

- `AWS::EC2::CapacityReservationPool`: garante que o grupo de recursos possa ser direcionado para execuções de instâncias.
- `AWS::ResourceGroups::Generic` com `allowed-resource-types` definido como `AWS::EC2::CapacityReservation`: garante que o grupo de recursos aceite apenas reservas de capacidade.

Após criar um grupo, você poderá adicionar Reservas de Capacidade ao grupo.

AWS CLI

Como criar um grupo para reservas de capacidade

Use o comando create-group da AWS CLI.

```
aws resource-groups create-group \
    --name MyCRGroup \
    --configuration \
        '{"Type": "AWS::EC2::CapacityReservationPool"}' \
        '{"Type": "AWS::ResourceGroups::Generic", "Parameters": [{"Name": "allowed-
resource-types", "Values": ["AWS::EC2::CapacityReservation"]}]}'
```

PowerShell

Como criar um grupo para reservas de capacidade

Use o cmdlet New-RGGroup.

```
New-RGGroup `
    -Name MyCRGroup `
    -Configuration `
        @{"Type"="AWS::EC2::CapacityReserationPool"} `
        @{"Type"="AWS::ResourceGroups::Generic"; "Parameters"=@{"allowed-resource-
types"=@{"Values"="AWS::EC2::CapacityReservations"}}}
```

Adicionar uma reserva de capacidade a um grupo

Se você adicionar uma reserva de capacidade compartilhada com você a um grupo e essa reserva de capacidade não for compartilhada, ela será automaticamente removida do grupo.

AWS CLI

Como adicionar uma Reserva de capacidade a um grupo

Use o comando group-resources.

O exemplo a seguir adiciona duas reservas de capacidade ao grupo especificado.

```
aws resource-groups group-resources \
    --group MyCRGroup \
    --resource-arns \
        arn:aws:ec2:sa-east-1:123456789012:capacity-reservation/cr-1234567890abcdef1
 \
        arn:aws:ec2:sa-east-1:123456789012:capacity-reservation/cr-54321abcdef567890
```

PowerShell

Como adicionar uma Reserva de capacidade a um grupo

Use o cmdlet Add-RGResource.

O exemplo a seguir adiciona duas reservas de capacidade ao grupo especificado.

```
Add-RGResource `
    -Group MyCRGroup `
    -ResourceArn `
        "arn:aws:ec2:sa-east-1:123456789012:capacity-
reservation/cr-1234567890abcdef1", `
        "arn:aws:ec2:sa-east-1:123456789012:capacity-
reservation/cr-54321abcdef567890"
```

Remover uma reserva de capacidade de um grupo

Os exemplos a seguir podem ser usados para remover uma reserva de capacidade de um grupo.

AWS CLI

Como remover uma Reserva de capacidade de um grupo

Use o comando ungroup-resources.

O exemplo a seguir remove duas reservas de capacidade do grupo especificado.

```
aws resource-groups ungroup-resources \
    --group MyCRGroup \
    --resource-arns \
        arn:aws:ec2:sa-east-1:123456789012:capacity-reservation/cr-0e154d26a16094dd
 \
        arn:aws:ec2:sa-east-1:123456789012:capacity-reservation/cr-54321abcdef567890
```

PowerShell

Como remover uma Reserva de capacidade de um grupo

Use o cmdlet Remove-RGResource.

O exemplo a seguir remove duas reservas de capacidade do grupo especificado.

```
Remove-RGResource `
    -Group MyCRGroup `
    -ResourceArn `
        "arn:aws:ec2:sa-east-1:123456789012:capacity-
reservation/cr-0e154d26a16094dd", `
        "arn:aws:ec2:sa-east-1:123456789012:capacity-
reservation/cr-54321abcdef567890"
```

Excluir um grupo de reserva de capacidade

Os exemplos a seguir podem ser usados para excluir um grupo de reservas de capacidade.

AWS CLI

Para excluir um grupo

Use o comando delete-group.

```
aws resource-groups delete-group --group MyCRGroup
```

PowerShell

Para excluir um grupo

Use o cmdlet Remove-RGGroup.

```
Remove-RGGroup -GroupName MyCRGroup
```

Usar reservas de capacidade em grupos de posicionamento de cluster com um grupo de reserva de capacidade

O Amazon EC2 fornece métodos diferentes para iniciar para você usar reservas de capacidade em um grupo de posicionamento de cluster com um grupo de reserva de capacidade. Você pode escolher um dos seguintes métodos para visar um grupo de reserva de capacidade com base em seus requisitos de workload.

- Especificar o ARN do grupo de posicionamento de cluster e o grupo de reserva de capacidade — Isso usará qualquer reserva de capacidade disponível com atributos correspondentes e capacidade disponível no grupo de reserva de capacidade selecionado. Se o grupo selecionado não tiver uma Reserva de capacidade com atributos correspondentes e capacidade disponível, as instâncias serão executadas na capacidade sob demanda.

  > **Note**
  >
  > Quando você inicia instâncias usando esse método, as instâncias são colocadas no grupo de posicionamento de cluster especificado.

- Especificar somente um grupo de reserva de capacidade — Isso usará toda a capacidade disponível dentro do grupo de reserva de capacidade especificando somente o grupo de reserva de capacidade. Ao iniciar instâncias, a capacidade é usada na seguinte ordem:
  - Reservas de capacidade não associadas com qualquer grupo de posicionamento de cluster.
  - Reservas de capacidade em qualquer grupo de posicionamento de cluster dentro do grupo de reserva de capacidade
  - Se o grupo não tiver uma reserva de capacidade com atributos correspondentes e capacidade disponível, as instâncias serão executadas usando a capacidade sob demanda, e elas não serão posicionadas em nenhum grupo de posicionamento de cluster.

  > **Note**
  >
  > Quando você executa instâncias especificando somente uma reserva de capacidade, as instâncias são iniciadas nas reservas de capacidade criadas no grupo de posicionamento

de cluster, mas as instâncias não são diretamente vinculadas ao grupo de posicionamento de cluster.

Reservas de Capacidade em zonas locais

Uma zona local é uma extensão de uma região da AWS que está geograficamente próxima de seus usuários. Os recursos criados em uma zona local podem atender usuários locais com comunicações de latência muito baixa. Para obter mais informações, consulte AWS Local Zones. .

É possível estender uma VPC de sua região da AWS pai para uma zona local criando uma sub-rede nessa zona local. Quando você criar uma sub-rede em uma zona local, sua VPC também será estendida para essa zona local. A sub-rede na zona local funciona da mesma forma que outras sub-redes na VPC.

Ao usar zonas locais, é possível colocar Reservas de Capacidade em vários locais que estão mais próximos de seus usuários. Você cria e usa Reservas de Capacidade em zonas locais da mesma forma que cria e usa Reservas de Capacidade em zonas de disponibilidade regulares. Os mesmos recursos e comportamento de correspondência de instâncias são aplicados. Para obter mais informações sobre os modelos de preços com suporte nas zonas locais, consulte Perguntas frequentes sobre AWS zonas locais.

Considerações

Não é possível usar grupos de Reserva de capacidade em uma zona local.

Para usar uma reserva de capacidade em uma zona local

1. Habilite a zona local para usar em sua conta da AWS. Para obter mais informações, consulte Getting started with AWS Local Zones no Guia de usuário de zona locais da AWS.
2. Crie uma reserva de capacidade na zona local. Para Availability Zone (Zona de disponibilidade), escolha a zona local. A zona local é representada por um código de região da AWS seguido por um identificador que indica o local, por exemplo, `us-west-2-lax-1a`. Para obter mais informações, consulte Criar uma Reserva de capacidade.
3. Crie uma sub-rede na zona local. Para Availability Zone (Zona de disponibilidade), escolha a zona local. Para obter mais informações, consulte Criar uma sub-rede em sua VPC no Guia do usuário da Amazon VPC.
4. Execute uma instância. Em Subnet (Sub-rede), escolha a sub-rede na zona local (por exemplo `subnet-123abc | us-west-2-lax-1a`) e em Capacity Reservation (Reserva

de capacidade), escolha a especificação (`open` ou indique seu ID) necessária para a reserva de capacidade que você criou na zona local. Para obter mais informações, consulte Iniciar instâncias em uma Reserva de capacidade existente.

Reservas de Capacidade em zonas Wavelength

AWS Wavelength O permite que os desenvolvedores criem aplicações que oferecem baixíssimas latências para dispositivos móveis e usuários finais. O Wavelength implanta os serviços de armazenamento e computação padrão da AWS até a borda das redes 5G de operadoras de telecomunicação. É possível estender um Amazon Virtual Private Cloud (VPC) para uma ou mais zonas do Wavelength. Em seguida, é possível usar recursos da AWS como instâncias do Amazon EC2 para executar aplicações que exigem latência ultrabaixa e uma conexão com produtos da AWS na região. Para obter mais informações, consulte Zonas AWS Wavelength.

Ao criar Reservas de Capacidade sob demanda, é possível escolher a zona de Wavelength e executar instâncias de Reserva de capacidade em uma zona de Wavelength especificando a sub-rede associada à zona de Wavelength. Uma zona do Wavelength é representada por um código de região da AWS seguido por um identificador que indica o local, por exemplo, `us-east-1-wl1-bos-wlz-1`.

As zonas de Wavelength não estão disponíveis em todas as regiões. Para obter informações sobre as regiões compatíveis com as zonas do Wavelength consulte Zonas do Wavelength disponíveis no Guia do desenvolvedor da AWS Wavelength.

Considerações

Não é possível usar grupos de Reserva de capacidade em uma zona de Wavelength.

Para usar uma Reserva de capacidade em uma zona de Wavelength

1. Habilite a zona do Wavelength para uso em sua conta da AWS. Para obter mais informações, consulte Conceitos básicos do AWS Wavelength no Guia do desenvolvedor do AWS Wavelength.
2. Crie uma Reserva de capacidade na zona de Wavelength. Para Availability Zone ((Zona de disponibilidade), escolha a Wavelength. O Wavelength é representado por um código de região da AWS seguido por um identificador que indica o local, por exemplo `us-east-1-wl1-bos-wlz-1`. Para obter mais informações, consulte Criar uma Reserva de capacidade.

3. Depois, crie uma sub-rede na zona de Wavelength. Para Availability Zone (Zona de disponibilidade), escolha a zona de Wavelength. Para obter mais informações, consulte Criar uma sub-rede em sua VPC no Guia do usuário da Amazon VPC.
4. Execute uma instância. Em Subnet ((Sub-rede), escolha a sub-rede na Wavelength (por exemplo `subnet-123abc | us-east-1-wl1-bos-wlz-1`) e em Reserva de capacidade, escolha a especificação (`open` ou indique seu ID) necessária para a Reserva de capacidade que você criou na Wavelength. Para obter mais informações, consulte Iniciar instâncias em uma Reserva de capacidade existente.

Reservas de Capacidade no AWS Outposts

O AWS Outposts é um serviço totalmente gerenciado que estende a infraestrutura, os serviços, as APIs e as ferramentas da AWS no local do cliente. Ao fornecer acesso local à infraestrutura gerenciada pela AWS, o AWS Outposts permite que os clientes criem e executem aplicações on-premises usando as mesmas interfaces de programação que nas regiões da AWS, ao mesmo tempo que usam recursos locais de computação e armazenamento para menor latência e necessidades de processamento de dados locais.

Um Outpost é um grupo de capacidade de computação e armazenamento da AWS implantado em um local do cliente. A AWS opera, monitora e gerencia essa capacidade como parte de uma região da AWS.

É possível criar Reservas de Capacidade nos Outposts que criou na sua conta. Isso permite que você reserve capacidade computacional em um Outpost em seu local. Você cria e usa Reservas de Capacidade em Outposts da mesma forma que cria e usa Reservas de Capacidade em zonas de disponibilidade regulares. Os mesmos recursos e comportamento de correspondência de instâncias são aplicados.

Também é possível compartilhar Reservas de Capacidade em Outposts com outros contas da AWS na organização usando o AWS Resource Access Manager. Para obter mais informações sobre o compartilhamento de Reservas de Capacidade, consulte Reservas de capacidade compartilhadas.

Pré-requisito

É necessário ter um Outpost instalado em seu local. Para obter mais informações, consulte Criar um Outpost e solicitar capacidade do Outpost no Manual do usuário do AWS Outposts.

Considerações

- Não é possível usar grupos de reserva de capacidade em um Outpost.

Para usar um grupo de reserva de capacidade em um Outpost

1. Crie uma sub-rede no Outpost. Para obter mais informações, consulte Criar uma sub-rede no Manual do usuário do AWS Outposts.
2. Crie uma reserva de capacidade no Outpost.
   a. Abra o console do AWS Outposts em https://console.aws.amazon.com/outposts/.
   b. No painel de navegação, selecione Outposts e, em seguida, escolha Actions (Ações), Create Capacity Reservation (Criar reserva de capacidade).
   c. Configure a reserva de capacidade conforme necessário e escolha Create (Criar). Para obter mais informações, consulte Criar uma Reserva de capacidade.

   > **Note**
   >
   > O menu suspenso Instance Type (Tipo de instância) lista somente os tipos de instância que são compatíveis com o Outpost selecionado, e o menu suspenso Availability Zone (Zona de disponibilidade) lista somente a zona de disponibilidade à qual o Outpost selecionado está associado.

3. Iniciar uma instância na reserva de capacidade Em Subnet (Sub-rede), escolha a sub-rede criada na Etapa 1 e, em Capacity Reservation (Reserva de capacidade), selecione a reserva de capacidade criada na Etapa 2. Para obter mais informações, consulte Executar uma instância no Outpost no Manual do usuário do AWS Outposts.

Reservas de capacidade compartilhadas

O compartilhamento de reserva de capacidade permite que os proprietários de reservas de capacidade compartilhem sua capacidade reservada com outras contas da AWS em um departamento da AWS. Isso permite criar e gerenciar as Reservas de Capacidade centralmente e compartilhar a capacidade reservada entre várias contas da AWS ou em sua organização da AWS.

Nesse modelo, a conta da AWS que possui a Reserva de capacidade (proprietária) compartilha-a com outras contas da AWS (consumidores). Os consumidores podem executar instâncias nas Reservas de Capacidade que são compartilhadas com eles da mesma maneira que executam instâncias em Reservas de Capacidade que possuem em sua própria conta. O proprietário

da Reserva de capacidade é responsável pelo gerenciamento da Reserva de capacidade e pelas instâncias que executa nela. Os proprietários não podem modificar as instâncias que os consumidores executam nas Reservas de Capacidade que compartilharam. Os consumidores são responsáveis por gerenciar as instâncias que executam em Reservas de Capacidade compartilhadas com eles. Os consumidores não podem visualizar ou modificar instâncias de propriedade de outros consumidores ou do proprietário da Reserva de capacidade.

O proprietário de uma Reserva de capacidade pode compartilhar uma Reserva de capacidade com:

- Contas específicas da AWS dentro ou fora de sua organização na AWS
- Uma unidade organizacional dentro de sua organização da AWS
- Toda a sua organização da AWS

Pré-requisitos para compartilhar Reservas de Capacidade

- Para compartilhar uma reserva de capacidade, é necessário ser o proprietário dela em sua conta da AWS. Não é possível compartilhar uma Reserva de capacidade que tenha sido compartilhada com você.
- Só é possível compartilhar Reservas de Capacidade para instâncias de locação compartilhada. Não é possível compartilhar Reservas de Capacidade para instâncias de locação dedicada.
- O compartilhamento de Reserva de capacidade não está disponível para contas novas da AWS ou para contas da AWS que tenham um histórico limitado de faturamento.
- Para compartilhar uma reserva de capacidade com a sua organização da AWS ou com uma unidade organizacional de sua organização da AWS, é necessário habilitar o compartilhamento com o AWS Organizations. Para obter mais informações, consulte Habilitar o compartilhamento com o AWS Organizations no Guia do usuário do AWS RAM.
- Você pode compartilhar uma reserva de capacidade no estado `active` ou `scheduled`. Você não pode compartilhar a reserva de capacidade em outros estados , como `assessing` ou`unsupported`.

Serviços relacionados

O compartilhamento de reserva de capacidade integra-se ao AWS Resource Access Manager (AWS RAM). O AWS RAM é um serviço que permite compartilhar seus recursos da AWS com qualquer conta da AWS ou por meio do AWS Organizations. Com o AWS RAM, você compartilha recursos que possui criando um compartilhamento de recursos. Um compartilhamento de recursos

especifica os recursos a serem compartilhados, e os consumidores com os quais compartilhá-los. Os consumidores podem ser contas individuais da AWS, unidades organizacionais ou toda uma organização do AWS Organizations.

Para obter mais informações sobre o AWS RAM, consulte o Manual do usuário do AWS RAM.

Compartilhamento entre zonas de disponibilidade

Para garantir a distribuição de recursos entre as zonas de disponibilidade de uma região, mapeamos as zonas de disponibilidade de forma independente para os nomes de cada conta. Isso pode resultar em diferenças na nomenclatura de zonas de disponibilidade entre contas. Por exemplo, a zona de disponibilidade `us-east-1a` de sua conta da AWS pode não ter o mesmo local que a `us-east-1a` de outra conta da AWS.

Para identificar o local de suas Reservas de Capacidade relativo a suas contas, use o ID da zona de disponibilidade (ID da AZ). O ID da AZ é um identificador exclusivo e consistente de uma zona de disponibilidade em todas as contas da AWS. Por exemplo, `use1-az1` é um AZ ID da região `us-east-1` e é o mesmo local em cada conta da AWS.

Para visualizar os AZ IDs das zonas de disponibilidade em sua conta

1. Abra o console do AWS RAM em https://console.aws.amazon.com/ram/home.
2. Os IDs de AZs da região atual são exibidos no painel Your AZ ID (Seu ID de AZ) no lado direito da tela.

Compartilhar uma Reserva de capacidade

Quando você compartilha uma reserva de capacidade de sua propriedade com outras Contas da AWS, você permite que elas executem instâncias em sua capacidade reservada. Se você compartilhar uma Reserva de capacidade aberta, lembre-se do seguinte, pois isso pode resultar em uso não intencional da Reserva de capacidade:

- Se os consumidores tiverem instâncias em execução que correspondam aos atributos da Reserva de capacidade, tenham o parâmetro `CapacityReservationPreference` definido como `open` e ainda não estejam em execução na capacidade reservada, eles usarão a Reserva de capacidade compartilhada automaticamente.
- Se os consumidores executarem instâncias que tenham atributos correspondentes (por exemplo, tipo de instância, plataforma, zona de disponibilidade e locação) e tiverem o parâmetro

`CapacityReservationPreference` definido como `open`, as instâncias serão iniciadas automaticamente na reserva de capacidade compartilhada.

Para compartilhar uma Reserva de capacidade, é necessário adicioná-la um compartilhamento de recursos. Um compartilhamento de recursos é um recurso do AWS RAM que permite que você compartilhe seus recursos entre contas da AWS. Um compartilhamento de recursos especifica os recursos a serem compartilhados, e os consumidores com os quais compartilhá-los. Ao compartilhar uma Reserva de capacidade usando o console do Amazon EC2, você a adiciona a um compartilhamento de recursos existente. Para adicionar a reserva de capacidade a um novo compartilhamento de recursos, crie o compartilhamento de recursos usando o console do AWS RAM.

Se você fizer parte de uma organização no AWS Organizations e ela tiver o compartilhamento habilitado, os consumidores da organização receberão acesso à reserva de capacidade se os pré-requisitos de compartilhamento forem atendidos. Se a reserva de capacidade estiver compartilhada com contas externas, eles receberão um convite para ingressar no compartilhamento de recursos e acesso à reserva de capacidade compartilhada após aceitar o convite.

> **Important**
>
> Antes de executar instâncias em uma reserva de capacidade que seja compartilhada com você, verifique se tem acesso à reserva de capacidade compartilhada exibindo-a no console ou descrevendo-a usando o comando describe-capacity-reservations da AWS CLI. Se conseguir exibir a reserva de capacidade compartilhada no console ou descrevê-la usando a AWS CLI, ela está disponível para seu uso e é possível executar instâncias nela. Se tentar executar instâncias na reserva de capacidade e ela não estiver acessível devido a uma falha de compartilhamento, as instâncias serão executadas na capacidade sob demanda.

Console

Para compartilhar uma Reserva de capacidade de sua propriedade usando o console do Amazon EC2

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Reservas de Capacidade.
3. Escolha a Reserva de capacidade a ser compartilhada e escolha Actions (Ações), Share reservation (Compartilhar reserva).

4. Selecione o compartilhamento de recursos ao qual adicionar a Reserva de capacidade e escolha Share Reserva de capacidade (Compartilhar Reserva de capacidade).

   Pode levar alguns minutos para que os consumidores obtenham acesso à Reserva de capacidade compartilhada.

Para compartilhar uma reserva de capacidade de sua propriedade usando o console do AWS RAM

Consulte Creating a resource share no Guia do usuário do AWS RAM.

AWS CLI

Para compartilhar uma reserva de capacidade de sua propriedade

Use o comando create-resource-share.

```
aws ram create-resource-share \
    --name my-resource-share \
    --resource-arns arn:aws:ec2:us-east-2:123456789012:capacity-
reservation/cr-1234abcd56EXAMPLE
```

PowerShell

Para compartilhar uma reserva de capacidade de sua propriedade

Use o cmdlet New-RAMResourceShare.

```
New-RAMResourceShare `
    -Name my-resource-share `
    -ResourceArn "arn:aws:ec2:us-east-2:123456789012:capacity-
reservation/cr-1234abcd56EXAMPLE"
```

Parar de compartilhar uma Reserva de capacidade

O proprietário da Reserva de capacidade pode parar de compartilhar a Reserva de capacidade a qualquer momento. As seguintes regras se aplicam:

- As instâncias de propriedade de consumidores que estavam em execução na capacidade compartilhada na hora do cancelamento do compartilhamento continuam sendo executadas

normalmente fora da capacidade reservada, e a capacidade é restaurada para a Reserva de capacidade sujeita à disponibilidade da capacidade do Amazon EC2.

- Os consumidores com quem a Reserva de capacidade era compartilhada não podem mais executar novas instâncias na capacidade reservada.

Para interromper o compartilhamento de uma Reserva de capacidade que você possui, remova-a do compartilhamento de recursos.

Console

Como interromper o compartilhamento de uma Reserva de capacidade que você possui usando o console do Amazon EC2

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Reservas de Capacidade.
3. Selecione a Reserva de capacidade e escolha a guia Sharing (Compartilhamento).
4. A guia Sharing (Compartilhamento) lista os compartilhamentos de recursos aos quais a Reserva de capacidade foi adicionada. Selecione o compartilhamento de recursos do qual remover a Reserva de capacidade e escolha Remove from resource share (Remover do compartilhamento de recursos).

Para interromper o compartilhamento de uma reserva de capacidade que você possui usando o console do AWS RAM

Consulte Atualização de um compartilhamento de atributos no Guia do usuário do AWS RAM.

AWS CLI

Para interromper o compartilhamento de uma reserva de capacidade de sua propriedade

Use o comando disassociate-resource-share.

```
aws ram disassociate-resource-share \
    --resource-share-arn arn:aws:ram:us-east-2:123456789012:resource-share/7ab63972-b505-7e2a-420d-6f5d3EXAMPLE \
 --resource-arns arn:aws:ec2:us-east-2:123456789012:capacity-reservation/cr-1234abcd56EXAMPLE
```

PowerShell

Para interromper o compartilhamento de uma reserva de capacidade de sua propriedade

Use o cmdlet Disconnect-RAMResourceShare.

```
Disconnect-RAMResourceShare `
    -ResourceShareArn "arn:aws:ram:us-east-2:123456789012:resource-share/7ab63972-b505-7e2a-420d-6f5d3EXAMPLE" `
    -ResourceArn "arn:aws:ec2:us-east-2:123456789012:capacity-reservation/cr-1234abcd56EXAMPLE"
```

Atribuição de faturamento para reservas de capacidade compartilhadas do Amazon EC2

Por padrão, quando uma reserva de capacidade é compartilhada, o proprietário é cobrado pelas instâncias que executa na reserva de capacidade e por qualquer capacidade disponível, também chamada de capacidade não utilizada, na reserva de capacidade; enquanto os consumidores são cobrados apenas pelas instâncias que executam na reserva de capacidade compartilhada.

Se necessário, o proprietário da reserva de capacidade pode atribuir o faturamento de qualquer capacidade disponível na reserva de capacidade a qualquer uma das contas com as quais a reserva de capacidade é compartilhada. Depois que o faturamento é atribuído a outra conta, essa conta torna-se a proprietária do faturamento de qualquer capacidade disponível na reserva de capacidade. Qualquer cobrança pela capacidade disponível na reserva de capacidade, a partir desse momento, será cobrada na conta atribuída em vez de na conta do proprietário. O proprietário da reserva de capacidade e as contas com as quais a reserva de capacidade é compartilhada continuam sendo cobrados pelas instâncias que executam na reserva de capacidade.

> **Important**
>
> O proprietário da reserva de capacidade permanece o proprietário do recurso e responsável pelo gerenciamento da reserva de capacidade. A conta à qual o faturamento é atribuído não recebe nenhum privilégio adicional; ela não pode cancelar, modificar ou compartilhar a reserva de capacidade de nenhuma forma.

Tópicos

- Como funciona
- Considerações

- Atribuir o faturamento de uma reserva de capacidade compartilhada do EC2 a outra conta
- Visualizar solicitações de atribuição de faturamento para reservas de capacidade compartilhadas do EC2
- Aceitar ou rejeitar o faturamento de uma reserva de capacidade compartilhada do EC2
- Cancelar ou revogar solicitações de atribuição de faturamento para reservas de capacidade compartilhadas do EC2
- Monitorar as solicitações de atribuição de faturamento para reservas de capacidade compartilhadas

Como funciona

Somente o proprietário da reserva de capacidade pode atribuir o faturamento de uma reserva de capacidade compartilhada a outra conta. O faturamento só pode ser atribuído a uma conta com a qual a reserva de capacidade seja compartilhada e que esteja integrada na mesma conta pagante do AWS Organizations do proprietário da reserva de capacidade.

Para atribuir o faturamento da capacidade disponível de uma reserva de capacidade a outra conta, o proprietário da reserva de capacidade deve iniciar uma solicitação para a conta pretendida. A conta especificada recebe a solicitação e deve aceitá-la ou rejeitá-la em até 12 horas.

- Caso aceite, ela torna-se a proprietária do faturamento de qualquer capacidade disponível, também chamada de capacidade não utilizada, na reserva de capacidade. A partir desse momento, qualquer cobrança pela capacidade disponível na reserva de capacidade será cobrada na conta atribuída em vez de na conta do proprietário. Após aceita, somente o proprietário da reserva de capacidade poderá revogar o faturamento da conta atribuída.
- Caso rejeite, o proprietário da reserva de capacidade continuará sendo o responsável pelo faturamento da capacidade disponível na reserva de capacidade. As cobranças por qualquer capacidade disponível na reserva de capacidade continurão sendo cobradas na conta do proprietário.
- Caso não aceite ou rejeite a solicitação em até 12 horas, ela expirará e as cobranças por qualquer capacidade disponível na reserva de capacidade continuarão sendo cobradas na conta do proprietário.

Durante o período em que o faturamento é atribuído a outra conta, os itens de linha `Reservation` e `UnusedBox` aparecem no Relatório de Custos e Uso (CUR) da conta atribuída em vez de no CUR do proprietário.

A tabela a seguir mostra quais itens de linha aparecem no CUR para as contas do proprietário e do consumidor da reserva de capacidade antes que o faturamento seja atribuído a outra conta.

Conta	Itens de linha do CUR antes da atribuição do faturamento
Proprietário da reserva de capacidade	• `Reservation` • `BoxUsage *` • `UnusedBox`
Contas de consumidores com as quais a reserva de capacidade é compartilhada	• `BoxUsage *`

A tabela a seguir mostra quais itens de linha aparecem no CUR para as contas do proprietário e do consumidor da reserva de capacidade depois que o faturamento for atribuído a outra conta.

Conta	Itens de linha do CUR depois da atribuição do faturamento
Proprietário da reserva de capacidade	• `BoxUsage *`
Conta de consumidor à qual o faturamento é atribuído	• `Reservation` • `BoxUsage *` • `UnusedBox`

Conta	Itens de linha do CUR depois da atribuição do faturamento
Outras contas de consumidores com as quais a reserva de capacidade é compartilhada	• `BoxUsage *`

> **Note**
>
> - * O item de linha `BoxUsage` aparecerá no CUR de uma conta somente se ela tiver instâncias em execução na reserva de capacidade. Para obter mais informações sobre os itens de linha do CUR, consulte Monitoring Capacity Reservations.
> - Use o ARN da reserva de capacidade no CUR para determinar quem é o proprietário da reserva de capacidade. Se o ARN incluir o ID da conta da AWS, você será o proprietário da reserva de capacidade. Caso contrário, a reserva de capacidade será de propriedade de outra conta, mas o faturamento será atribuído a você.
> - As tags de alocação de custos atribuídas à reserva de capacidade pelo proprietário não aparecerão no CUR da conta do consumidor. As tags de alocação de custos aparecem somente no CUR do proprietário da reserva de capacidade.

Considerações

Lembre-se do seguinte ao atribuir o faturamento de uma reserva de capacidade compartilhada:

- Você não pode fazer atribuições de faturamento parcial ou dividido. O faturamento de toda a capacidade disponível de uma reserva de capacidade só pode ser atribuído a uma conta por vez.
- A capacidade disponível de uma reserva de capacidade pode mudar com o tempo. Isso afetará o faturamento da conta atribuída. Por exemplo, a capacidade disponível poderá aumentar se o proprietário da reserva de capacidade aumentar o tamanho da reserva de capacidade ou se outras contas de consumidores interromperem ou encerrarem as instâncias em execução na reserva de capacidade.
- O faturamento só pode ser atribuído a uma conta de consumidor integrada na mesma conta pagante do AWS Organizations. O faturamento será automaticamente revogado da conta do consumidor se ele deixar a organização ou se a reserva de capacidade não for mais compartilhada com ele.

- Somente o proprietário da reserva de capacidade pode cancelar uma solicitação de atribuição de faturamento pendente e revogar o faturamento de uma conta atribuída depois que a solicitação for aceita.

Atribuir o faturamento de uma reserva de capacidade compartilhada do EC2 a outra conta

Para atribuir o faturamento da capacidade disponível de uma reserva de capacidade compartilhada a outra conta, o proprietário da reserva de capacidade deve iniciar uma solicitação para a conta pretendida. No console do Amazon EC2, essa solicitação é chamada de solicitação de transferência.

O proprietário de uma reserva de capacidade poderá atribuir o faturamento da capacidade disponível da reserva de capacidade a uma conta somente se:

- A reserva de capacidade já estiver compartilhada com a conta.
- A conta for integrada na mesma conta pagante do AWS Organizations que aquela do proprietário da reserva de capacidade.

O faturamento é atribuído à conta especificada somente quando ela aceita a solicitação.

Quando o proprietário de uma reserva de capacidade inicia uma solicitação, um evento do Amazon EventBridge é enviado para a conta solicitada. Para obter mais informações, consulte Monitorar as solicitações de atribuição de faturamento para reservas de capacidade compartilhadas.

Console

Para atribuir o faturamento de uma reserva de capacidade compartilhada

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Reservas de capacidade, e depois escolha a reserva de capacidade compartilhada.
3. Na seção Faturamento da capacidade disponível, escolha Atribuir faturamento.
4. Na tela Atribuir faturamento, selecione a conta do consumidor à qual atribuir o faturamento e, em seguida, escolha Solicitar.

AWS CLI

Para atribuir o faturamento de uma reserva de capacidade compartilhada

Use o comando associate-capacity-reservation-billing-owner. Em `--capacity-reservation-id`, especifique o ID da reserva de capacidade compartilhada. Em `--unused-reservation-billing-owner-id`, especifique o ID da conta da AWS à qual a cobrança será atribuída.

```
aws ec2 associate-capacity-reservation-billing-owner \
    --capacity-reservation-id cr-01234567890abcdef \
    --unused-reservation-billing-owner-id 123456789012
```

PowerShell

Para atribuir o faturamento de uma reserva de capacidade compartilhada

Use o cmdlet Register-EC2CapacityReservationBillingOwner. Em `-CapacityReservationId`, especifique o ID da reserva de capacidade compartilhada. Em `-UnusedReservationBillingOwnerId`, especifique o ID da conta da AWS à qual a cobrança será atribuída.

```
Register-EC2CapacityReservationBillingOwner `
    -CapacityReservationId cr-01234567890abcdef `
    -UnusedReservationBillingOwnerId 123456789012
```

Visualizar solicitações de atribuição de faturamento para reservas de capacidade compartilhadas do EC2

O proprietário de uma reserva de capacidade pode visualizar somente a solicitação de atribuição de faturamento mais recente que ele iniciou. E as contas de consumidores podem visualizar somente as solicitações de atribuição de faturamento mais recentes enviadas para elas.

As solicitações poderão ser visualizadas por 24 horas após entrarem no estado `cancelled`, `expired` ou `revoked`. Após 24 horas, elas não poderão mais ser visualizadas.

Console

(Proprietário da reserva de capacidade) Para visualizar as solicitações que você iniciou

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Reservas de capacidade e escolha a reserva de capacidade compartilhada da qual visualizar as solicitações.

3. A seção Faturamento da capacidade disponível mostra a solicitação mais recente e seu estado atual.

(Conta de consumidor) Para solicitações enviadas para você

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Reservas de capacidade.
3. Se você tiver solicitações pendentes, o banner Solicitações de atribuição de faturamento pendentes aparecerá na parte superior da tela. Se o banner não aparecer, você não tem nenhuma solicitação pendente.

   Para ver as solicitações, escolha Revisar solicitações no banner.

AWS CLI

(Proprietário da reserva de capacidade) Para visualizar as solicitações que você iniciou

Use o comando describe-capacity-reservation-billing-requests.

```
aws ec2 describe-capacity-reservation-billing-requests \
    --role odcr-owner
```

(Conta de consumidor) Para ver as solicitações enviadas para você

Use o comando describe-capacity-reservation-billing-requests.

```
aws ec2 describe-capacity-reservation-billing-requests \
    --role unused-reservation-billing-owner
```

PowerShell

(Proprietário da reserva de capacidade) Para visualizar as solicitações que você iniciou

Use o cmdlet Get-EC2CapacityReservationBillingRequest.

```
Get-EC2CapacityReservationBillingRequest `
    -Role odcr-owner
```

(Conta de consumidor) Para ver as solicitações enviadas para você

Use o cmdlet Get-EC2CapacityReservationBillingRequest.

```
Get-EC2CapacityReservationBillingRequest `
    -Role unused-reservation-billing-owner
```

Uma solicitação pode estar em um dos estados a seguir.

Estado	Descrição
`pending`	A solicitação não foi aceita nem rejeitada, mas ainda não expirou.
`accepted`	A solicitação foi aceita pela conta especificada. O faturamento da capacidad e disponível da reserva de capacidade é atribuído à conta do consumidor.
`rejected`	A solicitação foi rejeitada pela conta do consumidor.
`cancelled`	A solicitação foi cancelada pelo proprietário da reserva de capacidade enquanto ela estava no estado `pending`.
`revoked`	O faturamento foi revogado da conta do consumidor por um dos seguintes motivos: • Foi explicitamente revogado pelo proprietário da reserva de capacidade. •

Estado	Descrição
	A reserva de capacidade não é mais compartilhada com a conta do consumidor. • A conta do consumidor não faz mais parte da organizaç ão da AWS.
`expired`	A solicitação expirou porque a conta do consumidor não a aceitou nem a rejeitou no prazo de 12 horas.

Aceitar ou rejeitar o faturamento de uma reserva de capacidade compartilhada do EC2

Caso receba uma solicitação de atribuição de faturamento para uma reserva de capacidade compartilhada com você, será possível aceitá-la ou rejeitá-la. A solicitação permanecerá no estado `pending` até que seja aceita ou rejeitada.

Se você aceitar a solicitação, ela entrará no estado `accepted`, e o faturamento de qualquer capacidade disponível ou não utilizada dessa reserva de capacidade será atribuída à conta a partir desse momento. Depois de aceitar uma solicitação, somente o proprietário da reserva de capacidade poderá revogar o faturamento da conta.

Se você rejeitar a solicitação, ela entrará no estado `rejected`, e o faturamento da capacidade disponível da reserva de capacidade permanecerá atribuído ao proprietário da reserva de capacidade.

As solicitações expirarão se não forem aceitas ou rejeitadas em até 12 horas. Se uma solicitação expirar, o faturamento de qualquer capacidade não utilizada da reserva de capacidade permanecerá atribuído ao proprietário da reserva de capacidade.

Quando uma solicitação é aceita ou rejeitada, um evento do Amazon EventBridge é enviado para a conta do proprietário da reserva de capacidade. Quando uma solicitação expira, um evento do

Amazon EventBridge é enviado ao proprietário da reserva de capacidade e à conta do consumidor. Para obter mais informações, consulte Monitorar as solicitações de atribuição de faturamento para reservas de capacidade compartilhadas.

Console

Para aceitar ou rejeitar uma solicitação

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Reservas de capacidade.
3. Se você tiver solicitações pendentes, o banner Solicitações de atribuição de faturamento pendentes aparecerá na parte superior da tela. Se o banner não aparecer, você não tem nenhuma solicitação pendente.

   Para ver as solicitações, escolha Revisar solicitações no banner.
4. Selecione a solicitação para aceitar ou rejeitar e, em seguida, escolha Aceitar ou Rejeitar.

AWS CLI

Para aceitar uma solicitação

Use o comando accept-capacity-reservation-billing-ownership. Em `--capacity-reservation-id`, especifique o ID da reserva de capacidade da qual aceitar a solicitação.

```
aws ec2 accept-capacity-reservation-billing-ownership \
    --capacity-reservation-id cr-01234567890abcdef
```

Para rejeitar uma solicitação

Use o comando reject-capacity-reservation-billing-ownership. Em `--capacity-reservation-id`, especifique o ID da reserva de capacidade da qual rejeitar a solicitação.

```
aws ec2 reject-capacity-reservation-billing-ownership \
    --capacity-reservation-id cr-01234567890abcdef
```

PowerShell

Para aceitar uma solicitação

Use o cmdlet Approve-EC2CapacityReservationBillingOwnership.

```
Approve-EC2CapacityReservationBillingOwnership `
    -CapacityReservationId cr-01234567890abcdef
```

Para rejeitar uma solicitação

Use o cmdlet Deny-EC2CapacityReservationBillingOwnership.

```
Deny-EC2CapacityReservationBillingOwnership `
    -CapacityReservationId cr-01234567890abcdef
```

Cancelar ou revogar solicitações de atribuição de faturamento para reservas de capacidade compartilhadas do EC2

Somente o proprietário da reserva de capacidade pode cancelar uma solicitação de atribuição de faturamento `pending`. Se uma solicitação pendente for cancelada, ela entrará no estado `cancelled`, e o faturamento de qualquer capacidade disponível ou não utilizada da reserva de capacidade permanecerá atribuído ao proprietário da reserva de capacidade.

Depois que a solicitação é `accepted`, somente o proprietário da reserva de capacidade pode revogar a cobrança da conta atribuída. Se o faturamento for revogado, a solicitação entrará no estado `revoked`, e o faturamento de qualquer capacidade disponível da reserva de capacidade será reatribuído ao proprietário da reserva de capacidade.

Quando uma solicitação é cancelada ou revogada, os eventos do Amazon EventBridge são enviados para o proprietário da reserva de capacidade e para a conta do consumidor especificada. Para obter mais informações, consulte Monitorar as solicitações de atribuição de faturamento para reservas de capacidade compartilhadas.

Console

Para cancelar ou revogar uma solicitação

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Reservas de capacidade e depois escolha a reserva de capacidade da qual cancelar ou revogar a solicitação.
3. Na seção Faturamento da capacidade disponível, escolha Cancelar transferência ou Revogar transferência, dependendo do estado atual da solicitação.

AWS CLI

Para cancelar ou revogar uma solicitação

Use o comando disassociate-capacity-reservation-billing-owner. Em `--unused-reservation-billing-owner-id`, especifique o ID da conta da AWS da qual a solicitação foi enviada.

```
aws ec2 disassociate-capacity-reservation-billing-owner \
    --capacity-reservation-id cr-01234567890abcdef \
    --unused-reservation-billing-owner-id 123456789012
```

PowerShell

Para cancelar ou revogar uma solicitação

Use o cmdlet Unregister-EC2CapacityReservationBillingOwner. Em `-UnusedReservationBillingOwnerId`, especifique o ID da conta da AWS da qual a solicitação foi enviada.

```
Unregister-EC2CapacityReservationBillingOwner `
    -CapacityReservationId cr-01234567890abcdef `
    -UnusedReservationBillingOwnerId 123456789012
```

Monitorar as solicitações de atribuição de faturamento para reservas de capacidade compartilhadas

O Amazon EC2 envia eventos do Amazon EventBridge quando o estado de uma solicitação de atribuição de faturamento muda.

- Os eventos são enviados para o proprietário da reserva de capacidade quando uma solicitação entra nos seguintes estados: `accepted` | `rejected` | `expired` | `revoked`.
- Os eventos são enviados para a conta do consumidor solicitada quando uma solicitação entra nos seguintes estados: `pending` | `expired` | `cancelled` | `revoked`.

Para obter mais informações sobre o Amazon EventBridge, consulte o Guia do usuário do Amazon EventBridge.

A seguir está o padrão de eventos do Amazon EventBridge.

```
{
```

```
   "version":"0",
   "id":"12345678-1234-1234-1234-123456789012",
   "detail-type":"On-Demand Capacity Reservation Billing Ownership Request pending|
accepted|rejected|cancelled|revoked|expired",
   "source":"aws.ec2",
   "account":"account_id",
   "time":"state_change_timestamp",
   "region":"region",
   "resources":[
      "arn:aws:ec2:region:cr_owner_account_id:capacity-reservation/cr_id"
   ],
   "detail":{
      "capacity-reservation-id":"cr_id",
      "updateTime":timestamp,
      "ownerAccountId":"cr_owner_account_id",
      "unusedReservationChargesOwnerID":"consumer_account_id",
      "status":"pending|accepted|rejected|cancelled|revoked|expired",
      "statusMessage":"message
   }
}
```

O exemplo a seguir é de um evento enviado ao proprietário da reserva de capacidade (222222222222) quando uma conta de consumidor (111111111111) aceita uma solicitação de atribuição de faturamento para uma reserva de capacidade compartilhada (cr-01234567890abcdef).

```
{
   "version":"0",
   "id":"12345678-1234-1234-1234-123456789012",
   "detail-type":"On-Demand Capacity Reservation Billing Ownership Request accepted",
   "source":"aws.ec2",
   "account":"222222222222",
   "time":"2024-09-01Thh:59:59Z",
   "region":"us-east-1",
   "resources":[
      "arn:aws:ec2:us-east-1:222222222222:capacity-reservation/cr-01234567890abcdef"
   ],
   "detail":{
      "capacity-reservation-id":"cr-01234567890abcdef",
      "updateTime":"2024-08-01Thh:59:59Z",
      "ownerAccountId":"222222222222",
      "unusedReservationChargesOwnerID":"111111111111",
      "status":"accepted",
```

```
      "statusMessage":"billing transfer status message"
   }
}
```

Permissões de Reserva de capacidade compartilhada

Permissões para proprietários

Os proprietários são responsáveis por gerenciar e cancelar suas Reservas de Capacidade compartilhadas. Os proprietários não podem modificar instâncias em execução na Reserva de capacidade compartilhada que sejam de propriedade de outras contas. Os proprietários continuam responsáveis pelo gerenciamento das instâncias que executam na Reserva de capacidade compartilhada.

Permissões para consumidores

Os consumidores são responsáveis pelo gerenciamento de suas instâncias que estão em execução na Reserva de capacidade compartilhada. Os consumidores não podem modificar a Reserva de capacidade compartilhada de nenhuma forma e não podem visualizar nem modificar instâncias que são de propriedade de outros consumidores ou do proprietário da Reserva de capacidade. Os consumidores só podem visualizar a capacidade total e a capacidade disponível na reserva compartilhada.

Faturamento e medição

Não há cobranças adicionais pelo compartilhamento de Reservas de Capacidade.

Por padrão, o proprietário da reserva compartilhada é cobrado pelas instâncias que executa na reserva de capacidade e por qualquer capacidade não utilizada, enquanto os consumidores são cobrados pelas instâncias que executam na reserva de capacidade compartilhada. No entanto, você pode atribuir o faturamento da capacidade disponível de uma reserva de capacidade compartilhada a uma conta de consumidor específica. Para obter mais informações, consulte Atribuição de faturamento para reservas de capacidade compartilhadas do Amazon EC2.

Se o proprietário da reserva de capacidade pertencer a uma conta de pagador diferente e a reserva de capacidade estiver coberta por uma instância reservada regional ou por um Savings Plan, o proprietário da reserva de capacidade continuará sendo cobrado pela instância reservada regional ou pelo Savings Plan. Nesses casos, o proprietário da reserva de capacidade paga pela instância reservada regional ou pelo Savings Plan, e os consumidores são cobrados pelas instâncias que executam na reserva de capacidade compartilhada.

Limites de instâncias

Todo o uso da Reserva de capacidade é contado em relação aos limites de instância sob demanda do proprietário da Reserva de capacidade. Isso inclui:

- Capacidade reservada não utilizada
- Uso por instâncias de propriedade do proprietário da Reserva de capacidade
- Uso por instâncias de propriedade de consumidores

As instâncias executadas na capacidade reservada por consumidores são contadas em relação ao limite de instância sob demanda do proprietário da Reserva de capacidade. Os limites de instâncias dos consumidores são a soma de seus próprios limites de instância sob demanda e a capacidade disponível nas Reservas de Capacidade compartilhadas que podem acessar.

Frotas de reserva de capacidade

Umafrota de reserva de capacidade sob demanda é um grupo de reservas de capacidade.

Uma solicitação de frota de reserva de capacidade contém todas as informações de configuração necessárias para iniciar uma frota de reserva de capacidade. Com uma só solicitação, é possível reservar grandes quantidades de capacidade do Amazon EC2 para sua workload em vários tipos de instância, até uma capacidade de destino especificada.

Após criar uma frota de reserva de capacidade, é possível gerenciar coletivamente as reservas de capacidade na frota modificando ou cancelando a frota de reserva de capacidade.

Tópicos

- Funcionamento das frotas de reserva de capacidade
- Considerações
- Preços
- Conceitos e planejamento de frota de reserva de capacidade
- Criar uma frota de reserva de capacidade
- Modificar uma frota de reserva de capacidade
- Cancelar uma frota de reserva de capacidade
- Exemplo de configurações de frota de reserva de capacidade

- Uso de funções vinculadas aos serviços para a frota de reserva de capacidade

Funcionamento das frotas de reserva de capacidade

Quando você cria uma frota de reserva de capacidade, a frota tenta criar reservas individuais de capacidade para atender à capacidade total de destino especificada na solicitação de frota.

O número de instâncias para as quais a frota reserva capacidade depende da capacidade total pretendida e dos pesos dos tipos de instâncias especificados por você. O tipo de instância para o qual a capacidade é reservada depende da estratégia de alocação e das prioridades de tipos de instâncias que você usa.

Se não houver capacidade suficiente no momento de criação da frota e ela não conseguir atingir imediatamente sua capacidade total de destino, a frota tentará criar assíncronamente reservas de capacidade até que tenha reservado a quantidade de capacidade solicitada.

Quando a frota atinge sua capacidade total de destino, ela tenta manter essa capacidade. Se houver o cancelamento de uma reserva de capacidade na frota, dependendo da configuração da frota, ela criará automaticamente uma ou mais reservas de capacidade para substituir a capacidade perdida e manter a capacidade total de destino.

Não é possível gerenciar as reservas de capacidade na frota individualmente. Elas devem ser gerenciadas coletivamente modificando a frota. Quando você modifica uma frota, as reservas de capacidade na frota são atualizadas automaticamente para refletir as alterações.

Atualmente, as frotas de reserva de capacidade são compatíveis com os critérios `open` de correspondência de instâncias, e todas as reservas de capacidade executadas por uma frota usam automaticamente esses critérios de correspondência de instâncias. Com esse critério, novas instâncias e instâncias existentes que têm atributos correspondentes (por exemplo: tipo de instância, plataforma, zona de disponibilidade e locação) são executadas automaticamente nas reservas de capacidade criadas por uma frota. As frotas de reserva de capacidade não são compatíveis com critérios de correspondência de instâncias direcionadas.

Considerações

Ao trabalhar com frotas de reserva de capacidade, lembre-se do seguinte:

- Uma frota de reserva de capacidade pode ser criada, modificada, visualizada e cancelada usando a AWS CLI e API da AWS.

- Não é possível gerenciar as reservas de capacidade em uma frota individualmente. Elas devem ser gerenciadas coletivamente modificando ou cancelando a frota.
- Uma frota de reserva de capacidade não pode abranger regiões.
- Uma frota de reserva de capacidade não pode abranger zonas de disponibilidade.
- Reservas de capacidade criadas por uma frota de reserva de capacidade são marcadas automaticamente com a seguinte etiqueta gerada da AWS:
  - Chave – — `aws:ec2-capacity-reservation-fleet`
  - Valor – — *`fleet_id`*

  É possível usar essa etiqueta para identificar reservas de capacidade que foram criadas por uma frota de reserva de capacidade.

Preços

Não há cobranças adicionais pelo uso de frotas de reserva de capacidade. Você recebe cobranças pelas reservas de capacidade individuais criadas por suas frotas de reserva de capacidade. Para mais informações sobre o faturamento de reservas de capacidade, consulte Definição de preços e faturamento da Reserva de capacidade.

Conceitos e planejamento de frota de reserva de capacidade

As informações a seguir descrevem como planejar uma frota de reserva de capacidade e descrevem os conceitos de frota de reserva de capacidade, incluindo capacidade total de destino, estratégia de alocação, peso do tipo de instância e prioridade do tipo de instância.

Tópicos

- Planejar uma frota de reserva de capacidade
- Capacidade total de destino
- Estratégia de alocação
- Peso do tipo de instância
- Prioridade do tipo de instância

Planejar uma frota de reserva de capacidade

Ao planejar uma frota de reserva de capacidade, recomendamos que você faça o seguinte:

1. Determine a quantidade de capacidade computacional necessária para sua workload.
2. Decida os tipos de instância e zonas de disponibilidade que deseja usar.
3. Atribua uma prioridade a cada tipo de instância com base em suas necessidades e preferências. Para obter mais informações, consulte Prioridade do tipo de instância.
4. Crie um sistema de ponderação de capacidade que faça sentido para sua workload. Atribua um peso a cada tipo de instância e determine sua capacidade total de destino. Para obter mais informações, consulte Peso do tipo de instância e Capacidade total de destino.
5. Determine se precisa da reserva de capacidade indefinidamente ou apenas por um período de tempo específico.

Capacidade total de destino

A capacidade total de destino define a quantidade total de capacidade computacional que a frota de reserva de capacidade reserva. Você especifica a capacidade total de destino ao criar a frota de reserva de capacidade. Após a criação da frota, o Amazon EC2 cria automaticamente reservas de capacidade para reservar capacidade até a capacidade total de destino.

O número de instâncias para as quais a frota de reserva de capacidade reserva a capacidade é determinado pela capacidade total de destino e pelo peso do tipo de instância que você especificar para cada tipo de instância na frota de reserva de capacidade (`total target capacity/instance type weight = number of instances`).

É possível atribuir uma capacidade total de destino com base em unidades que são significativas para sua workload. Por exemplo, se sua workload exigir um determinado número de vCPUs, será possível atribuir a capacidade total de destino com base no número necessário de vCPUs. Se sua workload exigir `2048` vCPUs, especifique uma capacidade total de destino de `2048` e, em seguida, atribua pesos de tipo de instância com base no número de vCPUs fornecidas pelos tipos de instância na frota. Para ver um exemplo, consulte Peso do tipo de instância.

Estratégia de alocação

A estratégia de alocação para sua frota de reserva de capacidade determina como ela atenderá a solicitações de capacidade reservada das especificações de tipo de instância na configuração da frota de reserva de capacidade.

Atualmente, só há compatibilidade com a estratégia de alocação `prioritized`. Com essa estratégia, a frota de reserva de capacidade cria reservas de capacidade usando as prioridades que você atribuiu a cada uma das especificações de tipo de instância na configuração da frota de reserva

de capacidade. Valores mais baixos de prioridade indicam maior prioridade para uso. Por exemplo, digamos que você crie uma frota de reserva de capacidade que use os seguintes tipos de instância e prioridades:

- `m4.16xlarge` – prioridade = 1
- `m5.16xlarge` – prioridade = 3
- `m5.24xlarge` – prioridade = 2

Primeiramente a frota tenta criar reservas de capacidade para `m4.16xlarge`. Se o Amazon EC2 tiver capacidade insuficiente da `m4.16xlarge`, a frota tenta criar reservas de capacidade para `m5.24xlarge`. Se o Amazon EC2 tiver capacidade insuficiente da `m5.24xlarge`, a frota cria reservas de capacidade para `m5.16xlarge`.

Peso do tipo de instância

O peso do tipo de instância é um peso que você atribui a cada tipo de instância na frota de reserva de capacidade. O peso determina quantas unidades de capacidade cada instância do tipo específico de instância são contabilizadas na capacidade total de destino da frota.

É possível atribuir pesos com base em unidades que são significativas para sua workload. Por exemplo, se sua workload exigir um determinado número de vCPUs, será possível atribuir pesos com base no número de vCPUs fornecidas por cada tipo de instância na frota de reserva de capacidade. Nesse caso, se você criar uma frota de reserva de capacidade usando instâncias `m4.16xlarge` e `m5.24xlarge`, você atribuiria pesos que correspondem ao número de vCPUs para cada instância da seguinte forma:

- `m4.16xlarge` – `64` vCPUs, peso = `64` unidades
- `m5.24xlarge` – `96` vCPUs, peso = `96` unidades

O peso do tipo de instância determina o número de instâncias para as quais a frota de reserva de capacidade reserva a capacidade. Por exemplo, se uma frota de reserva de capacidade com uma capacidade de destino total de `384` unidades usar os tipos e pesos de instância do exemplo anterior, a frota poderia reservar capacidade para 6 instâncias `m4.16xlarge` (384 de capacidade total de destino/64 de tipo de instância com peso = 6 instâncias), ou `4` instâncias `m5.24xlarge` (384/96 = 4).

Se você não atribuir pesos de tipo de instância ou se atribuir um peso de tipo de instância de 1, a capacidade total de destino é baseada puramente na contagem de instâncias. Por exemplo, se uma

frota de reserva de capacidade com uma capacidade total de destino de 384 unidades usar os tipos de instância do exemplo anterior, mas omitir os pesos ou especificar um peso de 1 para ambos os tipos de instância, a frota poderia reservar capacidade para 384 instâncias `m4.16xlarge` ou 384 instâncias `m5.24xlarge`.

Prioridade do tipo de instância

A prioridade do tipo de instância é um valor que você atribui aos tipos de instância na frota. As prioridades são usadas para determinar quais dos tipos de instância especificados para a frota devem ter o uso priorizado.

Valores mais baixos de prioridade indicam uma maior prioridade para uso.

Criar uma frota de reserva de capacidade

Quando você cria uma frota de reserva de capacidade, ela cria automaticamente reservas de capacidade para os tipos de instância especificados na solicitação de frota, até a capacidade total de destino especificada. O número de instâncias para as quais a frota de reserva de capacidade reserva capacidade depende da capacidade total de destino e dos pesos de tipo de instância que você especifica na solicitação. Para obter mais informações, consulte Peso do tipo de instância e Capacidade total de destino.

Ao criar a frota, especifique os tipos de instância a serem usados e uma prioridade para cada um desses tipos de instância. Para obter mais informações, consulte Estratégia de alocação e Prioridade do tipo de instância.

> **Note**
>
> A função AWSServiceRoleForEC2CapacityReservationFleet vinculada a serviço é criada automaticamente em sua conta na primeira vez que você cria uma frota de reserva de capacidade. Para obter mais informações, consulte Uso de funções vinculadas aos serviços para a frota de reserva de capacidade.

Atualmente, as frotas de reserva de capacidade são compatíveis apenas com os critérios `open` de correspondência de instâncias.

AWS CLI

Para criar uma frota de reserva de capacidade

Use o comando create-capacity-reservation-fleet.

```
aws ec2 create-capacity-reservation-fleet \
    --total-target-capacity 24 \
    --allocation-strategy prioritized \
    --instance-match-criteria open \
    --tenancy default \
    --end-date 2021-12-31T23:59:59.000Z \
    --instance-type-specifications file://instanceTypeSpecification.json
```

Veja a seguir o conteúdo de `instanceTypeSpecification.json`.

```
[
  {
    "InstanceType": "m5.xlarge",
    "InstancePlatform": "Linux/UNIX",
    "Weight": 3.0,
    "AvailabilityZone":"us-east-1a",
    "EbsOptimized": true,
    "Priority" : 1
  }
]
```

O seguinte é um exemplo de saída.

```
{
    "Status": "submitted",
    "TotalFulfilledCapacity": 0.0,
    "CapacityReservationFleetId": "crf-abcdef01234567890",
    "TotalTargetCapacity": 24
}
```

PowerShell

Para criar uma frota de reserva de capacidade

Use o cmdlet New-EC2CapacityReservationFleet.

```
New-EC2CapacityReservationFleet `
    -TotalTargetCapacity 24 `
    -AllocationStrategy "prioritized" `
    -InstanceMatchCriterion "open" `
```

```
    -Tenancy "default" `
    -EndDate 2021-12-31T23:59:59.000Z `
    -InstanceTypeSpecification $specification
```

A especificação é definida conforme a seguir.

```
$specification = New-Object Amazon.EC2.Model.ReservationFleetInstanceSpecification
$specification.InstanceType = "m5.xlarge"
$specification.InstancePlatform = "Linux/UNIX"
$specification.Weight = 3.0
$specification.AvailabilityZone = "us-east-1a"
$specification.EbsOptimized = $true
$specification.Priority = 1
```

Modificar uma frota de reserva de capacidade

É possível modificar a qualquer momento a capacidade total de destino e a data de uma frota de reserva de capacidade. Ao modificar a capacidade total de destino de uma frota de reserva de capacidade, a frota cria automaticamente novas reservas de capacidade ou modifica ou cancela as reservas de capacidade existentes na frota para atender à nova capacidade total de destino. Quando você modifica a data de término da frota, as datas de término de todas as reservas de capacidade individuais são atualizadas de maneira adequada.

Considerações

- Após modificar uma frota, o status dela muda para `modifying`. Não é possível tentar fazer modificações adicionais em uma frota enquanto ela estiver no estado `modifying`.
- Você não pode modificar a locação, a zona de disponibilidade, os tipos de instância, as plataformas de instância, as prioridades ou os pesos usados por uma frota de reserva de capacidade. Se precisar alterar qualquer um desses parâmetros, talvez seja necessário cancelar a frota existente e criar uma nova com os parâmetros necessários.
- Não é possível especificar `--end-date` e `--remove-end-date` no mesmo comando.

AWS CLI

Para modificar uma frota de reserva de capacidade

Use o comando modify-capacity-reservation-fleet.

Exemplo 1: modificar a capacidade total do destino

```
aws ec2 modify-capacity-reservation-fleet \
    --capacity-reservation-fleet-id crf-01234567890abcedf \
    --total-target-capacity 160
```

Exemplo 2: modificar a data de término

```
aws ec2 modify-capacity-reservation-fleet \
    --capacity-reservation-fleet-id crf-01234567890abcedf \
    --end-date 2021-07-04T23:59:59.000Z
```

Exemplo 3: remover a data de término

```
aws ec2 modify-capacity-reservation-fleet \
    --capacity-reservation-fleet-id crf-01234567890abcedf \
    --remove-end-date
```

PowerShell

Para modificar uma frota de reserva de capacidade

Use o cmdlet Edit-EC2CapacityReservationFleet.

Exemplo 1: modificar a capacidade total do destino

```
Edit-EC2CapacityReservationFleet `
    -CapacityReservationFleetId crf-01234567890abcedf `
    -TotalTargetCapacity 160
```

Exemplo 2: modificar a data de término

```
Edit-EC2CapacityReservationFleet `
    -CapacityReservationFleetId crf-01234567890abcedf `
    -EndDate 2021-07-04T23:59:59.000Z
```

Exemplo 3: remover a data de término

```
Edit-EC2CapacityReservationFleet `
    -CapacityReservationFleetId crf-01234567890abcedf `
```

```
    -RemoveEndDate
```

Cancelar uma frota de reserva de capacidade

Quando não precisar mais de uma frota de reserva de capacidade e da capacidade que ela reserva, é possível cancelá-la. Quando você cancela uma frota, o status muda para `cancelled` e ela não poderá mais criar novas reservas de capacidade. Além disso, todas as reservas de capacidade individuais na frota são canceladas. As instâncias que estavam em execução anteriormente na capacidade reservada continuam a ser executadas normalmente na capacidade compartilhada.

AWS CLI

Para cancelar uma frota de reserva de capacidade

Use o comando cancel-capacity-reservation-fleets.

```
aws ec2 cancel-capacity-reservation-fleets \
    --capacity-reservation-fleet-ids crf-abcdef01234567890
```

O seguinte é um exemplo de saída.

```
{
    "SuccessfulFleetCancellations": [
        {
            "CurrentFleetState": "cancelling",
            "PreviousFleetState": "active",
            "CapacityReservationFleetId": "crf-abcdef01234567890"
        }
    ],
    "FailedFleetCancellations": []
}
```

PowerShell

Para cancelar uma frota de reserva de capacidade

Use o cmdlet Stop-EC2CapacityReservationFleet.

```
Stop-EC2CapacityReservationFleet `
    -CapacityReservationFleetId crf-abcdef01234567890
```

Exemplo de configurações de frota de reserva de capacidade

O exemplo a seguir cria uma frota de reserva de capacidade que usa dois tipos de instância: `m5.4xlarge` e `m5.12xlarge`.

Ele usa um sistema de ponderação com base no número de vCPUs fornecidas pelos tipos de instância especificados. A capacidade total de destino é de `480` vCPUs. O tipo `m5.4xlarge` fornece 16 vCPUs e tem um peso de 16, enquanto o `m5.12xlarge` fornece 48 vCPUs e tem um peso de 48. Este sistema de ponderação configura a frota de reserva de capacidade para reservar capacidade para 30 instâncias `m5.4xlarge` (480/16 = 30) ou 10 instâncias `m5.12xlarge` (480/48 = 10).

A frota está configurada para priorizar a capacidade de `m5.12xlarge` e obtém prioridade de 1, enquanto `m5.4xlarge` obtém uma prioridade mais baixa de 2. Isso significa que a frota tentará reservar primeiramente a capacidade de `m5.12xlarge`, e só tentará reservar `m5.4xlarge` se o Amazon EC2 tiver capacidade insuficiente de `m5.12xlarge`.

A frota reserva a capacidade para `Windows` instâncias e a reserva expira automaticamente em `October 31, 2021` às `23:59:59` UTC.

```
aws ec2 create-capacity-reservation-fleet \
    --total-target-capacity 480 \
    --allocation-strategy prioritized \
    --instance-match-criteria open \
    --tenancy default \
    --end-date 2021-10-31T23:59:59.000Z \
    --instance-type-specifications file://instanceTypeSpecification.json
```

Veja a seguir o conteúdo de `instanceTypeSpecification.json`.

```
[
    {
        "InstanceType": "m5.4xlarge",
        "InstancePlatform":"Windows",
        "Weight": 16,
        "AvailabilityZone":"us-east-1a",
        "EbsOptimized": true,
        "Priority" : 2
    },
    {
        "InstanceType": "m5.12xlarge",
        "InstancePlatform":"Windows",
```

```
        "Weight": 48,
        "AvailabilityZone":"us-east-1a",
        "EbsOptimized": true,
        "Priority" : 1
    }
]
```

Uso de funções vinculadas aos serviços para a frota de reserva de capacidade

A frota de reserva de capacidade sob demanda usa funções vinculadas a serviço do AWS Identity and Access Management (IAM). Uma função vinculada a serviço é um tipo exclusivo de função do IAM vinculada diretamente à frota de reserva de capacidade. As funções vinculadas a serviço são predefinidas pela frota de reserva de capacidade e incluem todas as permissões que o serviço requer para chamar outros serviços da AWS em seu nome.

Uma função vinculada a serviço facilita a configuração da frota de reserva de capacidade porque você não precisa adicionar as permissões necessárias manualmente. A frota de reserva de capacidade define as permissões das funções vinculadas a serviço e, exceto se definido de outra forma, somente a frota de reserva de capacidade pode assumir suas funções. As permissões definidas incluem a política de confiança e a política de permissões, que não pode ser anexada a nenhuma outra entidade do IAM.

Um perfil vinculado ao serviço poderá ser excluído somente após excluir seus atributos relacionados. Isso protege seus recursos da frota de reserva de capacidade, pois você não pode remover por engano as permissões para acessar os recursos.

Permissões de funções vinculadas aos serviços para a frota de reserva de capacidade

A Frota de reservas de capacidade usa o perfil vinculado ao serviço denominado AWSServiceRoleForEC2CapacityReservationFleet para criar, descrever, modificar e cancelar Reservas de capacidade em uma Frota de reservas de capacidade em seu nome.

O perfil vinculado a serviço AWSServiceRoleForEC2CapacityReservationFleet confia nas entidades a seguir para assumir o perfil:

- `capacity-reservation-fleet.amazonaws.com`

Esse perfil usa a política gerenciada pela AWS `AWSEC2CapacityReservationFleetRolePolicy`. Para obter mais informações, consulte AWS Política gerenciada da: AWSEC2CapacityReservationFleetRolePolicy.

Você deve configurar permissões para que uma entidade do IAM (por exemplo, um usuário, grupo ou função) crie, edite ou exclua um perfil vinculado a serviço. Para obter mais informações, consulte Permissões de perfil vinculado a serviços no Guia do usuário do IAM.

Criar uma função vinculada ao serviço para a frota de reserva de capacidade

Não é necessário criar manualmente um perfil vinculado ao serviço. Quando você cria uma frota de reserva de capacidade usando o comando `create-capacity-reservation-fleet` da AWS CLI ou a API `CreateCapacityReservationFleet`, a função vinculada a serviço é criada automaticamente para você.

Se excluir esse perfil vinculado ao serviço e precisar criá-lo novamente, será possível usar esse mesmo processo para recriar o perfil em sua conta. Quando você cria uma frota de reserva de capacidade, a frota de reserva de capacidade cria a função vinculada a serviço para você novamente.

Editar uma função vinculada ao serviço para a frota de reserva de capacidade

A frota de reserva de capacidade não permite que você edite a função vinculada a serviço AWSServiceRoleForEC2CapacityReservationFleet. Depois que criar um perfil vinculado ao serviço, você não poderá alterar o nome do perfil, pois várias entidades podem fazer referência a ele. No entanto, será possível editar a descrição do perfil usando o IAM. Para obter mais informações, consulte Editar uma descrição de perfil vinculado ao serviço no Guia do usuário do IAM.

Excluir uma função vinculada ao serviço para a frota de reserva de capacidade

Se você não precisar mais usar um recurso ou serviço que requer um perfil vinculado ao serviço, é recomendável excluí-lo. Dessa forma, você não tem uma entidade não utilizada que não seja monitorada ativamente ou mantida. No entanto, é necessário excluir os recursos de sua função vinculada a serviço antes que seja possível exclui-la manualmente.

> **Note**
>
> Se o serviço da frota de reserva de capacidade estiver usando a função quando você tentar excluir os recursos, a exclusão poderá falhar. Se isso acontecer, espere alguns minutos e tente a operação novamente.

Para excluir a função vinculada a serviço AWSServiceRoleForEC2CapacityReservationFleet

1. Use o comando `delete-capacity-reservation-fleet` da AWS CLI ou a API `DeleteCapacityReservationFleet` para excluir as frotas de reserva de capacidade em sua conta.
2. Use o console do IAM, a AWS CLI ou a API da AWS para excluir a função vinculada a serviço AWSServiceRoleForEC2CapacityReservationFleet. Para obter mais informações, consulte Excluir uma função vinculada ao serviço no Guia do usuário do IAM.

Regiões com suporte a funções vinculadas aos serviços para frota de reserva de capacidade

A frota de reserva de capacidade é compatível com o uso de funções vinculadas a serviço em todas as regiões nas quais o serviço esteja disponível. Para mais informações, consulte Regiões e endpoints da AWS.

Monitorar o uso de reservas de capacidade com métricas do CloudWatch

Com as métricas do CloudWatch, é possível monitorar as Reservas de Capacidade e identificar a capacidade não utilizada configurando os alarmes do CloudWatch para notificá-lo quando os limites de uso forem atingidos. Isso pode ajudá-lo a manter um volume constante de Reserva de capacidade e atingir um nível mais alto de utilização.

As reservas de capacidade enviam dados de métricas ao CloudWatch a cada cinco minutos. Não há suporte para métricas de Reservas de Capacidade que estejam ativas por menos de cinco minutos.

Para obter mais informações sobre como visualizar métricas no console do CloudWatch, consulte Usar as métricas do Amazon CloudWatch. Para obter mais informações sobre como criar alarmes, consulte Criar alarmes do Amazon CloudWatch.

Tópicos

- Métricas de uso da Reserva de capacidade
- Dimensões de métricas da Reserva de capacidade
- Visualizar métricas do CloudWatch nas Reservas de Capacidade

Métricas de uso da Reserva de capacidade

O namespace `AWS/EC2CapacityReservations` inclui as seguintes métricas de uso que é possível usar para monitorar e manter a capacidade sob demanda dentro dos limites especificados para sua reserva.

Métrica	Descrição
`UsedInstanceCount`	O número de instâncias que estão em uso no momento. Unidade: contagem
`AvailableInstanceCount`	O número de instâncias disponíveis. Unidade: contagem
`TotalInstanceCount`	O número total de instâncias reservadas. Unidade: contagem
`InstanceUtilization`	A porcentagem de instâncias de capacidade reservada que estão em uso no momento. Unidade: percentual

Dimensões de métricas da Reserva de capacidade

É possível usar as dimensões a seguir para refinar as métricas listadas na tabela anterior na região e na conta selecionada.

Dimensão	Descrição
(Nenhuma dimensão)	Esta dimensão filtra a métrica especificada para todas as reservas de capacidade.

Dimensão	Descrição
`CapacityReservationId`	Esta dimensão filtra a métrica especificada para a reserva de capacidade identificada.
`InstanceType`	Esta dimensão filtra a métrica especificada para o tipo de instância identificado.
`AvailabilityZone`	Esta dimensão filtra a métrica especificada para a zona de disponibilidade identificada.
`InstanceMatchCriteria`	Esta dimensão filtra a métrica especificada para os critérios de correspondência da instância identificados (`open` ou `targeted`).
`InstancePlatform`	Esta dimensão filtra os dados da métrica especificada para a plataforma identificada.
`Tenancy`	Esta dimensão filtra a métrica especificada para a locação identificada.

Visualizar métricas do CloudWatch nas Reservas de Capacidade

As métricas são agrupadas primeiro pelo namespace do serviço e, em seguida, pelas várias dimensões com suporte. É possível usar os procedimentos a seguir para visualizar as métricas de suas Reservas de Capacidade.

Para visualizar as métricas da Reserva de capacidade usando o console do CloudWatch

1. Abra o console do CloudWatch em https://console.aws.amazon.com/cloudwatch/.
2. Se necessário, altere a região. Na barra de navegação, selecione a região em que a Reserva de capacidade reside. Para obter mais informações, consulte Regiões e endpoints.
3. No painel de navegação, selecione Metrics (Métricas).
4. Para Todas as métricas, escolha Reservas de Capacidade do EC2.

5. Escolha entre as dimensões métricas anteriores Para todas as reservas de capacidade, Por reserva de capacidade, Por tipo de instância, Por zona de disponibilidade, Por plataforma, Por critérios de correspondência de instância ou Por locação, e as métricas serão agrupadas por Nenhuma dimensão, `CapacityReservationId`, `InstanceType`, `AvailabilityZone`, `Platform`, `InstanceMatchCriteria` e `Tenancy`, respectivamente.
6. Para classificar a métrica, use o cabeçalho da coluna. Para criar um gráfico de uma métrica, marque a caixa de seleção ao lado da métrica.

Para visualizar métricas da reserva de capacidade via AWS CLI

Use o comando list-metrics a seguir:

```
aws cloudwatch list-metrics --namespace "AWS/EC2CapacityReservations"
```

Monitorar a subutilização da Reserva de capacidade

É possível monitorar a subutilização da Reserva de capacidade usando o seguinte:

Tópicos

- Eventos do Amazon EventBridge
- Notificações por e-mail e no painel do AWS Health

Eventos do Amazon EventBridge

O AWS Health envia eventos para o Amazon EventBridge quando uma reserva de capacidade em sua conta está abaixo de 20% do uso em determinados períodos. Com o EventBridge, é possível estabelecer regras que acionam ações programáticas em resposta a tais eventos. Por exemplo, você pode criar uma regra que vai cancelar automaticamente uma reserva de capacidade quando a utilização estiver abaixo de 20% em um período de sete dias.

Os eventos no EventBridge são representados como objetos JSON. Os campos que são exclusivos do evento estão contidos na seção "detalhes" do objeto JSON. O campo "evento" contém o nome do evento. O campo "resultados" contém o status concluído da ação que acionou o evento. Para obter mais informações, consulte Amazon EventBridge event patterns no Amazon EventBridge User Guide.

Para saber mais, consulte o Guia do Usuário do Amazon EventBridge.

Não há suporte a este recurso na AWS GovCloud (US).

Eventos

O AWS Health enviará os eventos a seguir quando o uso de capacidade para uma reserva de capacidade estiver abaixo de 20%.

- `AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION`

  Veja a seguir um exemplo de evento gerado quando uma reserva de capacidade recém-criada está abaixo de 20% do uso da capacidade em um período de 24 horas.

```
{
    "version": "0",
    "id": "b3e00086-f271-12a1-a36c-55e8ddaa130a",
    "detail-type": "AWS Health Event",
    "source": "aws.health",
    "account": "123456789012",
    "time": "2023-03-10T12:03:38Z",
    "region": "ap-south-1",
    "resources": [
        "cr-01234567890abcdef"
    ],
    "detail": {
        "eventArn": "arn:aws:health:ap-south-1::event/EC2/
AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION/
AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION_cr-01234567890abcdef-6211-4d50-9286-0c9fbc243f04",
        "service": "EC2",
        "eventTypeCode": "AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION",
        "eventTypeCategory": "accountNotification",
        "startTime": "Fri, 10 Mar 2023 12:03:38 GMT",
        "endTime": "Fri, 10 Mar 2023 12:03:38 GMT",
        "eventDescription": [
            {
                "language": "en_US",
                "latestDescription": "A description of the event will be provided
 here"
            }
        ],
        "affectedEntities": [
            {
                "entityValue": "cr-01234567890abcdef"
            }
```

```
        ]
    }
    }
```

- AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION_SUMMARY

  Veja a seguir um exemplo de evento gerado quando uma ou mais reservas de capacidade estão abaixo de 20% do uso da capacidade em um período de sete dias.

```
{
    "version": "0", "id":"7439d42b-3c7f-ad50-6a88-25e2a70977e2",
    "detail-type": "AWS Health Event",
    "source": "aws.health",
    "account": "123456789012",
    "time": "2023-03-07T06:06:01Z",
    "region": "us-east-1",
    "resources": [
        "cr-01234567890abcdef | us-east-1b | t3.medium | Linux/UNIX | 0.0%",
        "cr-09876543210fedcba | us-east-1a | t3.medium | Linux/UNIX | 0.0%"
    ],
    "detail": {
        "eventArn": "arn:aws:health:us-east-1::event/
EC2/AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION_SUMMARY/
AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION_SUMMARY_726c1732-d6f6-4037-b9b8-
bec3c2d3ba65",
        "service": "EC2",
        "eventTypeCode": "AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION_SUMMARY",
        "eventTypeCategory": "accountNotification",
        "startTime": "Tue, 7 Mar 2023 06:06:01 GMT",
        "endTime": "Tue, 7 Mar 2023 06:06:01 GMT",
        "eventDescription": [
            {
                "language": "en_US",
                "latestDescription": "A description of the event will be provided
 here"
            }
        ],
        "affectedEntities": [
            {
                "entityValue": "cr-01234567890abcdef | us-east-1b | t3.medium |
 Linux/UNIX | 0.0%"
            },
            {
```

```
                "entityValue": "cr-09876543210fedcba | us-east-1a | t3.medium |
 Linux/UNIX | 0.0%"
            }
        ]
    }
}
```

Criar uma regra de EventBridge

Para receber notificações por e-mail quando a utilização da reserva de capacidade estiver abaixo de 20%, crie um tópico do Amazon SNS e, em seguida, crie uma regra do EventBridge para o evento `AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION`.

Para criaro tópico do Amazon SNS

1. Abra o console do Amazon SNS em https://console.aws.amazon.com/sns/v3/home.
2. No painel de navegação, selecione Topics (Tópicos) e Create topic (Criar tópico).
3. Em Tipo, escolha Padrão.
4. Em Nome, digite um nome para o novo tópico.
5. Escolha Criar tópico.
6. Selecione Criar assinatura.
7. Em Protocolo, escolha E-mail e, em seguida, para Endpoint, insira o endereço de e-mail que receberá as notificações.
8. Selecione Criar assinatura.
9. O endereço de e-mail inserido acima receberá uma mensagem de e-mail com a seguinte linha de assunto: `AWS Notification - Subscription Confirmation`. Siga as instruções para confirmar sua assinatura.

Como criar a regra do EventBridge

1. Abra o console do Amazon EventBridge em https://console.aws.amazon.com/events/.
2. No painel de navegação, escolha Rules (Regras) e Create rule (Criar regras).
3. Em Nome, digite um nome para a nova regra.
4. Em Rule type, escolha Rule with an event pattern.
5. Escolha Próximo.

6. Em Padrão de evento, faça o seguinte:
    a. Em Fonte do evento, selecione Serviços da AWS.
    b. Em Serviço da AWS, escolha AWS Health.
    c. Em Tipo de evento, escolha Notificação de subutilização de ODCR do EC2.
7. Escolha Próximo.
8. Em Destino 1, faça o seguinte:
    a. Em Tipos de destino, escolha Serviço da AWS.
    b. Em Select a target (Selecionar um destino), escolha SNS topic (Tópico do SNS).
    c. Em Tópico, escolha o tópico criado anteriormente.
9. Selecione Próximo e, em seguida, Próximo novamente.
10. Escolha Criar regra.

Notificações por e-mail e no painel do AWS Health

O AWS Health enviará o e-mail e as notificações do Health Dashboard a seguir quando a utilização da capacidade para reservas de capacidade em sua conta estiver abaixo de 20%.

- Notificações individuais para cada reserva de capacidade recém-criada que esteve abaixo de 20% de utilização nas últimas 24 horas.
- Uma notificação resumida para todas as reservas de capacidade que estiveram abaixo de 20% de utilização nos últimos sete dias.

As notificações por e-mail e as notificações do Health Dashboard serão enviadas para o endereço de e-mail associado à conta da AWS que tem as reservas de capacidade como propriedade. As notificações incluem as seguintes informações:

- O ID da reserva de capacidade.
- A zona de disponibilidade da reserva de capacidade.
- A taxa de utilização média para a reserva de capacidade.
- O tipo de instância e a plataforma (sistema operacional) da reserva de capacidade.

Além disso, quando a utilização da capacidade de uma reserva de capacidade em sua conta estiver abaixo de 20% em um período de 24 horas e sete dias, o AWS Health enviará eventos para o

EventBridge. Com o EventBridge, é possível criar regras que ativam ações automáticas, como o envio de notificações por e-mail ou o acionamento de funções do AWS Lambda, em resposta a esses eventos. Para obter mais informações, consulte Monitorar a subutilização da Reserva de capacidade.

Monitorar alterações de estado para Reservas de capacidade com data no futuro

O Amazon EC2 envia um evento ao Amazon EventBridge quando o estado de uma Reserva de capacidade com data no futuro é alterado.

Veja a seguir um exemplo desse evento. Neste exemplo, a Reserva de capacidade com data futura entrou no estado `scheduled`. Observe o estado realçado no campo `detail-type`.

```
{
   "version":"0",
   "id":"12345678-1234-1234-1234-123456789012",
   "detail-type":"EC2 Capacity Reservation Scheduled",
   "source":"aws.ec2",
   "account":"123456789012",
   "time":"yyyy-mm-ddThh:mm:ssZ",
   "region":"us-east-1",
   "resources":[
      "arn:aws:ec2:us-east-1:123456789012:capacity-reservation/cr-1234567890abcdefg"
   ],
   "detail":{
      "capacity-reservation-id":"cr-1234567890abcdefg",
      "state":"scheduled"
   }
}
```

Os valores possíveis para o campo `detail-type` são:

- `Scheduled`
- `Active`
- `Delayed`
- `Unsupported`
- `Failed`
- `Expired`

Para mais informações sobre esses estados, consulte Visualizar o estado de uma reserva de capacidade.

É possível criar eventos do Amazon EventBridge que monitoram esses eventos e, em seguida, acionam ações específicas quando eles ocorrerem. Para obter mais informações, consulte Criar regras que reagem a eventos no Amazon EventBridge.

Para criar uma regra que monitora todos os eventos de alteração de estado, você pode usar o seguinte padrão de evento.

```
{
  "source": ["aws.ec2"],
  "detail-type": [{
    "prefix": "EC2 Capacity Reservation"
  }]
}
```

Para criar uma regra que monitora apenas alterações de estado específicas, você pode usar o seguinte padrão de evento.

```
{
  "source": ["aws.ec2"],
  "detail-type": [{
    "prefix": "EC2 Capacity Reservation state"
  }]
}
```

Por exemplo, o padrão de eventos a seguir monitora os eventos que são enviados quando uma Reserva de capacidade com data no futuro entra no estado `active`.

```
{
  "source": ["aws.ec2"],
  "detail-type": [{
    "prefix": "EC2 Capacity Reservation Active"
  }]
}
```

Reservas de capacidade

As Reservas de capacidade interruptíveis ajudam você a disponibilizar temporariamente a capacidade não utilizada para outras workloads em sua conta. Isso lhe dá controle para recuperar

a capacidade quando necessário. Quando você recupera a capacidade, todas as instâncias em execução dentro da reserva interruptível são encerradas. Depois de criar uma reserva interruptível, você pode compartilhá-la com contas AWS adicionais ou com sua organização AWS usando o AWS Resource Access Manager (RAM).

Use Reservas de capacidade interruptíveis quando tiver capacidade reservada não utilizada fora dos períodos de pico, entre implantações ou quando a workload diminui. Se você conhece outra equipe que poderia usar essa capacidade, pode disponibilizá-la criando uma Reserva de capacidade interruptível. Quando sua workload crítica precisar de capacidade de volta, você pode recuperá-la.

Você pode usar Reservas de capacidade interruptíveis como uma das seguintes opções:

- Proprietário da capacidade — Você é o proprietário da Reserva de capacidade de origem e cria a reserva de capacidade interruptível para compartilhar a capacidade não utilizada com outras equipes, mantendo o controle para recuperá-la quando necessário.
- Consumidor de capacidade — Você inicia instâncias em reservas interruptíveis compartilhadas, entendendo que suas instâncias podem ser encerradas quando o proprietário recupera a capacidade.

Tópicos

- Como funciona
- Faturamento
- Considerações
- Reservas de capacidade interruptíveis para proprietários de capacidade
- Reservas de capacidade interruptíveis para consumidores de capacidade
- Monitore Reservas de capacidade interruptíveis com o EventBridge e o CloudTrail

Como funciona

Para disponibilizar a capacidade não utilizada para outras equipes, crie uma reserva interruptível especificando o número de instâncias não utilizadas que você deseja compartilhar da sua reserva de origem. Quando você cria a reserva interruptível, transferimos essas instâncias da sua reserva de origem para a nova reserva interruptível em sua conta.

Mantemos a associação entre a reserva de origem e a Reserva de capacidade interruptível. Como resultado, quando você recupera sua capacidade, todas as instâncias de consumo em execução são encerradas e a capacidade é restaurada para sua reserva de origem original.

Principais recursos:

- Disponibilize temporariamente a capacidade não utilizada, mantendo o controle para recuperá-la
- Recupere a capacidade a qualquer momento. Para obter mais informações, consulte . Processo de recuperação e rastreamento
- Compartilhe com contas adicionais ou com sua organização AWS usando o AWS Resource Access Manager (RAM)

Faturamento

Quando você cria uma reserva interruptível, ela é cobrada como uma nova reserva independente. Isso divide seu faturamento:

- Reserva de origem: você é cobrado pela capacidade total menos a capacidade alocada
- Reserva interruptível: você é cobrado pela capacidade alocada

Para obter mais informações sobre o faturamento de Reservas de capacidade sob demanda, consulte Preços e faturamento de Reservas de capacidade.

Considerações

Antes de usar Reservas de capacidade interruptíveis, analise as seguintes limitações e requisitos que se aplicam aos proprietários e consumidores de capacidade.

Proprietários de capacidade

- Você não pode modificar ou cancelar diretamente uma Reserva de capacidade interruptível. Para editá-la, atualize a capacidade alocada da Reserva de Capacidade de origem.
- Você só pode visualizar, lançar, marcar, compartilhar e atribuir faturamento para reservas interruptíveis.
- Só é possível criar uma alocação interruptível por Reserva de capacidade de origem.

Consumidores de capacidade

- As Reservas de capacidade interruptíveis são, por padrão, Reservas de capacidade direcionadas, então você precisa direcioná-las na execução da sua instância.

- Você não pode adicionar Reservas de capacidade interruptíveis aos grupos de reserva de capacidade.
- Recomendamos que você só use Reservas de capacidade interruptíveis para aplicativos que podem ser interrompidos.
- Suas instâncias serão encerradas quando o proprietário recuperar a capacidade — não há alternativa para o On-Demand ou o Spot. Para obter mais informações, consulte Experiência de interrupção.

Reservas de capacidade interruptíveis para proprietários de capacidade

O proprietário da capacidade é a conta que possui a Reserva de capacidade de origem e cria a Reserva de capacidade interruptível para compartilhar a capacidade não utilizada com outras equipes, mantendo o controle para recuperá-la quando necessário.

Esta seção aborda como você (o proprietário da capacidade) pode criar, modificar, recuperar e rastrear uma Reserva de capacidade interruptível.

Tópicos

- Criar uma Reserva de capacidade interruptível
- Veja sua Reserva de capacidade interruptível
- Modificando sua Reserva de capacidade interruptível
- Processo de recuperação e rastreamento
- Compartilhamento de reservas interruptíveis

Criar uma Reserva de capacidade interruptível

Crie uma Reserva de capacidade interruptível para disponibilizar a capacidade não utilizada de sua reserva de origem para outras workloads, mantendo o controle para recuperá-la quando necessário.

Pré-requisitos

Antes de criar uma alocação interruptível, certifique-se de que sua Reserva de capacidade sob demanda de origem atenda aos seguintes requisitos:

- Sua Reserva de capacidade deve estar ativa sem data de término definida. Você não pode criar alocações a partir de reservas pendentes, expiradas, canceladas ou com datas de término programadas.

- Sua Reserva de capacidade deve ter capacidade disponível para alocação. Você só pode alocar instâncias disponíveis (também chamada de capacidade não utilizada).
- Só é possível criar uma alocação interruptível por Reserva de capacidade de origem. Se uma alocação já existir, você deverá modificá-la ou cancelá-la antes de criar uma nova.
- Você pode alocar no máximo 1.000 instâncias de uma vez para uma Reserva de capacidade interruptível.

O usuário pode usar o console ou o AWS CLI para criar uma Reserva de capacidade interruptível.

Console

Criar uma Reserva de capacidade interruptível

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Escolha Reservas de capacidade.
3. Selecione sua Reserva de capacidade.
4. Escolha Ações, Criar alocação interruptível.
5. Em Instâncias a alocar, insira o número de instâncias para alocação.
6. (Opcional) Adicione tags.
7. Escolha Criar alocação de capacidade interruptível.

AWS CLI

Para criar uma Reserva de capacidade interruptível

Use o comando create-interruptible-capacity-reservation-allocation:

```
aws ec2 create-interruptible-capacity-reservation-allocation \
    --capacity-reservation-id cr-1234567890abcdef0 \
    --instance-count 10
```

Veja sua Reserva de capacidade interruptível

Depois de criar uma Reserva de capacidade interruptível, você pode ver a reserva interruptível em sua conta ou em um recurso específico.

Visualize todas as Reservas de capacidade interruptíveis em sua conta

Use o procedimento a seguir para visualizar Reservas de capacidade interruptíveis em sua conta.

Console

Para visualizar Reservas de capacidade interruptíveis em sua conta

1. Acesse a página de Reservas de capacidade no console.
2. Procure reservas com a indicação Interruptível na coluna de tipos.
3. Selecione a reserva interruptível para visualizar detalhes.

AWS CLI

Para ver as Reservas de capacidade interruptíveis em sua conta

```
aws ec2 describe-capacity-reservations \
    --capacity-reservation-id cr-interruptible-id \
    --filters Name=interruptible,Values=true
```

Exibir Reserva de capacidade interruptível de uma fonte específica

Use o procedimento a seguir para visualizar a Reserva de capacidade interruptível criada a partir de uma Reserva de capacidade de origem específica.

```
aws ec2 describe-capacity-reservations \
    --capacity-reservation-id cr-source-id
```

Na resposta, você encontrará um objeto `interruptibleCapacityAllocations` que contém o ID de Reserva de capacidade interruptível e os detalhes da alocação. Para obter informações sobre a estrutura de resposta, consulte InterruptibleCapacityAllocation na Referência da API do Amazon EC2.

Modificando sua Reserva de capacidade interruptível

Use os procedimentos a seguir para editar ou cancelar sua Reserva de capacidade interruptível.

> **Note**
>
> - Quando você reduz a alocação, primeiro recuperamos as instâncias disponíveis e, em seguida, as instâncias em execução, até atingirmos a contagem solicitada. Se conseguirmos atender à contagem inteiramente com as instâncias disponíveis, nenhuma rescisão ocorrerá. Todas as modificações na contagem de instâncias alocadas são feitas por meio da Reserva de capacidade de origem, não diretamente na Reserva de capacidade interruptível.
> - Você só pode modificar uma Reserva de capacidade interruptível em no máximo 1000 instâncias de uma vez (aumento ou diminuição).

Edite sua Reserva de capacidade interruptível

Use o procedimento a seguir para editar sua Reserva de capacidade interruptível.

Console

1. Na página de detalhes da Reserva de capacidade de origem, escolha Ações. Em seguida, edite a Reserva de capacidade interruptível.
2. Para alocar Instâncias, insira o novo número:
   - Adicione mais capacidade de compartilhamento
   - Recupere a capacidade de sua reserva de capacidade de origem
3. Selecione Atualizar.

AWS CLI

```
aws ec2 update-interruptible-capacity-reservation-allocation \
    --capacity-reservation-id cr-1234567890abcdef0 \
    --target-instance-count 80
```

Cancele sua Reserva de capacidade interruptível

Use o procedimento a seguir para remover permanentemente a alocação e retornar toda a capacidade.

Console

1. Na página de detalhes da Reserva de capacidade de origem, navegue até os detalhes da alocação de capacidade interruptível.
2. Escolha Editar alocação interruptível.
3. Em Contagem de instâncias, insira 0.
4. Selecione Atualizar.

AWS CLI

```
aws ec2 update-interruptible-capacity-reservation-allocation \
--capacity-reservation-id cr-1234567890abcdef0 \
--target-instance-count 0
```

Processo de recuperação e rastreamento

Quando você recupera a capacidade:

- As instâncias em execução recebem um aviso de interrupção de 2 minutos por meio de eventos do EventBridge.
- Após o período de notificação, as instâncias em execução na capacidade recuperada entram em um estado de desligamento e são encerradas.
- Quando encerradas, as instâncias recuperadas ficam disponíveis em sua Reserva de capacidade de origem para uso imediato.
- Seu status de alocação muda de atualizado para ativo quando concluído.

A recuperação completa pode levar alguns minutos, dependendo do tipo de instância e do tempo de desligamento. Para obter mais informações sobre a notificação do EventBridge que você recebe quando o processo é concluído, consulte Conclusão de recuperação.

Rastrear o status da recuperação

Monitore o progresso da recuperação descrevendo sua reserva de origem:

```
aws ec2 describe-capacity-reservations \
--capacity-reservation-id cr-1234567890abcdef0
```

A resposta mostra esses campos dentro do objeto `interruptibleCapacityAllocation`:

- `instance-count`: instâncias alocadas atuais
- `target-instance-count`: quantidade solicitada após a reclamação
- `status`: atualizando durante a recuperação e ativo quando concluído

Compartilhamento de reservas interruptíveis

Você pode compartilhar reservas interruptíveis somente dentro da sua organização AWS usando o AWS Resource Access Manager (RAM).

Considerações:

- Se uma conta de consumidor sair da sua organização, a reserva interruptível será automaticamente descompartilhada dessa conta.
- Todas as instâncias em execução na reserva não compartilhada serão eventualmente encerradas.
- Todas as outras funcionalidades de compartilhamento funcionam da mesma forma que as Reservas de capacidade padrão.

Para obter os procedimentos completos de compartilhamento, consulte Compartilhar reservas de capacidade.

Reservas de capacidade interruptíveis para consumidores de capacidade

O consumidor de capacidade é a conta que inicia instâncias em Reservas de capacidade interruptíveis compartilhadas, entendendo que suas instâncias podem ser encerradas quando o proprietário recupera a capacidade.

Esta seção aborda como você (o consumidor de capacidade) pode iniciar instâncias em uma Reserva de capacidade interruptível e aprender sobre o que acontece quando a capacidade é recuperada pelo proprietário.

Tópicos

- Exibir uma Reserva de capacidade interruptível
- Iniciar instâncias em Reservas interruptíveis
- Experiência de interrupção

Exibir uma Reserva de capacidade interruptível

Use os procedimentos a seguir para visualizar uma Reserva de capacidade interruptível.

Console

Visualizar Reservas de capacidade interruptíveis em sua conta

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Escolha Reservas de capacidade.
3. Na coluna Tipo, procure as reservas marcadas como Interruptíveis.
4. Anote os IDs de reserva para uso nas execuções de sua instância.

AWS CLI

Para encontrar todas as Reservas de capacidade interruptíveis em sua conta

Use o comando describe-capacity-reservations:

```
aws ec2 describe-capacity-reservations \
--filters Name=state,Values=active
```

Procure as reservas onde `Interruptible` está definido como `true` na resposta.

Para filtrar especificamente por reservas interruptíveis

Use o seguinte comando:

```
aws ec2 describe-capacity-reservations \
--capacity-reservation-ids cr-example123 \
--query 'CapacityReservations[?Interruptible==`true`]'
```

> **Note**
>
> As Reservas de capacidade interruptíveis são, por padrão, Reservas de capacidade direcionadas, então você precisa direcioná-las especificamente na execução da sua instância. Ao contrário das reservas abertas, as reservas interruptíveis não cobrirão

automaticamente as instâncias correspondentes. Você deve especificar explicitamente o ID da reserva no lançamento.

Iniciar instâncias em Reservas interruptíveis

Use o procedimento a seguir para iniciar instâncias do Amazon EC2 em Reservas de capacidade interruptíveis em sua conta.

> **Note**
>
> Recomendamos que você só use Reservas de capacidade interruptíveis para aplicativos que podem ser interrompidos.

Console

Para iniciar instâncias em Reservas de capacidade interruptíveis

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. Defina suas configurações de instância.
4. Em Detalhes avançados para Reserva de capacidade, escolha Iniciar instâncias interruptíveis em sua reserva ativa.
5. Selecione o ID de reserva interruptível e a nova opção de compra da instância.
6. Escolha Iniciar instância.

AWS CLI

```
aws ec2 run-instances \
--instance-type m5.large \
--count 2 \
--image-id ami-12345678 \
--instance-market-options '{
    "MarketType": "interruptible-capacity-reservation"
}' \
--capacity-reservation-specification '{
    "CapacityReservationTarget": {
```

```
        "CapacityReservationId": "cr-abcdef1234567890"
    }
}'
```

Execute instâncias com Grupos do Auto Scaling

Você também pode iniciar instâncias em reservas interruptíveis usando Grupos do Auto Scaling com modelos de lançamento. Configure o modelo de lançamento com o tipo de mercado interruptível e o ID de reserva e, em seguida, crie seu Grupo do Auto Scaling usando esse modelo. Para obter mais informações, consulte Reservas de capacidade de interrupção com o EC2 Auto Scaling.

Experiência de interrupção

Quando a capacidade é recuperada pelo proprietário, você recebe um aviso de interrupção 2 minutos antes do encerramento da instância. Esse aviso vem por meio de eventos do EventBridge, dando a você tempo para:

- Salve seu trabalho ou verifique seus aplicativos
- Encerrar processos
- Preparar o término de uma instância

O evento EventBridge inclui detalhes sobre quais instâncias serão encerradas e o horário exato da rescisão. Para obter mais informações, consulte Alerta de interrupção da instância.

Monitore Reservas de capacidade interruptíveis com o EventBridge e o CloudTrail

As Reservas de capacidade interruptíveis enviam notificações do EventBridge e eventos do CloudTrail para ajudá-lo a monitorar e responder às mudanças de capacidade.

Tópicos

- Notificações do EventBridge
- Eventos do CloudTrail

Notificações do EventBridge

Você recebe dois tipos de notificações do EventBridge. Para obter informações sobre a configuração de notificações do EventBridge, consulte Criação de regras do Amazon EventBridge.

Alerta de interrupção da instância

Se você estiver executando instâncias em uma reserva interruptível, receberá essa notificação 2 minutos antes de suas instâncias serem encerradas:

```
{
    "version": "0",
    "id": "12345678-1234-1234-1234-123456789012",
    "detail-type": "EC2 Capacity Reservation Instance Interruption Warning",
    "source": "aws.ec2",
    "account": "[instance owner Account ID]",
    "time": "[Current time in yyyy-mm-ddThh:mm:ssZ]",
    "resources": "[instance arn]",
    "region": "[region]",
    "detail": {
        "instance-id": "[instance-id]",
        "instance-action": "terminate",
        "instance-termination-time": "yyyy-mm-ddThh:mm:ssZ",
        "azId": "[availability-zone-id]"
    }
}
```

Conclusão de recuperação

Se você for proprietário da reserva de origem, receberá esta notificação quando a recuperação de capacidade for concluída:

```
{
    "version": "0",
    "id": "12345678-1234-1234-1234-123456789012",
    "detail-type": "EC2 Interruptible Capacity Reservation Allocation Reclamation
 Completed",
    "source": "aws.ec2",
    "account": "[source Capacity Reservation Owner Account ID]",
    "time": "[Current time in yyyy-mm-ddThh:mm:ssZ]",
    "region": "us-east-1",
    "resources": ["source_cr_arn"],
    "detail": {
        "sourceCapacityReservationId": "string",
        "instanceType": "string",
        "availabilityZoneId": "string",
        "TotalInstanceCount": "current total count in the source",
        "ReclaimedInstanceCount": "count of instances added to the source",
```

```
        "targetInstanceCount": "number"
    }
}
```

Eventos do CloudTrail

O CloudTrail registra esses eventos para Reservas de capacidade interruptíveis:

- `InterruptibleCapacityReservationCreated`— Quando você cria uma alocação interruptível
- `InterruptibleCapacityReservationAllocationUpdated`— Quando você modifica a alocação
- `InterruptibleCapacityReservationCancelled`— Quando você cancela a alocação
- `CapacityReservationModified`— Quando modificamos a reserva de origem para alocação
- `InterruptibleCapacityReservationInstancesTerminated`— Quando encerramos instâncias durante a reclamação

Blocos de capacidade para ML

Os blocos de capacidade para ML permitem que você reserve instâncias de computação acelerada baseadas em GPU em uma data futura para acomodar suas workloads de machine learning (ML) de curta duração. As instâncias executadas em um bloco de capacidade são automaticamente colocadas próximas umas das outras nos Amazon EC2 UltraClusters para redes sem bloqueio de baixa latência com escala de petabits.

Também é possível usar os blocos de capacidade para reservar capacidade nos servidores UltraServers do Amazon EC2. Os servidores UltraServers conectam várias instâncias do Amazon EC2 em uma interconexão aceleradora de baixa latência e alta largura de banda. Você pode usar os servidores UltraServers para lidar com as workloads de IA e ML que mais utilizam computação e memória em treinamento, ajuste e inferência. Para obter mais informações, consulte Amazon EC2 UltraServers.

Com blocos de capacidade, você pode ver quando a capacidade da instância de GPU está disponível em datas futuras e agendar um bloco de capacidade para começar na hora que for melhor para você. Quando você reserva um bloco de capacidade, garante capacidade previsível de instâncias de GPU e pagando apenas pelo tempo que precisar. Recomendamos blocos de capacidade quando você precisa de GPUs para lidar com workloads de ML durante dias ou semanas seguidos e não deseja pagar por uma reserva enquanto as instâncias de GPU não estão em uso.

Estes são alguns casos de uso comuns de blocos de capacidade.

- Treinamento e ajuste fino de modelo de ML: tenha acesso ininterrupto às instâncias de GPU que você reservou para realizar treinamento e ajuste fino do modelo de ML.
- Experimentos e protótipos de ML: executar experimentos e desenvolver protótipos que exigem instâncias de GPU por períodos curtos.

Os Blocos de capacidade estão disponíveis para determinados tipos de instância em algumas regiões da AWS. Para obter mais informações, consulte Tipos de instância e regiões compatíveis.

É possível reservar um bloco de capacidade para uma hora de início em até oito semanas no futuro. Cada bloco de capacidade pode ter até 64 instâncias, e você pode ter até 256 instâncias nos blocos de capacidade.

Tópicos

- Tipos de instância e regiões compatíveis
- Plataformas compatíveis
- Considerações
- Recursos relacionados
- Como funcionam os blocos de capacidade do Amazon EC2
- Preços e faturamento de blocos de capacidade
- Encontrar e comprar blocos de capacidade
- Iniciar instâncias usando blocos de capacidade
- Visualizar blocos de capacidade
- Estender blocos de capacidade
- Compartilhar Blocos de capacidade
- Criar um grupo de recursos para Blocos de capacidade do UltraServer
- Monitorar blocos de capacidade usando o EventBridge
- Registrar em log chamadas de API de blocos de capacidade com o AWS CloudTrail

Tipos de instância e regiões compatíveis

Os blocos de capacidade da instância e UltraServer podem ser usados com os seguintes tipos de instância e regiões da AWS.

> **Note**
>
> Tamanhos de blocos de capacidade de 64 instâncias não são compatíveis com todos os tipos de instância em todas as Regiões da AWS.

Blocos de capacidade da instância

- **p6-b300.48xlarge**
  - Oeste dos EUA (Oregon): | | |) — us-west-2
- **p6-b200.48xlarge**
  - Leste dos EUA (Norte da Virgínia) — us-east-1
  - Leste dos EUA (Ohio): us-east-2
  - Oeste dos EUA (Oregon): | | |) — us-west-2
- **p5.4xlarge**
  - Leste dos EUA (Norte da Virgínia) — us-east-1
  - Leste dos EUA (Ohio): us-east-2
  - Oeste dos EUA (Oregon): | | |) — us-west-2
  - Europa (Londres): eu-west-2
  - Ásia-Pacífico (Mumbai): ap-south-1
  - Ásia-Pacífico (Tóquio): ap-northeast-1
  - Ásia-Pacífico (Sydney): ap-southeast-2
  - América do Sul (São Paulo): sa-east-1
- **p5.48xlarge**
  - Leste dos EUA (Norte da Virgínia) — us-east-1
  - Leste dos EUA (Ohio): us-east-2
  - Oeste dos EUA (Norte da Califórnia): us-west-1
  - Oeste dos EUA (Oregon): | | |) — us-west-2
  - Europa (Estocolmo): eu-north-1
  - Europa (Londres): eu-west-2
  - América do Sul (São Paulo): sa-east-1
  - Ásia-Pacífico (Tóquio): ap-northeast-1

  - Ásia-Pacífico (Mumbai): `ap-south-1`
  - Ásia-Pacífico (Sydney): `ap-southeast-2`
  - Ásia-Pacífico (Jacarta): `ap-southeast-3`
- **`p5e.48xlarge`**
  - Leste dos EUA (Norte da Virgínia) — `us-east-1`
  - Leste dos EUA (Ohio): `us-east-2`
  - Oeste dos EUA (Norte da Califórnia): `us-west-1`
  - Oeste dos EUA (Oregon): | | |) — `us-west-2`
  - Europa (Estocolmo): `eu-north-1`
  - Europa (Londres): `eu-west-2`
  - Europa (Espanha): `eu-south-2`
  - América do Sul (São Paulo): `sa-east-1`
  - Ásia-Pacífico (Tóquio): `ap-northeast-1`
  - Ásia-Pacífico (Seul): `ap-northeast-2`
  - Ásia-Pacífico (Mumbai): `ap-south-1`
  - Ásia-Pacífico (Jacarta): `ap-southeast-3`
- **`p4d.24xlarge`**
  - Leste dos EUA (Norte da Virgínia) — `us-east-1`
  - Leste dos EUA (Ohio): `us-east-2`
  - Oeste dos EUA (Oregon): | | |) — `us-west-2`
- **`p4de.24xlarge`**
  - Leste dos EUA (Norte da Virgínia):) — `us-east-1`
  - Oeste dos EUA (Oregon):) — `us-west-2`
- **`trn1.32xlarge`**
  - Leste dos EUA (Norte da Virgínia) — `us-east-1`
  - Leste dos EUA (Ohio): `us-east-2`
  - Oeste dos EUA (Norte da Califórnia): `us-west-1`
  - Oeste dos EUA (Oregon): | | |) — `us-west-2`
  - Europa (Estocolmo): `eu-north-1`
  - Ásia-Pacífico (Mumbai): `ap-south-1`

  - Ásia-Pacífico (Sydney): `ap-southeast-2`
  - Ásia-Pacífico (Melbourne): `ap-southeast-4`
- **`trn2.3xlarge`**
  - Ásia-Pacífico (Melbourne): `ap-southeast-4`
  - América do Sul (São Paulo): `sa-east-1`
- **`trn2.48xlarge`**
  - Leste dos EUA (Ohio): `us-east-2`

Blocos de capacidade UltraServer

- **`Trn2`**
  - Leste dos EUA (Ohio): `us-east-2`
- **`P6e-GB200`**
  - Zona local de Dallas (Norte da Virgínia) — `us-east-1-dfw-2a`

Plataformas compatíveis

Atualmente, os blocos de capacidade para ML são compatíveis apenas com instâncias e UltraServers que tenham locação padrão. Quando você usa o Console de gerenciamento da AWS para comprar um bloco de capacidade, a opção de plataforma padrão é a Linux/UNIX. Quando você usa a AWS Command Line Interface (AWS CLI) ou o AWS SDK para comprar um bloco de capacidade, as seguintes opções de plataforma estão disponíveis:

- Linux/UNIX
- Red Hat Enterprise Linux
- RHEL com HA
- SUSE Linux
- Ubuntu Pro

Considerações

Antes de usar os blocos de capacidade, considere os seguintes detalhes e limitações.

- Se detectarmos uma deficiência afetando um Bloco de Capacidade do UltraServer, notificaremos você, mas geralmente não tomaremos medidas para encerrar suas instâncias no Bloco de

Capacidade. O objetivo é minimizar a interrupção não intencional em suas workloads. Você pode continuar usando o Bloco de Capacidade do UltraServer como está após receber essa notificação ou solicitar a correção encerrando todas as instâncias no bloco de capacidade e enviando um caso de suporte. AWS Após recebermos seu caso de suporte, notificaremos você quando concluirmos a correção e você poderá reiniciar as instâncias em seu Bloco de Capacidade UltraServer.

- Nos blocos de capacidade do UltraServer `P6e-GB200`, é necessário encerrar suas instâncias pelo menos 60 minutos antes do horário de término do bloco de capacidade.
- Para usar os blocos de capacidade do UltraServer `P6e-GB200`, é necessário se inscrever na zona local de Dallas (Norte da Virgínia).
- Cada bloco de capacidade pode ter até 64 instâncias, e você pode ter até 256 instâncias nos blocos de capacidade.
- É possível descrever as ofertas do bloco de capacidade que podem começar em apenas 30 minutos.
- Os blocos de capacidade terminam às 11h30, Horário Universal Coordenado (UTC).
- O processo de encerramento de instâncias em execução em um bloco de capacidade começa às 11h, Horário Universal Coordenado (UTC) no último dia da reserva.
- Os blocos de capacidade podem ser reservados para uma hora de início em até oito semanas no futuro.
- Não são permitidos cancelamentos de bloqueios de capacidade.
- Os Blocos de capacidade do UltraServer não podem ser compartilhados entre contas da AWS nem dentro da sua organização da AWS.
- O bloco de capacidade não pode ser movido ou dividido.
- Apenas blocos de capacidade UltraServer podem ser utilizados com grupos de recursos. Blocos de capacidade de instância não podem ser utilizados com grupos de recursos. Para obter mais informações, consulte Criar um grupo de recursos para Blocos de capacidade do UltraServer.
- O número total de instâncias que podem ser reservadas em blocos de capacidade entre todas as contas da sua organização da AWS não pode ultrapassar 256 instâncias em uma determinada data.
- Para usar um bloco de capacidade, as instâncias devem ser direcionadas especificamente para o ID da reserva.
- As instâncias em um bloco de capacidade não contam para seus limites de instâncias sob demanda.

- Para instâncias P5 usando uma AMI personalizada, verifique se você tem os softwares e a configuração necessários para EFA.
- Para grupos de nós gerenciados do Amazon EKS, consulte Criar um grupo de nós gerenciados com blocos de capacidade do Amazon EC2 para ML. Para grupos de nós autogerenciados do Amazon EKS, consulte Usar blocos de capacidade para ML com nós autogerenciados.

Recursos relacionados

Após criar um bloco de capacidade, será possível fazer o seguinte com ele:

- Iniciar instâncias no bloco de capacidade. Para obter mais informações, consulte Iniciar instâncias usando blocos de capacidade.
- Crie um grupo do Amazon EC2 Auto Scaling. Para obter mais informações, consulte Usar blocos de capacidade para workloads de machine learning no Guia do usuário do Amazon EC2 Auto Scaling.

  > **Note**
  >
  > Se você usa o Amazon EC2 Auto Scaling ou o Amazon EKS, é possível programar a escalabilidade para ser executada no início da reserva do bloco de capacidade. Com o escalamento programado, o AWS gerencia automaticamente as novas tentativas para que você não precise se preocupar em implementar uma lógica de repetições para lidar com falhas transitórias.

- Melhore os fluxos de trabalho de ML com o AWS ParallelCluster. Para obter mais informações, consulte Aprimorar fluxos de trabalho de ML com o AWS ParallelCluster e blocos de capacidade do Amazon EC2 para ML.

Para obter mais informações sobre o AWS ParallelCluster, consulte O que é o AWS ParallelCluster.

Como funcionam os blocos de capacidade do Amazon EC2

Você pode reservar um bloco de capacidade com as seguintes especificações:

- Reserve um horário de início com até oito semanas de antecedência
- Defina a duração de uma reserva de 1 a 14 dias ou um múltiplo de 7 dias, até 182 dias (exemplos: 21 dias, 28 dias)

- Configure até 64 instâncias por bloco de capacidade
- Configure até 256 instâncias em vários blocos de capacidade

Nos servidores UltraServers do Amazon EC2, cada um corresponde a um bloco de capacidade. Você pode fazer uma única solicitação para vários servidores UltraServers.

Você pode usar blocos de capacidade para reservar instâncias `p6-b200`, `p5`, `p5e`, `p5en`, `p4d`, `p4de`, `trn1` e `trn2`. Compre os seguintes tipos de servidores UltraServer usando blocos de capacidade: `P6e-GB200` e `Trn2` (em pré-visualização).

Para reservar um bloco de capacidade, você começa especificando suas necessidades de capacidade, incluindo o tipo de instância ou o tipo de servidor UltraServer, o número de instâncias ou de UltraServers, a quantidade de tempo, a data de início mais antiga e a última data de término de que precisa. Depois, você vê uma oferta disponível do bloco de capacidade que atende às suas especificações. A oferta do bloco de capacidade inclui detalhes como hora de início, zona de disponibilidade e preço da reserva. O preço de oferta de um bloco de capacidade depende da disponibilidade e da demanda no momento em que a oferta é feita. Depois que você reserva um bloco de capacidade, o preço não muda mais. Para obter mais informações, consulte Preços e faturamento de blocos de capacidade.

Quando você compra uma oferta de bloco de capacidade, a reserva é criada para a data e o número de instâncias selecionados. Quando sua reserva de bloco de capacidade começa, você pode direcionar as inicializações de instância especificando o ID da reserva nas solicitações de inicialização.

É possível usar todas as instâncias reservadas por até 30 minutos (para os tipos de instância) ou 60 minutos (para o tipo de servidor UltraServer) antes da hora de término do bloco de capacidade. Faltando 30 minutos (para os tipos de instância) ou 60 minutos (para os tipos de servidor UltraServer) para o fim da reserva do bloco de capacidade, começamos a encerrar todas as instâncias em execução no bloco de capacidade. Usamos esse tempo para limpar as instâncias antes de entregar o bloco de capacidade ao próximo cliente. Emitimos um evento por meio do EventBridge 10 minutos antes do início do processo de encerramento. Para obter mais informações, consulte Monitorar blocos de capacidade usando o EventBridge.

Preços e faturamento de blocos de capacidade

Com os blocos de capacidade para ML do Amazon EC2, você só paga pelo que reserva. O preço de um bloco de capacidade depende da disponibilidade e da demanda de blocos de capacidade

no momento da compra. É possível ver o preço de uma oferta de bloco de capacidade antes de fazer a reserva. O preço do bloco de capacidade é cobrado à vista no momento em que a reserva é feita. Quando você pesquisa um bloco de capacidade em um intervalo de datas, retornamos a oferta de bloco de capacidade com o menor preço disponível. Depois que você reservou um bloco de capacidade, o preço não muda mais.

Quando você usa um bloco de capacidade, paga pelo sistema operacional que usa quando as instâncias estão em execução. Para obter mais informações sobre os preços de sistemas operacionais, consulte Amazon EC2 Capacity Blocks for ML Pricing.

Faturamento

O preço de uma oferta de bloco de capacidade é cobrado à vista. O pagamento é faturado na sua conta da AWS dentro de 5 minutos a 12 horas após a compra de um bloco de capacidade. Enquanto seu pagamento é processado, o recurso de reserva do bloco de capacidade permanece em um estado `payment-pending`. Se o pagamento não puder ser processado pelo menos cinco minutos antes do horário de início do bloco ou em 12 horas (o que ocorrer primeiro), o bloco de capacidade será liberado e o estado da reserva passará a ser `payment-failed`.

Depois que o pagamento é processado com sucesso, o estado do recurso do bloco de capacidade passa de `payment-pending` para `scheduled`. Você recebe uma fatura que reflete o pagamento antecipado à vista. Na fatura, você pode associar o valor pago ao ID da reserva do bloco de capacidade.

Quando a reserva do bloco de capacidade começa, você é cobrado com base apenas no sistema operacional que usa enquanto as instâncias estão em execução na reserva. É possível ver o uso e as cobranças associadas até a data de fechamento da sua fatura mensal de uso no AWS Cost and Usage Report.

> **Note**
>
> Os descontos dos Savings Plans e das instâncias reservadas não se aplicam aos blocos de capacidade.

Visualizar sua fatura

É possível visualizar sua conta no console do AWS Billing and Cost Management. O pagamento antecipado do bloco de capacidade aparece no mês em que você adquiriu a reserva.

Depois que sua reserva começa, sua fatura mostra linhas separadas para o tempo usado e não usado da reserva do bloco. É possível usar esses itens de linha para ver quanto tempo foi usado de sua reserva. Você só verá uma cobrança por uso na linha de tempo usado se usar um sistema operacional premium. Para obter mais informações, consulte Preços e faturamento de blocos de capacidade. Não há custo adicional por tempo não usado.

Para obter mais informações, consulte Exibição da sua fatura no Guia do usuário do AWS Billing and Cost Management.

Se o bloco de capacidade começar em um mês diferente do mês em que você adquiriu a reserva, o preço inicial e o uso da reserva aparecerão em meses de cobrança diferentes. No seu AWS Cost and Usage Report, o ID da reserva do bloco de capacidade está listado no item da linha reservation/ReservationARN do pagamento antecipado e o lineItem/ResourceID na fatura mensal fechada para que você possa associar o uso ao preço pago antecipadamente correspondente.

Encontrar e comprar blocos de capacidade

Para reservar um bloco de capacidade, primeiro, você precisa encontrar um bloco de tempo durante o qual a capacidade esteja disponível e que atenda às suas necessidades. Para encontrar um bloco de capacidade disponível para reservar, você deve especificar os itens a seguir.

- O número de instâncias de que você precisa
- O tempo durante o qual você precisa das instâncias
- O intervalo de datas quando você precisa da reserva

Para pesquisar uma oferta disponível de bloco de capacidade, você especifica a duração da reserva e o número de instâncias. É necessário especificar durações de reserva em incrementos de 1 dia até um total de 14 dias e incrementos de 7 dias até um total de 182 dias. Cada bloco de capacidade pode ter até 64 instâncias, e você pode ter até 256 instâncias nos blocos de capacidade.

Ao solicitar um bloco de capacidade que atenda às suas especificações, fornecemos os detalhes de até três blocos disponíveis. Todos os blocos de capacidade terminam às 11h30 UTC, então os blocos que começam no mesmo dia terão durações mais próximas da duração desejada. Um bloco terá uma duração um pouco menor que a duração desejada, enquanto a de outro será um pouco maior.

Os detalhes da oferta incluem a hora de início da reserva, a zona de disponibilidade da reserva e o preço da reserva. Para obter mais informações, consulte Preços e faturamento de blocos de capacidade.

É possível comprar a oferta de bloco de capacidade exibida ou modificar os critérios de pesquisa para ver as outras opções disponíveis. Não há prazo de validade predefinido para a oferta, mas as ofertas só estão disponíveis por ordem de chegada.

Ao comprar uma oferta de bloco de capacidade, você recebe uma resposta imediata confirmando que o bloco de capacidade foi reservado. Após a confirmação, você verá uma nova reserva de capacidade em sua conta com um tipo de reserva de `capacity-block` e uma `start-date` definida como a hora de início da oferta que você comprou. A reserva do bloco de capacidade é criada em um estado de `payment-pending`. Depois que o pagamento antecipado é processado com sucesso, o estado da reserva passa a ser `scheduled`. Para obter mais informações, consulte Faturamento.

> **Note**
>
> Para usar os blocos de capacidade do UltraServer `P6e-GB200`, é necessário se inscrever na zona local de Dallas (Norte da Virgínia).

Console

Para encontrar e comprar um bloco de capacidade

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Na barra de navegação na parte superior da tela, selecione uma Região da AWS. Essa escolha é importante porque os tamanhos de blocos de capacidade de 64 instâncias não são compatíveis com todos os tipos de instância em todas as regiões.
3. No painel de navegação, escolha Reservas de capacidade, Criar bloco de capacidade.
4. Em Tipos de blocos de capacidade, escolha Instâncias ou UltraServers.
5. Em Atributos de capacidade, você pode definir os parâmetros da pesquisa de bloco de capacidade. Por padrão, a plataforma é Linux. Se você quiser selecionar outro sistema operacional, use a AWS CLI. Para obter mais informações, consulte Plataformas compatíveis.
6. Em Capacidade total (para instâncias) ou Contagem de UltraServer (para UltraServers), especifique o número de instâncias ou UltraServers que deseja reservar.
7. Em Duração, insira o número de dias ou semanas durante os quais você precisa da reserva.
8. Em Intervalo de datas para pesquisar blocos de capacidade, insira a data mais antiga em que você deseja que a reserva comece.

9. Escolha Encontrar blocos de capacidade.
10. Se houver um bloco de capacidade disponível que atenda às suas especificações, você verá uma oferta em Blocos de capacidade recomendados. Se houver várias ofertas que atendam às suas especificações, a oferta de bloco de capacidade disponível mais antiga será exibida. Para ver outras ofertas de blocos de capacidade, ajuste as entradas da pesquisa e escolha Localizar blocos de capacidade novamente.
11. Quando encontrar uma oferta do bloco de capacidade que você queira comprar, escolha Avançar.
12. (Opcional) Na página Adicionar tags, escolha Adicionar nova tag.
13. A página Revisar e comprar lista a data de início e a data de término, a duração, o número total de instâncias e o preço.

> **Note**
>
> Blocos de capacidade não podem ser cancelados depois que você os reserva.

14. Na janela pop-up Comprar um bloco de capacidade, digite confirmar e depois escolha Comprar.

AWS CLI

Para encontrar um Bloco de Capacidade de instância

Use o comando describe-capacity-block-extension-offerings.

O exemplo a seguir encontra Blocos de Capacidade de instância.

```
aws ec2 describe-capacity-block-offerings \
--instance-type p5.48xlarge \
--instance-count 16 \
--start-date-range 2023-08-14T00:00:00Z \
--end-date-range 2023-10-22-T00:00:00Z \
--capacity-duration-hours 48
```

O exemplo a seguir encontra Blocos de Capacidade do UltraServer.

```
aws ec2 describe-capacity-block-offerings \
--ultraserver-type u-p6e-gb200x72 \
```

```
--ultraserver-count 1 \
--start-date-range 2023-08-14T00:00:00Z \
--end-date-range 2023-10-22-T00:00:00Z \
--capacity-duration-hours 48
```

Para comprar um bloco de capacidade

Use o comando purchase-capacity-block com o ID de oferta do Bloco de Capacidade da saída do exemplo anterior.

```
aws ec2 purchase-capacity-block \
--capacity-block-offering-id cb-0123456789abcdefg \
--instance-platform Linux/UNIX
```

PowerShell

Para encontrar Blocos de Capacidade

Use o cmdlet Get-EC2CapacityBlockOffering.

O exemplo a seguir encontra Blocos de Capacidade de instância.

```
Get-EC2CapacityBlockOffering `
-InstanceType p5.48xlarge `
-InstanceCount 16 `
-CapacityDurationHour 48 `
-StartDateRange 2023-08-14T00:00:00Z `
-EndDateRange 2023-10-22-T00:00:00Z
```

O exemplo a seguir encontra Blocos de Capacidade do UltraServer.

```
Get-EC2CapacityBlockOffering `
-UltraserverType u-p6e-gb200x72 `
-UltraserverCount  1 `
-CapacityDurationHour 48 `
-StartDateRange 2023-08-14T00:00:00Z `
-EndDateRange 2023-10-22-T00:00:00Z
```

Para comprar um bloco de capacidade

Use o cmdlet New-EC2EC2CapacityBlock com o ID de oferta do bloco de capacidade da saída do exemplo anterior.

```
New-EC2EC2CapacityBlock `
-CapacityBlockOfferingId cb-0123456789abcdefg `
-InstancePlatform Linux/UNIX
```

Iniciar instâncias usando blocos de capacidade

Para usar o bloco de capacidade, você deve especificar o ID da reserva do bloco de capacidade ao iniciar as instâncias. A inicialização de uma instância em uma reserva de capacidade reduz a capacidade disponível de acordo com o número de instâncias iniciadas. Por exemplo, se a capacidade de instância comprada for de oito instâncias e você executar quatro instâncias, a capacidade disponível será reduzida em quatro.

Se você encerrar uma instância em execução no bloco de capacidade antes que a reserva termine, poderá iniciar uma nova instância em seu lugar. Quando você interrompe ou encerra uma instância em um bloco de capacidade, são necessários vários minutos para limpar sua instância antes que você possa executar outra instância para substituí-la. Durante esse tempo, a instância ficará em um estado de Interrompendo ou `shutting-down`. Depois que esse processo é concluído, o estado da sua instância passa para `stopped` ou `terminated`. Em seguida, a capacidade disponível no bloco de capacidade é atualizada para mostrar outra instância disponível para uso.

Requisitos

- A instância não pode ser iniciada em uma sub-rede em uma zona de disponibilidade diferente da zona de disponibilidade em que o bloco de capacidade está localizado.
- Sua instância não pode ser iniciada usando uma AMI com uma plataforma diferente da plataforma em seu bloco de capacidade.
- Para usar os blocos de capacidade do UltraServer `P6e-GB200`, é necessário se inscrever na zona local de Dallas (Norte da Virgínia).

Console

Para iniciar instâncias em um bloco de capacidade

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Na barra de navegação na parte superior da tela, selecione uma região para a reserva do bloco de capacidade.
3. No painel do console do Amazon EC2, selecione Launch instance (Executar instância).

4. Siga o procedimento para iniciar uma instância.
5. Expanda Detalhes avançados e, para Opção de compra, escolha Blocos de capacidade. Depois, siga um destes procedimentos:
   - Para iniciar as instâncias em um bloco de capacidade específico, em Reserva de capacidade, escolha Especificar reserva de capacidade e selecione o bloco de capacidade.
   - (Apenas UltraServers) Para iniciar as instâncias em um grupo de recursos do Bloco de capacidade do UltraServer, em Reserva de capacidade, escolha Especificar grupo de recursos de Reserva de capacidade e depois selecione o grupo de recursos.
6. Escolha Iniciar instância.

AWS CLI

Para iniciar instâncias usando um Bloco de capacidade

Use o comando run-instances com a opção `instance-market-options MarketType`.

O exemplo a seguir inicia uma instância em um Bloco de capacidade específico.

```
aws ec2 run-instances \
--image-id ami-0abcdef1234567890 \
--count 1 \
--instance-type p5.48xlarge \
--key-name my-key-pair \
--subnet-id subnet-0abcdef1234567890 \
--instance-market-options MarketType='capacity-block' \
--capacity-reservation-specification
 CapacityReservationTarget={CapacityReservationId=capacity_block_id}
```

O exemplo a seguir inicia uma instância em um grupo de recursos de Bloco de capacidade do UltraServer.

```
aws ec2 run-instances \
--image-id ami-0abcdef1234567890 \
--count 1 \
--instance-type p6e-gb200.36xlarge \
--key-name my-key-pair \
--subnet-id subnet-0abcdef1234567890 \
--instance-market-options MarketType='capacity-block' \
```

```
--capacity-reservation-specification
 CapacityReservationTarget={CapacityReservationResourceGroupArn=resource_group_arn}
```

PowerShell

Para iniciar instâncias em um bloco de capacidade

Use o cmdlet New-EC2Instance com a opção `-InstanceMarketOption` definida da seguinte maneira.

```
$marketoption = New-Object Amazon.EC2.Model.InstanceMarketOptionsRequest
$marketoption.MarketType = "capacity-block"
```

O exemplo a seguir inicia uma instância em um Bloco de capacidade específico.

```
New-EC2Instance `
-ImageId ami-0abcdef1234567890 `
-InstanceType p5.48xlarge `
-KeyName "my-key-pair" `
-SubnetId subnet-0abcdef1234567890 `
-InstanceMarketOptions $marketoption `
-CapacityReservationTarget_CapacityReservationId capacity_block_id
```

O exemplo a seguir inicia uma instância em um grupo de recursos de Bloco de capacidade do UltraServer.

```
New-EC2Instance `
-ImageId ami-0abcdef1234567890 `
-InstanceType p6e-gb200.36xlarge `
-KeyName "my-key-pair" `
-SubnetId subnet-0abcdef1234567890 `
-InstanceMarketOptions $marketoption `
-CapacityReservationTarget_CapacityReservationResourceGroupArn "resource_group_arn"
```

Recursos relacionados

- Para criar um modelo de execução direcionado para um bloco de capacidade, consulte the section called “Modelos de execução”
- Para iniciar instâncias em um bloco de capacidade usando a Frota do EC2, consulte Tutorial: configurar o EC2 Fleet para executar instâncias em blocos de capacidade.

- Para configurar um grupo de nós gerenciados do EKS com um bloco de capacidade, consulte Criar um grupo de nós gerenciados com blocos de capacidade para ML no Guia do usuário do Amazon EKS.
- Para configurar AWS ParallelCluster usando um Bloco de Capacidade, consulte ML em AWS ParallelCluster.

Visualizar blocos de capacidade

Depois que reservar um bloco de capacidade, será possível visualizar a reserva do bloco de capacidade em sua conta da AWS. É possívelrá visualizar a `start-date` e a `end-date` para saber quando sua reserva começará e terminará. Antes do início de uma reserva do bloco de capacidade, a capacidade disponível aparece como zero. É possível ver quantas instâncias estarão disponíveis em seu bloco de capacidade pelo valor da tag da chave de tag `aws:ec2capacityreservation:incrementalRequestedQuantity`.

Quando uma reserva de bloco de capacidade começa, o estado da reserva passa de `scheduled` para `active`. Emitimos um evento por meio do Amazon EventBridge para notificar você de que o bloco de capacidade está disponível para uso. Para obter mais informações, consulte Monitorar blocos de capacidade usando o EventBridge.

Os blocos de capacidade têm os seguintes status:

- `payment-pending`: o pagamento antecipado ainda não foi processado.
- `payment-failed`: não foi possível processar o pagamento no prazo de 12 horas. O bloco de capacidade foi liberado.
- `scheduled`: o pagamento foi processado e a reserva do bloco de capacidade ainda não começou.
- `active`: a capacidade reservada está disponível para seu uso.
- `expired`: a reserva do bloco de capacidade expirou automaticamente na data e hora especificadas na solicitação da reserva. A capacidade reservada não está mais disponível para uso.

Console

Para visualizar blocos de capacidade

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Reservas de Capacidade.

3. Na página Visão geral das reservas de capacidade, você vê uma tabela de recursos com detalhes sobre todos os seus recursos de reserva de capacidade. Para encontrar suas reservas de blocos de capacidade, selecione Blocos de capacidade na lista suspensa acima de ID da reserva de capacidade. Na tabela, você pode ver informações sobre os blocos de capacidade, como datas de início e término, duração e status.
4. Para obter mais detalhes sobre um bloco de capacidade, selecione o ID da reserva do bloco de capacidade que você deseja visualizar. A página Detalhes da reserva de capacidade exibe todas as propriedades da reserva e o número de instâncias que estão em uso ou que estão disponíveis no bloco de capacidade.

> **Note**
>
> Antes do início de uma reserva do bloco de capacidade, a capacidade disponível aparece como zero. É possível ver quantas instâncias estarão disponíveis quando a reserva de bloco de capacidade começar usando o seguinte valor de tag para a chave de tag: `aws:ec2capacityreservation:incrementalRequestedQuantity`.

AWS CLI

Para visualizar blocos de capacidade

Por padrão, quando você usa o comando describe-capacity-reservations, as reservas de capacidade sob demanda e as reservas de blocos de capacidade são listadas. Para visualizar somente as suas reservas de bloco de capacidade, filtre as reservas do tipo `capacity-block`.

```
aws ec2 describe-capacity-reservations \
    --filters Name=reservation-type,Values=capacity-block
```

PowerShell

Para visualizar blocos de capacidade

Use o cmdlet Get-EC2CapacityReservation. Por padrão, tanto as reservas de capacidade sob demanda quanto as reservas de blocos de capacidade são listadas. Para visualizar somente as suas reservas de bloco de capacidade, filtre as reservas do tipo `capacity-block`.

```
Get-EC2CapacityReservation `
```

```
    -Filter @{Name="reservation-type"; Values="capacity-block"}
```

Estender blocos de capacidade

Com os blocos de capacidade, você reserva a capacidade computacional das workloads, garantindo disponibilidade e consistência. Para acomodar suas necessidades em constante mudança, você pode estender a duração dos blocos de capacidade existentes conforme necessário.

Para estender um bloco de capacidade, ele deve ter um status de `active` ou `scheduled` e não ter extensões que estejam como `payment-pending`. Você pode solicitar a prorrogação da duração do seu bloco de capacidade até no mínimo 1 hora ou no máximo 56 dias antes que ele expire. É possível estender o bloco de capacidade em incrementos de 1 a 14 dias e em incrementos de 7 dias até 182 dias (26 semanas) no total. Ao estender o bloco de capacidade, a data de término dele será atualizada para que suas instâncias possam continuar funcionando sem interrupções.

- Não há limite para o número de extensões que você pode aplicar a um bloco de capacidade
- O ID de reserva de capacidade permanecerá o mesmo após a extensão do bloco
- Os blocos de capacidade só podem ser estendidos se houver capacidade suficiente disponível para comportá-los, o que não é garantido.

Faturamento

O preço de uma oferta de bloco de capacidade é cobrado à vista. A extensão permanecerá como `payment-pending` até que a fatura seja paga. Se o pagamento não puder ser processado dentro de 12 horas ou até 35 minutos antes do término programado do bloco de capacidade (o que ocorrer primeiro), sua extensão não terá êxito e o status mudará para `payment-failed`. A reserva do bloco de capacidade permanecerá `active` e será encerrada na data de término original.

Depois que o pagamento for processado com êxito, o status da extensão do bloco de capacidade mudará para `payment-succeeded` e a data de término da reserva do bloco de capacidade será atualizada para a nova. Os detalhes da extensão podem ser consultados na seção Detalhes da extensão do bloco de capacidade do console ou usando o comando describe-capacity-block-extension-history.

Estender blocos de capacidade

Console

Para estender um bloco de capacidade

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Reservas de Capacidade.
3. Na página Visão geral das reservas de capacidade, você vê uma tabela de recursos com detalhes sobre todos os seus recursos das reservas de capacidade. Selecione o ID da reserva referente ao bloco de capacidade que você deseja estender.
4. No menu suspenso Ações, escolha Estender bloco de capacidade.
5. Em Duração, insira o número de dias ou semanas pelos quais você precisa estender a reserva.
6. Escolha Encontrar bloco de capacidade.
7. Se houver um bloco de capacidade disponível que atenda às suas especificações, uma oferta aparecerá em Blocos de capacidade recomendados. Para ver outras ofertas de blocos de capacidade, ajuste as entradas da pesquisa e escolha Localizar blocos de capacidade novamente.
8. Quando encontrar uma oferta do bloco de capacidade que deseja comprar, escolha Estender.
9. Na janela pop-up Estender bloco de capacidade, insira confirmar e escolha Estender.

AWS CLI

Para encontrar uma extensão de bloco de capacidade

Use o comando describe-capacity-block-extension-offerings. O exemplo a seguir pesquisa uma extensão de bloco de capacidade de 48 horas para a reserva especificada.

```
aws ec2 describe-capacity-block-extension-offerings \
    --capacity-reservation-id cr-1234567890abcdefg \
    --capacity-block-extension-duration-hours 48
```

Para estender um bloco de capacidade

Use o comando purchase-capacity-block-extension. Especifique o ID da oferta de extensão da saída do exemplo anterior.

```
aws ec2 purchase-capacity-block-extension \
    --capacity-block-extension-offering-id cbe-0123456789abcdefg \
    --capacity-reservation-id cr-1234567890abcdefg
```

PowerShell

Para encontrar uma extensão de bloco de capacidade

Use o cmdlet Get-EC2CapacityBlockExtensionOffering. O exemplo a seguir pesquisa uma extensão de bloco de capacidade de 48 horas para a reserva especificada.

```
Get-EC2CapacityBlockExtensionOffering `
    -CapacityReservationId cr-1234567890abcdefg `
    -CapacityBlockExtensionDurationHour 48
```

Para estender um bloco de capacidade

Use o cmdlet Invoke-EC2CapacityBlockExtension. Especifique o ID da oferta de extensão da saída do exemplo anterior.

```
Invoke-EC2CapacityBlockExtension `
    -CapacityBlockExtensionOfferingId cbe-0123456789abcdefg `
    -CapacityReservationId cr-1234567890abcdefg
```

Compartilhar Blocos de capacidade

O compartilhamento de Blocos de capacidade permite que os proprietários do Bloco de Capacidade compartilhem os Blocos de Capacidade do Amazon EC2 com outras contas da AWS dentro de uma organização da AWS. Assim você pode maximizar o uso da capacidade reservada da GPU em diferentes equipes e projetos para usar com eficiência os Blocos de capacidade.

A conta da AWS proprietária do Bloco de capacidade (proprietário) pode compartilhá-lo com outras contas da AWS (consumidores). Um proprietário pode compartilhar um Bloco de capacidade com contas da AWS específicas dentro de sua organização da AWS, uma unidade organizacional dentro de sua organização da AWS ou toda a organização da AWS. Os consumidores podem iniciar instâncias em Blocos de capacidade que foram compartilhados da mesma forma que iniciam instâncias em Blocos de capacidade de sua propriedade.

Pré-requisitos para compartilhar Blocos de capacidade

Para que você possa compartilhar um Bloco de capacidade, as seguintes condições devem ser atendidas:

- Você deve possuir o Bloco de capacidade: não é possível compartilhar um Bloco de capacidade que tenha sido compartilhado com você.
- O estado do Bloco de capacidade deve estar ativo ou programado: Blocos de capacidade que estão em outros estados, como `expired` ou `payment-pending` não podem ser compartilhados.
- Compartilhamento somente dentro da sua organização da AWS: um proprietário pode compartilhar um Bloco de capacidade com contas da AWS específicas dentro de sua organização da AWS, uma unidade organizacional dentro de sua organização da AWS ou toda a organização da AWS.
- Blocos de capacidade do UltraServer não compatíveis: você não pode compartilhar Blocos de capacidade para Amazon EC2 UltraServers.
- Qualificação da conta: o compartilhamento de Blocos de capacidade não está disponível para novas contas da AWS ou contas da AWS com histórico de faturamento limitado.

Serviços relacionados

O compartilhamento de Blocos de capacidade integra-se ao AWS Resource Access Manager (AWS RAM). O AWS RAM é um serviço que permite compartilhar seus recursos da AWS com qualquer conta da AWS ou por meio do AWS Organizations. Com o AWS RAM, você compartilha recursos que possui criando um compartilhamento de recursos. Um compartilhamento de recursos especifica os recursos a serem compartilhados, e os consumidores com os quais compartilhá-los. Os consumidores podem ser contas individuais da AWS, unidades organizacionais ou toda uma organização do AWS Organizations.

Para obter mais informações sobre o AWS RAM, consulte o Manual do usuário do AWS RAM.

Permissões de Blocos de capacidade compartilhada

Permissões para proprietários

O proprietário do Bloco de capacidade permanece responsável pelo gerenciamento do Bloco de capacidade (por exemplo, extensão, compartilhamento) e pelas instâncias que executa nele. Os proprietários não podem modificar as instâncias que os consumidores executam nos Blocos de capacidade que compartilharam.

Permissões para clientes

Os consumidores podem iniciar instâncias na capacidade compartilhada e são responsáveis por gerenciar essas instâncias. Os consumidores não podem visualizar ou modificar instâncias de propriedade de outros consumidores ou do proprietário do Bloco de capacidade. Os consumidores também podem visualizar apenas a capacidade total e a capacidade disponível no Bloco de capacidade compartilhado.

Compartilhar Blocos de capacidade

Para compartilhar um Bloco de capacidade, é necessário adicioná-lo um compartilhamento de recursos. Um compartilhamento de recursos é um recurso do AWS RAM que permite que você compartilhe seus recursos entre Contas da AWS.

Se você adicionar o Bloco de capacidade a um compartilhamento de recursos compartilhado com toda organização da AWS, os consumidores da organização terão acesso ao Bloco de capacidade compartilhado.

Console

Para compartilhar um Bloco de capacidade de sua propriedade usando o console do Amazon EC2

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Reservas de Capacidade.
3. Escolha o Bloco de capacidade a ser compartilhado e escolha Ações, Compartilhar reserva.
4. Selecione o compartilhamento de recursos ao qual adicionar o Bloco de capacidade e escolha Compartilhar Reserva de capacidade).

   Pode levar alguns minutos para que os consumidores obtenham acesso ao Bloco de capacidade compartilhado.

Para adicionar um Bloco de capacidade para um novo recurso compartilhado

Primeiro, você precisa criar o compartilhamento de recursos usando o console do AWS RAM. Para obter mais informações, consulte Criar um compartilhamento de recurso no Guia do usuário do AWS RAM.

AWS CLI

Para compartilhar um Bloco de capacidade de sua propriedade

Use os comandos create-resource-share e associate-resource-share.

```
aws ram create-resource-share \
    --name my-resource-share \
    --resource-arns arn:aws:ec2:us-east-2:123456789012:capacity-
reservation/cr-1234abcd56EXAMPLE
```

```
aws ram associate-resource-share \
    --resource-share-arn arn:aws:ram:us-east-2:123456789012:resource-share/7ab63972-
b505-7e2a-420d-6f5d3EXAMPLE \
    --resource-arns arn:aws:ec2:us-east-2:123456789012:capacity-
reservation/cr-1234abcd56EXAMPLE
```

PowerShell

Para compartilhar um Bloco de capacidade de sua propriedade

Use os cmdlets New-RAMResourceShare e Connect-RAMResourceShare.

```
New-RAMResourceShare `
    -Name my-resource-share `
    -ResourceArn "arn:aws:ec2:us-east-2:123456789012:capacity-
reservation/cr-1234abcd56EXAMPLE"
```

```
Connect-RAMResourceShare `
    -ResourceShareArn "arn:aws:ram:us-east-2:123456789012:resource-share/7ab63972-
b505-7e2a-420d-6f5d3EXAMPLE" `
    -ResourceArn "arn:aws:ec2:us-east-2:123456789012:capacity-
reservation/cr-1234abcd56EXAMPLE"
```

Os Blocos de capacidade operam por ordem de chegada para todas as contas, independentemente do status de propriedade. Quando você compartilha um Bloco de capacidade, se um consumidor inicia instâncias antes do proprietário, essas instâncias ocupam a capacidade até que o consumidor encerre as instâncias ou até 30 minutos antes da expiração do Bloco de capacidade.

Parar de compartilhar um Bloco de capacidade

Você pode parar de compartilhar um Bloco de capacidade a qualquer momento até 30 minutos antes da data de expiração do bloco.

O que acontece quando você para de compartilhar:

- Os consumidores não podem mais executar novas instâncias no Bloco de capacidade que não era compartilhado.
- Todas as instâncias em execução continuam funcionando até 30 minutos antes da data de expiração do Bloco de capacidade, a menos que sejam encerradas pelo consumidor.

Console

Para interromper o compartilhamento de um Bloco de capacidade que você possui usando o console do Amazon EC2, clique aqui.

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Reservas de Capacidade.
3. Selecione o Bloco de capacidade e escolha a guia Compartilhamento.
4. A guia Compartilhamento lista os compartilhamentos de recursos aos quais o Bloco de capacidade foi adicionado. Selecione o compartilhamento de recursos do qual remover o Bloco de capacidade.
5. Escolha Remover do compartilhamento de recursos.

AWS CLI

Para parar de compartilhar um Bloco de capacidade de sua propriedade

Use o comando disassociate-resource-share.

```
aws ram disassociate-resource-share \
    --resource-share-arn arn:aws:ram:us-east-2:123456789012:resource-share/7ab63972-b505-7e2a-420d-6f5d3EXAMPLE \
    --resource-arns arn:aws:ec2:us-east-2:123456789012:capacity-reservation/cr-1234abcd56EXAMPLE
```

PowerShell

Para parar de compartilhar um Bloco de capacidade de sua propriedade

Use o cmdlet Disconnect-RAMResourceShare.

```
Disconnect-RAMResourceShare `
    -ResourceShareArn "arn:aws:ram:us-east-2:123456789012:resource-share/7ab63972-
b505-7e2a-420d-6f5d3EXAMPLE" `
    -ResourceArn "arn:aws:ec2:us-east-2:123456789012:capacity-
reservation/cr-1234abcd56EXAMPLE"
```

Monitore o uso compartilhado do Bloco de capacidade

Os proprietários do Bloco de capacidade podem monitorar quais contas estão usando seus Blocos de capacidade compartilhados e monitorar o uso de instâncias por conta.

AWS CLI

Para monitorar o uso de um Bloco de capacidade

Use o comando get-capacity-reservation-usage.

```
aws ec2 get-capacity-reservation-usage \
    --capacity-reservation-id cr-1234abcd56EXAMPLE
```

Essa API permite que os proprietários:

- Ver quais contas estão usando o Bloco de capacidade no momento.
- Ver o número de instâncias que cada conta está executando.

Notificações de encerramento de instância

As contas do proprietário e do consumidor que tiverem instâncias em execução no Bloco de capacidade receberão um evento do EventBridge 40 minutos antes do término da reserva do Bloco de capacidade, indicando que todas as instâncias em execução na reserva começarão a ser encerradas em dez minutos. Para obter mais informações, consulte Monitorar blocos de capacidade usando o EventBridge.

Extensões do Bloco de capacidade

Os Blocos de capacidade podem ser estendidos enquanto são compartilhados. Somente a conta do proprietário pode estender um Bloco de capacidade compartilhado.

Quando um Bloco de capacidade é estendido, as instâncias em execução lançadas pelo proprietário ou pelos consumidores herdam automaticamente a nova data de expiração, e os consumidores podem continuar usando a capacidade compartilhada até a nova data de expiração sem nenhuma interrupção da instância.

Definição de preço e faturamento

Os proprietários são cobrados pelos Blocos de capacidade que compartilham e pagam antecipadamente pelo Bloco de capacidade quando o compram. Os proprietários também pagam pelas taxas do sistema operacional pelas instâncias que executam no Bloco de capacidade.

Os consumidores são cobrados somente pelas cobranças do sistema operacional pelas instâncias que executam no Bloco de capacidade compartilhado. Os consumidores não são cobrados pela reserva do Bloco de capacidade em si.

Criar um grupo de recursos para Blocos de capacidade do UltraServer

É possível usar o AWS Resource Groups para criar coleções lógicas de Blocos de capacidade do UltraServer. Depois de criar o grupo de recursos, é possível adicionar Blocos de capacidade do UltraServer que você possui em sua conta. Depois de adicionar os Blocos de capacidade do UltraServer, é possível direcionar o lançamento de instâncias para o grupo de recursos em vez dos blocos de capacidade individuais. As instâncias direcionadas a um grupo de recursos correspondem a qualquer Bloco de capacidade do UltraServer no grupo que tenha atributos correspondentes e capacidade disponível. Se o grupo de recursos não tiver um Bloco de capacidade do UltraServer com atributos correspondentes e capacidade disponível, a inicialização da instância falhará.

Se um Bloco de capacidade do UltraServer for removido de um grupo de recursos enquanto houver instâncias em execução, essas instâncias continuarão em execução no Bloco de capacidade. Se um Bloco de capacidade do UltraServer em um grupo terminar enquanto houver instâncias em execução, as instâncias serão encerradas.

Não é possível adicionar Blocos de capacidade de instância a um grupo de recursos.

Para criar um grupo de recursos para Blocos de capacidade do UltraServer, use um dos métodos a seguir.

AWS CLI

Para criar um grupo de recursos para Blocos de capacidade do UltraServer

Use o comando AWS CLIcreate-group e, para `--configuration`, especifique o seguinte:

```
{
  "Configuration": [
    {
      "Type": "AWS::EC2::CapacityReservationPool",
      "Parameters": [
        {
          "Name": "instance-type",
          "Values": [
            "instance_type"
          ]
        },
        {
          "Name": "reservation-type",
          "Values": [
            "capacity-block"
          ]
        }
      ]
    },
    {
      "Type": "AWS::ResourceGroups::Generic",
      "Parameters": [
        {
          "Name": "allowed-resource-types",
          "Values": [
            "AWS::EC2::CapacityReservation"
          ]
        }
      ]
    }
  ]
}
```

PowerShell

Para criar um grupo de recursos para Blocos de capacidade do UltraServer

Use o cmdlet New-RGGroup. Para `-Configuration`, especifique o seguinte:

```
{
  "Configuration": [
    {
      "Type": "AWS::EC2::CapacityReservationPool",
      "Parameters": [
        {
          "Name": "instance-type",
          "Values": [
            "instance_type"
          ]
        },
        {
          "Name": "reservation-type",
          "Values": [
            "capacity-block"
          ]
        }
      ]
    },
    {
      "Type": "AWS::ResourceGroups::Generic",
      "Parameters": [
        {
          "Name": "allowed-resource-types",
          "Values": [
            "AWS::EC2::CapacityReservation"
          ]
        }
      ]
    }
  ]
}
```

Depois de criar um grupo de recursos para o Bloco de capacidade do UltraServer, utilize um dos métodos a seguir para adicionar Blocos de capacidade do UltraServer existentes a ele.

AWS CLI

Para adicionar um Bloco de capacidade do UltraServer a um grupo de recursos

Use o comando group-resources. Para `--group`, especifique o nome do grupo de recursos que você criou. Para `--resource-arns`, especifique os ARNs dos Blocos de capacidade do UltraServer a serem adicionados.

```
aws resource-groups group-resources \
--group MyCRGroup \
--resource-arns CapacityReservationArn
```

PowerShell

Para adicionar um Bloco de capacidade do UltraServer a um grupo de recursos

Use o cmdlet Add-RGResource. Para `-Group`, especifique o nome do grupo de recursos que você criou. Para `-ResourceArn` , especifique os ARNs dos Blocos de capacidade do UltraServer a serem adicionados.

O exemplo a seguir adiciona duas reservas de capacidade ao grupo especificado.

```
Add-RGResource `
-Group MyCRGroup `
-ResourceArn CapacityReservationArn
```

Monitorar blocos de capacidade usando o EventBridge

Quando a reserva do bloco de capacidade começa, o Amazon EC2 emite um evento por meio do EventBridge que indica que a capacidade está pronta para ser usada. Quarenta minutos antes do término da reserva do bloco de capacidade, você recebe outro evento do EventBridge informando que todas as instâncias em execução na reserva começarão a ser encerradas em dez minutos. Para obter mais informações sobre eventos do EventBridge, consulte Eventos do Amazon EventBridge.

As seguintes estruturas de eventos para eventos emitidos para blocos de capacidade:

Bloco de capacidade fornecido

O exemplo a seguir mostra um evento para o bloco de capacidade fornecido.

```
{
  "customer_event_id": "[Capacity Reservation Id]-delivered",
  "detail_type": "Capacity Block Reservation Delivered",
  "source": "aws.ec2",
```

```
  "account": "[Customer Account ID]",
  "time": "[Current time]",
  "resources": [
    "[ODCR ARN]"
  ],
  "detail": {
    "capacity-reservation-id": "[ODCR ID]",
    "end-date": "[ODCR End Date]"
  }
}
```

Aviso de expiração do bloco de capacidade

O exemplo a seguir mostra um evento para aviso de expiração do bloco de capacidade.

```
{
  "customer_event_id": "[Capacity Reservation Id]-approaching-expiry",
  "detail_type": "Capacity Block Reservation Expiration Warning",
  "source": "aws.ec2",
  "account": "[Customer Account ID]",
  "time": "[Current time]",
  "resources": [
    "[ODCR ARN]"
  ],
  "detail": {
    "capacity-reservation-id": "[ODCR ID]",
    "end-date": "[ODCR End Date]"
  }
}
```

Aviso de interrupção da instância de reserva de capacidade

O exemplo a seguir mostra um evento para aviso de interrupção da instância de reserva de capacidade do EC2.

```
{
    "version": "0",
    "id": "12345678-1234-1234-1234-123456789012",
    "detail_type": "EC2 Capacity Reservation Instance Interruption Warning",
    "source": "aws.ec2",
    "account": "[Customer Account ID]",
    "time": "[Current time]",
    "region": "[Region]",
```

```
    "resources": [
        "[Instance ARN]"
    ],
    "detail": {
        "instance-id": "[Instance ID]",
        "instance-action": "terminate",
        "instance-termination-time": "[Current time]",
        "availability-zone-id": "[Availability Zone ID]",
        "instance-lifecycle": "capacity-block"
    }
}
```

Registrar em log chamadas de API de blocos de capacidade com o AWS CloudTrail

Os blocos de capacidade são integrados ao AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, um perfil ou um serviço da AWS em blocos de capacidade. O CloudTrail captura chamadas de API para blocos de capacidade como eventos. As chamadas capturadas incluem chamadas do console de blocos de capacidade e chamadas de código para as operações de API de blocos de capacidade. Se você criar uma trilha, poderá habilitar a entrega contínua de eventos do CloudTrail a um bucket do Amazon S3, incluindo eventos para blocos de capacidade. Se você não configurar uma trilha, ainda poderá visualizar os eventos mais recentes no console do CloudTrail no Histórico de eventos. Com as informações coletadas pelo CloudTrail, você pode determinar a solicitação que foi feita para os blocos de capacidade, o endereço IP do qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita e outros detalhes.

Para saber mais sobre o CloudTrail, consulte o Guia do usuário do AWS CloudTrail.

Informações sobre blocos de capacidade no CloudTrail

O CloudTrail é habilitado em sua Conta da AWS quando ela é criada. Quando ocorre alguma atividade nos blocos de capacidade, essa atividade é registrada em um evento do CloudTrail junto com outros eventos de serviço da AWS em Histórico de eventos. Você pode visualizar, pesquisar e baixar eventos recentes em sua Conta da AWS. Para saber mais, consulte Como visualizar eventos com o histórico de eventos do CloudTrail.

Para ter um registro contínuo de eventos na Conta da AWS, incluindo os para blocos de capacidade, crie uma trilha. Uma trilha permite que o CloudTrail entregue arquivos de log a um bucket do Amazon S3. Por padrão, quando você cria uma trilha no console, ela é aplicada a todas as Regiões da AWS. A trilha registra eventos de todas as regiões na partição da AWS e entrega os arquivos de log no bucket do Amazon S3 que você especifica. Além disso, é possível configurar outros AWS serviços

para melhor analisar e agir de acordo com dados coletados do evento nos logs CloudTrail. Para saber mais, consulte:

- Visão geral da criação de uma trilha
- Serviços e integrações compatíveis com o CloudTrail
- Configuração notificações do Amazon SNS para o CloudTrail
- Como receber arquivos de log do CloudTrail de várias regiões e Como receber arquivos de log do CloudTrail de várias contas

Todas os blocos de capacidade são registrados em log pelo CloudTrail e são documentados na Amazon EC2 API Reference. Por exemplo, as chamadas para as ações `CapacityBlockScheduled` e `CapacityBlockActive` geram entradas nos arquivos de log do CloudTrail.

Cada entrada de log ou evento contém informações sobre quem gerou a solicitação. As informações de identidade ajudam a determinar:

- Se a solicitação foi feita com credenciais de usuário-raiz ou usuário do AWS Identity and Access Management (IAM).
- Se a solicitação foi feita com credenciais de segurança temporárias de um perfil ou de um usuário federado.
- Se a solicitação foi feita por outro serviço da AWS.

Para saber mais, consulte Elemento userIdentity do CloudTrail.

Entender as entradas nos arquivos de log de capacidade

Uma trilha é uma configuração que permite a entrega de eventos como arquivos de log a um bucket Amazon S3 especificado. Os arquivos de log do CloudTrail contêm uma ou mais entradas de log. Um evento representa uma única solicitação de qualquer fonte, e inclui informações sobre a ação solicitada, data e hora da ação, parâmetros da solicitação e assim por diante. Os arquivos de log do CloudTrail não são um rastreamento de pilha ordenada de chamadas de API pública, portanto, não são exibidos em uma ordem específica.

Os seguintes exemplos mostram entradas no log do CloudTrail para:

- TerminateCapacityBlocksInstances

- CapacityBlockPaymentFailed
- CapacityBlockScheduled
- CapacityBlockActive
- CapacityBlockFailed
- CapacityBlockExpired

> **Note**
>
> Alguns campos foram ocultados nos exemplos por questão de privacidade dos dados.

TerminateCapacityBlocksInstances


```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "accountId": "123456789012",
    "invokedBy": "AWS Internal;"
  },
  "eventTime": "2023-10-02T00:06:08Z",
  "eventSource": "ec2.amazonaws.com",
  "eventName": "TerminateCapacityBlockInstances",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "203.0.113.25",
  "userAgent": "aws-cli/1.15.61 Python/2.7.10 Darwin/16.7.0 botocore/1.10.60",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "a1b2c3d4-EXAMPLE",
  "readOnly": false,
  "resources": [
    {
      "accountId": "123456789012",
      "type": "AWS::EC2::Instance",
      "ARN": "arn:aws:ec2:us-east-1:123456789012:instance/i-1234567890abcdef0"
    }
    {
      "accountId": "123456789012",
      "type": "AWS::EC2::Instance",
      "ARN": "arn:aws:ec2:us-east-1:123456789012:instance/i-0598c7d356eba48d7"
    }
```

```
  ],
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "123456789012",
  "serviceEventDetails": {
      "capacityReservationId": "cr-12345678",
      }
}
```

CapacityBlockPaymentFailed

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "accountId": "123456789012",
    "invokedBy": "AWS Internal;"
  },
  "eventTime": "2023-10-02T00:06:08Z",
  "eventSource": "ec2.amazonaws.com",
  "eventName": "CapacityBlockPaymentFailed",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "203.0.113.25",
  "userAgent": "aws-cli/1.15.61 Python/2.7.10 Darwin/16.7.0 botocore/1.10.60",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "a1b2c3d4-EXAMPLE",
  "readOnly": false,
  "resources": [
    {
      "ARN": "arn:aws:ec2:us-east-1:123456789012:capacity-reservation/cr-12345678",
      "accountId": "123456789012",
      "type": "AWS::EC2::CapacityReservation"
    }
  ],
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "123456789012",
  "serviceEventDetails": {
      "capacityReservationId": "cr-12345678",
      "capacityReservationState": "payment-failed"
      }
}
```

CapacityBlockScheduled


```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "accountId": "123456789012",
    "invokedBy": "AWS Internal;"
  },
  "eventTime": "2023-10-02T00:06:08Z",
  "eventSource": "ec2.amazonaws.com",
  "eventName": "CapacityBlockScheduled",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "203.0.113.25",
  "userAgent": "aws-cli/1.15.61 Python/2.7.10 Darwin/16.7.0 botocore/1.10.60",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "a1b2c3d4-EXAMPLE",
  "readOnly": false,
  "resources": [
    {
      "ARN": "arn:aws:ec2:us-east-1:123456789012:capacity-reservation/cr-12345678",
      "accountId": "123456789012",
      "type": "AWS::EC2::CapacityReservation"
    }
  ],
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "123456789012",
  "serviceEventDetails": {
      "capacityReservationId": "cr-12345678",
      "capacityReservationState": "scheduled"
      }
}
```


CapacityBlockActive


```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "accountId": "123456789012",
    "invokedBy": "AWS Internal;"
  },
  "eventTime": "2023-10-02T00:06:08Z",
  "eventSource": "ec2.amazonaws.com",
```

```
  "eventName": "CapacityBlockActive",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "203.0.113.25",
  "userAgent": "aws-cli/1.15.61 Python/2.7.10 Darwin/16.7.0 botocore/1.10.60",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "a1b2c3d4-EXAMPLE",
  "readOnly": false,
  "resources": [
    {
      "ARN": "arn:aws:ec2:us-east-1:123456789012:capacity-reservation/cr-12345678",
      "accountId": "123456789012",
      "type": "AWS::EC2::CapacityReservation"
    }
  ],
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "123456789012",
  "serviceEventDetails": {
      "capacityReservationId": "cr-12345678",
      "capacityReservationState": "active"
      }
 }
```

CapacityBlockFailed

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "accountId": "123456789012",
    "invokedBy": "AWS Internal;"
  },
  "eventTime": "2023-10-02T00:06:08Z",
  "eventSource": "ec2.amazonaws.com",
  "eventName": "CapacityBlockFailed",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "203.0.113.25",
  "userAgent": "aws-cli/1.15.61 Python/2.7.10 Darwin/16.7.0 botocore/1.10.60",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "a1b2c3d4-EXAMPLE",
  "readOnly": false,
  "resources": [
    {
```

```
      "ARN": "arn:aws:ec2:us-east-1:123456789012:capacity-reservation/cr-12345678",
      "accountId": "123456789012",
      "type": "AWS::EC2::CapacityReservation"
    }
  ],
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "123456789012",
  "serviceEventDetails": {
      "capacityReservationId": "cr-12345678",
      "capacityReservationState": "failed"
      }
 }
```

CapacityBlockExpired

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "accountId": "123456789012",
    "invokedBy": "AWS Internal;"
  },
  "eventTime": "2023-10-02T00:06:08Z",
  "eventSource": "ec2.amazonaws.com",
  "eventName": "CapacityBlockExpired",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "203.0.113.25",
  "userAgent": "aws-cli/1.15.61 Python/2.7.10 Darwin/16.7.0 botocore/1.10.60",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "a1b2c3d4-EXAMPLE",
  "readOnly": false,
  "resources": [
    {
      "ARN": "arn:aws:ec2:us-east-1:123456789012:capacity-reservation/cr-12345678",
      "accountId": "123456789012",
      "type": "AWS::EC2::CapacityReservation"
    }
  ],
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "123456789012",
  "serviceEventDetails": {
      "capacityReservationId": "cr-12345678",
      "capacityReservationState": "expired"
```

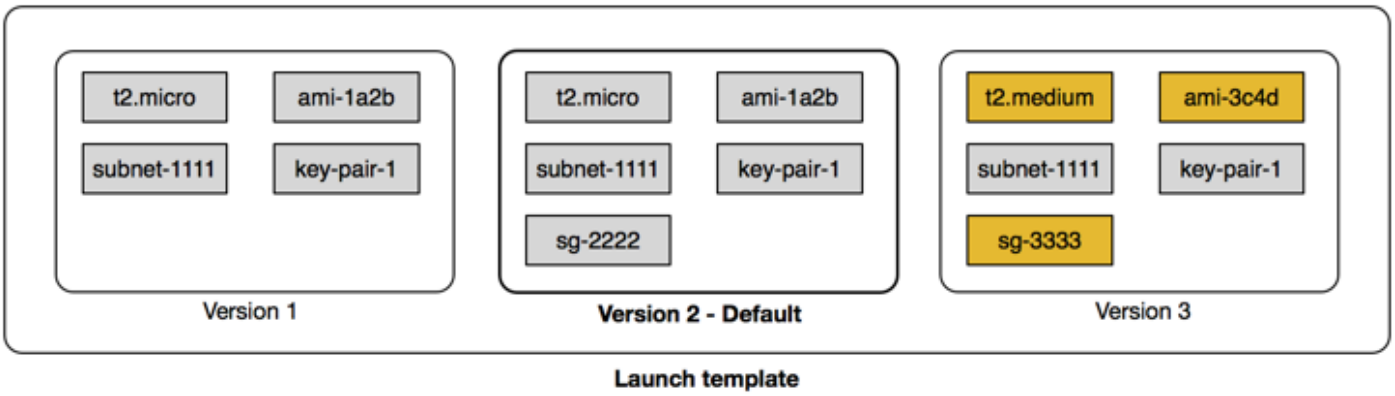
```
        }
}
```

Armazenar os parâmetros de execução de instâncias nos modelos de execução do Amazon EC2

É possível usar um modelo de execução do Amazon EC2 para armazenar parâmetros de execução de instâncias para que não seja necessário especificá-los sempre que executar uma instância do Amazon EC2. Por exemplo, você pode criar um modelo de execução que armazene o ID da AMI, o tipo de instância e as configurações de rede que normalmente usa para executar instâncias. Ao iniciar uma instância usando o console do Amazon EC2, um AWS SDK ou uma ferramenta de linha de comando, é possível especificar o modelo de execução em vez de inserir os parâmetros novamente.

Para cada modelo de execução, é possível 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, será possível usar qualquer versão do modelo de execução. Se você não especificar a versão, a versão padrão será usada. É possível 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 grupo de segurança 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.



Conteúdo

- Restrições para modelos de execução do Amazon EC2
- Permissões do IAM necessárias para modelos de execução do Amazon EC2
- Usar modelos de execução do Amazon EC2 para controlar a execução de instâncias do Amazon EC2
- Criar um modelo de execução do Amazon EC2
- Modificar um modelo de inicialização (gerenciar versões do modelo de inicialização)
- Excluir um modelo de execução ou uma versão de modelo de execução

Restrições para modelos de execução do Amazon EC2

As seguintes restrições se aplicam aos modelos de execução e às respectivas versões:

- Cotas: para visualizar as cotas para os modelos de execução e as versões de modelos de execução, abra o console do Service Quotas ou use o comando da AWS CLI list-service-quotas. Cada conta da AWS pode ter até 5 mil modelos de execução por região e até 10 mil versões por modelo de execução. Suas contas podem ter cotas diferentes com base na idade e no histórico de uso.
- Os parâmetros são opcionais: os parâmetros do modelo de inicialização são opcionais. No entanto, você precisa garantir que a solicitação de execução de uma instância inclua todos os parâmetros necessários. Por exemplo, se o modelo de execução não incluir um ID de AMI, você deverá especificar um ID de AMI ao executar uma instância com esse modelo de execução.
- Parâmetros não validados: os parâmetros do modelo de inicialização não são totalmente validados quando você cria o modelo. Se você especificar valores incorretos ou usar combinações de parâmetros não compatíveis, as instâncias não serão executadas com esse modelo de execução. Para evitar problemas, certifique-se de especificar os valores corretos e de usar as combinações de parâmetros compatíveis. Por exemplo, para executar uma instância em um grupo de posicionamento, especifique um tipo de instância compatível.
- Tags: você pode marcar um modelo de execução, mas não pode marcar uma versão de modelo de execução.
- Imutável: os modelos de execução são imutáveis. Para modificar um modelo de inicialização, é necessário criar uma nova versão do modelo de inicialização.

- Números de versão: as versões de modelo de inicialização 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.

Permissões do IAM necessárias para modelos de execução do Amazon EC2

É possível usar permissões do IAM para controlar se os usuários podem listar, visualizar, criar ou excluir modelos de execução ou versões de modelos de execução.

> **Important**
>
> Você não pode usar as permissões em nível de recurso para restringir os recursos que os usuários podem especificar em um modelo de execução ao criar um modelo de execução ou uma versão de modelo de execução. Portanto, certifique-se de conceder permissões para a criação de modelos de execução e versões de modelos de execução somente aos administradores confiáveis.

Você deve conceder as permissões necessárias para a criação e para o acesso aos recursos especificados no modelo de execução a qualquer pessoa que usará um modelo de execução. Por exemplo:

- Para iniciar uma instância usando uma imagem de máquina da Amazon (AMI) privada compartilhada, o usuário deve ter permissão para iniciar a AMI.
- Para criar volumes do EBS com etiquetas usando snapshots existentes, o usuário deve ter acesso de leitura aos snapshots e permissões para criar e fazer a marcação dos volumes.

Conteúdo

- ec2:CreateLaunchTemplate
- ec2:DescribeLaunchTemplates
- ec2:DescribeLaunchTemplateVersions
- ec2:DeleteLaunchTemplate
- Controlar permissões de controle de versão
- Controlar o acesso a tags em modelos de execução

ec2:CreateLaunchTemplate

Para criar um modelo de execução no console ou usando as APIs, a entidade principal deve ter a permissão `ec2:CreateLaunchTemplate` em uma política do IAM. Sempre que possível, use tags para ajudar você a controlar o acesso aos modelos de execução na conta.

Por exemplo, a declaração de política do IAM a seguir concede à entidade principal permissão para criar modelos de execução somente se o modelo usa a tag especificada (*purpose*=*testing*).

```
{
    "Sid": "IAMPolicyForCreatingTaggedLaunchTemplates",
    "Action": "ec2:CreateLaunchTemplate",
    "Effect": "Allow",
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:ResourceTag/purpose": "testing"
        }
    }
}
```

As entidades principais que criam modelos de execução podem precisar de algumas permissões relacionadas, como:

- ec2:CreateTags: para adicionar tags ao modelo de execução durante a operação `CreateLaunchTemplate`, o chamador de `CreateLaunchTemplate` deve ter a permissão `ec2:CreateTags` em uma política do IAM.
- ec2:RunInstances: para iniciar instâncias do EC2 a partir do modelo de execução que criou, a entidade principal também deve ter a permissão `ec2:RunInstances` em uma política do IAM.

Para ações de criação de recursos que aplicam tags, os usuários devem ter a permissão `ec2:CreateTags`. A declaração de política do IAM a seguir usa a chave de condição `ec2:CreateAction` para permitir que os usuários criem tags somente no contexto de `CreateLaunchTemplate`. Os usuários não podem marcar modelos de execução existentes nem nenhum outro recurso. Para obter mais informações, consulte Conceder permissão para marcar recursos do Amazon EC2 durante a criação.

```
{
    "Sid": "IAMPolicyForTaggingLaunchTemplatesOnCreation",
```

```
    "Action": "ec2:CreateTags",
    "Effect": "Allow",
    "Resource": "arn:aws:ec2:us-east-1:111122223333:launch-template/*",
    "Condition": {
        "StringEquals": {
            "ec2:CreateAction": "CreateLaunchTemplate"
        }
    }
}
```

O usuário do IAM que cria um modelo de execução não recebe automaticamente permissão para usar o modelo de execução que criou. Como qualquer outra entidade principal, o criador do modelo de execução precisa obter permissão por meio de uma política do IAM. Se um usuário do IAM quiser iniciar uma instância do EC2 a partir de um modelo de execução, ele deverá ter a permissão `ec2:RunInstances`. Ao conceder essas permissões, é possível especificar que os usuários só poderão usar modelos de execução com tags ou IDs específicos. Você também pode controlar a AMI e outros recursos aos quais qualquer pessoa que use modelos de execução possa fazer referência e usar ao iniciar instâncias especificando permissões em nível de recurso para a chamada `RunInstances`. Para obter exemplos de políticas, consulte Modelos de execução.

ec2:DescribeLaunchTemplates

Para listar e visualizar modelos de execução na conta, a entidade principal deve ter a permissão `ec2:DescribeLaunchTemplates` em uma política do IAM. Porque as ações `Describe` não oferecem suporte a permissões em nível de recurso, é necessário especificá-las sem condições, e o valor do elemento de recurso na política deve ser `"*"`.

Por exemplo, a instrução de política do IAM a seguir concede à entidade principal permissão para listar e visualizar todos os modelos de execução na conta.

```
{
    "Sid": "IAMPolicyForDescribingLaunchTemplates",
    "Action": "ec2:DescribeLaunchTemplates",
    "Effect": "Allow",
    "Resource": "*"
}
```

ec2:DescribeLaunchTemplateVersions

As entidades principais que listam e visualizam modelos de execução também devem ter a permissão `ec2:DescribeLaunchTemplateVersions` para recuperar todo o conjunto de atributos que compõem os modelos de execução.

Para listar e visualizar versões de modelos de execução na conta, a entidade principal deve ter a permissão `ec2:DescribeLaunchTemplateVersions` em uma política do IAM. Porque as ações `Describe` não oferecem suporte a permissões em nível de recurso, é necessário especificá-las sem condições, e o valor do elemento de recurso na política deve ser `"*"`.

Por exemplo, a instrução de política do IAM a seguir concede à entidade principal permissão para listar e visualizar todas as versões de modelos de execução na conta.

```
{
    "Sid": "IAMPolicyForDescribingLaunchTemplateVersions",
    "Effect": "Allow",
    "Action": "ec2:DescribeLaunchTemplateVersions",
    "Resource": "*"
}
```

ec2:DeleteLaunchTemplate

> **Important**
>
> Tenha cuidado ao conceder permissão às entidades principais para excluir um recurso. A exclusão de um modelo de execução pode causar uma falha em um recurso da AWS que depende desse modelo.

Para excluir um modelo de execução, a entidade principal deve ter a permissão `ec2:DeleteLaunchTemplate` em uma política do IAM. Sempre que possível, use chaves de condição baseadas em tag para limitar as permissões.

Por exemplo, a instrução de política do IAM a seguir concederá à entidade principal permissão para excluir modelos de execução somente se o modelo tiver a tag especificada (*`purpose`*=*`testing`*).

```
{
    "Sid": "IAMPolicyForDeletingLaunchTemplates",
    "Action": "ec2:DeleteLaunchTemplate",
```

```
    "Effect": "Allow",
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:ResourceTag/purpose": "testing"
        }
    }
}
```

Como alternativa, é possível usar ARNs para identificar o modelo de execução ao qual a política do IAM se aplica.

Um modelo de execução tem o ARN a seguir.

```
"Resource": "arn:aws:ec2:us-east-1:111122223333:launch-template/lt-09477bcd97b0d310e"
```

É possível especificar vários ARNs colocando-os em uma lista ou especificar um valor de `Resource` igual a `"*"` sem o elemento `Condition` para permitir que a entidade principal exclua qualquer modelo de execução na conta.

Controlar permissões de controle de versão

Para administradores confiáveis, é possível conceder acesso para criar e excluir versões de um modelo de execução e para alterar a versão padrão de um modelo de execução usando políticas do IAM semelhantes aos exemplos a seguir.

Important

Tenha cuidado ao conceder permissão às entidades principais para criar versões de modelos de execução ou modificar esses modelos.

- Ao criar uma versão do modelo de execução, você afetará todos os recursos da AWS que permitem que o Amazon EC2 inicie instâncias em seu nome com a versão `Latest`.
- Ao modificar um modelo de execução, você pode alterar qual versão é a `Default` e, consequentemente, afetar quaisquer recursos da AWS permitem que o Amazon EC2 inicie instâncias em seu nome com essa versão modificada.

Além disso, é necessário ter cuidado ao lidar com os recursos da AWS que interagem com a versão do modelo de execução `Latest` ou `Default`, como o EC2 Fleet e o Frota

Spot. Quando uma versão diferente do modelo de execução é usada para `Latest` ou `Default`, o Amazon EC2 não verifica novamente as permissões para que as ações sejam concluídas ao iniciar novas instâncias para atender à capacidade desejada da frota porque não há interação do usuário com o recurso da AWS. Ao conceder permissão ao usuário para chamar as APIs `CreateLaunchTemplateVersion` e `ModifyLaunchTemplate`, o usuário receberá efetivamente a permissão `iam:PassRole` se apontar a frota para uma versão do modelo de execução diferente que contenha um perfil de instância (um contêiner para um perfil do IAM). Isso significa que um usuário pode atualizar um modelo de execução para transferir um perfil do IAM para uma instância, mesmo que não tenha a permissão `iam:PassRole`. É possível gerenciar esse risco tomando cuidado ao conceder permissões para quem pode criar e gerenciar versões de modelos de execução.

ec2:CreateLaunchTemplateVersion

Para criar uma nova versão de um modelo de execução, a entidade principal deve ter a permissão `ec2:CreateLaunchTemplateVersion` para o modelo de execução em uma política do IAM.

Por exemplo, a declaração de política do IAM a seguir concede à entidade principal permissão para criar versões de modelos de execução somente se a versão usa a tag especificada (*`environment`*=*`production`*). Como alternativa, você pode especificar um ou vários ARNs de modelo de execução ou especificar um valor de `Resource` igual a `"*"` sem o elemento `Condition` para permitir que a entidade principal crie versões de qualquer modelo de execução na conta.

```
{
    "Sid": "IAMPolicyForCreatingLaunchTemplateVersions",
    "Action": "ec2:CreateLaunchTemplateVersion",
    "Effect": "Allow",
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:ResourceTag/environment": "production"
        }
    }
}
```

ec2:DeleteLaunchTemplateVersion

> **Important**
>
> Como sempre, tenha cuidado ao conceder permissão às entidades principais para excluir um recurso. A exclusão de uma versão de modelo de execução pode causar uma falha em um recurso da AWS que depende dessa versão.

Para excluir uma versão de modelo de execução, a entidade principal deve ter a permissão `ec2:DeleteLaunchTemplateVersion` para o modelo de execução em uma política do IAM.

Por exemplo, a declaração de política do IAM a seguir concede à entidade principal permissão para excluir versões de modelos de execução somente se a versão usa a tag especificada (*`environment`*=*`production`*). Como alternativa, você pode especificar um ou vários ARNs de modelo de execução ou especificar um valor de `Resource` igual a `"*"` sem o elemento `Condition` para permitir que a entidade principal exclua versões de qualquer modelo de execução na conta.

```
{
    "Sid": "IAMPolicyForDeletingLaunchTemplateVersions",
    "Action": "ec2:DeleteLaunchTemplateVersion",
    "Effect": "Allow",
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:ResourceTag/environment": "production"
        }
    }
}
```

ec2:ModifyLaunchTemplate

Para alterar a versão `Default` associada a um modelo de execução, a entidade principal deve ter a permissão `ec2:ModifyLaunchTemplate` para o modelo de execução em uma política do IAM.

Por exemplo, a declaração de política do IAM a seguir concede à entidade principal permissão para modificar modelos de execução somente se o modelo de execução usa a tag especificada (*`environment`*=*`production`*). Como alternativa, você pode especificar um ou vários ARNs de modelo de execução ou especificar um valor de `Resource` igual a `"*"` sem o elemento `Condition` para permitir que a entidade principal modifique qualquer modelo de execução na conta.

```
{
    "Sid": "IAMPolicyForModifyingLaunchTemplates",
    "Action": "ec2:ModifyLaunchTemplate",
    "Effect": "Allow",
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:ResourceTag/environment": "production"
        }
    }
}
```

Controlar o acesso a tags em modelos de execução

É possível usar chaves de condição para limitar permissões de tag quando o recurso é um modelo de execução. Por exemplo, a política do IAM a seguir permite remover somente a tag com a chave *temporary* dos modelos de lançamento na conta e região especificadas.

```
{
    "Sid": "IAMPolicyForDeletingTagsOnLaunchTemplates",
    "Action": "ec2:DeleteTags",
    "Effect": "Allow",
    "Resource": "arn:aws:ec2:us-east-1:111122223333:launch-template/*",
    "Condition": {
        "ForAllValues:StringEquals": {
            "aws:TagKeys": ["temporary"]
        }
    }
}
```

Para obter mais informações sobre as chaves de condições que você pode usar para controlar as chaves e valores de tag que podem ser aplicados aos recursos do Amazon EC2, consulte Controlar o acesso a tags específicas.

Usar modelos de execução do Amazon EC2 para controlar a execução de instâncias do Amazon EC2

É possível controlar a configuração das instâncias do Amazon EC2 ao especificar que os usuários só poderão executar instâncias se usarem um modelo de execução, e que só poderão usar um modelo

de execução específico. Você também pode controlar quem pode criar, modificar, descrever e excluir modelos de inicialização e versões do modelo de inicialização.

Uso de modelos de execução para controlar parâmetros de execução

Um modelo de execução pode conter todos ou alguns parâmetros para configurar uma instância na execução. No entanto, ao executar uma instância usando um modelo de execução, será possível substituir os parâmetros especificados nele. Ou pode especificar parâmetros adicionais que não estão no modelo de execução.

> **Note**
>
> Você não remover os parâmetros do modelo de execução durante a execução (por exemplo, não é possível 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 devem ter permissão para usar a ação `ec2:RunInstances`. Os usuários também devem ter permissões para criar ou usar os recursos que são criados ou estão associados à instância. É possível 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, é possível 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, é possível especificar que os usuários só podem executar instâncias usando um modelo de execução e só podem usar um modelo de execução específico. Também é possível controlar os parâmetros de execução que os usuários podem substituir no modelo de execução. Para obter exemplos de políticas do , consulte Modelos de execução.

Controlar o uso dos modelos de execução

Por padrão, os usuários não têm permissões para trabalhar com modelos de execução. É possível criar uma política que concede aos usuários permissões para criar, modificar, descrever e excluir modelos de execução e versões do modelo de execução. Também é possível aplicar permissões no nível do recurso a algumas ações do modelo de execução para controlar a capacidade de um usuário de usar recursos específicos nessas ações. Para obter mais informações, consulte as seguintes políticas de exemplo: Exemplo: trabalhar com modelos de execução.

Tenha cuidado ao conceder aos usuários permissões para usar as ações `ec2:CreateLaunchTemplate` e `ec2:CreateLaunchTemplateVersion`. Você não pode usar permissões em nível de recurso para controlar quais recursos os usuários podem especificar no modelo de execução. Para restringir os recursos usados para executar uma instância, conceda permissões para criar modelos de execução e versões de modelo de execução somente a administradores apropriados.

Aspectos importantes de segurança ao usar modelos de execução com o EC2 Fleet ou o frota spot

Ao usar modelos de execução, você também deve conceder aos usuários permissões para criar, modificar, descrever e excluir modelos de execução e versões de modelo de execução. É possível controlar quem pode criar modelos de lançamento e iniciar versões de modelos controlando o acesso às ações `ec2:CreateLaunchTemplate` e `ec2:CreateLaunchTemplateVersion`. . Também é possível controlar quem pode modificar os modelos de execução controlando o acesso à ação `ec2:ModifyLaunchTemplate`.

> **Important**
>
> Se uma frota spot ou EC2 Fleet estiver configurada para usar a versão mais recente ou padrão do modelo de execução, a frota não saberá se a mais recente ou a padrão foram alteradas posteriormente para apontar para uma versão diferente do modelo de execução. Quando uma versão diferente do modelo de execução é usada para Mais recente ou Padrão, o Amazon EC2 não verifica novamente as permissões para que as ações sejam concluídas ao iniciar novas instâncias para atender à capacidade desejada da frota. Essa é uma consideração importante ao conceder permissões a quem pode criar e gerenciar versões do modelo de execução, especialmente a ação `ec2:ModifyLaunchTemplate`, que permite ao usuário alterar a versão Padrão do modelo de execução.

Ao conceder permissão ao usuário para usar as ações do EC2 para as APIs do modelo de execução, o usuário também recebe efetivamente a permissão `iam:PassRole` se criar ou atualizar uma frota spot ou EC2 Fleet para apontar para uma versão diferente do modelo de execução que contenha um perfil de instância (um contêiner para um perfil do IAM). Isso significa que um usuário pode atualizar um modelo de execução para transferir um perfil do IAM para uma instância, mesmo que não tenha a permissão `iam:PassRole`. Para obter mais informações e um exemplo de política do IAM, consulte Uso de um perfil do IAM para conceder permissões a aplicações em execução em instâncias do Amazon EC2 no Guia do usuário do IAM.

Para obter mais informações, consulte Controlar o uso dos modelos de execução e Exemplo: trabalhar com modelos de execução.

Criar um modelo de execução do Amazon EC2

É possível criar um modelo de execução do Amazon EC2 especificando seus próprios valores para os parâmetros de configuração da instância ou obtendo os valores de um modelo de execução existente ou de uma instância do Amazon EC2.

Você não precisa especificar um valor para cada parâmetro no modelo de execução; você só precisa especificar um parâmetro de configuração da instância para criar um modelo de execução. Para indicar parâmetros que você opta por não especificar, selecione Não incluir no modelo de execução ao usar o console. Ao usar uma ferramenta de linha de comandos, não inclua os parâmetros para indicar que você está optando por não especificá-los no modelo de execução.

Se você quiser especificar uma AMI no modelo de execução, você pode selecionar uma AMI ou especificar um parâmetro do Systems Manager que aponte para uma AMI na execução da instância.

Quando uma instância é executada com um modelo de execução, os valores especificados no modelo de execução são usados para configurar os parâmetros de instância correspondentes. Se um valor não for especificado no modelo de execução, o valor padrão para o parâmetro de instância correspondente será usado.

Tarefas

- Criar um modelo de execução especificando parâmetros
- Criar um modelo de execução a partir de um modelo de execução existente
- Criar um modelo de execução a partir de uma instância
- Use um parâmetro de Systems Manager em vez de um ID de AMI

Criar um modelo de execução especificando parâmetros

Para criar um modelo de execução, especifique o nome do modelo de execução e, pelo menos, um parâmetro de configuração de instância.

Para uma descrição de cada parâmetro, consulte Referência para parâmetros de configuração de instâncias do Amazon EC2.

Console

Para criar um modelo de execução

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Launch Templates (Modelos de execução) e Create launch template (Criar modelo de execução).
3. Em Nome e descrição do modelo de execução, faça o seguinte:

   a. Em Device template name (Nome do modelo de dispositivo), insira um nome descritivo para o modelo.

   b. Em Template version description (Descrição da versão do modelo), forneça uma descrição breve da versão do modelo de execução.

   c. Para marcar o modelo de execução na criação, expanda Tags do modelo, escolha Adicionar nova tag e insira um par de chave e valor de tag. Escolha Adicionar nova tag novamente para cada tag adicional a acrescentar.

   > **Note**
   >
   > Para marcar os recursos que são criados quando uma instância é executada, você deve especificar as etiquetas em Resource tags (Etiquetas de recursos). Para obter mais informações, consulte a Etapa 9 neste procedimento.

4. Em Imagens de SO e aplicações (Amazon Machine Image), você pode manter a opção Não incluir no modelo de execução selecionada, ou escolher o sistema operacional (SO) da instância, e então escolher uma AMI. Como alternativa, você pode especificar um parâmetro do Systems Manager em vez de especificar uma AMI. Para obter mais informações, consulte Use um parâmetro de Systems Manager em vez de um ID de AMI.

   Uma AMI é um modelo que contém o sistema operacional e o software necessários para executar uma instância.

5. Em Tipo de instância, você pode manter a opção Não incluir no modelo de execução selecionada, pode selecionar um tipo de instância ou pode especificar atributos de instância e deixar que o Amazon EC2 identifique os tipos de instância com esses atributos.

> **Note**
>
> A especificação de atributos de instância é compatível somente quando o modelo de execução é usado pelos grupos do Auto Scaling, pelo EC2 Fleet e pela frota spot para executar instâncias. Para obter mais informações, consulte Create mixed instances group using attribute-based instance type selection e Especificar atributos para seleção de tipo de instância para frota do EC2 ou frota spot.
> Caso planeje usar o modelo de execução no assistente de inicialização de instâncias ou com a API RunInstances, você deve especificar os atributos do tipo de instância.

O tipo de instância determina a configuração de hardware (CPU, memória, armazenamento e capacidade de rede) e o tamanho do computador host usado para uma instância.

Se você não tiver certeza de qual tipo de instância escolher, você pode fazer o seguinte:

- Escolha Comparar tipos de instâncias para comparar diferentes tipos de instâncias pelos seguintes atributos: número de vCPUs, arquitetura, quantidade de memória (GiB), quantidade de armazenamento (GB), tipo de armazenamento e performance de rede.
- Escolha Obter conselho para obter orientações e sugestões de tipos de instância no localizador de tipo de instâncias do EC2. Para obter mais informações, consulte Obtenha recomendações do localizador de tipo de instância do EC2.

> **Note**
>
> Dependendo de quando sua conta foi criada, ela pode ser elegível para usar o Amazon EC2 no nível gratuito.
> Caso tenha criado sua Conta da AWS antes de 15 de julho de 2025 e ela tenha menos de 12 meses, você pode usar o Amazon EC2 no nível gratuito selecionando o tipo de instância t2.micro ou o tipo de instância t3.micro em regiões onde o tipo t2.micro está indisponível. Lembre-se de que, quando você executa uma instância t3.micro, o padrão é o modo Ilimitado, o que pode gerar cobranças adicionais com base no uso da CPU. Se um tipo de instância puder ser usada no nível gratuito, ela terá o rótulo Elegível para o nível gratuito.

Se você tiver criado sua Conta da AWS a partir de 15 de julho de 2025, poderá usar os tipos de instância t3.micro, t3.small, t4g.micro, t4g.small, c7i-flex.large e m7i-flex.large durante 6 meses ou até seus créditos acabarem.
Para obter mais informações, consulte Benefícios do nível gratuito antes e depois de 15 de julho de 2025.

6. Em Par de chaves (login), em Nome do par de chaves, mantenha a opção Não incluir no modelo de execução selecionada ou escolha um par de chaves existente ou crie um novo.
7. Em Configurações de rede, você pode manter a opção Não incluir no modelo de execução selecionada ou especificar valores para as várias configurações de rede.
8. Em Configurar armazenamento, se você especificar uma AMI no modelo de execução, a AMI incluirá um ou mais volumes de armazenamento, incluindo o volume raiz (Volume 1 [Raiz da AMI]). Você opcionalmente especificar volumes adicionais a serem anexados à instância. Para adicionar um novo volume, escolha Add new volume (Adicionar novo volume).
9. Em Tags de recursos, para marcar os recursos que são criados quando uma instância é executada, escolha Adicionar tag e, em seguida, insira um par de chave e valor de tag. Em Resource types (Tipos de recursos), especifique os recursos para marcar na criação. É possível especificar a mesma etiqueta para todos os recursos ou especificar etiquetas diferentes para recursos diferentes. Escolha Add tag (Adicionar tag) para cada tag adicional a acrescentar.

   É possível especificar etiquetas tags para os seguintes recursos que são criados quando um modelo de inicialização é usado:

   - Instâncias
   - Volumes
   - Elastic Graphics
   - Solicitações de instância Spot
   - Interfaces de rede

   Note

   Para marcar o modelo de execução em si, é necessário especificar as tags em Template tags (Etiquetas de modelo). Para obter mais informações, consulte a Etapa 3 neste procedimento.

10. Em Detalhes avançados, expanda a seção para visualizar os campos e, opcionalmente, especifique quaisquer parâmetros adicionais para a instância.
11. Use o painel Resumo para analisar a configuração do modelo de execução. É possível navegar para qualquer seção ao escolher um link e, em seguida, realizar as alterações necessárias.
12. Quando você estiver pronto para criar seu modelo de execução, escolha Create launch template (Criar modelo de execução).

AWS CLI

Para criar um modelo de execução

Use o comando create-launch-template.

```
aws ec2 create-launch-template \
    --launch-template-name TemplateForWebServer \
    --version-description WebVersion1 \
    --tag-specifications 'ResourceType=launch-
template,Tags=[{Key=purpose,Value=production}]' \
    --launch-template-data file://template-data.json
```

Veja a seguir um exemplo em JSON que especifica os dados do modelo de execução para a configuração da instância. Salve o formato JSON em um arquivo e inclua-o no parâmetro `--launch-template-data`, conforme mostrado no comando de exemplo.

```
{
    "NetworkInterfaces": [{
        "AssociatePublicIpAddress": true,
        "DeviceIndex": 0,
        "Ipv6AddressCount": 1,
        "SubnetId": "subnet-0abcdef1234567890"
    }],
    "ImageId": "ami-0abcdef1234567890",
    "InstanceType": "r5.4xlarge",
    "TagSpecifications": [{
        "ResourceType": "instance",
        "Tags": [{
            "Key":"Name",
            "Value":"webserver"
        }]
```

```
    }],
    "CpuOptions": {
        "CoreCount":4,
        "ThreadsPerCore":2
    }
}
```

O seguinte é 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"
    }
}
```

PowerShell

Para criar um modelo de execução

Use o cmdlet New-EC2LaunchTemplate.

```
$launchTemplateData = [Amazon.EC2.Model.RequestLaunchTemplateData]@{
    ImageId = 'ami-0abcdef1234567890'
    InstanceType = 'r5.4xlarge'
    NetworkInterfaces = @(

 [Amazon.EC2.Model.LaunchTemplateInstanceNetworkInterfaceSpecificationRequest]@{
            AssociatePublicIpAddress = $true
            DeviceIndex = 0
            Ipv6AddressCount = 1
            SubnetId = 'subnet-0abcdef1234567890'
        }
    )
    TagSpecifications = @(
        [Amazon.EC2.Model.LaunchTemplateTagSpecificationRequest]@{
            ResourceType = 'instance'
            Tags = [Amazon.EC2.Model.Tag]@{
                Key = 'Name'
```

```
                Value = 'webserver'
            }
        }
    )
    CpuOptions = [Amazon.EC2.Model.LaunchTemplateCpuOptionsRequest]@{
        CoreCount = 4
        ThreadsPerCore = 2
    }
}
$tagSpecificationData = [Amazon.EC2.Model.TagSpecification]@{
    ResourceType = 'launch-template'
    Tags = [Amazon.EC2.Model.Tag]@{
        Key = 'purpose'
        Value = 'production'
    }
}
New-EC2LaunchTemplate -LaunchTemplateName 'TemplateForWebServer' `
    -VersionDescription 'WebVersion1' `
    -LaunchTemplateData $launchTemplateData `
    -TagSpecification $tagSpecificationData
```

O seguinte é um exemplo de saída.

```
CreatedBy            : arn:aws:iam::123456789012:root
CreateTime           : 9/19/2023 16:57:55
DefaultVersionNumber : 1
LatestVersionNumber  : 1
LaunchTemplateId     : lt-01238c059eEXAMPLE
LaunchTemplateName   : TemplateForWebServer
Tags                 : {purpose}
```

Criar um modelo de execução a partir de um modelo de execução existente

É possível clonar um modelo de inicialização existente e ajustar os parâmetros para criar um novo modelo de inicialização. No entanto, você só pode fazer isso ao usar o console do Amazon EC2. A AWS CLI não é compatível a clonagem de um modelo. Para uma descrição de cada parâmetro, consulte Referência para parâmetros de configuração de instâncias do Amazon EC2.

Console

Para criar um modelo de inicialização a partir de um modelo de inicialização existente

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Launch Templates (Modelos de execução) e Create launch template (Criar modelo de execução).
3. Em Device template name (Nome do modelo de dispositivo), insira um nome descritivo para o modelo.
4. Em Template version description (Descrição da versão do modelo), forneça uma descrição breve da versão do modelo de execução.
5. Para marcar o modelo de execução na criação, expanda Tags de modelo, escolha Adicionar nova tag e então insira um par de chave e valor de tag.
6. Expanda o Modelo de origem e, em Nome do modelo de execução, escolha um modelo de execução no qual o novo modelo de execução se baseará.
7. Em Source template version (Versão do modelo de origem), escolha a versão do modelo de execução no qual o novo modelo de execução se baseará.
8. Ajuste todos os parâmetros de execução quando necessário e escolha Create launch template (Criar modelo de execução).

Criar um modelo de execução a partir de uma instância

É possível clonar os parâmetros de uma instância existente do Amazon EC2 e ajustá-los para criar um modelo de execução. Para uma descrição de cada parâmetro, consulte Referência para parâmetros de configuração de instâncias do Amazon EC2.

Console

Para criar um modelo de inicialização a partir 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 Ações, Imagem e modelos, Criar modelo da instância.
4. Forneça um nome, uma descrição e tags e ajuste os parâmetros de execução conforme necessário.

> **Note**
>
> Quando você cria um modelo de execução de uma instância, os IDs da interface de rede da instância e os endereços IP não são incluídos no modelo.

5. Escolha Create launch template (Criar modelo de execução).

AWS CLI

É possível usar a AWS CLI para criar um modelo de execução de uma instância existente ao obter os dados do modelo de execução primeiro e depois criar um modelo de execução usando os dados dele.

Para obter dados de modelo de inicialização de uma instância

- Use o comando get-launch-template-data e especifique o ID da instância. É possível 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"
            }
        ]
    }
```

É possível gravar o resultado diretamente em um arquivo, por exemplo:

```
aws ec2 get-launch-template-data \
    --instance-id i-0123d646e8048babc \
    --query "LaunchTemplateData" >> instance-data.json
```

Para criar um modelo de execução usando dados do modelo de execução

- Use o comando create-launch-template para criar um modelo de execução usando a saída do procedimento anterior. Para obter mais informações sobre como criar um modelo

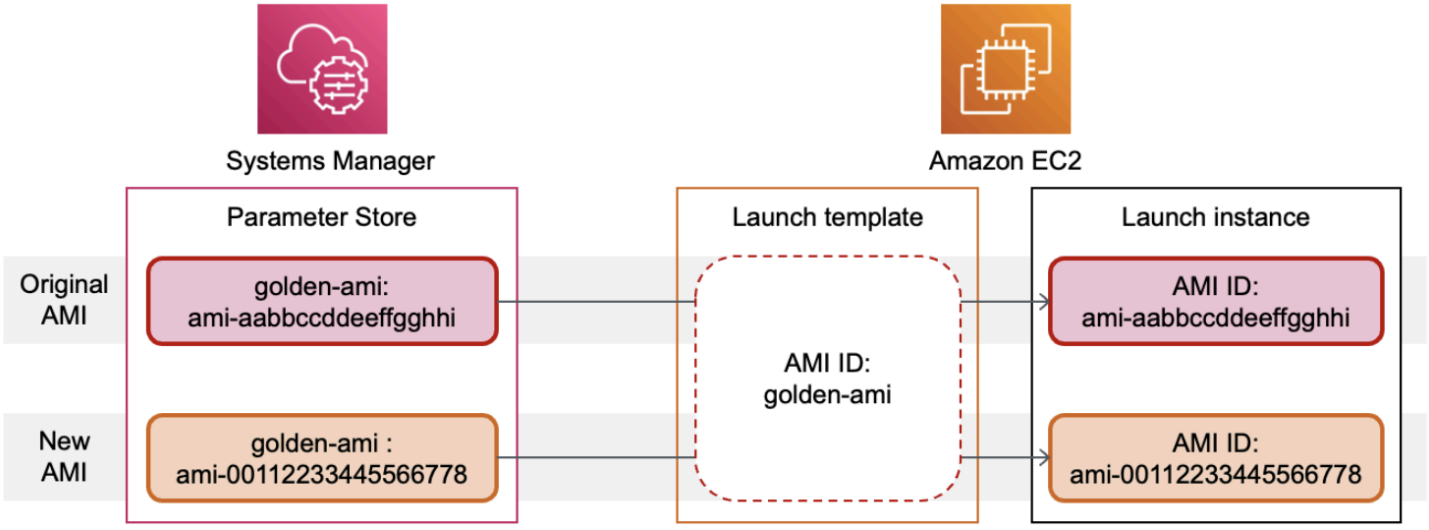
de execução usando a AWS CLI, consulte Criar um modelo de execução especificando parâmetros.

Use um parâmetro de Systems Manager em vez de um ID de AMI

Em vez de especificar um ID de AMI em seus modelos de inicialização, você pode especificar um parâmetro AWS Systems Manager. Se o ID da AMI for alterado, será possível atualizar o ID da AMI em um único lugar atualizando o parâmetro Systems Manager no Systems Manager Parameter Store. Os parâmetros também podem ser compartilhados com outras Contas da AWS. É possível armazenar e gerenciar os parâmetros da AMI de forma centralizada em uma conta e compartilhá-los com todas as outras contas que precisam referenciá-los. Usando um parâmetro do Systems Manager, todos os seus modelos de inicialização podem ser atualizados em uma única ação.

Um parâmetro do Systems Manager é um par chave-valor definido pelo usuário que pode ser criado no Parameter Store do AWS Systems Manager. O Parameter Store fornece um lugar central para armazenar os valores de configuração da aplicação.

No diagrama a seguir, o parâmetro `golden-ami` é mapeado primeiro para a AMI original `ami-aabbccddeeffgghhi` no Parameter Store. No modelo de inicialização, o valor do ID da AMI é `golden-ami`. Quando uma instância é iniciada usando esse modelo de inicialização, o ID da AMI é resolvido para `ami-aabbccddeeffgghhi`. Posteriormente, a AMI é atualizada, resultando em um novo ID de AMI. No Parameter Store, o parâmetro `golden-ami` é mapeado para o novo `ami-00112233445566778`. O modelo de inicialização permanece inalterado. Quando uma instância é iniciada usando esse modelo de inicialização, o ID de AMI é resolvido para `ami-00112233445566778`.



Formato de parâmetros do Systems Manager para IDs de AMI

Os modelos de inicialização exigem que os parâmetros do Systems Manager definidos pelo usuário sigam o seguinte formato quando usados no lugar de um ID de AMI:

- Tipo de parâmetro: `String`
- Tipo de dados do parâmetro: `aws:ec2:image`; garante que o Parameter Store valide que o valor inserido está no formato adequado para um ID de AMI.

Para obter mais informações sobre como criar um parâmetro válido para um ID de AMI, consulte Crie um parâmetro do Systems Manager no Guia do usuário do AWS Systems Manager.

Formato de parâmetros do Systems Manager em modelos de inicialização

Para usar um parâmetro do Systems Manager no lugar de um ID de AMI em um modelo de inicialização, você deve usar um dos seguintes formatos ao especificar o parâmetro no modelo de inicialização:

Para fazer referência a um parâmetro público:

- `resolve:ssm:`*`public-parameter`*

Para fazer referência a um parâmetro armazenado na mesma conta:

- `resolve:ssm:`*`parameter-name`*
- `resolve:ssm:`*`parameter-name`*`:`*`version-number`*: o número da versão em si é um rótulo padrão
- `resolve:ssm:`*`parameter-name`*`:`*`label`*

Para fazer referência a um parâmetro compartilhado de outra Conta da AWS:

- `resolve:ssm:`*`parameter-ARN`*
- `resolve:ssm:`*`parameter-ARN`*`:`*`version-number`*
- `resolve:ssm:`*`parameter-ARN`*`:`*`label`*

Versões de parâmetros

Os parâmetros do Systems Manager são recursos versionados. Ao atualizar um parâmetro, você cria novas versões sucessivas do parâmetro. O Systems Manager é compatível com rótulos de parâmetros que você pode mapear para versões específicas de um parâmetro.

Por exemplo, o parâmetro `golden-ami` pode ter três versões: `1`, `2` e `3`. É possível criar um rótulo de parâmetro `beta` que é mapeado para a versão `2` e um rótulo de parâmetro `prod` que é mapeado para a versão `3`.

Em um modelo de inicialização, você pode especificar a versão 3 do parâmetro `golden-ami` usando um dos seguintes formatos:

- `resolve:ssm:golden-ami:3`
- `resolve:ssm:golden-ami:prod`

Especificar a versão ou o rótulo é opcional. Por padrão, a versão mais recente do parâmetro é usada quando nenhuma versão é especificada.

Especificar um parâmetro do Systems Manager em um modelo de inicialização

É possível especificar um parâmetro do Systems Manager em um modelo de inicialização em vez de um ID de AMI ao criar um modelo de inicialização ou uma nova versão de um modelo de inicialização.

Console

Para especificar um parâmetro do Systems Manager em um modelo de inicialização

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Launch Templates (Modelos de execução) e Create launch template (Criar modelo de execução).
3. Em Device template name (Nome do modelo de dispositivo), insira um nome descritivo para o modelo.
4. Em Application and OS Images (Amazon Machine Image) (Imagens de aplicações e sistemas operacionais [imagem de máquina da Amazon]), escolha Browse more AMIs (Procurar mais AMIs).
5. Escolha o botão de seta à direita da barra de pesquisa e escolha Especificar valor personalizado/parâmetro do Systems Manager.

6. Na caixa de diálogo Especificar valor personalizado ou parâmetro do Systems Manager, faça o seguinte:

   a. Em ID de AMI ou string de parâmetros do Systems Manager, insira o nome do parâmetro do Systems Manager usando um destes formatos:

      Para fazer referência a um parâmetro público:

      - **resolve:ssm:*public-parameter***

      Para fazer referência a um parâmetro armazenado na mesma conta:

      - **resolve:ssm:*parameter-name***
      - **resolve:ssm:*parameter-name*:*version-number***
      - **resolve:ssm:*parameter-name*:*label***

      Para fazer referência a um parâmetro compartilhado de outra Conta da AWS:

      - **resolve:ssm:*parameter-ARN***
      - **resolve:ssm:*parameter-ARN*:*version-number***
      - **resolve:ssm:*parameter-ARN*:*label***

   b. Escolha Salvar.

7. Especifique quaisquer outros parâmetros do modelo de inicialização conforme necessário e escolha Criar modelo de inicialização.

Para obter mais informações, consulte Criar um modelo de execução especificando parâmetros.

AWS CLI

Para especificar um parâmetro do Systems Manager em um modelo de inicialização

- Use o comando create-launch-template para criar o modelo de inicialização. Para especificar a AMI a ser usada, insira o nome do parâmetro do Systems Manager usando um dos seguintes formatos:

  Para fazer referência a um parâmetro público:

  - **resolve:ssm:*public-parameter***

Para fazer referência a um parâmetro armazenado na mesma conta:

- **resolve:ssm:*parameter-name***
- **resolve:ssm:*parameter-name*:*version-number***
- **resolve:ssm:*parameter-name*:*label***

Para fazer referência a um parâmetro compartilhado de outra Conta da AWS:

- **resolve:ssm:*parameter-ARN***
- **resolve:ssm:*parameter-ARN*:*version-number***
- **resolve:ssm:*parameter-ARN*:*label***

O exemplo a seguir cria um modelo de execução que especifica o seguinte:

- Um nome para o modelo de inicialização (*TemplateForWebServer*)
- Uma etiqueta para o modelo de execução (*purpose*=*production*)
- Os dados para a configuração da instância, especificados em um arquivo JSON:
  - A AMI a ser usada (`resolve:ssm:`*golden-ami*)
  - O tipo de instância a ser executada iniciada (*m5.4xlarge*)
  - Uma etiqueta para a instância (*Name*=*webserver*)

```
aws ec2 create-launch-template \
    --launch-template-name TemplateForWebServer \
    --tag-specifications 'ResourceType=launch-
template,Tags=[{Key=purpose,Value=production}]' \
    --launch-template-data file://template-data.json
```

Veja a seguir um exemplo de arquivo JSON que contém os dados do modelo de execução para a configuração da instância. O valor de `ImageId` é o nome do parâmetro do Systems Manager, inserido no formato exigido `resolve:ssm:`*golden-ami*.

```
{"LaunchTemplateData": {
    "ImageId": "resolve:ssm:golden-ami",
    "InstanceType": "m5.4xlarge",
```

```
    "TagSpecifications": [{
        "ResourceType": "instance",
        "Tags": [{
            "Key":"Name",
            "Value":"webserver"
        }]
    }]
  }
}
```

Verifique se um modelo de execução obtém o ID da AMI correto

Como resolver o parâmetro do Systems Manager para o ID da AMI real

Use o comando describe-launch-template-versions e inclua o parâmetro `--resolve-alias`.

```
aws ec2 describe-launch-template-versions \
    --launch-template-name my-launch-template \
    --versions $Default \
    --resolve-alias
```

A resposta inclui o ID da AMI para `ImageId`. Neste exemplo, quando uma instância é iniciada usando esse modelo de execução, o ID da AMI é resolvido como `ami-0ac394d6a3example`.

```
{
    "LaunchTemplateVersions": [
        {
            "LaunchTemplateId": "lt-089c023a30example",
            "LaunchTemplateName": "my-launch-template",
            "VersionNumber": 1,
            "CreateTime": "2022-12-28T19:52:27.000Z",
            "CreatedBy": "arn:aws:iam::123456789012:user/Bob",
            "DefaultVersion": true,
            "LaunchTemplateData": {
                "ImageId": "ami-0ac394d6a3example",
                "InstanceType": "t3.micro",
            }
        }
    ]
}
```

Recursos relacionados

Para obter mais informações sobre como trabalhar com os parâmetros do Systems Manager, consulte os materiais de referência apresentados a seguir na documentação do Systems Manager.

- Para obter informações sobre como pesquisar os parâmetros públicos da AMI com suporte para o Amazon EC2, consulte Calling AMI public parameters.
- Para obter informações sobre como compartilhar os parâmetros com outras contas da AWS ou por meio do AWS Organizations, consulte Working with shared parameters.
- Para obter informações sobre como monitorar se os parâmetros foram criados com êxito, consulte Native parameter support for Amazon Machine Image IDs.

Limitações

- Somente as frotas do EC2 do tipo `instant` oferecem suporte ao uso de um modelo de inicialização que tenha um parâmetro do Systems Manager especificado no lugar de um ID de AMI.
- As frotas do EC2 dos tipos `maintain` e `request` e as frotas spot não são compatíveis com o uso de um modelo de inicialização que tenha um parâmetro do Systems Manager especificado no lugar de um ID de AMI. Para frotas do EC2 dos tipos `maintain` e `request` e frotas spot, se você especificar uma AMI no modelo de inicialização, deverá especificar o ID da AMI.
- Se você usar a seleção de instância baseada em atributos na frota do EC2, não poderá especificar um parâmetro do Systems Manager no lugar de um ID de AMI. Ao usar a seleção de instância baseada em atributos, você deve especificar o ID da AMI.
- O Amazon EC2 Auto Scaling fornece outras restrições. Para obter mais informações, consulte Use AWS Systems Manager parameters instead of AMI IDs in launch templates no Guia do usuário do Amazon EC2 Auto Scaling.

Modificar um modelo de inicialização (gerenciar versões do modelo de inicialização)

Os modelos de inicialização são imutáveis. Após criar um modelo de inicialização, você não poderá modificá-lo. Em vez disso, é possível criar uma nova versão do modelo de inicialização que inclua as alterações necessárias.

É possível criar diferentes versões de um modelo de execução, definir a versão padrão, descrever uma versão de modelo de execução e excluir versões que não sejam mais necessárias.

Tarefas

- Criar uma versão de modelo de execução
- Definir a versão do modelo de execução padrão
- Descrever uma versão de modelo de execução

Criar uma versão de modelo de execução

Ao criar uma versão de modelo de execução, é possível especificar novos parâmetros de execução ou usar uma versão existente como base para a nova versão. Para uma descrição de cada parâmetro, consulte Referência para parâmetros de configuração de instâncias do Amazon EC2.

Console

Para criar uma versão de modelo de inicialização

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Launch Templates (Modelos de execução).
3. Selecione um modelo de execução e escolha Actions (Ações), Modify template (Create new version) (Modificar modelo (Criar versão)).
4. Em Template version description (Descrição da versão do modelo), insira uma descrição para a versão do modelo de execução.
5. (Opcional) Expanda o Source template (Modelo de origem) e selecione uma versão do modelo de execução a ser usado como base para a nova versão do modelo de execução. A nova versão de modelo de execução herdará os parâmetros de execução desta versão do modelo de execução.
6. Modifique os parâmetros de execução conforme necessário.
7. Escolha Criar modelo de execução.

AWS CLI

Para criar uma versão de modelo de inicialização

Use o comando create-launch-template-version. É possível especificar uma versão de origem na qual a nova versão será baseada. A nova versão herdará os parâmetros de execução desta

versão, e será possível 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-0abcdef1234567890"
```

PowerShell

Para criar uma versão de modelo de inicialização

Use o cmdlet New-EC2LaunchTemplateVersion. É possível especificar uma versão de origem na qual a nova versão será baseada. A nova versão herdará os parâmetros de execução desta versão, e será possível substituí-los usando `LaunchTemplateData`. O exemplo a seguir cria uma nova versão com base na versão 1 do modelo de execução e especifica um ID de AMI diferente.

```
New-EC2LaunchTemplateVersion `
    -LaunchTemplateId lt-0abcd290751193123 `
    -VersionDescription WebVersion2 `
    -SourceVersion 1 `
    -LaunchTemplateData (
        New-Object `
            -TypeName Amazon.EC2.Model.RequestLaunchTemplateData `
            -Property @{ImageId = 'ami-0abcdef1234567890'}
    )
```

Definir a versão do modelo de execução padrão

É possível definir a versão padrão do modelo de execução. Quando você executa uma instância a partir de um modelo de execução e não especifica uma versão, a instância é executada por meio dos parâmetros da versão padrão.

Console

Para definir a versão do modelo de inicialização padrão

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

2. No painel de navegação, selecione Launch Templates (Modelos de execução).
3. Selecione o modelo de execução e escolha Actions (Ações), Set default version (Definir versão padrão).
4. Em Template version (Versão do modelo), selecione o número da versão a ser definida como versão padrão e escolha Set as default version (Definir como versão padrão).

AWS CLI

Para definir a versão do modelo de inicialização padrão

Use o comando modify-launch-template.

```
aws ec2 modify-launch-template \
    --launch-template-id lt-0abcd290751193123 \
    --default-version 2
```

PowerShell

Para definir a versão do modelo de inicialização padrão

Use o cmdlet Edit-EC2LaunchTemplate.

```
Edit-EC2LaunchTemplate `
    -LaunchTemplateId lt-0abcd290751193123 `
    -DefaultVersion 2
```

Descrever uma versão de modelo de execução

Usando o console, é possível visualizar todas as versões do modelo de execução selecionado ou obter uma lista dos modelos de execução cuja versão mais recente ou padrão corresponde a um número de versão específico. Usando o AWS CLI, é possível descrever todas as versões, versões individuais ou um intervalo de versões de um modelo de execução especificado. Também é possível descrever todas as versões mais recentes ou todas as versões padrão de todos os modelos de execução da sua conta.

Console

Para descrever uma versão de modelo de inicialização

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. É possível visualizar uma versão de um modelo de lançamento específico ou obter uma lista dos modelos de execução cuja versão mais recente ou padrão corresponde a um número de versão específico.
   - Para visualizar uma versão de um modelo de execução: selecione o modelo de execução. Na guia Versões em Versão, selecione uma versão para visualizar seus detalhes.
   - Para obter uma lista de todos os modelos de execução cuja versão mais recente corresponde a um número de versão específico: na barra de pesquisa, escolha Versão mais recente e selecione um número de versão.
   - Para obter uma lista de todos os modelos de execução cuja versão padrão corresponde a um número de versão específico: na barra de pesquisa, escolha Versão padrão e selecione um número de versão.

AWS CLI

Para descrever uma versão de modelo de inicialização

Use o comando delete-launch-template-versions e especifique os números de versão. No exemplo a seguir, as versões *1* e *3* são especificadas.

```
aws ec2 describe-launch-template-versions \
    --launch-template-id lt-0abcd290751193123 \
    --versions 1 3
```

Para descrever as versões mais recentes e padrão do modelo de inicialização da sua conta

Use o comando describe-launch-template-versions e especifique `$Latest`, `$Default`, ou ambos. É necessário omitir o ID e o nome do modelo de execução na chamada. Não é possível especificar números de versão.

```
aws ec2 describe-launch-template-versions \
    --versions "$Latest,$Default"
```

PowerShell

Para descrever uma versão de modelo de inicialização

Use o cmdlet Get-EC2TemplateVersion e especifique os números da versão. No exemplo a seguir, as versões *1* e *3* são especificadas.

```
Get-EC2TemplateVersion `
    -LaunchTemplateId lt-0abcd290751193123 `
    -Version 1,3
```

Para descrever as versões mais recentes e padrão do modelo de inicialização da sua conta

Use o cmdlet Get-EC2TemplateVersion e especifique `$Latest`, `$Default` ou ambos. É necessário omitir o ID e o nome do modelo de execução na chamada. Não é possível especificar números de versão.

```
Get-EC2TemplateVersion `
    -Version '$Latest','$Default'
```

Excluir um modelo de execução ou uma versão de 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. Caso queira excluir apenas uma versão específica de um modelo de execução, será possível fazê-lo e manter as outras versões do modelo de execução.

Excluir um modelo de execução ou uma versão de modelo de execução não afetará nenhuma instância que você executou nele.

Excluir um modelo de execução e todas as suas versões

Caso não precise mais de um modelo de execução, incluindo todas as suas versões, você pode excluí-lo. A exclusão de um modelo de execução excluirá todas as suas versões.

Console

Para excluir um modelo de execução e todas as suas versões

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

2. No painel de navegação, selecione Launch Templates (Modelos de execução).
3. Selecione o modelo de execução e escolha Actions (Ações), Delete template (Excluir modelo).
4. Digite **`Delete`** para confirmar a exclusão e escolha Delete (Excluir).

AWS CLI

Para excluir um modelo de execução e todas as suas versões

Use o comando delete-launch-template e especifique o modelo de execução.

```
aws ec2 delete-launch-template --launch-template-id lt-01238c059e3466abc
```

PowerShell

Para excluir um modelo de execução e todas as suas versões

Use o comando Remove-EC2LaunchTemplate (AWS Tools for PowerShell) e especifique o modelo de execução. Se `-Force` for omitido, o PowerShell solicitará uma confirmação.

```
Remove-EC2LaunchTemplate -LaunchTemplateId lt-0123456789example -Force
```

Excluir uma versão de modelo de execução

Caso não precise mais de uma versão de modelo de execução, exclua-a.

Considerações

- Não é possível substituir o número de versão após excluí-lo.
- Não é possível excluir a versão padrão do modelo de execução; antes é necessário atribuir outra versão como a padrão. Se a versão padrão for a única versão para o modelo de execução, exclua todo o modelo de execução.
- No console, é possível excluir uma versão do modelo de execução por vez. Usando a AWS CLI, é possível excluir até 200 versões do modelo de execução em uma única solicitação. Para excluir mais de 200 versões em uma única solicitação, exclua o modelo de execução, o que também exclui todas as suas versões.

Console

Para excluir uma versão de modelo de inicialização

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Launch Templates (Modelos de execução).
3. Selecione o modelo de execução e escolha Actions (Ações), Delete template version (Excluir versão de modelo).
4. Selecione a versão a ser excluída e escolha Delete (Excluir).

AWS CLI

Para excluir uma versão de modelo de inicialização

Use o comando delete-launch-template-versions e especifique os números de versão a serem excluídos. É possível especificar até 200 versões do modelo de execução para excluir em uma única solicitação.

```
aws ec2 delete-launch-template-versions \
    --launch-template-id lt-0abcd290751193123 \
    --versions 1
```

PowerShell

Para excluir uma versão de modelo de inicialização

Use o cmdlet Remove-EC2TemplateVersion e especifique os números de versão a serem excluídos. É possível especificar até 200 versões do modelo de execução para excluir em uma única solicitação.

```
Remove-EC2TemplateVersion `
    -LaunchTemplateId lt-0abcd290751193123 `
    -Version 1
```

Iniciar uma instância do Amazon EC2

Uma instância é um servidor virtual na Nuvem AWS. Você executa uma instância a partir de uma imagem de máquina da Amazon (AMI). A AMI fornece o sistema operacional, o servidor de aplicações e as aplicações para sua instância.

Ao criar sua Conta da AWS, comece a usar o Amazon EC2 gratuitamente com o Nível gratuito da AWS. Os benefícios do nível gratuito dependem de quando sua Conta da AWS foi criada. Caso tenha criado sua Conta da AWS antes de 15 de julho de 2025 e ela tenha menos de 12 meses, você poderá utilizar o nível gratuito para inicializar e usar uma instância `t2.micro` gratuitamente (em regiões onde `t2.micro` não estiver disponível, é possível usar uma instância `t3.micro` no nível gratuito). Você incorrerá em custos para a sua instância ou uso que conta para os limites do nível gratuito enquanto a instância estiver operacional, mesmo que ela permaneça inativa. Para obter mais informações, consulte Definição de preço do Amazon EC2. Caso tenha criado sua Conta da AWS em 15 de julho de 2025 ou após essa data, você pode usar os tipos de instância `t3.micro`, `t3.small`, `t4g.micro`, `t4g.small`, `c7i-flex.large` e `m7i-flex.large` por seis meses ou até que os créditos acabem. Para obter mais informações, consulte Benefícios do nível gratuito antes e depois de 15 de julho de 2025.

Ao executar a instância, é possível executá-la em uma sub-rede associada a um dos seguintes recursos:

- Uma zona de disponibilidade: esta opção é o padrão.
- Uma zona local: para executar uma instância em uma zona local, é necessário optar pela zona local e depois criar uma sub-rede na zona. Para obter mais informações, consulte Conceitos básicos de zonas locais.
- Uma zona do Wavelength: para executar uma instância em uma zona do Wavelength, é necessário optar pela zona de Wavelength e depois criar uma sub-rede na zona. Para obter informações sobre como iniciar uma instância em uma zona do Wavelength, consulte Get started with AWS Wavelength.
- Um Outpost: para executar uma instância em um Outpost, é necessário criar um Outpost. Para obter informações sobre como criar um Outpost, consulte Get started with AWS Outposts.

Após executar a instância, é possível 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. Pôde passar um breve tempo antes de você se conectar à instância. Observe que os tipos de instância bare metal podem levar mais tempo para serem executados.

Dependendo de como você planeja se conectar à sua instância, talvez você queira fazer determinadas configurações ao iniciar sua instância. Essas configurações podem incluir a especificação de regras de grupo de segurança de entrada para determinado tráfego ou a associação de uma função de perfil de instância. Para obter mais informações sobre os métodos de

conexão que você pode usar para se conectar e seus requisitos, consulte Conexão com a instância do EC2.

A instância recebe um nome DNS público que é possível 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.

Quando você tiver terminado com uma instância, para evitar incorrer em custos desnecessários, certifique-se de encerrá-la. Para obter mais informações, consulte Encerramento de instâncias do Amazon EC2.

Os métodos a seguir são algumas das formas pelas quais você pode executar uma instância.

Método	Ferramenta	Documentação
Use o assistente de inicializ ação de instâncias para especificar os parâmetros de execução.	Console do Amazon EC2	Executar uma instância do EC2 usando o assistente de inicialização de instâncias no console
Crie um modelo de execução e execute a instância nesse modelo.	Console do Amazon EC2	Executar instâncias do Ec2 usando um modelo de execução
Use uma instância existente como base.	Console do Amazon EC2	Executar uma instância do EC2 usando detalhes de uma instância existente
Use uma AMI adquirida no AWS Marketplace.	Console do Amazon EC2	Executar uma instância do Amazon EC2 em uma AMI do AWS Marketplace
Use uma AMI que você especificar.	AWS CLI	Como inicializar, listar e excluir instâncias do Amazon EC2 na AWS CLI
Use uma AMI que você especificar.	AWS Tools for Windows PowerShell	Iniciar uma instância do Amazon EC2 usando o Windows PowerShell

Método	Ferramenta	Documentação
Use o EC2 Fleet para provisionar capacidade em diferentes zonas de disponibilidade e tipos de instância do EC2, e em opções de compra de instância sob demanda, instância reservada e instância spot.	AWS CLI	Frota do EC2 e frota spot
Use um modelo do CloudFormation para especificar uma instância.	AWS CloudFormation	AWS::EC2::Instance no Manual do usuário do AWS CloudFormation
Use um SDK da AWS específico do idioma para executar uma instância.	AWS SDK	AWS SDK para .NET AWS SDK para C++ AWS SDK for Go AWS SDK for Java AWS SDK for JavaScript AWS SDK for PHP V3 AWS SDK for Python AWS SDK para Ruby V3

Tutoriais para executar instâncias do EC2

Há diversas formas de executar e configurar uma instância do Amazon EC2. O método e aconfiguração que você usa depende do seu caso de uso específico.

Os tutoriais a seguir podem ajudar a entender como executar instâncias do EC2. Se você é novo no Amazon EC2, recomendamos que comece com o primeiro tutorial. Os tutoriais começam

apresentando o básico e ajudam a desenvolver com base nele conforme vai apresentando mais opções de configuração.

Objetivo	Link para o tutorial
Executar a primeira instância do EC2 Saiba como executar rapidamente uma instância do Amazon EC2 usando as configurações padrão no assistente de inicialização de instâncias do Amazon EC2. Saiba também como analisar os campos de configuração da instância e encerrá-la. Duração: 10 minutos	Tutorial 1: Executar minha primeira instância do Amazon EC2
Executar uma instância de teste do Amazon EC2 e conectar-se a ela Saiba como executar uma instância do Amazon EC2 que pode ser usada para fins de teste. Essa instância não terá configuração avançada e não armazenará informações confidenciais. Você também aprenderá sobre as configurações essenciais da instância, como se conectar a ela e como interrompê-la. Duração: 30 minutos	Tutorial 2: Executar uma instância de teste do EC2 e conectar-se a ela

Está a procura de outros tutoriais?

- Tutorial: Install a LAMP server on AL2023
- Tutorial: Configure SSL/TLS on AL2023
- Tutorial: Host a WordPress blog on AL2023
- Tutorial: Concluir a configuração necessária para se conectar à sua instância usando o EC2 Instance Connect
- Tutorial: conectar uma instância do Amazon EC2 a um banco de dados do Amazon RDS

Tutorial 1: Executar minha primeira instância do Amazon EC2

Objetivo do tutorial	Saiba como executar rapidamente uma instância do Amazon EC2 usando as configurações padrão no assistente de inicialização de instâncias do Amazon EC2. Saiba também como analisar os campos de configuração da instância e encerrá-la.
Experiência do EC2	Iniciante
Duração	10 minutos
Custo	Elegível para o nível gratuito Ao criar sua Conta da AWS, comece a usar o Amazon EC2 gratuitamente com o Nível gratuito da AWS. Caso tenha criado sua Conta da AWS antes de 15 de julho de 2025, ela tenha menos de 12 meses e ainda não tenha excedido os benefícios do nível gratuito para o Amazon EC2, você não pagará nada para concluir este tutorial, pois ajudamos a selecionar opções com os benefícios do nível gratuito. Caso contrário, você incorrerá em taxas de uso padrão do Amazon EC2 desde o momento em que executar a instância (mesmo que ela permaneça ociosa) até encerrá-la. Caso tenha criado sua Conta da AWS em 15 de julho de 2025 ou após essa data, ela tenha menos de seis meses e não tenha usado todos os créditos, a conclusão deste tutorial não custará nada, pois ajudamos você a selecionar opções que estão dentro dos benefícios do nível gratuito.

	Para obter informações sobre como determinar se você é elegível para o nível gratuito, consulte the section called “Acompanhar seu uso do nível gratuito”.
Pré-requisitos	• Você deve ter uma conta da AWS, configurar um usuário com acesso de administrador e usar o usuário administrador para entrar no Console de gerenciamento da AWS. Não sabe como fazer isso? Experimente este tutorial: Como configurar seu ambiente da AWS • Você deve ter uma familiaridade geral com o console da AWS. Não sabe por onde começar? Experimente este guia de introdução: Conceitos básicos do Console de gerenciamento da AWS

Visão geral do tutorial

Este tutorial foi desenvolvido para iniciantes sem experiência prévia com o Amazon EC2. Orientaremos você nas etapas para criar (chamamos isso de execução) sua primeira instância do EC2 usando o console do EC2. Uma instância é essencialmente um servidor Web na Nuvem AWS. Depois de executar a instância, mostraremos como encontrá-la no console. Por fim, para ajudar a gerenciar os custos, mostraremos como excluir (chamamos isso de encerrar) a instância.

Este tutorial está dividido nas pequenas tarefas abaixo: Você deve concluir cada tarefa antes de passar para a próxima.

- Tarefa 1: executar a instância
- Tarefa 2: encontrar a instância
- Tarefa 3: visualizar a configuração da instância
- Etapa 4: encerrar a instância

Tarefa 1: executar a instância

Nessa tarefa, você seguirá o caminho mais rápido para executar a instância fazendo apenas o essencial. Usaremos o assistente de inicialização de instâncias do EC2, um formulário baseado na Web que fornece todos os campos para configurar e executar a instância. Ele simplifica o processo fornecendo valores padrão para os campos de configuração da instância.

Antes de começar

Verifique se você concluiu os pré-requisitos listados na tabela anterior, incluindo entrar no Console de gerenciamento da AWS com o usuário administrador.

Siga estas etapas para executar rapidamente a instância

1. Abrir o console do Amazon EC2:

   Acesse https://console.aws.amazon.com/ec2/.
2. Abrir o assistente de inicialização de instâncias do EC:

   No painel do EC2, escolha Executar instância.

   O formulário baseado na Web Executar uma instância é aberto. Este é o assistente de inicialização de instâncias do EC2.
3. Dar um nome para a instância:

   Em Nome e tags, para Nome, insira um nome descritivo como **`My first EC2 instance`**.

   Embora não seja necessário dar um nome à instância, isso ajuda a identificá-la posteriormente.
4. Continuar sem um par de chaves:

   Em Par de chaves (login), em Nome do par de chaves, escolha Continuar sem um par de chaves (não recomendado).

   Um par de chaves pode ser usado para um login seguro. No entanto, como não faremos login na instância neste tutorial, você não precisa de um par de chaves por enquanto.
5. Executar a instância:

   No painel Summary (Resumo) painel, escolha Launch instance (Iniciar instância).

   O Amazon EC2 executa a instância rapidamente usando as configurações padrão. Um banner de Êxito confirma a execução.

Parabéns! Você executou com êxito sua primeira instância do EC2.

Tarefa 2: encontrar a instância

Nessa tarefa, você localizará a instância que acabou de executar no console do EC2.

Siga estas etapas para encontrar a instância no console do EC2

1. Abrir a página Instâncias:

   Se você ainda estiver na página de êxito, escolha Instâncias na navegação estrutural na parte superior da tela. É possível precisar escolher as três elipses primeiro para acessá-la.

   Se você saiu da navegação, escolha Instâncias no painel de navegação.
2. Localizar a instância:

   Na coluna Nome, encontre a instância pelo nome que você deu a ela.

Tarefa 3: visualizar a configuração da instância

Nessa tarefa, você se familiarizará com a visualização dos detalhes de configuração da instância.

Siga estas etapas para visualizar a configuração da instância

1. Localizar o ID da instância:

   Na coluna ID da instância, anote o ID exclusivo da instância. Ele começa com i– seguido por 17 caracteres alfanuméricos, por exemplo, i-01aeed690c9fb5322.

   O ID da instância é atribuído automaticamente à instância quando ela é executada.
2. Abrir a página de detalhes da instância:

   Na coluna ID da instância, escolha o link do ID para abrir a página de detalhes da instância, na qual será possível revisar a configuração.
3. Explorar os detalhes da configuração da instância:

   Reserve alguns minutos para explorar os detalhes de configuração da instância. No próximo tutorial, vamos nos aprofundar na configuração. Por enquanto, use esse tempo para se familiarizar com a página de detalhes da instância.

   Dica: para encontrar rapidamente um campo, pressione Ctrl+F ou command+F no teclado.

a. Tipo de instância: você consegue encontrar o tipo de instância? Pode ser t3.micro, por exemplo.

b. Endereço IPv4 público: você consegue encontrar o endereço IPv4 público que foi alocado para a instância? Está em um formato semelhante ao seguinte exemplo: 34.242.148.128.

c. Proprietário da instância: você consegue identificar o proprietário dessa instância? É você. O número da Conta da AWS está listado no campo Proprietário.

d. Tags de instância: o nome que você deu à instância é, na verdade, uma tag. Você consegue encontrar as tags de instância? Escolha a guia Tags. A chave é Nome, e o valor é o nome que você forneceu.

e. Horário da execução: você consegue saber quando executou a instância? Escolha a guia Detalhes e localize o campo Hora da execução.

f. Estado da instância: você pode verificar o estado da instância? Deve ser Executando.

Reserve mais alguns minutos para explorar os outros campos de configuração da instância. Quando estiver pronto, vá para a próxima tarefa.

Etapa 4: encerrar a instância

> **Warning**
>
> O encerramento de uma instância é permanente e irreversível.
> Depois de encerrar uma instância, não será mais possível se conectar a ela e ela não poderá ser recuperada. Todos os volumes anexados do Amazon EBS configurados para serem excluídos no encerramento também serão excluídos permanentemente e não poderão ser recuperados. Todos os dados armazenados em volumes de armazenamento de instância serão perdidos permanentemente. Para obter mais informações, consulte Como funciona o encerramento de uma instância.
> Antes de encerrar uma instância, certifique-se de ter feito backup de todos os dados que você precise reter após o encerramento no armazenamento persistente.

Nesta tarefa, você excluirá a instância para preservar os benefícios do nível gratuito. No EC2, encerrar é o termo usado para excluir uma instância.

Siga estas etapas para encerrar a instância

1. Iniciar encerramento:

   Se você ainda estiver na página de detalhes da instância, escolha o menu Estado da instância (canto superior direito) e depois Encerrar (excluir) instância.

   Se você saiu da navegação, escolha Instâncias no painel de navegação. Em seguida, na página Instâncias, marque a caixa de seleção ao lado do nome da instância, escolha o menu Estado da instância (canto superior direito) e depois Encerrar (excluir) instância.

2. Confirmar o encerramento:

   Na janela Encerrar (excluir) instância que é exibida, escolha o botão Encerrar (excluir) para confirmar que você deseja encerrar a instância.

3. Monitorar o estado da instância:

   Na página Instâncias, verifique a coluna Estado da instância. O estado da instância muda para Desligando. Caso não veja todo o texto, tente ampliar a coluna.

   Depois que a instância é deligada, o Amazon EC2 exclui a instância e ela desaparece da página Instâncias.

Principais conclusões

Neste tutorial, foram abordados os seguintes conceitos-chave:

- Instância refere-se a um servidor Web do Amazon EC2 na Nuvem AWS.
- Executar refere-se à criação de uma instância do EC2.
- Encerrar refere-se à exclusão de uma instância do EC2.
- O assistente de inicialização de instâncias do EC2 contém valores padrão para a configuração da instância, permitindo uma execução rápida e fácil da instância.
- O ID da instância é um identificador exclusivo atribuído automaticamente à instância, enquanto o nome da instância é uma tag opcional que pode ser atribuída para facilitar a identificação.

Próximas etapas

Para criar confiança na execução e no encerramento de instâncias, considere repetir as etapas deste tutorial. Certifique-se de encerrar todas as instâncias que você executar para preservar os benefícios do nível gratuito.

Quando se sentir preparado com esses princípios básicos, vá para o próximo tutorial, que fornece uma análise mais aprofundada dos principais campos de configuração de instâncias.

Tutorial 2: Executar uma instância de teste do EC2 e conectar-se a ela

Objetivo do tutorial	Saiba como executar uma instância do Amazon EC2 que pode ser usada para fins de teste. Essa instância não terá configuração avançada e não armazenará informações confidenciais. Você também aprenderá sobre as configura ções essenciais da instância, como se conectar a ela e como interrompê-la.
Experiência do EC2	Iniciante
Duração	30 minutos
Custo	Elegível para o nível gratuito Ao criar sua Conta da AWS, comece a usar o Amazon EC2 gratuitamente com o Nível gratuito da AWS. Caso tenha criado sua Conta da AWS antes de 15 de julho de 2025, ela tenha menos de 12 meses e ainda não tenha excedido os benefícios do nível gratuito para o Amazon EC2, você não pagará nada para concluir este tutorial, pois ajudamos a selecionar opções com os benefícios do nível gratuito. Caso contrário, você incorrerá em taxas de uso padrão do Amazon EC2 desde o momento

	em que executar a instância (mesmo que ela permaneça ociosa) até encerrá-la. Caso tenha criado sua Conta da AWS em 15 de julho de 2025 ou após essa data, ela tenha menos de seis meses e não tenha usado todos os créditos, a conclusão deste tutorial não custará nada, pois ajudamos você a seleciona r opções que estão dentro dos benefícios do nível gratuito. Para obter informações sobre como determina r se você é elegível para o nível gratuito, consulte the section called “Acompanhar seu uso do nível gratuito”.
Pré-requisitos	Completa Tutorial 1: Executar minha primeira instância do Amazon EC2.

Visão geral do tutorial

Este tutorial foi desenvolvido para iniciantes que desejam executar uma instância do EC2 que eles possam usar para fins de teste.

Explicaremos os principais campos de configuração da instância e, em seguida, guiaremos você pelas etapas para executar uma instância de teste usando os valores padrão no console do EC2. Depois de executar a instância, mostraremos como fazer login (chamamos isso de conectar-se a) na instância. Também mostraremos como criar um par de chaves, que é necessário para se conectar à instância neste tutorial. Por fim, para ajudar a gerenciar os custos, mostraremos como interromper a instância para evitar cobranças de uso.

Você executará uma instância do Linux neste tutorial. Embora as etapas deste tutorial possam ser usadas para executar instâncias com outros sistemas operacionais, as instruções para se conectar a uma instância são específicas para instâncias do Linux.

Este tutorial está dividido nas pequenas tarefas abaixo: Você deve concluir cada tarefa antes de passar para a próxima.

- Tarefa 1: familiarizar-se com os principais componentes para executar uma instância

- Tarefa 2: revisar um diagrama técnico
- Tarefa 3: criar um par de chaves
- Tarefa 4: executar a instância de teste
- Tarefa 5: encontrar a instância
- Tarefa 6: visualizar a configuração da instância
- Tarefa 7: familiarizar-se com os principais componentes para se conectar a uma instância
- Tarefa 8: conectar-se à instância
- Tarefa 9: interromper a instância

Tarefa 1: familiarizar-se com os principais componentes para executar uma instância

Nesta tarefa, você explorará os principais componentes necessários para executar uma instância do EC2. São eles: AMI, tipo de instância, par de chaves, grupo de segurança, rede (VPC e sub-rede) e volume do Amazon EBS. Você também vai examinar um componente opcional, a tag Nome.

Para ajudar a visualizar esses componentes, pense em uma instância como uma casa para alugar. Assim como alugar uma casa oferece um lugar para morar sem a necessidade de possuir e manter a propriedade, as instâncias do EC2 fornecem poder de computação sem a necessidade de possuir e manter a infraestrutura subjacente.

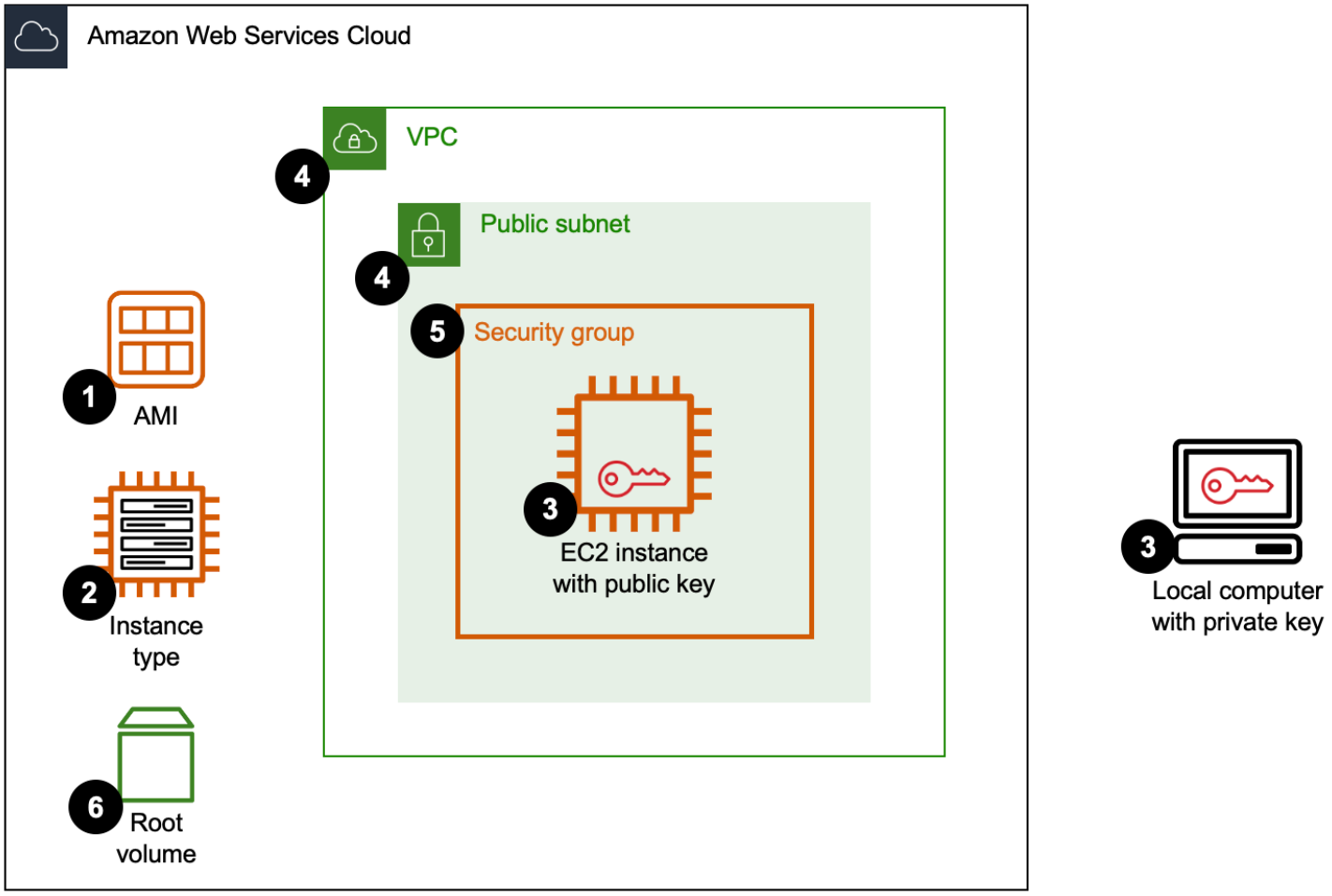
Ao decidir o tipo de instância a ser executada, você vai considerar os critérios de configuração da instância, da mesma forma como consideraria os critérios que gostaria de ter em uma casa. Embora essa analogia simplifique as coisas, ela oferece uma maneira útil de visualizar os componentes até que você esteja mais familiarizado com eles.

- AMI | Materiais e comodidades para a construção da casa: a imagem de máquina da Amazon (AMI) determina o sistema operacional e as aplicaçõess com os quais a instância começa. É como escolher os materiais de construção (como tijolo, aço ou madeira) e comodidades (como eletrodomésticos e móveis) de sua casa. Uma AMI básica é como uma casa sem mobília com aparelhos básicos, enquanto uma AMI personalizada com software pré-instalado é como uma casa totalmente mobiliada.
- Tipo de instância | Tamanho e potência da casa: o tipo de instância define o tamanho e os recursos da instância do EC2, assim como escolher o tamanho de uma casa, o número de cômodos e a capacidade de energia. Cada tipo de instância determina a quantidade de CPU, memória, armazenamento e capacidade de rede da instância. A AMI selecionada pode limitar os tipos de instância que você pode escolher.

- Par de chaves | Chave da porta da frente: um par de chaves é como a fechadura e a chave da porta da frente de sua casa. A chave pública age como o bloqueio da instância, enquanto a chave privada é a chave que você deve manter com segurança no computador local. Se outra pessoa tiver acesso à chave privada, ela poderá acessar a instância, da mesma forma que alguém com a chave da porta da frente poderá entrar em sua casa.
- Rede (VPC e sub-rede) | Limite da propriedade, áreas divididas e número da casa: a nuvem privada virtual (VPC) é como toda a propriedade em que sua casa está localizada, e a sub-rede é a área dividida ao redor da casa. Se você tiver várias casas (instâncias) em sua propriedade, talvez queira dividi-las em áreas distintas (sub-redes diferentes), dependendo da finalidade. Algumas casas permitem que os visitantes percorram livremente os jardins (sub-redes públicas com acesso à internet), enquanto outras têm jardins cercados para restringir a entrada (sub-redes privadas sem acesso à internet). Cada sub-rede contém um intervalo de endereços IP, assim como números de casas, que podem ser atribuídos a instâncias dentro da sub-rede.
- Grupo de segurança | O porteiro: o grupo de segurança age como um guardião, controlando quem tem permissão para visitar sua casa. Ele impõe um conjunto de regras que controla qual tráfego pode chegar à instância. Por exemplo, uma regra que permite o tráfego SSH de um endereço IP específico é como o porteiro deixar entrar somente uma pessoa específica para entregar mantimentos. Da mesma forma, permitir o tráfego HTTPS de qualquer lugar é como deixar o público entrar e dar uma olhada no exterior da sua casa.
- Volume do Amazon EBS | Unidades de armazenamento: os volumes do EBS são como unidades de armazenamento em que você pode armazenar seus pertences. Cada instância tem um volume raiz (em que a AMI é armazenada), e você pode adicionar mais volumes (armazenamento) a qualquer momento, conforme necessário.
- Tag Nome | O nome da casa: a tag Nome funciona como uma placa em uma casa que ajuda a identificar facilmente quem mora nela. Embora a tag Nome facilite a distinção entre instâncias, ela não é obrigatória ao iniciar uma instância.

Tarefa 2: revisar um diagrama técnico

Nesta tarefa, você se familiarizará com um diagrama técnico típico que usamos na documentação da AWS. O diagrama a seguir representa a configuração da instância de teste que você executará neste tutorial. Na tarefa anterior, apresentamos esses componentes usando a analogia de uma casa para alugar. Agora, vamos nos concentrar nos componentes do EC2. Os rótulos numerados correspondem às descrições a seguir.



1. AMI: é a imagem que você escolhe ao executar uma instância. É um modelo que contém o sistema operacional e o software para executar a instância. Por exemplo, se quiser executar uma instância do Linux, será possível escolher a AMI do Amazon Linux 2023. Ou, se quiser executar uma instância do Windows, será possível escolher a AMI básica do Microsoft Windows Server 2022. O catálogo de AMIs no console do Amazon EC2 contém milhares de imagens para você escolher.
2. Tipo de instância: é o hardware que determina a CPU, a memória, o armazenamento e a capacidade de rede do computador host usado para a instância. O Amazon EC2 oferece mais de 600 tipos de instância para escolher, cada um variando na configuração e no tamanho do hardware, o que permite que você escolha a mais adequada às necessidades da sua aplicação.
3. Par de chaves: é um conjunto de credenciais de segurança que você usa para comprovar a identidade ao conectar-se à instância. A chave pública está na instância e a chave privada está no computador local.

No EC2, conectar-se à instância refere-se a fazer login na instância no computador local. Embora existam outras formas de se conectar com segurança à instância, neste tutorial, usamos um par de chaves.

4. Rede: é composta por uma VPC e uma ou mais sub-redes. Uma VPC é uma rede virtual na Nuvem AWS. Cada cliente da AWS tem sua própria VPC dedicada à Conta da AWS. Você inicializará a instância em uma sub-rede na VPC. Uma sub-rede é um intervalo de endereços IP em uma VPC. A sub-rede padrão é uma sub-rede pública, o que significa que ela atribuirá um endereço IP público e fornecerá acesso à internet à instância de fora da rede da Amazon.
5. Grupo de segurança: atua como um firewall para controlar o tráfego para a instância. Um grupo de segurança contém regras que permitem que certos tipos de tráfego entrem na instância. Para se conectar por SSH do computador local à instância (usando o par de chaves), você precisará de uma regra que permita o tráfego SSH do computador local.
6. Volume do EBS: é um dispositivo de armazenamento que funciona como um disco rígido físico. A instância vem com um volume raiz, que é um volume especial do EBS que armazena a AMI com o sistema operacional e o software necessários para inicializar a instância. Como opção, é possível adicionar volumes de dados. No entanto, como a instância de teste não armazenará dados confidenciais, você não precisa de volumes adicionais de dados criptografados.

Parabéns! Você concluiu as tarefas conceituais deste tutorial. Nas tarefas a seguir, você usará o console do Amazon EC2 para criar os componentes que aprendeu.

Tarefa 3: criar um par de chaves

Nesta tarefa, você criará um par de chaves. Um par de chaves consiste em duas partes: uma chave pública, que você adicionará à instância, e uma chave privada correspondente, que você usará para se conectar com segurança à instância. Na próxima tarefa, você selecionará esse par de chaves ao executar a instância, o que adicionará automaticamente a chave pública à instância. É fundamental armazenar a chave privada com segurança no computador local, pois qualquer pessoa com acesso a ela pode se conectar à instância.

Se você preferir usar um par de chaves existente ao executar a instância de teste, fique à vontade para pular esta tarefa. Caso contrário, continue para criar um par de chaves.

Antes de começar

Verifique se você concluiu os pré-requisitos listados na tabela anterior, incluindo entrar no Console de gerenciamento da AWS com o usuário administrador.

Siga estas etapas para criar um par de chaves

1. Abrir o console do Amazon EC2:

   Acesse https://console.aws.amazon.com/ec2/.

2. Navegar até a página do console de pares de chaves:

   No painel de navegação, em Rede e segurança, selecione Pares de chaves.

   - Se você criou pares de chaves anteriormente, eles aparecerão na tabela.
   - Se não existirem pares de chaves, a tabela ficará vazia.

3. Criar um par de chaves:

   Escolha o botão Criar par de chaves (canto superior direito) para abrir o formulário Criar par de chaves baseado na Web e insira os detalhes do par de chaves, da seguinte forma:

   a. Dê um nome ao par de chaves: em Nome, insira um nome que ajudará a reconhecer o par de chaves, como **`test-instance-key-pair`**.

      O nome pode ter até 255 caracteres ASCII. Não pode incluir espaços no início nem no final.

   b. Escolha o tipo de par de chaves: para Tipo de par de chaves, escolha ED25519.

      As instâncias do Linux são compatíveis com os tipos de chave RSA e ED25519, enquanto as instâncias do Windows são compatíveis somente com a RSA. Como você executará uma instância do Linux neste tutorial, você pode usar uma chave ED25519.

   c. Escolha o formato do arquivo da chave privada: em Formato de arquivo de chave privada, escolha .pem.

      Este é o formato no qual o arquivo da chave privada será salvo.

4. Salvar a chave pública no Amazon EC2 e fazer download da chave privada:

   Escolha o botão Criar par de chaves (canto inferior direito).

   O Amazon EC2 salva a chave pública, enquanto o navegador faz download do arquivo da chave privada automaticamente para o computador local. O arquivo é nomeado de acordo com o nome que você especificou para o par de chaves, e a extensão é o formato do arquivo escolhido. Mova o arquivo de chave privada para um local seguro no computador.

> **Important**
>
> Esta é a única chance que você terá para salvar o arquivo de chave privada.

5. Definir as permissões na chave (para usuários do macOS e Linux):

   Caso planeje se conectar à instância usando SSH em um computador macOS ou Linux, você deve definir as permissões corretas para o arquivo de chave privada. Abra uma janela de terminal e execute o seguinte comando, substituindo *test-instance-key-pair* pelo nome do par de chaves:

   ```
   chmod 400 test-instance-key-pair.pem
   ```

   Esse comando garante que somente você possa ler o arquivo de chave privada, necessário para estabelecer uma conexão segura com a instância. Sem essas permissões, você não poderá se conectar usando esse par de chaves.

Parabéns! Você criou um par de chave com êxito.

Tarefa 4: executar a instância de teste

Nesta tarefa, você executará rapidamente uma instância de teste usando o assistente de inicialização de instâncias do EC2. Você definirá as configurações da instância principal para uma instância do Linux e usará os valores padrão para os outros campos.

Para ajudar no gerenciamento de custos, recomendamos escolher componentes elegíveis para o nível gratuito.

Siga estas etapas para executar uma instância de teste

1. Abrir o console do Amazon EC2:

   Acesse https://console.aws.amazon.com/ec2/.

2. Abrir o assistente de inicialização de instâncias do EC2:

   No painel do EC2, escolha Executar instância.

   O formulário baseado na Web Executar uma instância é aberto. Este é o assistente de inicialização de instâncias do EC2.

3. Dar um nome para a instância:

   Em Nome e tags, para Nome, insira um nome descritivo como **`Test instance`**.

   O nome da instância é uma tag em que a chave é Name (Nome) e o valor é o nome que você especificar.

   Dica: para instâncias de teste, uma tag de nome é suficiente. No entanto, para instâncias de produção, é uma prática recomendada estabelecer uma política de marcação para padronizar a marcação em todos os recursos.
4. Escolher o sistema operacional e o software, a imagem de máquina da Amazon (AMI):

   Em Imagens de aplicações e sistemas operacionais (imagem de máquina da Amazon), em Imagem de máquina da Amazon (AMI), a seleção padrão é AMI do Amazon Linux 2023. Essa AMI está marcada como Qualificada para nível gratuito. Neste tutorial, você inicializará uma instância do Linux, portanto, deixe a configuração padrão para permanecer no nível gratuito.
5. Escolher o hardware, o tipo de instância:

   Em Tipo de instância, para Tipo de instância, mantenha a seleção padrão durante este tutorial. O tipo de instância padrão pode ser usado no nível gratuito, e o hardware é adequado para a instância de teste.
6. Preparar-se para um login seguro com um par de chaves:

   Em Par de chaves (login), em Nome do par de chaves, escolha o par de chaves que você criou na tarefa anterior. Caso não veja o par de chaves na lista, escolha o ícone de atualização (à direita da lista).

   Quando a instância for executada, ela colocará a chave pública na instância. Para se conectar à instância após a execução, você usará a chave privada correspondente que baixou na tarefa anterior.
7. Definir as configurações de rede para permitir o acesso à internet:

   Em Configurações de rede, os campos Rede (a VPC) e Sub-rede são configurados por padrão. Mantenha as configurações padrão deste tutorial para ajudar a começar rapidamente. Caso não tenha modificado a sub-rede padrão, a instância terá acesso à internet.

   Dica: a sub-rede padrão é uma sub-rede pública, o que significa que ela atribuirá um endereço IP público e fornecerá acesso à internet à instância de fora da rede da Amazon. Para instâncias de teste, não há problema em usar as configurações de sub-rede padrão que fornecem acesso

à internet. No entanto, para instâncias de produção, é uma prática recomendada atribuir apenas um endereço IP público e usar uma sub-rede com acesso à internet quando for absolutamente necessário.

8. Configurar o firewall da instância (grupo de segurança):

   Em Configurações de rede, em Firewall (grupos de segurança), mantenha a caixa de seleção Permitir tráfego SSH de qualquer lugar (0.0.0.0) marcada. Isso criará um grupo de segurança para a instância de teste que permite tráfego SSH de qualquer endereço IP.

   Um grupo de segurança age como um firewall para controlar o tráfego para a instância. Para se conectar por SSH do computador local à instância, você precisará de uma regra que permita o tráfego SSH do computador local.

   Dica: o endereço IP do computador local poderá mudar com o tempo se o provedor de serviços de Internet usar a atribuição dinâmica de IPs. Presumimos que, ao usar uma instância para fins de teste, você não usará a instância para armazenar informações confidenciais e, portanto, as medidas de segurança podem ser menos restritivas. Para instâncias de teste, geralmente é aceitável permitir o tráfego de qualquer endereço IP (`0.0.0.0/0`) para que você possa sempre se conectar, mesmo que o endereço IP mude. No entanto, para instâncias de produção, especialmente aquelas com dados confidenciais, é uma prática recomendada permitir o tráfego somente de endereços IP conhecidos.

9. Configure o armazenamento da instância:

   Em Configurar armazenamento, os campos Volume raiz (criptografado) são configurados por padrão. Deixe as configurações como estão para se manter no nível gratuito.

   Como nossa instância de teste não armazena dados confidenciais, não precisamos de volumes adicionais de dados criptografados.

10. Analisar a configuração da instância:

    No painel Resumo à direita, você pode revisar as configurações de alto nível antes de executar a instância.

11. Executar a instância:

    Quando estiver pronto para executar a instância, no painel Resumo escolha Executar instância.

O Amazon EC2 executa rapidamente a instância usando as configurações que você especificou. Caso não tenha especificado uma configuração, o padrão será usado. Um banner de Êxito confirma a execução.

Parabéns! A instância de teste foi executada com êxito.

Tarefa 5: encontrar a instância

Nessa tarefa, você localizará a instância que acabou de executar no console do EC2.

Siga estas etapas para encontrar a instância no console do EC2

1. Abrir a página Instâncias:

   Caso ainda esteja na página de êxito, escolha o ID da instância no banner Êxito.

   Se você saiu da navegação, escolha Instâncias no painel de navegação.
2. Localizar a instância:

   Na coluna Nome, encontre a instância pelo nome que você deu a ela.

Tarefa 6: visualizar a configuração da instância

Nessa tarefa, você se familiarizará com a visualização dos detalhes de configuração da instância.

Siga estas etapas para visualizar a configuração da instância

1. Localizar a instância:

   Na coluna Nome, encontre a instância pelo nome que você deu a ela.
2. Abrir a página de detalhes da instância:

   Marque a caixa de seleção ao lado do nome da instância e, em seguida, escolha o menu Ações (canto superior direito) e Visualizar detalhes para abrir a página de detalhes da instância, onde você pode revisar a configuração.

   No tutorial anterior, você escolheu o link do ID da instância para abrir a página de detalhes da instância. Você vai descobrir que há mais de uma maneira de realizar uma tarefa no console do EC2.

3. Explorar os detalhes da configuração da instância:

   Reserve alguns minutos para explorar os detalhes de configuração da instância.

   Dica: para encontrar rapidamente um campo, pressione Ctrl+F ou command+F no teclado.

   a. AMI: você consegue encontrar a AMI que usou para executar a instância? É possível encontrar as informações no ID da AMI e no Nome da AMI na guia Detalhes.
   b. Tipo de instância: você consegue encontrar o tipo de instância? Pode ser t3.micro, por exemplo.
   c. Par de chaves: você consegue encontrar o par de chaves que selecionou ao executar a instância? É especificado para o par de chaves atribuído na execução. Observe que, se você alterar o par de chaves no futuro, o valor aqui não mudará.
   d. VPC: você consegue encontrar o ID da VPC? Você encontrará todas as configurações relacionadas à rede na guia Rede. O ID da VPC está em um formato semelhante ao seguinte exemplo: vpc-1a2b3c4d
   e. Sub-rede: você consegue encontrar o ID da sub-rede na qual você executou a instância? Está em um formato semelhante ao seguinte exemplo: sub-rede-1a2b3c4d
   f. Endereço IPv4 público: você consegue encontrar o endereço IPv4 público que foi alocado para a instância? Está em um formato semelhante ao seguinte exemplo: 34.242.148.128.
   g. Grupo de segurança: você consegue encontrar a regra de entrada que foi criada para permitir o tráfego SSH de qualquer lugar (0.0.0.0./0)? Você encontrará todas as configurações relacionadas à segurança na guia Segurança.
   h. Armazenamento: você consegue encontrar o volume que foi criado para esta instância? Você encontrará todas as configurações relacionadas ao armazenamento na guia Armazenamento.
   i. Tags de instância: o nome que você deu à instância é, na verdade, uma tag. Você consegue encontrar as tags de instância? Escolha a guia Tags. A chave é Nome, e o valor é o nome que você forneceu.
   j. Estado da instância: você pode verificar o estado da instância? Deve ser Executando.

Reserve mais alguns minutos para explorar os outros campos de configuração da instância. Quando estiver pronto, vá para a próxima tarefa.

Tarefa 7: familiarizar-se com os principais componentes para se conectar a uma instância

Nesta tarefa, você vai explorar os principais componentes necessários para se conectar a uma instância do EC2. Eles são: o protocolo de conexão, o DNS público, o grupo de segurança, o par de chaves e o nome de usuário da instância.

Para ajudar a visualizar esses componentes, pense em se conectar a uma instância como sendo o mesmo que ir para a sua casa:

- Protocolo de conexão | Seu meio de transporte: assim como escolher como chegar à sua casa, você escolhe o protocolo de conexão que o levará à sua instância. Neste tutorial, usaremos o SSH (Secure Shell), que cria um túnel seguro para conectar o computador à instância pela internet.
- DNS público | O endereço da casa: assim como sua casa tem um endereço exclusivo, sua instância do EC2 tem seu próprio nome de DNS público (por exemplo, `ec2-18-201-118-201.eu-west-1.compute.amazonaws.com`). Esse nome de DNS público permite que o SSH se conecte diretamente à instância.
- Grupo de segurança | O porteiro: imagine que sua casa tenha um porteiro que controla quem pode entrar ou sair. Da mesma forma, a instância do EC2 tem um grupo de segurança que age como um guardião, controlando quais tipos de tráfego de rede são permitidos dentro ou fora da instância. Somente o tráfego que você permite explicitamente (por exemplo, tráfego SSH do endereço IP do computador) é permitido.
- Chave privada | Sua chave da porta da frente: ao executar a instância, você especificou um par de chaves. A chave pública encontra-se na instância e a chave privada, no computador. A chave privada desempenha o mesmo papel que sua chave da porta da frente. Sem ela, você não pode acessar a instância.
- Nome de usuário da instância | O morador: ao chegar à sua casa, você precisa se identificar para provar que é o morador. Da mesma forma, ao se conectar a uma instância, você fornece um nome de usuário. Instâncias diferentes têm nomes de usuário padrão diferentes, dependendo do sistema operacional. Por exemplo, as instâncias do Amazon Linux usam `ec2-user` como nome de usuário padrão.

O comando de conexão

Para se conectar à instância do EC2, use o seguinte comando na janela de terminal:

```
ssh -i "test-instance-key-pair.pem" ec2-user@ec2-18-201-118-201.eu-
west-1.compute.amazonaws.com
```

Veja abaixo a discriminação do que o comando faz:

- `ssh`: este comando especifica o protocolo de conexão, iniciando uma conexão SSH (Secure Shell) com a instância.
- `-i "test-instance-key-pair.pem"`: o sinalizador `-i` indica o arquivo de chave privada necessário para autenticar a conexão. Esse arquivo de chave privada deve corresponder ao par de chaves que você especificou ao executar a instância. Se o arquivo de chave privada estiver salvo em uma determinada pasta, especifique o caminho completo para o arquivo.
- `ec2-user`: este é o nome de usuário para fazer login na instância. Para as instâncias do Amazon Linux, o nome do usuário padrão é `ec2-user`. Outras AMIs podem usar nomes de usuário padrão diferentes, como `ubuntu` para instâncias do Ubuntu.
- `@`: este símbolo separa o nome de usuário do endereço da instância.
- `ec2-18-201-118-201.eu-west-1.compute.amazonaws.com`: este é o endereço público da instância (o DNS público), que inclui o endereço IPv4 público e a Região da AWS. Ele identifica exclusivamente a instância.

O que acontece quando você executa o comando

Depois de executar o comando, o SSH estabelece um túnel seguro e se autentica com a chave privada. Se o grupo de segurança da instância permitir o tráfego, você terá acesso à instância do EC2. Agora você pode controlar a instância no computador como se estivesse sentado bem na frente dela. É possível executar comandos, instalar software e gerenciar arquivos, exatamente como faria em sua máquina local.

Tarefa 8: conectar-se à instância

Nesta tarefa, você se conectará à instância usando um cliente SSH no computador. Na tarefa anterior, apresentamos os componentes para se conectar a uma instância usando a analogia de ir até a sua casa. Agora, vamos nos concentrar na conexão com a instância real do EC2.

Há diversas formas de se conectar a uma instância. O método usado para se conectar depende do sistema operacional da instância. Como você executou uma instância do Linux, você usará um cliente SSH no computador local.

Primeiro, verifique se o computador tem um cliente SSH instalado

A maioria dos computadores vem com um cliente SSH pré-instalado. Para verificar, abra uma janela de terminal no computador e execute o seguinte comando:

```
ssh
```

Se o comando for reconhecido, você estará pronto para se conectar.

Se o comando não for reconhecido, você deve instalar um cliente SSH. As instruções para instalar um cliente SSH estão fora do escopo deste tutorial. Se precisar de ajuda, consulte Pré-requisitos de conexão via SSH neste guia do usuário, ou pesquise on-line para obter instruções sobre como instalar um cliente SSH no sistema operacional.

Siga estas etapas para se conectar à instância

1. Iniciar a conexão:

   Se você estiver na página de detalhes da instância no console do Amazon EC2, escolha o botão Conectar (canto superior direito).

   Se você saiu da navegação, escolha Instâncias no painel de navegação. Depois, na página Instâncias, marque a caixa de seleção ao lado do nome da instância e escolha o botão Conectar (canto superior direito).

   Isso abre a página Conectar à instância.
2. Escolher o método de conexão:

   Na página Conectar-se à instância, escolha a guia Cliente SSH.

   Reserve um momento para revisar o texto desta página, pois estas são as etapas que você seguirá a seguir.
3. Revisar o comando SSH:

   Em Exemplo, você verá um comando que é gerado e personalizado automaticamente com os detalhes da instância. O nome da chave privada é derivado do nome da chave pública especificada na execução.

   Veja abaixo como pode ser o comando:

   ```
   ssh -i "test-instance-key-pair.pem" ec2-user@ec2-18-201-118-201.eu-
   west-1.compute.amazonaws.com
   ```
4. Copiar o comando SSH:

Escolha o ícone de cópia ao lado do comando SSH de exemplo.

5. Abrir uma janela de terminal:

   Abra uma janela de terminal no computador local.

6. Colar e executar o comando SSH:

   Cole o comando SSH na janela do terminal. Se o arquivo de chave privada estiver salvo em uma determinada pasta, edite o comando para incluir o caminho completo para o arquivo.

   Pressione Enter no teclado.

   Você verá uma resposta semelhante ao seguinte:

```
The authenticity of host 'ec2-18-201-118-201.eu-west-1.compute.amazonaws.com
 (18-201-118-201)' can't be established.
ED25519 key fingerprint is SHA256:examplehxj9aOr1MogvKOoMNskVVIRBQBoq0example.This
 key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])?
```

7. Concluir a conexão:

   Insira **`yes`** e pressione Return no teclado.

   A verificação da impressão digital está fora do escopo deste tutorial. Para saber mais, consulte (Opcional) Obter a impressão digital da instância.

   Após uma conexão com êxito, o prompt do terminal muda para exibir o DNS público da instância.

Parabéns! Você se conectou à instância com êxito.

Tarefa 9: interromper a instância

Nesta tarefa, você interromperá a instância para preservar os benefícios do nível gratuito. Quando a instância é interrompida, ela deixa de gerar custos. Caso tenha criado sua Conta da AWS antes de 15 de julho de 2025 e se qualifique para o nível gratuito, você continuará gerando custos com o armazenamento do EBS.

Siga estas etapas para interromper a instância

1. Iniciar a interrupção:

   Se você ainda estiver na página Conectar à instância, escolha Instâncias na navegação estrutural. Se você saiu da navegação, escolha Instâncias no painel de navegação.

   Depois, na página Instâncias, marque a caixa de seleção ao lado do nome da sua instância, escolha o menu Estado da instância (canto superior direito) e depois Interromper instância. Quando solicitado, selecione Interromper.
2. Monitorar o estado da instância:

   Na página Instâncias, verifique a coluna Estado da instância. O estado da instância muda para Interrompendo e depois Interrompida. Caso não veja todo o texto, tente ampliar a coluna.

   Se você acha que o estado da instância mudou de Interrompendo para Interrompida, mas ainda não o vê, escolha o ícone de atualização (acima da tabela) para atualizar a tabela Instâncias.

Principais conclusões

Neste tutorial, foram abordados os seguintes conceitos-chave:

- Uma AMI refere-se a uma imagem de máquina da Amazon, que é um modelo que contém o sistema operacional e o software necessários para executar uma instância.
- O tipo de instância determina o hardware do computador host usado para a instância. Determina a capacidade de CPU, memória, armazenamento e rede da instância.
- O par de chaves refere-se ao conjunto de chaves públicas e privadas que você pode usar para se conectar com segurança à instância.
- Rede refere-se a uma VPC (uma nuvem privada virtual dedicada à conta na Nuvem AWS) e uma sub-rede (um intervalo de endereços IP dentro da VPC).
- O grupo de segurança refere-se a um conjunto de regras que controla qual tráfego pode chegar à instância.
- O volume do EBS refere-se ao armazenamento de dados da instância. Toda instância tem um volume raiz para armazenar a AMI e um ou mais volumes de dados opcionais.
- As tags são metadados que você pode atribuir opcionalmente à instância. O nome da instância é uma tag, cuja chave é Nome, e o valor é da sua escolha.
- Conexão refere-se ao acesso à instância pela internet.

- SSH refere-se ao protocolo de conexão Secure Shell que você pode usar para se conectar à instância.
- O DNS público é o endereço público exclusivo da instância.
- O nome de usuário da instância é determinado pelo sistema operacional da instância e é necessário para a conexão.
- A interrupção da instância interrompe as cobranças da instância, mas as cobranças do armazenamento do EBS continuam.

Próximas etapas

Para criar confiança na execução, conexão e interrupção de instâncias, considere repetir as etapas deste tutorial. Certifique-se de encerrar todas as instâncias que você executar para preservar os benefícios do nível gratuito.

Quando estiver familiarizado com esses conceitos básicos, será possível examinar tutoriais mais avançados. Para obter mais tutoriais, consulte Está a procura de outros tutoriais?

Caso tenha criado sua Conta da AWS antes de 15 de julho de 2025, considere assistir ao seguinte vídeo de seis minutos: How can I avoid charges on my account when using Nível gratuito da AWS services

Caso tenha criado sua Conta da AWS em 15 de julho de 2025 ou após essa data, considere revisar as seguintes informações: Explore AWS services with AWS Free Tier no Guia do usuário do AWS Billing

Referência para parâmetros de configuração de instâncias do Amazon EC2

O assistente de inicialização de instâncias e o modelo de execução no console do Amazon EC2 fornecem todos os parâmetros para configurar uma instância do Amazon EC2.

Exceto pelo par de chaves, o assistente de inicialização de instâncias fornece um valor padrão para cada parâmetro. Você pode aceitar qualquer um ou todos os padrões ou pode configurar uma instância com seus próprios valores. Ao criar um modelo de execução, os parâmetros são opcionais. Se você usar um modelo de execução para executar uma instância, os parâmetros especificados no modelo de execução substituirão os valores padrão no assistente de inicialização de instâncias. Qualquer parâmetro não especificado no modelo de execução usará como padrão o valor fornecido pelo assistente de inicialização de instâncias.

Os parâmetros são agrupados no assistente de inicialização de instâncias e no modelo de execução. As descrições a seguir são apresentadas de acordo com os agrupamentos de parâmetros no console.

Parâmetros para configuração de instâncias

- Nome e tags
- Imagens de aplicações e sistemas operacionais (imagem de máquina da Amazon)
- Tipo de instância
- Par de chaves (login)
- Configurações de rede
- Configurar armazenamento
- Detalhes avançados
- Resumo

Nome e tags

O nome da instância é uma tag em que a chave é Name (Nome) e o valor é o nome que você especificar. É possível marcar a instância, os volumes e as interfaces de rede. Para instâncias spot, é possível marcar apenas a solicitação de instância spot. Para obter mais informações sobre tags, consulte Marcar com tag os recursos do Amazon EC2.

A especificação de um nome de instância e de tags adicionais é opcional.

- Em Name (Nome), insira um nome descritivo para a instância. Se você não especificar um nome, a instância poderá ser identificada por seu ID, que é gerado automaticamente quando você inicia a instância.
- Para adicionar mais tags, selecione Add additional tag (Adicionar outra tag). Escolha Add tag (Adicionar tag), insira uma chave e um valor, e selecione o tipo de recurso a aplicar a tag. Escolha Add tag (Adicionar tag) para cada tag adicional a acrescentar.

Você só pode especificar o nome da instância ao executá-la. Você não pode nomear a instância ao criar um modelo de execução, mas pode adicionar tags aos recursos criados quando a instância é executada.

Imagens de aplicações e sistemas operacionais (imagem de máquina da Amazon)

Uma imagem de máquina da Amazon (AMI) contém as informações necessárias para criar uma instância. Por exemplo, uma AMI pode conter o software que é necessário para atuar como um servidor Web, como o Linux, o Apache e seu site.

É possível encontrar uma AMI adequada da seguinte forma: Caso contrário, escolha Cancel (Cancelar) (no canto superior direito) para retornar ao assistente de lançamento de instâncias sem escolher uma AMI.

Barra de pesquisa

Para pesquisar todas as AMIs disponíveis, insira uma palavra-chave na barra de pesquisa de AMI e pressione Enter. Escolha Select para selecionar uma AMI.

Recents (Recentes

As AMIs que você usou recentemente.

Escolha Recently launched (Iniciadas recentemente) ou Currently in use (Atualmente em uso) e, em Amazon Machine Image (AMI) (Imagem de máquina da Amazon, AMI), selecione uma AMI.

Minhas AMIs

As AMIs privadas que você possui, ou as AMI privadas que foram compartilhadas com você.

Escolha Owned by me (De minha propriedade) ou Shared with me (Compartilhado comigo) e, em Amazon Machine Image (AMI) (Imagem de máquina da Amazon, AMI), selecione uma AMI.

Início rápido

As AMIs são agrupadas por sistema operacional (SO) para ajudá-lo a começar rapidamente.

Em primeiro lugar, selecione o sistema operacional de que precisa e, em Amazon Machine Image (AMI) (Imagem de máquina da Amazon, AMI), selecione uma AMI. Para selecionar uma AMI que pode ser usada no nível gratuito da AWS, confira se ela está marcada como Elegível para o nível gratuito.

Browse more AMIs (Procurar mais AMIs

Selecione Browse more AMIs (Procurar mais AMIs) para navegar pelo catálogo completo de AMIs.

- Para pesquisar todas as AMIs disponíveis, insira uma palavra-chave na barra de pesquisa e pressione Enter.
- Para encontrar uma AMI usando um parâmetro do Systems Manager, escolha o botão de seta à direita da barra de pesquisa e escolha Search by Systems Manager parameter (Pesquisar por parâmetro do Systems Manager). Para obter mais informações, consulte Referência às AMIs usando parâmetros do Systems Manager.
- Para pesquisar por categoria, escolha Quickstart AMIs (AMIS de início rápido), My AMIs (Minhas AMIs), AWS Marketplace AMIs ou Community AMIs (AMIs da comunidade).

  O AWS Marketplace é uma loja online onde é possível comprar software executado na AWS, inclusive AMIs. Para obter mais informações sobre como executar uma instância pelo AWS Marketplace, consulte Executar uma instância do Amazon EC2 em uma AMI do AWS Marketplace. Em Community AMIs (AMIs da comunidade), é possível encontrar AMIs que membros da comunidade AWS disponibilizaram para outras pessoas usarem. AMIs da Amazon ou de um parceiro verificado estão marcadas como Provedor verificado.
- Para filtrar a lista de AMIs, marque uma ou mais caixas de seleção em Refine results (Refinar resultados) do lado esquerdo da tela. As opções de filtro são diferentes dependendo da categoria de pesquisa selecionada.
- Verifique Root device type (Tipo de dispositivo raiz) listado para cada AMI. Observe quais AMIs são tipo de que você precisa: ebs (baseadas no Amazon EBS) ou instance-store (baseadas no armazenamento de instâncias). Para obter mais informações, consulte Tipo do volume de raiz.
- Verifique o Virtualization type (Tipo de virtualização) listado para cada AMI. Observe quais AMIs são tipo de que você precisa: hvm ou paravirtual. Por exemplo, alguns tipos de instância exigem HVM. Para obter mais informações sobre os tipos de virtualização do Linux, consulte Tipos de virtualização.
- Verifique o modo de inicialização listado para cada AMI. Observe quais AMIs usam o modo de inicialização de que você precisa: legacy-bios, uefi ou uefi-preferred. Para obter mais informações, consulte Comportamento de execução da instância com modos de inicialização do Amazon EC2.
- Escolha a AMI que atenda às suas necessidades e marque Select (Selecionar).

Aviso ao alterar a AMI

Ao executar uma instância, se você modificar a configuração de qualquer volume ou grupo de segurança associado à AMI selecionada e depois escolher uma AMI diferente, será exibida uma

janela para avisar que algumas das configurações atuais serão alteradas ou removidas. Você pode revisar as alterações nos grupos de segurança e nos volumes. Além disso, é possível visualizar quais volumes serão adicionados e excluídos ou visualizar apenas os volumes que serão adicionados. Esse aviso não aparece ao criar um modelo de lançamento.

Tipo de instância

O tipo de instância define a configuração do hardware e o tamanho da instância. Os tipos de instâncias maiores têm mais CPU e memória. Para obter mais informações, consulte Tipos de instância do Amazon EC2.

- 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 do Amazon EC2.

  Nível gratuito: use tipos de instância com o rótulo Elegível para o nível gratuito sem custos no nível gratuito. Os tipos de instância específicos dependem de quando você criou a Conta da AWS.

  Caso tenha criado sua Conta da AWS antes de 15 de julho de 2025 e ela tenha menos de 12 meses, você pode usar o Amazon EC2 no nível gratuito selecionando o tipo de instância t2.micro ou o tipo de instância t3.micro em regiões onde o tipo t2.micro está indisponível. Lembre-se de que, quando você executa uma instância t3.micro, o padrão é o modo Ilimitado, o que pode gerar cobranças adicionais com base no uso da CPU.

  Se você tiver criado sua Conta da AWS a partir de 15 de julho de 2025, poderá usar os tipos de instância t3.micro, t3.small, t4g.micro, t4g.small, c7i-flex.large e m7i-flex.large durante 6 meses ou até seus créditos acabarem.

  Para obter mais informações, consulte Benefícios do nível gratuito antes e depois de 15 de julho de 2025.
- Compare instance types (Comparar tipos de instâncias): é possível comparar diferentes tipos de instâncias pelos seguintes atributos: número de vCPUs, arquitetura, quantidade de memória (GiB), quantidade de armazenamento (GB), tipo de armazenamento e performance de rede.
- Obter conselho: você pode obter orientações e sugestões de tipos de instância no localizador de tipo de instâncias do EC2. Para obter mais informações, consulte Obtenha recomendações do localizador de tipo de instância do EC2.
- (Apenas modelos de execução) Avançado: para especificar atributos de instância e deixar o Amazon EC2 identificar os tipos de instância com esses atributos, escolha Avançado e depois Especificar atributos de tipos de instância.

- Number of vCPUs (Número de vCPUs): insira o número mínimo e máximo de vCPUs para seus requisitos de computação. Para indicar que não há limites, insira um mínimo de **0** e deixe o máximo em branco.
- Amount of memory (MiB) (Quantidade de memória: Insira a quantidade mínima e máxima de memória, em MiB, para seus requisitos de computação. Para indicar que não há limites, insira um mínimo de **0** e deixe o máximo em branco.
- Expanda Optional instance type attributes (Atributos opcionais de tipo de instância) e selecione Add attribute (Adicionar atributo) para expressar seus requisitos de computação com mais detalhes. Para obter informações sobre cada atributo, consulte InstanceRequirementsRequest na Referência de API do Amazon EC2.
- Resulting instance types (Tipos de instância resultantes): é possível previsualizar os tipos de instância que correspondam aos atributos especificados. Para excluir tipos de instância, escolha Add attribute (Adicionar atributo) e, na lista Attribute (Atributo), escolha Excluded instance types (Tipos de instância excluídos). Na lista Attribute value (Valor do atributo), selecione os tipos de instância a serem excluídos.

Par de chaves (login)

Em Key pair name (Nome do par de chaves), escolha um par de chaves existente ou escolha Create new key pair (Criar um novo par de chaves) para criar um novo. Para obter mais informações, consulte Pares de chaves do Amazon EC2 e instâncias do Amazon EC2.

> **Important**
>
> Se você escolher a opção Proceed without key pair (Not recommended) (Prosseguir sem par de chaves, não recomendado), não conseguirá se conectar à instância a menos que escolha uma AMI configurada para permitir que os usuários façam login de outro modo.

Configurações de rede

As configurações de rede definem os endereços IP, grupos de segurança e interfaces de rede das suas instâncias. É possível usar as configurações de rede padrão ou configurá-las conforme necessário.

- (Apenas assistente de inicialização de instâncias) VPC: escolha uma VPC existente para a instância. A VPC padrão da região é selecionada por padrão. Como alternativa, é possível

escolher uma VPC que você tenha criado ou que tenha sido compartilhada com você. Para obter mais informações, consulte Nuvens privadas virtuais para as instâncias do EC2.

- Sub-rede: escolha uma sub-rede para sua instância ou escolha Criar nova sub-rede para criar uma nova sub-rede usando o console da Amazon VPC.
  - É possível criar uma sub-rede em qualquer Zona de disponibilidade, Zona local, Zona do Wavelength ou Zona do Outpost para a VPC selecionada.
  - Para executar a instância em uma sub-rede somente IPv6, a instância deverá ser baseada em Nitro.
- (Apenas para o Assistente de inicialização de instâncias) Atribuir IP público automaticamente: habilite ou desabilite a atribuição automática de endereços IPv4 públicos. Ao iniciar instâncias em uma sub-rede padrão, o valor padrão é Habilitar. Ao iniciar instâncias em uma sub-rede não padrão, o valor padrão é Desabilitar. Para obter mais informações, consulte Endereços IPv4 públicos.

  Não será possível habilitar essa opção para sub-redes não padrão se você adicionar uma interface de rede secundária. Para obter mais informações, consulte the section called “Atribuir um endereço IPv4 público na inicialização”.
- (Apenas para o Assistente de inicialização de instâncias) Atribuir IP IPv6 automaticamente: habilite ou desabilite a atribuição automática de endereços IPv6. Para obter mais informações, consulte Endereços IPv6.
- Firewall (grupos de segurança): escolha um grupo de segurança existente ou crie um novo. Garanta que seu grupo de segurança tenha regras que permitam o tráfego de e para suas instâncias. Todo o tráfego é ignorado.

  Se você criar um novo grupo de segurança, criaremos automaticamente uma regra de entrada que permitirá a conexão com a sua instância a partir de todos os endereços IP via SSH (instâncias Linux) ou RDP (instâncias Windows). Você pode remover ou modificar essa regra conforme necessário. É possível adicionar regras conforme necessário. Para obter mais informações, consulte Configurar regras de grupos de segurança.

  > **Warning**
  >
  > Regras que permitem que todos os endereços IP acessem sua instância por SSH ou RDP serão aceitáveis se você estiver iniciando brevemente uma instância de teste e a interromperá ou encerrará após um curto período de tempo. Porém, eles não são seguros

para ambientes de produção. Você deve autorizar apenas um intervalo específico de endereços IP para acessar suas instâncias.

Esse grupo de segurança é adicionado à interface de rede primária e a quaisquer interfaces de rede secundárias. Você pode selecionar grupos de segurança adicionais para suas interfaces de rede, mas não pode remover o grupo de segurança que você selecionou aqui.

- Configuração de rede avançada: é possível configurar a interface de rede primária conforme necessário. Para adicionar uma interface de rede secundária, escolha Add network interface (Adicionar interface de rede). O número de interfaces de rede que você pode adicionar depende do tipo de instância selecionado. Observação: essa seção estará disponível apenas se você escolher uma sub-rede.
  - Índice do dispositivo: o índice do dispositivo. A interface de rede primária deve ser atribuída ao índice 0.
  - Interface de rede: a interface de rede. Selecione Nova interface para deixar o Amazon EC2 criar uma interface nova, ou selecione uma interface de rede existente que esteja disponível. Se você selecionar uma interface de rede existente como a primária, não poderá habilitar Atribuir IP público automaticamente para sub-redes não padrão.
  - Descrição: uma descrição da nova interface de rede.
  - Subnet (Sub-rede): a sub-rede na qual criar a nova interface de rede. A instância é iniciada na mesma sub-rede que a interface de rede primária.

    Você deve escolher uma sub-rede de uma interface de rede secundária na mesma Zona de disponibilidade que a sub-rede da interface de rede primária. Se você selecionar uma sub-rede de outra VPC, o rótulo Multi-VPC aparecerá ao lado da interface de rede. Isso permite que você crie instâncias de múltiplas hospedagens em VPCs com diferentes configurações de rede e segurança.

    Para executar uma instância do EC2 em uma sub-rede somente IPv6, você deverá usar uma instância baseada em Nitro. Ao iniciar uma instância somente de IPv6, é possível que o DHCPv6 não forneça imediatamente a instância com o servidor de nomes DNS IPv6. Durante esse atraso inicial, a instância pode não resolver domínios públicos. Você pode alterar o arquivo de configuração e refazer a imagem da sua AMI para que o arquivo obtenha o endereço do servidor de nomes DNS IPv6 de forma imediata na inicialização.
  - Grupos de segurança: os grupos de segurança para associar à interface de rede. É necessário escolher um grupo de segurança da mesma VPC que a sub-rede da interface de rede.

- (Apenas modelos de execução) Autoatribuir IP público: especifique se a instância receberá 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.
- Primary IP (IP principal): um endereço IPv4 privado no intervalo de sua sub-rede. Deixe em branco para que o Amazon EC2 escolha um endereço IPv4 privado para você.
- IP secundário: um ou mais endereços IPv4 privados adicionais do intervalo de endereços da sua sub-rede. Escolha Atribuir manualmente e insira um endereço IPv4. Escolha Adicionar IP para adicionar outro endereço IPv4. Ou então, escolha Atribuir automaticamente e insira um valor para indicar o número de endereços IPv4 que o Amazon EC2 escolherá para você.
- (Somente IPv6) IPs IPv6: endereços IPv6 do intervalo da sub-rede. Escolha Atribuir manualmente e insira um endereço IPv6. Escolha Adicionar IP para adicionar outro endereço IPv6. Ou escolha Atribuir automaticamente e insira um valor para indicar o número de endereços IPv6 que o Amazon EC2 escolherá para você.
- IPv4 Prefixes (Prefixos IPv4): os prefixos IPv4 para a interface de rede. Escolha Atribuir manualmente e insira um prefixo IPv4. Ou então, escolha Atribuir automaticamente e insira um valor para indicar o número de endereços IPv4 que o Amazon EC2 escolherá para você.
- IPv6 Prefixes (Prefixos IPv6): os prefixos IPv6 para a interface de rede. Escolha Atribuir manualmente e insira um prefixo IPv6. Ou então, escolha Atribuir automaticamente e insira um valor para indicar o número de endereços IPv6 que o Amazon EC2 escolherá para você.
- (Pilha dupla e somente IPv6) Atribuir IP IPv6 primário: se você selecionar uma sub-rede de pilha dupla ou somente IPv6, atribua um endereço IPv6 primário. Isso ajuda a evitar interrupções no tráfego para a instância ou para a interface de rede. Habilite essa opção se você confiar que o endereço IPv6 não será alterado. Você não poderá remover o endereço IPv6 primário posteriormente. Quando você habilita um endereço GUA IPv6 para ser um IPv6 primário, o primeiro GUA IPv6 se torna o endereço IPv6 primário até a instância ser terminada ou a interface de rede ser desconectada. Se você tiver vários endereços IPv6 associados a uma interface de rede e deixar o Amazon EC2 atribuir um endereço IPv6 primário, o primeiro endereço GUA IPv6 associado à interface de rede será o endereço IPv6 primário.
- Excluir ao terminar: indica se a interface de rede será excluída quando a instância for excluída.
- Tipo de interface: o tipo de interface de rede:
  - ENA: uma interface de rede de alta performance projetada para lidar com throughput elevado e altas taxas de pacotes por segundo para protocolos TCP/IP ao mesmo tempo que minimiza

o uso da CPU. Este é o valor padrão. Para obter mais informações sobre ENA, consulte Elastic Fabric Adapter.

- EFA com ENA: uma interface de rede que oferece suporte a dispositivos ENA e EFA para transporte tradicional baseado em TCP/IP junto com transporte baseado em SRD. Para obter mais informações sobre EFA, consulte Elastic Fabric Adapter.
- Somente EFA: uma interface de rede de alta performance projetada para lidar com comunicação entre nós com throughput elevado e baixa latência para transporte baseado em SRD enquanto ignora a pilha do sistema operacional. As interfaces de rede somente EFA não oferecem suporte a endereços IP. Para obter mais informações sobre EFA, consulte Elastic Fabric Adapter.

- Elastic Fabric Adapter: indica se a interface de rede é um Elastic Fabric Adapter. Para obter mais informações, consulte Elastic Fabric Adapter para workloads de IA/ML e HPC no Amazon EC2.
- Índice da placa de rede: O índice da placa de rede. A interface de rede primária deve ser atribuída ao índice 0 da placa de rede. Alguns tipos de instância oferecem suporte a várias placas de rede.
- ENA Express: o ENA Express tem a tecnologia Scalable Reliable Datagram (SRD) da AWS. A tecnologia SRD usa um mecanismo de pulverização de pacotes para distribuir carga e evitar congestionamento de rede. A ativação do ENA Express permite que as instâncias compatíveis se comuniquem usando SRD além do tráfego TCP normal, quando possível. O assistente de inicialização de instâncias ou o modelo de execução não inclui a configuração do ENA Express para a instância, a menos que você selecione Habilitar ou Desabilitar na lista.
- UDP do ENA Express: se habilitou o ENA Express, tem a opção de usá-lo para tráfego UDP. O assistente de inicialização de instâncias ou o modelo de execução não inclui a configuração do ENA Express para a instância, a menos que você selecione Habilitar ou Desabilitar.

Configurar armazenamento

A AMI que você selecionou inclui um ou mais volumes de armazenamento, incluindo o volume raiz. É possível especificar volumes adicionais a serem anexados à instância.

(Apenas assistente de inicialização de instâncias) Você pode usar a visualização Simples ou Avançada. Com a visualização Simple (Simples), especifique o tamanho e o tipo de volume. Para especificar todos os parâmetros de volume, use a exibição Advanced (Avançada), no canto superior direito do cartão.

Usando a exibição Advanced (Avançada), é possível configurar cada volume da seguinte forma:

- Storage type (Tipo de armazenamento): selecione os volumes do Amazon EBS ou de armazenamento de instância para associar à instância. Os tipos de volume disponíveis na lista dependem do tipo de instância escolhido. Para obter mais informações, consulte Armazenamento em bloco temporário do armazenamento de instância para instâncias do EC2 e Volumes do Amazon EBS.
- Device Name (Nome do dispositivo): selecione na lista de nomes de dispositivo disponíveis para o volume.
- Snapshot: selecione o snapshot ao qual o volume será restaurado. Também é possível pesquisar snapshots públicos e compartilhados que estão disponíveis, inserindo texto no campo Snapshot.
- Size (GiB) (Tamanho): para volumes do EBS, especifique um tamanho de armazenamento.
- Volume Type (Tipo de volume): para volumes do EBS, selecione um tipo de volume. Para obter mais informações, consulte Tipos de volumes do Amazon EBS no Guia do usuário do Amazon EC2.
- IOPS: se tiver selecionado o tipo de volume io1, io2 ou gp3, você poderá inserir o número de operações de E/S por segundo (IOPS) que o volume puder aceitar. Necessário para os volumes io1, io2 e gp3. Não compatível com os volumes gp2, st1, sc1 ou volumes padrão. Se omitir esse parâmetro para o modelo de execução, você deverá especificar um valor para ele ao executar uma instância com base no modelo de execução.
- Delete on termination (Excluir ao término): em volumes do Amazon EBS, escolha Yes (Sim), para excluir o volume quando a instância associada for terminada, ou escolha No (Não) para manter o volume. Para obter mais informações, consulte Preservação de dados quando uma instância for encerrada.
- Encrypted: (Criptografado): se o tipo de instância oferecer suporte à criptografia do EBS, será possível escolher Yes (Sim) para habilitar criptografia para o volume. Se você tiver habilitado a criptografia por padrão nessa região, a criptografia estará habilitada para você. Para obter mais informações, consulte Criptografia do Amazon EBS no Guia do usuário do Amazon EBS.
- KMS Key (Chave do KMS): se você selecionou Yes (Sim) para Encrypted (Criptografado), deve selecionar uma chave gerenciada pelo cliente a ser usada para criptografar o volume. Se tiver habilitado a criptografia por padrão nessa região, a chave gerenciada pelo cliente padrão será selecionada para você. É possível selecionar uma chave diferente ou especificar o ARN de qualquer chave gerenciada pelo cliente que você tenha criado.
- Throughput: se você selecionou o tipo de volume gp3, poderá inserir, em MiB/s, o throughput que o volume pode aceitar.

- Taxa de inicialização do volume: se você selecionou um snapshot, terá a opção de especificar, em MiB/s, a taxa de inicialização do volume em que os blocos do snapshot devem ser baixados do Amazon S3 para o volume. Para obter mais informações, consulte Use an Amazon EBS Provisioned Rate for Volume Initialization. Para usar a taxa de inicialização padrão ou a restauração rápida de snapshots (se habilitada para o snapshot selecionado), não especifique nenhuma taxa.
- Sistemas de arquivos: monte um sistema de arquivos Amazon EFS ou Amazon FSx na instância. Para obter mais informações sobre a montagem de um sistema de arquivos do Amazon EFS, consulte Usar o Amazon EFS com instâncias do Linux do Amazon EC2. Para obter mais informações sobre a montagem de um sistema de arquivos do Amazon FSx, consulte Usar o Amazon FSx com instâncias do Amazon EC2

Detalhes avançados

Em Advanced details (Detalhes avançados), expanda a seção para visualizar os campos e especifique quaisquer parâmetros adicionais para a instância.

- (Apenas assistente de inicialização de instâncias) Diretório de ingresso em domínio: selecione o diretório Directory Service (domínio) ao qual sua instância será associada após a execução. Se selecionar um domínio, é necessário selecionar a função do IAM com as permissões necessárias. Para obter mais informações sobre união de domínios, consulte Seamlessly join an Amazon EC2 Linux instance to your AWS Managed Microsoft AD directory (instâncias do Linux) e Seamlessly join an Amazon EC2 Windows instance to your AWS Managed Microsoft AD directory (instâncias do Windows).
- Perfil de instância do IAM: um perfil de instância do IAM a ser associado à instância. Este é um contêiner para um perfil do IAM. Para obter mais informações, consulte Funções do IAM para Amazon EC2.
- Hostname type (Tipo de nome do host): selecione se o nome do host do sistema operacional convidado da instância incluirá o nome do recurso ou o nome do IP. Para obter mais informações, consulte Nomes de host e domínios de instâncias do EC2.
- Hostname DNS (Nome de host DNS): determina se as consultas de DNS para o nome do recurso ou nome do IP (de acordo com o que você selecionou em Hostname type [Tipo de nome do host]) serão respondidas com o endereço IPv4 (registro A), o endereço IPv6 (registro AAAA) ou ambos. Para obter mais informações, consulte Nomes de host e domínios de instâncias do EC2.
- Recuperação automática da instância: quando habilitada, recuperará a instância se as verificações de status do sistema apresentarem falha. Essa configuração é habilitada por padrão na

inicialização para os tipos de instância compatíveis. Para obter mais informações, consulte Configurar a recuperação automática simplificada em uma instância do Amazon EC2.

- Shutdown behavior (Comportamento de desativação): selecione se a instância deve parar ou encerrar quando desativada. Para obter mais informações, consulte Alterar comportamento de desligamento iniciado da instância.
- Stop - Hibernate behavior (Comportamento Parar - Hibernar): para habilitar a hibernação, escolha Enable (Habilitar). Esse campo só está disponível se a instância atender aos pré-requisitos de hibernação. Para obter mais informações, consulte Hibernar sua instância do Amazon EC2.
- Termination protection (Proteção contra término): para evitar o término acidental, escolha Enable (Habilitar). Para obter mais informações, consulte Alterar proteção contra encerramento de instância.
- Stop protection (Proteção contra interrupção): para prevenir interrupções acidentais, escolha Enable (Habilitar). Para obter mais informações, consulte Habilitar a proteção contra interrupção.
- Detailed CloudWatch monitoring (Monitoramento detalhado do CloudWatch): escolha Enable (Habilitar) para ativar o monitoramento detalhado da instância usando o Amazon CloudWatch. Aplicam-se cobranças adicionais. Para obter mais informações, consulte Monitorar instâncias usando o CloudWatch.
- Credit specification (Especificação de crédito): escolha Unlimited (Ilimitado) para permitir que as aplicações ultrapassem linha de base pelo tempo que for necessário. Esse campo só é válido para instâncias T. Podem se aplicar cobranças adicionais. Para obter mais informações, consulte Instâncias expansíveis.
- Grupo de posicionamento: especifique um grupo de posicionamento no qual iniciar a instância. É possível selecionar um grupo de posicionamento existente ou crie um novo. Nem todos os tipos de instância oferecem suporte ao lançamento de uma instância em um grupo de posicionamento. Para obter mais informações, consulte Grupos de posicionamento para as instâncias do Amazon EC2.
- 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 oferecer suporte a esse recurso, escolha Enable (Habilitar) para habilitá-lo. Aplicam-se cobranças adicionais. Para obter mais informações, consulte the section called “Otimização de EBS”.
- Configuração de largura de banda da instância: é possível aumentar a largura de banda da rede ou a largura de banda do EBS. Somente para tipos de instância com suporte. Para obter mais informações, consulte Configuração de ponderação de largura de banda de instâncias do EC2.

- Opção de compra: escolha Solicitar instâncias spot para solicitar instâncias spot ao preço de spot, cujo limite máximo é o preço sob demanda, e escolha Personalizar opções de instância spot para alterar as configurações padrão de instância spot. É possível definir o preço máximo (não recomendado) e alterar o tipo de solicitação, a duração da solicitação e o comportamento de interrupção. Se você não solicitar uma instância spot, o Amazon EC2 iniciará uma instância sob demanda por padrão. Para obter mais informações, consulte Gerenciar as instâncias spot.
- Capacity Reservation (Reserva de capacidade): especifique se deseja iniciar a instância em qualquer reserva de capacidade aberta (Open, Aberta), uma reserva de capacidade específica (Target by ID, Alvo por ID) ou um grupo de reservas de capacidade (Target by group, Alvo por grupo). Para especificar que nenhuma reserva de capacidade deva ser usada, escolha None (Nenhuma). Para obter mais informações, consulte Iniciar instâncias em uma Reserva de capacidade existente.
- Tenancy (Locação): escolha se a instância deve ser executada em hardware compartilhado (Shared (Compartilhado)), isolado, hardware dedicado (Dedicated (Dedicado)) ou em um Host dedicado (Dedicated host (Host dedicado)). Se você optar por executar a instância em um Host dedicado, poderá especificar se deseja executar a instância em um grupo de recursos de host ou poderá segmentar um Host dedicado específico. Podem se aplicar cobranças adicionais. Para obter mais informações, consulte Instâncias dedicadas do Amazon EC2 e Hosts dedicados do Amazon EC2.
- RAM disk ID (ID do disco de RAM): (válido somente para AMIs paravirtuais, PV) selecione um disco de RAM para a instância. Se você tiver selecionado um kernel, pode precisar selecionar um disco de RAM específico com os drivers para oferecer suporte a ele.
- Kernel ID (ID do kernel): (válido somente para AMIs paravirtuais, PV) selecione um kernel para a instância.
- Nitro Enclave: permite criar ambientes isolados de execução, chamados de enclaves, com base em instâncias do Amazon EC2. Selecione Enable (Habilitar) para habilitar a instância para o AWS Nitro Enclaves. Para obter mais informações, consulte O que é o AWS Nitro Enclaves? no Guia do usuário do AWS Nitro Enclaves.
- Configurações de licenças: é possível executar instâncias com relação à configuração de licença especificada para rastrear o uso da licença. Para obter mais informações, consulte Crie uma configuração de licença no Guia do usuário do AWS License Manager.
- Especificar opções de CPU: no assistente de inicialização de instâncias, esse campo só estará visível se o tipo de instância selecionado for compatível com a especificação de opções de CPU. Escolha 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 Opções de CPU para instâncias do Amazon EC2.

- Metadados acessíveis: é possível habilitar ou desabilitar o acesso ao Serviço de metadados de instância (IMDS). Para obter mais informações, consulte Configurar opções de metadados da instância para novas instâncias.
- Endpoint IPv6 de metadados: você pode habilitar a instância para usar o endereço IPv6 do IMDS `[fd00:ec2::254]` para recuperar os metadados da instância. Essa opção só estará disponível se você for executar instâncias baseadas em Nitro em uma sub-rede compatível com IPv6 (pilha dupla ou IPv6 apenas). Para obter mais informações sobre a recuperação de metadados de instâncias, consulte Acessar metadados de instância para uma instância do EC2.
- Versão de metadados: se você habilitar o acesso ao IMDS, poderá optar por exigir o uso do Serviço de metadados de instância versão 2 ao solicitar metadados da instância. Para obter mais informações, consulte Configurar opções de metadados da instância para novas instâncias.
- Limite de salto de resposta de metadados: se você habilitar o IMDS, poderá definir o número permitido de saltos de rede para o token de metadados. Para obter mais informações, consulte Configurar opções de metadados da instância para novas instâncias.
- Permitir tags em metadados: se você selecionar Enable (Habilitar), a instância permitirá o acesso a todas as tags dos metadados. Se nenhum valor for especificado, por padrão, o acesso às etiquetas dos metadados da instância não será permitido. Para obter mais informações, consulte Habilitar o acesso a tags em metadados da instância.
- User data (Dados do usuário): é possível especificar dados do usuário para configurar uma instância durante a execução ou para executar um script de configuração. Para obter mais informações sobre os dados do usuário para as instâncias do Linux, consulte Executar comandos ao iniciar uma instância do EC2 com entrada de dados do usuário. Para obter mais informações sobre os dados do usuário para as instâncias do Windows, consulte Como o Amazon EC2 lida com os dados dos usuários para instâncias do Windows.

Resumo

Use o painel Summary (Resumo) para especificar o número de instâncias a serem iniciadas, revisar a configuração da instância e iniciar as instâncias.

- Number of instances (Número de instâncias): Digite o número de instâncias para executar. Todas as instâncias serão iniciadas com a mesma configuração.

> **Tip**
>
> Para garantir uma execução mais rápida da instância, divida solicitações grandes em lotes menores. Por exemplo, crie cinco solicitações de execução separadas para 100 instâncias cada em vez de uma solicitação de execução para 500 instâncias.

- (Opcional) Se você especificar mais de uma instância, para ajudar a manter o número correto de instâncias para lidar com a demanda da aplicação, escolha Consider EC2 Auto Scaling (Considerar o EC2 Auto Scaling) para criar um modelo de execução e um grupo do Auto Scaling. O Auto Scaling escala o número de instâncias no grupo de acordo com suas especificações. Para mais informações, consulte o Guia do usuário do Amazon EC2 Auto Scaling.

> **Note**
>
> Se o Amazon EC2 Auto Scaling marcar uma instância que está em um grupo do Auto Scaling como não íntegro, a instância será programada automaticamente para substituição quando for encerrada e outra for iniciada, e você perderá os dados na instância original. Uma instância será marcada como não íntegra se você parar ou reinicializar a instância, ou se outro evento marcar a instância como não íntegra. Para obter mais informações, consulte Health checks for instances in an Auto Scaling group no Amazon EC2 Auto Scaling User Guide.

- Revise os detalhes da instância e faça as alterações necessárias. É possível navegar diretamente para uma seção escolhendo seu link no painel Summary (Resumo).
- Quando estiver pronto para iniciar a instância, escolha Launch instance (Iniciar instância).

Executar uma instância do EC2 usando o assistente de inicialização de instâncias no console

Você pode executar uma instância do Amazon EC2 usando o assistente de inicialização de instâncias no console do Amazon EC2. O assistente fornece valores padrão para os parâmetros de execução, que você pode aceitar ou modificar para atender às suas necessidades. O único parâmetro que não está especificado é o par de chaves. Caso aceite os valores padrão, você poderá executar uma instância rapidamente selecionando apenas um par de chaves.

> **Important**
>
> Você incorrerá em cobranças para a instância enquanto ela estiver no estado `running`, mesmo que permaneça ociosa. No entanto, se você se qualificar para o nível gratuito, talvez não incorra em cobranças. Para obter mais informações, consulte Acompanhamento do uso do nível gratuito para o Amazon EC2.

Para obter uma descrição de cada parâmetro no assistente de inicialização de instâncias, consulte Referência para parâmetros de configuração de instâncias do Amazon EC2.

Tópicos

- Iniciar rapidamente uma instância
- Iniciar uma instância usando parâmetros definidos

Iniciar rapidamente uma instância

Para configurar uma instância rapidamente para fins de teste, siga estas etapas. Você selecionará o sistema operacional e o par de chaves e aceitará os valores padrão. Exceto pelo par de chaves, o assistente de lançamento de instâncias fornece valores padrão para todos os parâmetros. É possível aceitar qualquer um ou todos os padrões ou configurar uma instância especificando seus próprios valores para cada parâmetro.

Para obter uma descrição de cada parâmetro no assistente de inicialização de instâncias, consulte Referência para parâmetros de configuração de instâncias do Amazon EC2.

Para executar rapidamente uma instância usando o assistente de inicialização de instâncias

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 AWS é exibida [por exemplo, Leste dos EUA (Ohio)]. Se necessário, selecione outra região na qual a instância será executada.
3. No painel do console do Amazon EC2, selecione Launch instance (Executar instância).
4. (Opcional) Em Name and tags (Nome e tags), para Name (Nome), insira um nome descritivo para a instância.

5. Em Application and OS Images (Amazon Machine Image), (Imagens de aplicações e sistemas operacionais (imagem de máquina da Amazon), escolha Quick Start (Início rápido) e depois escolha o sistema operacional da sua instância.
6. Em Key pair (login) (Par de chaves, login), Key pair name (Nome do par de chaves), escolha um par de chaves existente ou crie um novo.
7. No painel Summary (Resumo) painel, escolha Launch instance (Iniciar instância).

Iniciar uma instância usando parâmetros definidos

Caso esteja executando uma instância que usará na produção, você precisará configurar a instância de acordo com seus requisitos. Para obter uma descrição de cada parâmetro no assistente de inicialização de instâncias, consulte Referência para parâmetros de configuração de instâncias do Amazon EC2.

Para executar uma instância definindo todos os parâmetros de execução usando o assistente de inicialização de instâncias

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 AWS é exibida [por exemplo, Leste dos EUA (Ohio)]. Se necessário, selecione outra região na qual a instância será executada.
3. No painel do console do Amazon EC2, selecione Launch instance (Executar instância).
4. (Opcional) Em Nome e tags, para Nome, insira um nome descritivo para a instância para que você possa rastreá-la facilmente.

   O nome da instância é uma tag em que a chave é Name (Nome) e o valor é o nome que você especificar.
5. Em Imagens de SO e aplicações (Amazon Machine Image), escolha o sistema operacional (SO) da instância e depois uma AMI.

   Uma AMI é um modelo que contém o sistema operacional e o software necessários para executar a instância.
6. Em Instance type (Tipo de instância), escolha um tipo de instância.

   O tipo de instância determina a configuração do hardware (CPU, memória, armazenamento e capacidade de rede) e o tamanho do computador host usado para a instância.

Se você não tiver certeza de qual tipo de instância escolher, você pode fazer o seguinte:

- Escolha Comparar tipos de instâncias para comparar diferentes tipos de instâncias pelos seguintes atributos: número de vCPUs, arquitetura, quantidade de memória (GiB), quantidade de armazenamento (GB), tipo de armazenamento e performance de rede.
- Escolha Obter conselho para obter orientações e sugestões de tipos de instância no localizador de tipo de instâncias do EC2. Para obter mais informações, consulte Obtenha recomendações do localizador de tipo de instância do EC2.

> **Note**
>
> Dependendo de quando sua conta foi criada, talvez você possa usar tipos de instância gratuitamente no nível gratuito. Esses tipos de instância recebem o rótulo elegíveis para o nível gratuito.
> Caso tenha criado sua Conta da AWS antes de 15 de julho de 2025 e ela tenha menos de 12 meses, você pode usar o Amazon EC2 no nível gratuito selecionando o tipo de instância t2.micro ou o tipo de instância t3.micro em regiões onde o tipo t2.micro está indisponível. Lembre-se de que, quando você executa uma instância t3.micro, o padrão é o modo Ilimitado, o que pode gerar cobranças adicionais com base no uso da CPU.
> Caso tenha criado sua Conta da AWS em 15 de julho de 2025 ou após essa data, você poderá usar os tipos de instância t3.micro, t3.small, t4g.micro, t4g.small, c7i-flex.large e m7i-flex.large por seis meses ou até que seus créditos acabem.
> Para obter mais informações, consulte Benefícios do nível gratuito antes e depois de 15 de julho de 2025.

7. Em Key pair (login) (Par de chaves, login), Key pair name (Nome do par de chaves), escolha um par de chaves existente ou crie um novo. Se você não precisar de um par de chaves para se conectar à instância, você pode escolher Continuar sem um par de chaves (não recomendado).
8. Em Configurações de rede, você pode manter os padrões caso esteja executando uma instância de teste. Se você estiver executando uma instância de produção, é uma prática recomendada controlar o tráfego de entrada e saída da instância usando as configurações de rede e os grupos de segurança definidos por você.
9. Em Configurar armazenamento, você pode manter os padrões ou especificar armazenamento adicional. A AMI que você selecionou inclui um ou mais volumes de armazenamento, incluindo o volume raiz. É possível especificar volumes adicionais a serem anexados à instância.

É possível usar a exibição Simple (Simples) ou Advanced (Avançada). Com a visualização Simple (Simples), especifique o tamanho e o tipo de volume. Para especificar todos os parâmetros de volume, use a exibição Advanced (Avançada), no canto superior direito do cartão.

10. Em Detalhes avançados, expanda a seção para visualizar os campos e especifique quaisquer parâmetros adicionais para a instância.
11. No painel Resumo, você pode fazer o seguinte:

    a. Especifique o número de instâncias a serem executadas.

    b. Analise a configuração da instância e navegue diretamente para uma seção escolhendo o link.

    c. Quando estiver pronto para iniciar a instância, escolha Launch instance (Iniciar instância).

    Se a instância não executar ou o estado passar imediatamente para `terminated`, em vez de `running`, consulte Solucionar problemas de inicialização de instâncias do Amazon EC2.
12. (Opcional) É possível criar um alerta de faturamento para a instância. Na tela de confirmação, em Next Steps (Próximos passos), escolha Create billing alerts (Criar alarmes de faturamento) e siga as instruções. Também poderão ser criados alertas de faturamento após iniciar a instância. Para obter mais informações, consulte Criar um alarme de faturamento para monitorar suas cobranças estimadas da AWS no Guia do usuário do Amazon CloudWatch.

Executar instâncias do Ec2 usando um modelo de execução

Um modelo de execução do Amazon EC2 armazena parâmetros de execução de instâncias para que não seja necessário especificá-los sempre que executar uma instância.

Vários serviços de execução de instâncias podem, opcionalmente, usar modelos de execução ao executar instâncias, enquanto para outros serviços, como o EC2 Fleet, as instâncias não podem ser executadas a menos que um modelo de execução seja usado. Este tópico descreve como usar um modelo de inicialização ao iniciar uma instância usando o assistente de inicialização de instâncias do EC2, o Amazon EC2 Auto Scaling, a Frota do EC2 e a frota spot.

Para obter mas informações sobre modelos de execução, incluindo como criar um modelo de execução, consulte Armazenar os parâmetros de execução de instâncias nos modelos de execução do Amazon EC2.

Tópicos

- Executar uma instância do Amazon EC2 usando um modelo de execução
- Executar instâncias em um grupo do Amazon EC2 Auto Scaling usando um modelo de execução
- Executar um EC2 Fleet usando um modelo de execução
- Executar uma frota spot usando um modelo de execução

Executar uma instância do Amazon EC2 usando um modelo de execução

Você pode usar os parâmetros incluídos em um modelo de execução para executar uma instância do Amazon EC2. Depois de selecionar o modelo de execução, mas antes de executar a instância, você pode modificar os parâmetros de execução.

As instâncias executadas por meio de um modelo de execução recebem automaticamente duas tags com as chaves `aws:ec2launchtemplate:id` e `aws:ec2launchtemplate:version`. Você não pode remover ou editar essas tags.

Console

Para executar uma instância usando um modelo de execução

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Use uma das seguintes opções para selecionar o modelo de execução:
   - No painel do console do Amazon EC2, escolha a seta para baixo ao lado de Executar instância e depois Executar instância no modelo. Em Modelo de origem, selecione um modelo de execução.
   - No painel de navegação, escolha Modelos de execução, selecione o modelo de execução e, então, escolha Ações, Executar instância no modelo.
3. Em Source template version (Versão do modelo de origem), selecione a versão do modelo de execução a ser usado.
4. (Opcional) Você pode modificar os valores de qualquer um dos parâmetros de execução. Se você não modificar um valor, o sistema usará o valor definido pelo modelo de execução. Se nenhum valor foi especificado no modelo de execução, o valor padrão do parâmetro será usado.
5. No painel Resumo, em Número de instâncias, especifique o número de instâncias a serem executadas.
6. Escolha Iniciar instância.

Se a instância não executar ou o estado passar imediatamente para `terminated`, em vez de `running`, consulte Solucionar problemas de inicialização de instâncias do Amazon EC2.

AWS CLI

Para executar uma instância em um modelo de execução

- Use o comando run-instances e especifique o parâmetro `--launch-template`. Se desejar, especifique a versão de modelo de execução a ser usada. Se você não especificar a versão, a versão padrão será usada.

```
aws ec2 run-instances \
    --launch-template LaunchTemplateId=lt-0abcd290751193123,Version=1
```

- Para substituir um parâmetro de modelo de execução, especifique o parâmetro no comando run-instances. O exemplo a seguir substitui o tipo de instância especificado no modelo de execução (se houver algum).

```
aws ec2 run-instances \
    --launch-template LaunchTemplateId=lt-0abcd290751193123 \
    --instance-type t2.small
```

- Se você especificar um parâmetro aninhado que faça parte de uma estrutura complexa, a instância será executada por meio da estrutura complexa conforme especificado no modelo de execução, além de quaisquer parâmetros aninhados adicionais que você especificar.

  No exemplo a seguir, a instância é executada com a tag *Owner*=*TeamA*, bem como com quaisquer outras tags especificadas no modelo de execução. Se o modelo de execução tiver uma tag com uma chave *Owner*, o valor será substituído por *TeamA*.

```
aws ec2 run-instances \
    --launch-template LaunchTemplateId=lt-0abcd290751193123 \
    --tag-specifications "ResourceType=instance,Tags=[{Key=Owner,Value=TeamA}]"
```

  No exemplo a seguir, a instância é executada com um volume com o nome de dispositivo */dev/xvdb*, bem como com quaisquer outros mapeamentos de dispositivos de blocos especificados no modelo de execução. Se o modelo de execução tiver um volume existente definido para */dev/xvdb*, seus valores serão substituídos pelos valores especificados.

```
aws ec2 run-instances \
    --launch-template LaunchTemplateId=lt-0abcd290751193123 \
    --block-device-mappings "DeviceName=/dev/
xvdb,Ebs={VolumeSize=20,VolumeType=gp2}"
```

Se a instância não executar ou o estado passar imediatamente para `terminated`, em vez de `running`, consulte Solucionar problemas de inicialização de instâncias do Amazon EC2.

PowerShell

Como executar uma instância a partir de um modelo de execução usando a AWS Tools for PowerShell

- Use o comando New-EC2Instance e especifique o parâmetro `-LaunchTemplate`. Se desejar, especifique a versão de modelo de execução a ser usada. Se você não especificar a versão, a versão padrão será usada.

```
Import-Module AWS.Tools.EC2
New-EC2Instance `
    -LaunchTemplate (
        New-Object -TypeName Amazon.EC2.Model.LaunchTemplateSpecification -
Property @{
            LaunchTemplateId = 'lt-0abcd290751193123';
            Version          = '4'
    }
)
```

- Para substituir um parâmetro de modelo de execução, especifique o parâmetro no comando New-EC2Instance. O exemplo a seguir substitui o tipo de instância especificado no modelo de execução (se houver algum).

```
Import-Module AWS.Tools.EC2
New-EC2Instance `
    -InstanceType t4g.small `
    -LaunchTemplate (
        New-Object -TypeName Amazon.EC2.Model.LaunchTemplateSpecification -
Property @{
            LaunchTemplateId = 'lt-0abcd290751193123';
            Version          = '4'
    }
```

```
)
```

- 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*.

```
Import-Module AWS.Tools.EC2
New-EC2Instance `
    -InstanceType t4g.small  `
    -LaunchTemplate (
        New-Object -TypeName Amazon.EC2.Model.LaunchTemplateSpecification -
Property @{
            LaunchTemplateId = 'lt-0abcd290751193123';
            Version          = '4'
        }
) `
    -TagSpecification (
        New-Object -TypeName Amazon.EC2.Model.TagSpecification -Property @{
            ResourceType = 'instance';
            Tags         = @(
                @{key = "Owner"; value = "TeamA" },
                @{key = "Department"; value = "Operations" }
            )
        }
)
```

  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.

```
Import-Module AWS.Tools.EC2
New-EC2Instance `
    -InstanceType t4g.small  `
    -LaunchTemplate (
        New-Object -TypeName Amazon.EC2.Model.LaunchTemplateSpecification -
Property @{
```

```
            LaunchTemplateId = 'lt-0abcd290751193123';
            Version          = '4'
    }
) `
    -BlockDeviceMapping  (
        New-Object -TypeName Amazon.EC2.Model.BlockDeviceMapping -Property @{
            DeviceName = '/dev/xvdb';
            EBS        = (
                New-Object -TypeName Amazon.EC2.Model.EbsBlockDevice -Property @{
                    VolumeSize = 25;
                    VolumeType = 'gp3'
                }
            )
        }
)
```

Se a instância não executar ou o estado passar imediatamente para `terminated`, em vez de `running`, consulte Solucionar problemas de inicialização de instâncias do Amazon EC2.

Executar instâncias em um grupo do Amazon EC2 Auto Scaling usando um modelo de execução

É possível 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.

Antes de criar um grupo do Auto Scaling usando um modelo de execução, você deve primeiro criar um modelo de execução que inclua os parâmetros necessários para executar uma instância em um grupo do Auto Scaling. Alguns parâmetros são obrigatórios, como o ID da AMI, e alguns parâmetros não estão disponíveis para uso com um grupo do Auto Scaling. O console fornece orientações para ajudar você a criar um modelo que pode ser usado com o Amazon EC2 Auto Scaling.

Para criar um grupo do Auto Scaling usando um modelo de execução usando o console

- Para verificar as instruções, consulte Create an Auto Scaling group using a launch template no Guia do usuário do Amazon EC2 Auto Scaling.

Criar ou atualizar um grupo do Auto Scaling com um modelo de execução usando a AWS CLI

- Use o comando create-auto-scaling-group ou update-auto-scaling-group e especifique o parâmetro `--launch-template`.

Para obter mais informações, consulte os seguintes tópicos no Guia do usuário do Amazon EC2 Auto Scaling:

- Create a launch template for an Auto Scaling group
- Create a launch template using advanced settings
- Examples for creating and managing launch templates with the AWS Command Line Interface (AWS CLI): fornece exemplos que mostram como criar modelos de execução com várias combinações de parâmetros.
- Create Auto Scaling groups using launch templates
- Update an Auto Scaling group

Executar um EC2 Fleet usando um modelo de execução

Um modelo de execução é um requisito ao criar uma solicitação do EC2 Fleet. Quando o Amazon EC2 atender à solicitação do Frota do EC2, ele usará os parâmetros de execução definidos no modelo de execução associado. É possível substituir alguns parâmetros especificados no modelo de execução. Para obter mais informações, consulte Criar uma Frota do EC2..

Para criar uma EC2 Fleet com um modelo de execução usando a AWS CLI

- Use o comando create-fleet. Use o parâmetro `--launch-template-configs` para especificar o modelo de execução e quaisquer substituições para o modelo de execução.

Executar uma frota spot usando um modelo de execução

Um modelo de execução é opcional ao criar uma solicitação de frota spot. Se você não usar um modelo de execução, você poderá especificar manualmente os parâmetros de execução. Caso use um modelo de execução, quando o Amazon EC2 atender à solicitação da frota spot, ele usará os parâmetros de execução definidos no modelo de execução associado. É possível substituir alguns parâmetros especificados no modelo de execução. Para obter mais informações, consulte Criar uma Frota spot.

Para criar uma solicitação de frota spot usando um modelo de execução

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Solicitações spot.
3. Selecione Request Spot Instances (Solicitar instâncias spot).
4. Em Launch parameters (Parâmetros de inicialização), escolha Use a launch template (Usar um modelo de inicialização).
5. Em Launch template (Modelo de inicialização), escolha um modelo de inicialização e, no campo à direita, escolha a versão do modelo de inicialização.
6. Configure a frota Spot selecionando diferentes opções nessa tela. Para saber mais sobre essas opções, consulte Criar uma solicitação de frota spot usando parâmetros definidos.
7. Quando você estiver pronto para criar uma frota spot, escolha Launch (Iniciar).

Para criar uma solicitação de frota spot usando um modelo de execução

- Use o comando request-spot-fleet. Use o parâmetro `LaunchTemplateConfigs` para especificar o modelo de execução e quaisquer substituições para o modelo de execução.

Executar uma instância do EC2 usando detalhes de uma instância existente

O console do Amazon EC2 fornece uma opção Launch more like this (Iniciar mais como esta) que permite usar uma instância atual como base para iniciar outras instâncias. Essa opção preenche automaticamente o assistente de execução de instâncias do Amazon EC2 com determinados detalhes de configuração da instância selecionada.

Considerações

- Não clonamos suas instâncias; replicamos apenas alguns detalhes da configuração. Para criar uma cópia da sua instância, primeiro crie uma AMI a partir dela e então execute mais instâncias a partir da AMI. Crie um modelo de execução para garantir que você execute as instâncias usando os mesmos detalhes de execução.
- A instância atual deve estar no estado `running`.

Detalhes copiados

Os detalhes de configuração a seguir são copiados da instância selecionada para o assistente de execução de instâncias:

- 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.
- 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
- Grupos de segurança associados à instância
- [Instâncias do Windows] Informações de associações. Se a instância selecionada estiver associada a um arquivo de configuração, o mesmo arquivo será automaticamente associado à nova instância. Se o arquivo de configuração incluir uma configuração de domínio ingressado, a nova instância será ingressada no mesmo domínio. Para obter mais informações sobre como ingressar em um domínio, consulte Seamlessly join a Windows EC2 instance to your AWS Managed Microsoft AD Active Directory no Guia de administração do AWS Directory Service.

Detalhes não copiados

Os seguintes detalhes da configuração não são copiados da instância selecionada. Em vez disso, o assistente aplica as configurações ou o comportamento padrão:

- Número de interfaces de rede: o padrão é uma interface de rede, que é a interface de rede primária (eth0).
- Armazenamento: a configuração de armazenamento padrão é determinada pela AMI e pelo tipo de instância.

Para executar mais instâncias como 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 uma instância e escolha Ações, Imagens e modelos e Executar mais como esta.
4. O assistente de execução de instância é aberto. É possível fazer as alterações necessárias na configuração da instância selecionando diferentes opções nesta tela.

   Quando estiver pronto para iniciar sua instância, escolha Launch instance (Iniciar instância).
5. Se a instância não executar ou o estado passar imediatamente para `terminated`, em vez de `running`, consulte Solucionar problemas de inicialização de instâncias do Amazon EC2.

Executar uma instância do Amazon EC2 em uma AMI do AWS Marketplace

É possível assinar uma AMI do AWS Marketplace e executar uma instância nela usando o console do Amazon EC2 ou uma ferramenta de linha de comandos. Para obter mais informações sobre as AMIs do AWS Marketplace, consulte AMIs pagas no AWS Marketplace para instâncias do Amazon EC2.

Para cancelar a assinatura da AMI após a execução, você deve primeiro encerrar todas as instâncias que foram executadas na AMI. Para obter mais informações, consulte Gerenciar suas assinaturas do AWS Marketplace.

Para executar uma instância em uma AMI do AWS Marketplace usando o console do Amazon EC2

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel do console do Amazon EC2, selecione Launch instance (Executar instância).
3. (Opcional) Em Name and tags (Nome e tags), para Name (Nome), insira um nome descritivo para a instância.
4. Em Imagens de aplicações e sistemas operacionais (imagem de máquina da Amazon) escolha Procurar mais AMIs e escolha a guia AMIs do AWS Marketplace. Encontre uma AMI adequada

navegando pelas categorias ou utilizando a funcionalidade de pesquisa. Para escolher seu produto, escolha Select (Selecionar).

5. O sistema apresentará uma janela com uma visão geral do produto selecionado. É possível visualizar as informações de preços, bem como quaisquer outras informações que o fornecedor fornecer. Quando estiver pronto, selecione Assinar e executar. Isso iniciará sua assinatura imediatamente. Enquanto a assinatura estiver a caminho, será possível configurar a instância seguindo as etapas deste procedimento. Se houver algum problema com os detalhes do cartão de crédito, você será convidado a atualizar os detalhes da conta.

   > **Note**
   >
   > Não será cobrado o uso do produto até você executar uma instância com a AMI. Ao selecionar um tipo de instância, anote o preço de cada tipo de instância compatível. Também poderão ser aplicados impostos adicionais ao produto.

6. Em Instance type (Tipo de instância), escolha um tipo de instância para a instância. O tipo de instância define a configuração do hardware e o tamanho da instância a ser iniciada.
7. Em Key pair (login) (Par de chaves, login), Key pair name (Nome do par de chaves), escolha um par de chaves existente ou crie um novo.
8. Em Configurações de rede, para Firewall (grupos de segurança), anote o novo grupo de segurança que foi criado conforme as especificações do fornecedor do produto. O grupo de segurança poderá conter regras que permitam 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.
9. É possível usar outros campos na tela para configurar sua instância e adicionar armazenamento e etiquetas. Para obter informações sobre as diferentes opções que é possível configurar, consulte Referência para parâmetros de configuração de instâncias do Amazon EC2.
10. No painel Summary (Resumo), em Software Image (AMI) (Imagem de software [AMI]), verifique os detalhes da AMI em que a instância será iniciada. Verifique também os outros detalhes de configuração que você especificou. Quando estiver pronto para iniciar a instância, escolha Launch instance (Iniciar instância).
11. Dependendo do produto no qual você se inscreveu, a instância poderá levar alguns minutos ou mais para 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 (Visualizar instâncias) para acessar a página Instances (Instâncias).

> **Note**
>
> Você pagará o preço da assinatura, desde que sua instância esteja no estado `running`, mesmo se estiver ociosa. Se sua instância for interrompida, você ainda poderá ser cobrado pelo armazenamento.

12. Quando o status da sua instância estiver no estado `running`, será possível se conectar a ela. Para isso, selecione sua instância na lista, escolha Connect (Conectar) e escolha uma opção de conexão. Para obter mais informações sobre como se conectar à sua instância, consulte Conexão com a instância do EC2.

> **Important**
>
> Verifique com atenção as instruções de uso do fornecedor, pois talvez seja necessário usar um nome de usuário específico para se conectar à instância. Para obter informações sobre como acessar os detalhes de assinatura, consulte Gerenciar suas assinaturas do AWS Marketplace.

13. Se a instância não executar ou o estado passar imediatamente para `terminated`, em vez de `running`, consulte Solucionar problemas de inicialização de instâncias do Amazon EC2.

Para executar uma instância em uma AMI do AWS Marketplace usando as ferramentas de linha de comandos

Para executar instâncias de produtos do AWS Marketplace usando a ferramenta de linha de comandos, primeiro certifique-se de que você esteja inscrito no produto. É possível então executar uma instância com o ID da AMI do produto usando os seguintes métodos:

Método	Documentação
AWS CLI	Use o comando run-instances ou consulte o tópico a seguir para obter mais informações: Executar sua instância no Guia do usuário da AWS Command Line Interface.

Método	Documentação
AWS Tools for Windows PowerShell	Use o comando New-EC2Instance ou consulte o tópico a seguir para obter mais informações: Executar uma instância do Amazon EC2 usando o Windows PowerShell
API de consulta	Use a solicitação RunInstances.

Conexão com a instância do EC2

Uma instância do Amazon EC2 é um servidor virtual na Nuvem AWS. Para fazer login na instância, você deve estabelecer uma conexão com a instância. A forma como você se conecta à instância depende do sistema operacional da instância e do sistema operacional do computador que você usa para se conectar à instância. A tabela a seguir detalha os requisitos para cada método de conexão.

Opção de conexão	Sistema operacional da instância	Regra do tráfego de entrada	permissões do IAM	Função do perfil de instância	Software na instância	Software no sistema de conexão	Par de chaves
Cliente SSH	Linux	Sim	Não	Não	Não	Sim	Sim
EC2 Instance Connect	Linux	Sim	Sim	Não	Sim [1]	Não	Não
PuTTY	Linux	Sim	Não	Não	Não	Sim	Sim
Cliente RDP	Windows	Sim	Não	Não	Não	Sim	Sim [2]
Fleet Manager	Windows	Não	Sim	Sim	Sim [1]	Não	Sim

Opção de conexão	Sistema operacional da instância	Regra do tráfego de entrada	permissões do IAM	Função do perfil de instância	Software na instância	Software no sistema de conexão	Par de chaves
Session Manager	Linux, Windows	Não	Sim	Sim	Sim [1]	Não	Não
Endpoint do EC2 Instance Connect	Linux, Windows	Sim	Sim	Não	Não	Não	Não [3]

[1] O software necessário é pré-instalado somente em determinadas AMIs. É possível instalar manualmente o software necessário, conforme necessário, nos sistemas operacionais compatíveis.

[2] O par de chaves só é necessário se você estiver usando a senha gerada aleatoriamente para a conta de usuário local do administrador.

[3] Um par de chaves será necessário se você usar o método de conexão SSH.

Para ter mais informações, consulte a documentação da opção de conexão que deseja usar.

Opções de conexão

- Conectar-se à instância do Linux usando um cliente SSH
- Conectar-se à instância do Linux usando PuTTY
- Conexão com a instância do Windows usando um cliente RDP
- Conectar a uma instância do Windows usando o Fleet Manager
- Conectar-se usando o Gerenciador de sessões
- Conecte-se usando um IP público e o EC2 Instance Connect
- Conecte-se usando um IP privado e uma instância do EC2 Conecte-se ao endpoint

Pré-requisitos gerais de conexão

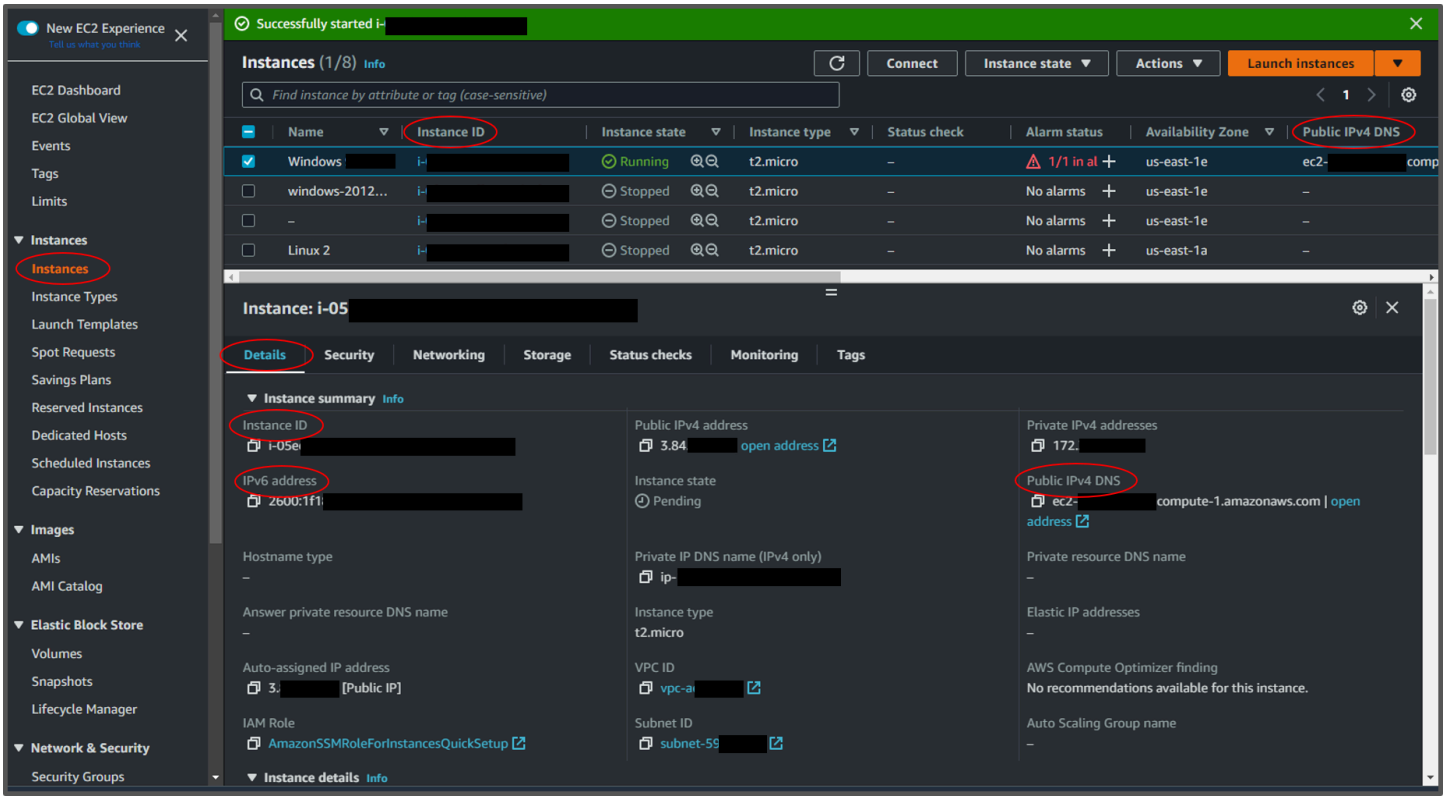
Veja a seguir os pré-requisitos gerais para se conectar a uma instância. Observe que poderá haver pré-requisitos adicionais específicos para a opção de conexão que você escolher.

Pré-requisitos gerais

- Verifique se a instância passou nas verificações de status. Pode demorar alguns minutos para que a instância fique pronta para aceitar solicitações de conexão. Para obter mais informações, consulte Visualizar verificações de status.
- Obter os detalhes necessários da instância.
- Localizar a chave privada e definir permissões.
- (Opcional) Obter a impressão digital da instância.

Obter os detalhes necessários da instância

Para preparar-se para a conexão com uma instância, obtenha as informações a seguir no console do Amazon EC2 ou use a linha de comando.



- Obtenha o nome do DNS público da instância.

É possível obter o DNS público da instância usando o console do Amazon EC2. Verifique a coluna DNS IPv4 público do painel Instâncias. Se essa coluna estiver oculta, escolha o ícone de configurações ( ) no canto superior direito da tela e selecione DNS público (IPv4). Você também pode encontrar o DNS público na seção de informações da instância do painel Instâncias. Quando você seleciona a instância no painel Instâncias do console do Amazon EC2, as informações sobre essa instância aparecem na metade inferior da página. Na guia Detalhes, procure DNS IPv4 público.

Se preferir, é possível usar o comando describe-instances (AWS CLI) ou Get-EC2Instance (AWS Tools for Windows PowerShell).

Se nenhum DNS IPv4 público for exibido, verifique se o estado da instância é em execução e se você não iniciou a instância em uma sub-rede privada. Se você iniciou a instância usando o assistente de inicialização de instância, talvez tenha editado o campo Atribuição automática de IP público em Configurações de rede e alterado o valor para Desabilitar. Se você desabilitar a opção Atribuição automática de IP públic, a instância não receberá um endereço IP público quando for iniciada.

- (Somente instâncias IPv6) Obtenha o endereço IPv6 da instância.

  Se você atribuiu um endereço IPv6 à instância, terá a opção de se conectar a ela usando o endereço IPv6 em vez de um endereço IPv4 ou o nome de host DNS público. Seu computador local deve ter um endereço IPv6 e configurado para usar IPv6. É possível obter o endereço IPv6 da instância no console do Amazon EC2. Verifique a coluna IPs IPv6 do painel Instâncias. Ou você pode encontrar o endereço IPv6 na seção de informações da instância. Quando você seleciona a instância no painel Instâncias do console do Amazon EC2, as informações sobre essa instância aparecem na metade inferior da página. Na guia Detalhes, procure Endereço IPv6.

  Se preferir, é possível usar o comando describe-instances (AWS CLI) ou Get-EC2Instance (AWS Tools for Windows PowerShell). Para obter mais informações sobre IPv6, consulte Endereços IPv6.

- (Instâncias do Linux) Obtenha o nome de usuário da instância.

  É possível se conectar à instância usando o nome de usuário da sua conta de usuário ou o nome de usuário padrão da AMI que você usou para iniciar a instância.

  - Obtenha o nome de usuário da sua conta de usuário.

Para obter mais informações sobre como criar uma conta de usuário, consulte Gerenciar usuários do sistema na instância do Linux do Amazon EC2.

- Obtenha o nome de usuário padrão da AMI que você usou para iniciar a instância.
  - Amazon Linux: `ec2-user`
  - CentOS: `centos` ou `ec2-user`
  - Debian – `admin`
  - Fedora: `fedora` ou `ec2-user`
  - FreeBSD: `ec2-user`
  - RHEL: `ec2-user` ou `root`
  - SUSE: `ec2-user` ou `root`
  - Ubuntu – `ubuntu`
  - Oracle – `ec2-user`
  - Bitnami – `bitnami`
  - Rocky Linux – `rocky`
  - Outro: verificar com o provedor da AMI

Localizar a chave privada e definir permissões

Você deve conhecer o local do arquivo de chave privada para fazer a conexão inicial com uma instância do Linux usando SSH ou com uma instância do Windows usando RDP. Para conexões SSH, você deve definir as permissões de arquivo para que somente você possa ler a chave privada.

Para obter informações sobre como os pares de chaves funcionam ao usar o Amazon EC2, consulte Pares de chaves do Amazon EC2 e instâncias do Amazon EC2.

- Localize a chave privada.

  Obtenha o caminho totalmente qualificado para o local em seu computador do arquivo `.pem` para o par de chaves que você especificou quando executou a instância. Para obter mais informações, consulte the section called “Identifique a chave pública que foi especificada na inicialização”.

  Se você não conseguir encontrar seu arquivo de chave privada, consulte . Perdi minha chave privada. Como posso me conectar à instância?

(Instâncias do Linux) Se você estiver se conectando à instância usando PuTTY e precisar converter o arquivo `.pem` em `.ppk`, consulte Converta a chave privada usando o PuTTYgen.

- (Instâncias do Linux) Defina as permissões da chave privada de modo que só você possa lê-la.
  - Conectar do macOS ou do Linux

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

    ```
    chmod 400 key-pair-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.
  - Conectar do Windows

    Abra o Explorador de Arquivos e clique com o botão direito do mouse no arquivo `.pem`. Selecione a guia Propriedades > Segurança e escolha Avançado. Escolha Desabilitar herança. Remova o acesso para todos os usuários, exceto para o usuário atual.

(Opcional) Obter a impressão digital da instância

Para se proteger de ataques “man-in-the-middle”, será possível verificar a autenticidade da instância à qual está prestes a se conectar, conferindo a impressão digital exibida. A verificação da impressão digital será útil se você executar a instância usando uma AMI pública fornecida por terceiros.

Visão geral da tarefa

Primeiro, obtenha a impressão digital da instância diretamente da instância. Em seguida, quando você se conectar à instância e receber a solicitação para verificar a impressão digital, compare a impressão digital que obteve nesse procedimento com a impressão digital exibida. Caso essas impressões digitais não correspondam, alguém pode estar tentando um ataque man-in-the-middle. Se elas corresponderem, será possível se conectar à instância com confiança.

Pré-requisitos para obter a impressão digital da instância

- A instância não deve estar no estado `pending`. A impressão digital só estará disponível após a conclusão da primeira inicialização da instância.

- Você deve ser o proprietário da instância para obter a saída do console.
- Há várias maneiras de obter a impressão digital da instância. Se você quiser usar a AWS CLI, ela deverá estar instalada no seu computador local. Para obter mais informações sobre a instalação do AWS CLI, consulte Conceitos básicos do AWS CLI no Guia do usuário do AWS Command Line Interface.

Para obter a impressão digital da instância

Na Etapa 1, você obtém a saída do console, que inclui a impressão digital da instância. Na Etapa 2, você encontra a impressão digital da instância na saída do console.

1. Use um dos métodos a seguir para obter a saída do console.

   Console

   1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
   2. No navegador à esquerda, escolha Instâncias.
   3. Selecione sua instância e escolha Ações, Monitorar e solucionar problemas e Obter log do sistema.

   AWS CLI

   No computador local (e não na instância com a qual você está se conectando), use o comando get-console-output. Se a saída for grande, será possível redirecioná-la para um arquivo de texto, onde poderá ser mais fácil lê-la.

   ```
   aws ec2 get-console-output \
       --instance-id i-1234567890abcdef0 \
       --query Output \
       --output text > temp.txt
   ```

   PowerShell

   No seu computador local, use o seguinte cmdlet Get-EC2ConsoleOutput.

   ```
   $encodedOutput = (Get-EC2ConsoleOutput -InstanceId i-1234567890abcdef0).Output
   [System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String($encodedOutput
   ```

2. Na saída do console, encontre a impressão digital da instância (host), localizada abaixo de `BEGIN SSH HOST KEY FINGERPRINTS`. Pode haver impressões digitais de várias instâncias. Quando você se conecta à sua instância, ela exibe somente uma das impressões digitais.

   A saída exata pode variar de acordo com o sistema operacional, a versão da AMI e se a AWS criou o par de chaves. O seguinte é um exemplo de saída.

```
ec2:#############################################################
ec2: -----BEGIN SSH HOST KEY FINGERPRINTS-----
ec2: 256 SHA256:l4UB/neBad9tvkgJf1QZWxheQmR59WgrgzEimCG6kZY no comment (ECDSA)
ec2: 256 SHA256:kpEa+rw/Uq3zxaYZN8KT501iBtJOIdHG52dFi66EEfQ no comment (ED25519)
ec2: 2048 SHA256:L8l6pepcA7iqW/jBecQjVZClUrKY+o2cHLI0iHerbVc no comment (RSA)
ec2: -----END SSH HOST KEY FINGERPRINTS-----
ec2: #############################################################
```

   > **Note**
   >
   > Você vai mencionar essa impressão digital quando se conectar à instância.

Conectar-se à instância do Linux usando SSH

Há várias maneiras de se conectar à instância do Linux usando SSH. Algumas maneiras dependem do sistema operacional do computador local do qual você se conecta. Outros métodos são baseados em navegador, como o EC2 Instance Connect ou o Gerenciador de Sessões do AWS Systems Manager, que podem ser usados em qualquer computador. Você pode usar o SSH para se conectar a uma instância do Linux e executar comandos ou usar o SSH para transferir arquivos entre o computador local e a instância.

Antes de você se conectar à instância do Linux usando o SSH, conclua os seguintes pré-requisitos:

- Verifique se a instância passou nas verificações de status. Pode demorar alguns minutos para que a instância fique pronta para aceitar solicitações de conexão. Para obter mais informações, consulte Visualizar verificações de status.
- Verifique se o grupo de segurança associado à instância permite tráfego SSH de entrada do endereço IP. Para obter mais informações, consulte Regras para se conectar a instâncias pelo computador.
- Obter os detalhes necessários da instância.

- Localizar a chave privada e definir permissões.
- (Opcional) Obter a impressão digital da instância.

Em seguida, escolha uma das opções a seguir para se conectar à instância do Linux usando o SSH.

- Conectar-se usando um cliente SSH
- Conectar-se usando PuTTY
- Transferir arquivos usando SCP

Se você não conseguir se conectar à instância e precisar de ajuda para solucionar o problema, consulte Solucionar problemas de conexão com a instância do Linux do Amazon EC2.

Conectar-se à instância do Linux usando um cliente SSH

Use o Secure Shell (SSH) para se conectar à instância do Linux no computador local. Para obter mais informações sobre outras opções, consulte Conexão com a instância do EC2.

> **Note**
>
> Se você receber um erro ao tentar se conectar à instância, certifique-se de que a instância atenda a todos os Pré-requisitos de conexão via SSH. Se ela atender a todos os pré-requisitos e, mesmo assim, você não conseguir se conectar à instância do Linux, consulte Solucionar problemas de conexão com a instância do Linux do Amazon EC2.

Conteúdo

- Pré-requisitos de conexão via SSH
- Conectar-se à instância do Linux usando um cliente SSH

Pré-requisitos de conexão via SSH

Antes de você se conectar à instância do Linux usando SSH, conclua as tarefas a seguir.

Conclua os pré-requisitos gerais.

- Verifique se a instância passou nas verificações de status. Pode demorar alguns minutos para que a instância fique pronta para aceitar solicitações de conexão. Para obter mais informações, consulte Visualizar verificações de status.

- Obter os detalhes necessários da instância.
- Localizar a chave privada e definir permissões.
- (Opcional) Obter a impressão digital da instância.

Permita tráfego SSH de entrada do seu endereço IP.

Verifique se o grupo de segurança associado à instância permite tráfego SSH de entrada do endereço IP. Para obter mais informações, consulte Regras para se conectar a instâncias pelo computador.

Instale um cliente SSH no computador local (se necessário).

O computador local pode ter um cliente SSH instalado por padrão. Você pode verificar isso ao inserir o comando a seguir em uma janela de terminal. Se o computador não reconhecer o comando, instale um cliente SSH.

```
ssh
```

A seguir, são mostradas algumas das possíveis opções para Windows. Se o computador executa um sistema operacional diferente, consulte a documentação desse sistema operacional para conhecer as opções do cliente SSH.

Instalar o OpenSSL no Windows

Depois de instalar o OpenSSH no Windows, você pode se conectar à instância do Linux pelo computador Windows usando SSH. Antes de começar, certifique-se de cumprir os requisitos a seguir.

Versão do Windows

A versão do Windows no computador deve ser Windows Server 2019 ou posterior.

Para versões anteriores do Windows, baixe e instale o Win32-OpenSSH.

Requisitos do PowerShell

Para instalar o OpenSSH no sistema operacional Windows usando o PowerShell, é necessário executar o PowerShell versão 5.1 ou posterior e sua conta deve ser membro do grupo de administradores do sistema. Execute o comando `$PSVersionTable.PSVersion` no PowerShell para verificar a versão do PowerShell.

Para verificar se você é membro do grupo de administradores do sistema, execute o seguinte comando do PowerShell:

```
(New-Object
 Security.Principal.WindowsPrincipal([Security.Principal.WindowsIdentity]::GetCurrent())).Is
```

Se você for membro do grupo de administradores do sistema, a saída será `True`.

Para instalar o OpenSSH para Windows usando o PowerShell, execute o comando do PowerShell a seguir.

```
Add-WindowsCapability -Online -Name OpenSSH.Client~~~~0.0.1.0
```

O seguinte é um exemplo de saída.

```
Path          :
Online        : True
RestartNeeded : False
```

Para instalar o OpenSSH do Windows usando o PowerShell, execute o comando do PowerShell a seguir.

```
Remove-WindowsCapability -Online -Name OpenSSH.Client~~~~0.0.1.0
```

O seguinte é um exemplo de saída.

```
Path          :
Online        : True
RestartNeeded : True
```

Instalar o Windows Subsystem para Linux (WSL)

Depois de instalar o WSL no Windows, você pode se conectar à instância do Linux pelo computador Windows usando ferramentas da linha de comando do Linux, como um cliente SSH.

Siga as instruções em Instalar o Windows Subsystem para Linux na instância do Windows do EC2. Se você seguir as instruções no guia de instalação da Microsoft, eles instalarão a distribuição Ubuntu do Linux. Você pode instalar uma distribuição do Linux diferente, se preferir.

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 use 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
```

Para obter informações sobre como desinstalar o Subsistema Windows para Linux, consulte Como desinstalar o WSL Distribution?.

Conectar-se à instância do Linux usando um cliente SSH

Use o procedimento a seguir para se conectar à sua Instância do Linux usando um cliente SSH.

Conectar-se à instância usando um cliente SSH

1. Abra uma janela de terminal no computador.
2. Use o comando ssh para se conectar à instância. Você precisa dos detalhes da instância que você coletou como parte dos pré-requisitos. Por exemplo, você precisa do local da chave privada (arquivo `.pem`), do nome de usuário e do nome DNS público ou do endereço IPv6. Veja a seguir exemplos de comando.
   - (DNS público) Para usar o nome DNS público, insira o comando a seguir.

     ```
     ssh -i /path/key-pair-name.pem instance-user-name@instance-public-dns-name
     ```

   - (IPv6) Como alternativa, se a instância tiver um endereço IPv6, insira o comando a seguir para usar o endereço IPv6.

     ```
     ssh -i /path/key-pair-name.pem instance-user-name@2001:db8::1234:5678:1.2.3.4
     ```

   O seguinte é um exemplo de resposta.

   ```
   The authenticity of host 'ec2-198-51-100-1.compute-1.amazonaws.com (198-51-100-1)'
    can't be established.
   ECDSA key fingerprint is l4UB/neBad9tvkgJf1QZWxheQmR59WgrgzEimCG6kZY.
   Are you sure you want to continue connecting (yes/no)?
   ```

3. (Opcional) Verifique se a impressão digital no alerta de segurança corresponde à impressão digital. Caso essas impressões digitais não correspondam, alguém pode estar tentando um ataque man-in-the-middle. Se corresponderem, continue para a próxima etapa. Para obter mais informações, consulte Get the instance fingerprint.
4. Digite **`yes`**.

   Você verá uma resposta como a seguinte:

```
Warning: Permanently added 'ec2-198-51-100-1.compute-1.amazonaws.com' (ECDSA) to
 the list of known hosts.
```

Conectar-se à instância do Linux usando PuTTY

Você pode se conectar a uma instância do Linux usando o PuTTY, um cliente SSH gratuito para Windows.

Se você estiver executando o Windows Server 2019 ou posterior, recomendamos que você use o OpenSSH, uma ferramenta de conectividade de código aberto para login remoto usando o protocolo SSH.

> **Note**
>
> Se você receber um erro ao tentar se conectar à instância, certifique-se de que a instância atenda a todos os Pré-requisitos de conexão via SSH. Se ela atender a todos os pré-requisitos e, mesmo assim, você não conseguir se conectar à instância do Linux, consulte Solucionar problemas de conexão com a instância do Linux do Amazon EC2.

Conteúdo

- Pré-requisitos
- (Opcional) Converter a chave privada usando o PuTTYgen
- Conecte-se à sua instância do Linux

Pré-requisitos

Antes de você se conectar à instância do Linux usando o PuTTY, conclua as tarefas a seguir.

Conclua os pré-requisitos gerais.

- Verifique se a instância passou nas verificações de status. Pode demorar alguns minutos para que a instância fique pronta para aceitar solicitações de conexão. Para obter mais informações, consulte Visualizar verificações de status.
- Obter os detalhes necessários da instância.
- Localizar a chave privada e definir permissões.
- (Opcional) Obter a impressão digital da instância.

Permita tráfego SSH de entrada do seu endereço IP.

Verifique se o grupo de segurança associado à instância permite tráfego SSH de entrada do endereço IP. Para obter mais informações, consulte Regras para se conectar a instâncias pelo computador.

Instale o PuTTY no computador local (se necessário).

Faça download e instale o PuTTY pela página de download do PuTTY. Se já houver uma versão anterior do PuTTY instalada, recomendamos fazer download da versão mais recente. Instale o pacote inteiro.

Converta a chave privada no formato PPK usando PuTTYgen.

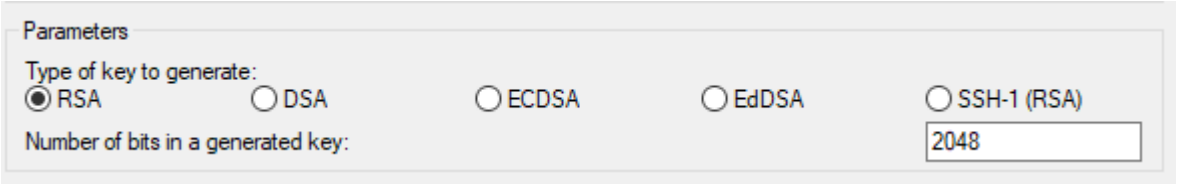
Você deve especificar a chave privada do par de chaves que especificou quando iniciou a instância. Se você tiver criado a chave privada no formato .pem, será necessário convertê-la em um arquivo PPK para usá-la com o PuTTY. Localize a chave privada (arquivo .pem) e siga as etapas em Converta a chave privada usando o PuTTYgen.

(Opcional) Converter a chave privada usando o PuTTYgen

O PuTTY não é originalmente compatível com o formato PEM para chaves SSH. O PuTTY fornece uma ferramenta chamada PuTTYgen, que converte as chaves PEM para o formato PPK necessário para PuTTY. Se você tiver criado a chave usando o formato PEM em vez do formato PPK, será necessário converter a chave privada (arquivo .pem) neste formato (arquivo .ppk) para usá-la com o PuTTY.

Converter a chave privada do formato PEM para o formato PPK

1. No menu Start (Iniciar), selecione All Programs (Todos os programas), PuTTY, PuTTYgen.
2. Em Tipo de chave a ser gerada, escolha RSA. Se a sua versão de PuTTYgen não inclui esta opção, escolha SSH-2 RSA.



3. Escolha Load. Por padrão, o PuTTYgen exibe somente arquivos com a extensão `.ppk`. Para localizar o arquivo `.pem`, escolha a opção para exibir arquivos de todos os tipos.

4. Selecione o arquivo `.pem` para o par de chaves que você especificou ao executar a instância e selecione Open (Abrir). A PuTTYgen exibe um aviso de que o arquivo `.pem` foi importado com êxito. Escolha OK.
5. Escolha Save private key (Salvar chave privada) para salvar a chave no formato PuTTY. A PuTTYgen exibe um aviso sobre salvar a chave sem uma senha. Escolha Sim.

> **Note**
>
> Uma senha em uma chave privada é uma camada extra de proteção. Mesmo se a chave privada for descoberta, ela não pode ser usada sem a senha. A desvantagem de se usar uma senha é que a automação se torna mais difícil porque a intervenção humana é necessária para fazer login em uma instância, ou para copiar arquivos a uma instância.

6. Especifique o mesmo nome da chave usado para o par de chaves (por exemplo, `key-pair-name`) e escolha Save (Salvar). O PuTTY adiciona automaticamente a extensão de arquivo `.ppk`.

Sua chave privada está agora no formato correto para uso com o PuTTY. Agora é possível conectar a sua instância usando o cliente SSH do PuTTY.

Conecte-se à sua instância do Linux

Use o procedimento a seguir para se conectar à sua Instância do Linux usando o PuTTY. Você precisa do arquivo `.ppk` que criou para sua chave privada. Para obter mais informações, consulte (Opcional) Converter a chave privada usando o PuTTYgen na seção anterior. Se você receber um erro ao tentar se conectar à instância, consulte Solucionar problemas de conexão com a instância do Linux do Amazon EC2.

Última versão testada: PuTTY .78

Para se conectar à instância usando PuTTY

1. Inicie o PuTTY (no menu Iniciar, pesquise PuTTY e escolha Abrir).
2. No painel Categoria, selecione Sessão e preencha os seguintes campos:

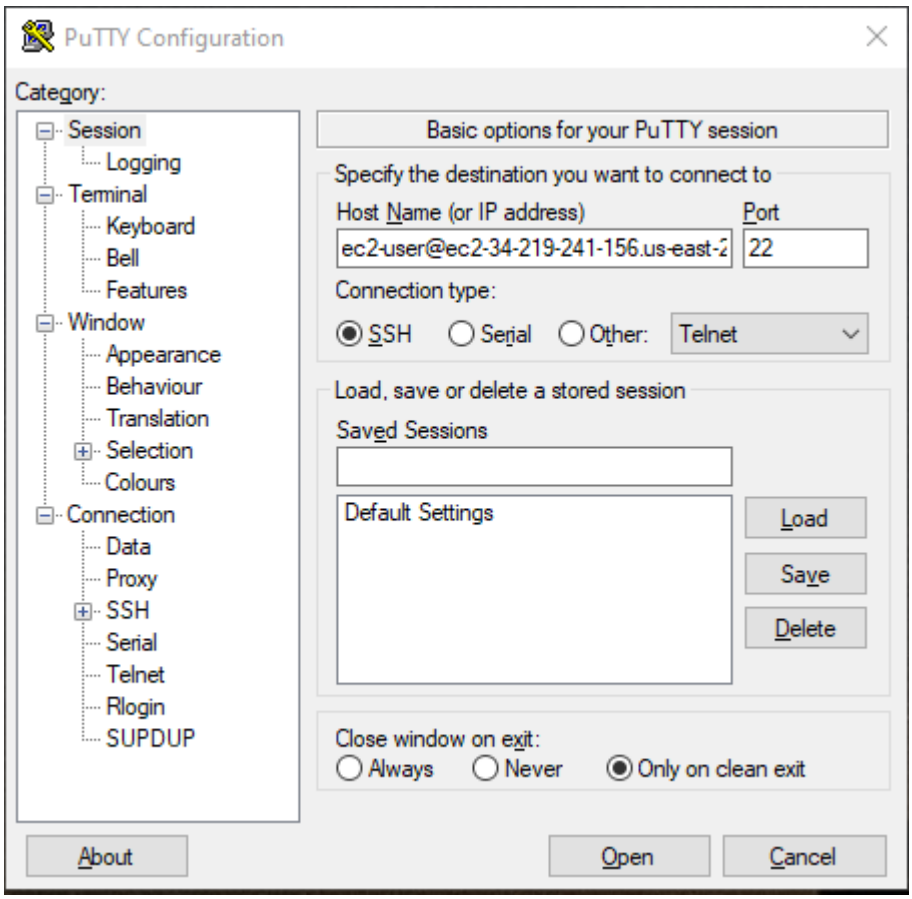
   a. Na caixa Host Name (Nome do host), execute uma das ações a seguir:

      - (DNS Público) Para se conectar usando o nome DNS público da instância, insira *instance-user-name*@*instance-public-dns-name*.
      - (IPv6) Como alternativa, se a instância tiver um endereço IPv6, para se conectar usando o endereço IPv6 da instância, insira *instance-user-name*@*2001:db8::1234:5678:1.2.3.4*.

      Para obter informações sobre como obter o nome de usuário da instância e o nome de DNS público ou o endereço IPv6 da instância, consulte Obter os detalhes necessários da instância.

   b. Verifique se o valor do Port é 22.

   c. Em Tipo de conexão, selecione SSH.



3. (Opcional) É possível 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 Categoria, escolha Conexão e insira o intervalo necessário no campo Segundos entre keepalives. Por exemplo, se a sessão desconectar após 10 minutos de inatividade, insira 180 para configurar o PuTTY para enviar dados keepalive a cada 3 minutos.
4. No painel Categoria, expanda Conexão, SSH e Auth. Escolha Credenciais.
5. Ao lado de Arquivo de chave privada para autenticação, escolha Procurar. Na caixa de diálogo Selecionar arquivo de chave privada, selecione o arquivo `.ppk` que você gerou para seu par de chaves. Clique duas vezes no arquivo ou escolha Abrir na caixa de diálogo Selecionar arquivo de chave privada.
6. (Opcional) Se você planeja se conectar a esta instância novamente após esta sessão, poderá salvar as informações para uso futuro. No painel Categoria, escolha Sessão. Insira um nome para a sessão em Sessõe salvas e, em seguida, escolha Salvar.
7. Para se conectar à instância, escolha Abrir.

8. Se essa for a primeira vez você se conectou a esta instância, o PuTTY exibirá uma caixa de diálogo de alerta de segurança perguntando se você confia no host ao qual está se conectando.

   a. (Opcional) Verifique se a impressão digital na caixa de diálogo do alerta de segurança corresponde à impressão digital que você obteve anteriormente em (Opcional) Obter a impressão digital da instância. Caso essas impressões digitais não correspondam, alguém pode estar tentando um ataque "man-in-the-middle". Se corresponderem, continue para a próxima etapa.

   b. Escolha Accept (Aceitar). Uma janela se abrirá e você estará conectado à sua instância.

   > **Note**
   >
   > Se você especificou uma senha ao converter sua chave privada em formato PuTTY, forneça essa senha ao efetuar o login na instância.

Se você receber um erro ao tentar se conectar à instância, consulte Solucionar problemas de conexão com a instância do Linux do Amazon EC2.

Transferir arquivos para uma instância 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. O SCP é uma boa opção para operações simples, como cópias de arquivos únicas. O SCP protege as transferências de arquivos usando o mesmo arquivo .pem que você usa para se conectar a uma instância usando SSH. Se você precisa manter os arquivos sincronizados, ou se os arquivos são grandes, rsync é mais rápido e eficiente do que o SCP. Por segurança, use rsync via SSH, pois, por padrão, rsync transfere dados usando texto simples.

Antes de você se conectar à instância do Linux usando o SCP, conclua as seguintes tarefas:

- Conclua os pré-requisitos gerais.
  - Verifique se a instância passou nas verificações de status. Pode demorar alguns minutos para que a instância fique pronta para aceitar solicitações de conexão. Para obter mais informações, consulte Visualizar verificações de status.
  - Obter os detalhes necessários da instância.
  - Localizar a chave privada e definir permissões.
  - (Opcional) Obter a impressão digital da instância.

- Permita tráfego SSH de entrada do seu endereço IP.

  Verifique se o grupo de segurança associado à instância permite tráfego SSH de entrada do endereço IP. Para obter mais informações, consulte Regras para se conectar a instâncias pelo computador.

- Instale 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 grátis do pacote completo das ferramentas SSH, inclusive um cliente SCP. Para obter mais informações, consulte https://www.openssh.com.

O procedimento a seguir acompanha o uso do SCP para transferir um arquivo usando o nome DNS público da instância ou o endereço IPv6 se sua instância tiver um.

Para usar o SCP para transferir arquivos entre o computador e a sua instância

1. Determine a localização do arquivo de origem no seu computador e o caminho de destino na instância. Nos exemplos a seguir, o nome do arquivo de chave privada é `key-pair-name.pem`, o arquivo a ser transferido é `my-file.txt`, o nome de usuário da instância é ec2-user, o nome de DNS público da instância é `instance-public-dns-name` e o endereço IPv6 da instância é `2001:db8::1234:5678:1.2.3.4`.
   - (DNS público) Para transferir um arquivo para o destino na instância, insira o seguinte comando do seu computador.

     ```
     scp -i /path/key-pair-name.pem /path/my-file.txt ec2-user@instance-public-dns-name:path/
     ```

   - (IPv6) Para transferir um arquivo para o destino na instância, se ela tiver um endereço IPv6, insira o seguinte comando no seu computador. O endereço IPv6 deve vir entre colchetes ([ ]), que devem ser recuados (\).

     ```
     scp -i /path/key-pair-name.pem /path/my-file.txt ec2-user@
     \[2001:db8::1234:5678:1.2.3.4\]:path/
     ```

2. Se ainda não tiver conectado à instância usando SSH, você verá uma resposta como a seguinte:

   ```
   The authenticity of host 'ec2-198-51-100-1.compute-1.amazonaws.com (10.254.142.33)'
   can't be established.
   RSA key fingerprint is 1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f.
   ```

```
Are you sure you want to continue connecting (yes/no)?
```

(Opcional) Também é possível verificar se a impressão digital no alerta de segurança corresponde à impressão digital da instância. Para obter mais informações, consulte (Opcional) Obter a impressão digital da instância.

Insira **yes**.

3. Se a transferência for bem-sucedida, a resposta será semelhante à seguinte:

```
Warning: Permanently added 'ec2-198-51-100-1.compute-1.amazonaws.com' (RSA)
to the list of known hosts.
my-file.txt                                   100%   480     24.4KB/s   00:00
```

4. Para transferir um arquivo na outra direção (de uma instância do Amazon EC2 para o seu computador), basta inverter a ordem dos parâmetros do host. Por exemplo, é possível transferir o `my-file.txt` da instância do EC2 para um destino no seu computador local `my-file2.txt`, conforme exibido nos exemplos a seguir.

   - (DNS Público) Para transferir um arquivo para um destino no seu computador, insira o seguinte comando do seu computador.

     ```
     scp -i /path/key-pair-name.pem ec2-user@instance-public-dns-name:path/my-file.txt path/my-file2.txt
     ```

   - (IPv6) Para transferir um arquivo para um destino no computador se a instância tiver um endereço IPv6, insira o seguinte comando do seu computador. O endereço IPv6 deve vir entre colchetes (`[ ]`), que devem ser recuados (\).

     ```
     scp -i /path/key-pair-name.pem ec2-user@\[2001:db8::1234:5678:1.2.3.4\]:path/my-file.txt path/my-file2.txt
     ```

Gerenciar usuários do sistema na instância do Linux do Amazon EC2

Cada tipo de instância do Linux é iniciada com um usuário padrão do sistema Linux. Você pode adicionar e excluir usuários da instância.

Para o usuário padrão, o nome de usuário padrão é determinado pela AMI especificada quando você executou a instância.

> **Note**
>
> Por padrão, a autenticação por senha e o login raiz estão desabilitados e o sudo está habilitado. Para fazer login na instância, você deve criar um par de chaves. Para obter mais informações sobre login, consulte Conectar-se à instância do Linux usando SSH.
> Você pode permitir a autenticação por senha e o login raiz na instância. Para obter mais informações, consulte a documentação do seu sistema operacional.

> **Note**
>
> Os usuários do sistema Linux não devem ser confundidos com os usuários do IAM. Para obter mais informações, consulte Usuários IAM no Manual do usuário IAM.

Conteúdo

- Nomes de usuário padrão
- Considerações
- Criar um usuário
- Remover um usuário

Nomes de usuário padrão

O nome de usuário padrão para a instância do EC2 é determinado pela AMI especificada quando você executou a instância.

Os nomes de usuário padrão são:

- Para uma AMI do Amazon Linux, o nome do usuário é `ec2-user`.
- Para uma AMI do CentOS, o nome do usuário é `centos` ou `ec2-user`.
- Para uma AMI do Debian, o nome do usuário é `admin`.
- Para uma AMI do Fedora, o nome do usuário é `fedora` ou `ec2-user`.
- Para uma AMI FreeBSD, o nome do usuário é `ec2-user`.
- Para uma AMI do RHEL, o nome do usuário é `ec2-user` ou `root`.
- Para uma AMI do SUSE, o nome do usuário é `ec2-user` ou `root`.

- Para uma AMI Ubuntu, o nome de usuário é `ubuntu`.
- Para uma AMI do Oracle, o nome do usuário é `ec2-user`.
- Para uma AMI do Bitnami, o nome do usuário é `bitnami`.

> **Note**
>
> Para encontrar o nome de usuário padrão para outras distribuições do Linux, verifique com o fornecedor da AMI.

Considerações

O uso do usuário padrão é adequado para muitas aplicações. Porém, você pode escolher adicionar usuários para que as pessoas possam ter seus próprios arquivos e espaços de trabalho. Além disso, a criação usuários para novos usuários é muito mais segura do que conceder a vários usuários (possivelmente inexperientes) acesso ao usuário padrão, pois essa conta pode causar muitos danos a um sistema quando usada de modo inadequado. Para obter mais informações, consulte Dicas para proteger sua instância do EC2.

Para permitir aos usuários acesso SSH à sua instância do EC2 usando um usuário do sistema Linux, é necessário compartilhar a chave SSH com o usuário. Uma outra opção é usar o EC2 Instance Connect para fornecer acesso aos usuários sem precisar compartilhar e gerenciar as chaves SSH. Para obter mais informações, consulte Conecte-se à sua instância Linux usando um endereço IP público e o EC2 Instance Connect.

Criar um usuário

Primeiro crie o usuário e, depois, adicione a chave pública SSH que permitirá que ele se conecte e faça login na instância.

> **Important**
>
> Na Etapa 1 desse procedimento, você cria um novo par de chaves. Como o par de chaves funciona como uma senha, é fundamental lidar com ele de forma segura. Caso crie um par de chaves para um usuário, você deverá garantir que a chave privada seja enviada para ele com segurança. Como alternativa, o usuário pode concluir as Etapas 1 e 2 criando seu próprio par de chaves, mantendo a chave privada segura em sua máquina e enviando a chave pública para concluir o procedimento da Etapa 3.

Para criar um usuário

1. Crie um novo par de chaves. É necessário fornecer o arquivo `.pem` ao usuário para o qual você está criando o usuário. Ele deve usar esse arquivo para se conectar à instância.
2. Recupere a chave pública do par de chaves criado na etapa anterior.

   ```
   $ ssh-keygen -y -f /path_to_key_pair/key-pair-name.pem
   ```

   O comando retorna a chave pública, como mostrado no exemplo a seguir.

   ```
   ssh-rsa
    AAAAB3NzaC1yc2EAAAADAQABAAABAQClKsfkNkuSevGj3eYhCe53pcjqP3maAhDFcvBS7O6Vhz2ItxCih
   +PnDSUaw+WNQn/mZphTk/a/gU8jEzoOWbkM4yxyb/wB96xbiFveSFJuOp/
   d6RJhJOI0iBXrlsLnBItntckiJ7FbtxJMXLvvwJryDUilBMTjYtwB+QhYXUMOzce5Pjz5/
   i8SeJtjnV3iAoG/cQk+0FzZqaeJAAHco
   +CY/5WrUBkrHmFJr6HcXkvJdWPkYQS3xqC0+FmUZofz221CBt5IMucxXPkX4rWi
   +z7wB3RbBQoQzd8v7yeb7OzlPnWOyN0qFU0XA246RA8QFYiCNYwI3f05p6KLxEXAMPLE
   ```

3. Conecte-se à instância.
4. Use o comando adduser para criar o usuário e adicioná-lo ao sistema (com uma entrada no arquivo `/etc/passwd`). O comando também cria um grupo e um diretório inicial para o usuário. Neste exemplo de configuração, o usuário é deniminado *`newuser`*.

   - AL2023 e Amazon Linux 2

     Com o AL2023 e o Amazon Linux 2, o usuário é criado com a autenticação por senha desabilitada por padrão.

     ```
     [ec2-user ~]$ sudo adduser newuser
     ```

   - Ubuntu

     Inclua o parâmetro `--disabled-password` para criar o usuário com autenticação por senha desabilitada.

     ```
     [ubuntu ~]$ sudo adduser newuser --disabled-password
     ```

5. Mude para o novo usuário, de modo que o diretório e o arquivo criados pertençam aos proprietários adequados.

```
[ec2-user ~]$ sudo su - newuser
```

O prompt é alterado de `ec2-user` para *`newuser`* para indicar que você mudou a sessão do shell para o novo usuário.

6. Adicione a chave pública SSH ao usuário. Primeiro, crie um diretório no diretório inicial do usuário para o arquivo de chave SSH. Depois disso, crie o arquivo de chave e, por fim, cole a chave pública no arquivo de chave, conforme descrito nas etapas secundárias a seguir.

   a. Crie um diretório `.ssh` no diretório inicial *`newuser`* e altere suas permissões de arquivos para `700` (somente o proprietário pode ler, gravar ou abrir o diretório).

   ```
   [newuser ~]$ mkdir .ssh
   ```

   ```
   [newuser ~]$ chmod 700 .ssh
   ```

   > **Important**
   >
   > Sem essas permissões de arquivos, o usuário não poderá se conectar.

   b. Crie um arquivo chamado `authorized_keys` no diretório `.ssh` e altere suas permissões de arquivos para `600` (somente o proprietário pode ler ou gravar no arquivo).

   ```
   [newuser ~]$ touch .ssh/authorized_keys
   ```

   ```
   [newuser ~]$ chmod 600 .ssh/authorized_keys
   ```

   > **Important**
   >
   > Sem essas permissões de arquivos, o usuário não poderá se conectar.

   c. Abra o arquivo `authorized_keys` usando seu editor de texto favorito (como vim ou nano).

   ```
   [newuser ~]$ nano .ssh/authorized_keys
   ```

   Cole a chave pública recuperada na Etapa 2 no arquivo e salve as alterações.

> **Important**
>
> Cole a chave pública em uma linha contínua. A chave pública não deve ser dividida em várias linhas.

Agora, o usuário deve poder fazer login no usuário *newuser* na instância usando a chave privada correspondente à chave pública adicionada ao arquivo `authorized_keys`. Para obter mais informações sobre os diferentes métodos de conexão a uma instância do Linux, consulte Conectar-se à instância do Linux usando SSH.

Remover um usuário

Se um usuário não for mais necessário, será possível removê-lo para que não possa mais ser usado.

Use o comando userdel para remover o 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
```

Conectar-se à instância do Windows no usando RDP

É possível se conectar às instâncias do Amazon EC2 criadas da maioria das imagens de máquina da Amazon (AMIs) no Windows usando a Área de Trabalho Remota. O Remote Desktop usa o Remote Desktop Protocol (RDP) para se conectar e usar sua instância da mesma forma que você usa um computador que esteja na sua frente (computador local). Ele está disponível na maioria das edições do Windows e também para Mac OS.

A licença do sistema operacional (SO) Windows Server permite duas conexões remotas simultâneas para fins administrativos. A licença para Windows Server está incluída no preço da sua instância do Windows. Caso precise de mais de duas conexões remotas simultâneas, você deverá adquirir uma licença do Remote Desktop Services (RDS). Se você tentar uma terceira conexão, ocorrerá um erro.

> **Tip**
>
> Se precisar se conectar à instância para solucionar problemas de inicialização, configuração de rede e outros problemas para instâncias criadas no AWS Nitro System, use o EC2 Serial Console para instâncias do.

Conteúdo

- Conexão com a instância do Windows usando um cliente RDP
- Conectar a uma instância do Windows usando o Fleet Manager
- Transferir arquivos para uma instância do Windows usando o RDP

Conexão com a instância do Windows usando um cliente RDP

É possível se conectar à instância do Windows usando um cliente RDP conforme mostrado a seguir.

> **Tip**
>
> Como alternativa, você pode se conectar à instância do Windows usando o Systems Manager Fleet Manager ou o Endpoint de conexão da instância do EC2.

Pré-requisitos

É necessário atender aos pré-requisitos apresentados a seguir para se conectar à instância do Windows usando um cliente RDP.

- Conclua os pré-requisitos gerais.
  - Verifique se a instância passou nas verificações de status. Pode demorar alguns minutos para que a instância fique pronta para aceitar solicitações de conexão. Para ter mais informações, consulte Visualizar verificações de status.
  - Obter os detalhes necessários da instância.
  - Localizar a chave privada e definir permissões.
  - (Opcional) Obter a impressão digital da instância.
- Instalar um cliente RDP.

  - (Windows) O Windows inclui um cliente RDP por padrão. Para verificar, digite mstsc em uma janela de Prompt de Comando. Se o seu computador não reconhecer esse comando, baixe a aplicação Área de Trabalho Remota da Microsoft na Microsoft Store.
  - (macOS X) Faça o download da aplicação Windows para Mac (anteriormente chamada de Área de Trabalho Remota da Microsoft) usando a Mac App Store.
  - (Linux) Use o Remmina.
- Permitir tráfego RDP de entrada do seu endereço IP.

  Verifique se o grupo de segurança associado à instância permite tráfego RDP de entrada do seu endereço IP. Para ter mais informações, consulte Regras para se conectar a instâncias pelo computador.

Recuperar a senha de administrador

Caso tenha associado a instância a um domínio, será possível se conectar a ela usando as credenciais de domínio do Directory Service. Na tela de login da área de trabalho remota, em vez de usar o nome do computador local e a senha gerada, use o nome de usuário totalmente qualificado para o administrador (por exemplo, **`corp.example.com\Admin`**) e a senha dessa conta.

Para você se conectar a uma instância do Windows, é necessário recuperar a senha de administrador inicial e inserir essa senha quando se conectar à instância. Após a execução da instância, leva alguns minutos para que a senha fique disponível. Sua conta precisa ter permissão para chamar a ação GetPasswordData. Para ter mais informações, consulte Exemplo de políticas para controlar o acesso à API do Amazon EC2.

O nome de usuário padrão correspondente à conta de administrador depende do idioma do sistema operacional (SO) contido na AMI. Para determinar o nome de usuário correto, identifique o idioma do sistema operacional e escolha o nome de usuário correspondente. Por exemplo, para um sistema operacional em inglês, o nome de usuário será `Administrator`, para um sistema operacional francês, será `Administrateur` e para um sistema operacional português, será `Administrador`. Se uma versão de idioma do sistema operacional não tiver um nome de usuário no mesmo idioma, escolha o nome de usuário `Administrator (Other)`. Para obter mais informações, consulte Nomes localizados da conta de administrador no Windows no site da Microsoft.

Recuperar a senha de administrador inicial

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 Conectar.
4. Na página Conectar à instância, escolha a guia Cliente RDP.
5. Em Nome de usuário, escolha o nome de usuário padrão para a conta do administrador. O nome de usuário escolhido deverá corresponder ao idioma do sistema operacional (SO) contido na AMI que você usou para executar a instância. Se não houver um nome de usuário no mesmo idioma do seu sistema operacional, escolha Administrador (Outro).
6. Escolha Obter senha.
7. Na página Obter senha do Windows, faça o seguinte:

    a. Escolha Fazer upload de arquivo de chave privada e localize o arquivo de chave privada (`.pem`) que especificou ao executar a instância. Selecione o arquivo e escolha Open (Abrir) para copiar todo o conteúdo do arquivo para essa janela.

    b. Escolha Descriptografar senha. A página Obter senha do Windows será fechada e a senha padrão do administrador para a instância será exibida em Senha, substituindo o link Obter senha exibido anteriormente.

    c. Copie e salve a senha em um lugar seguro. Essa senha é necessária para se conectar à instância.

Conectar-se à sua instância do Windows do

O procedimento a seguir usa o cliente Remote Desktop Connection para Windows (MSTSC). Se você estiver usando um cliente RDP diferente, baixe o arquivo RDP e consulte a sua documentação para conhecer as etapas para estabelecer a conexão RDP.

Conectar-se a uma instância do Windows usando um cliente RDP

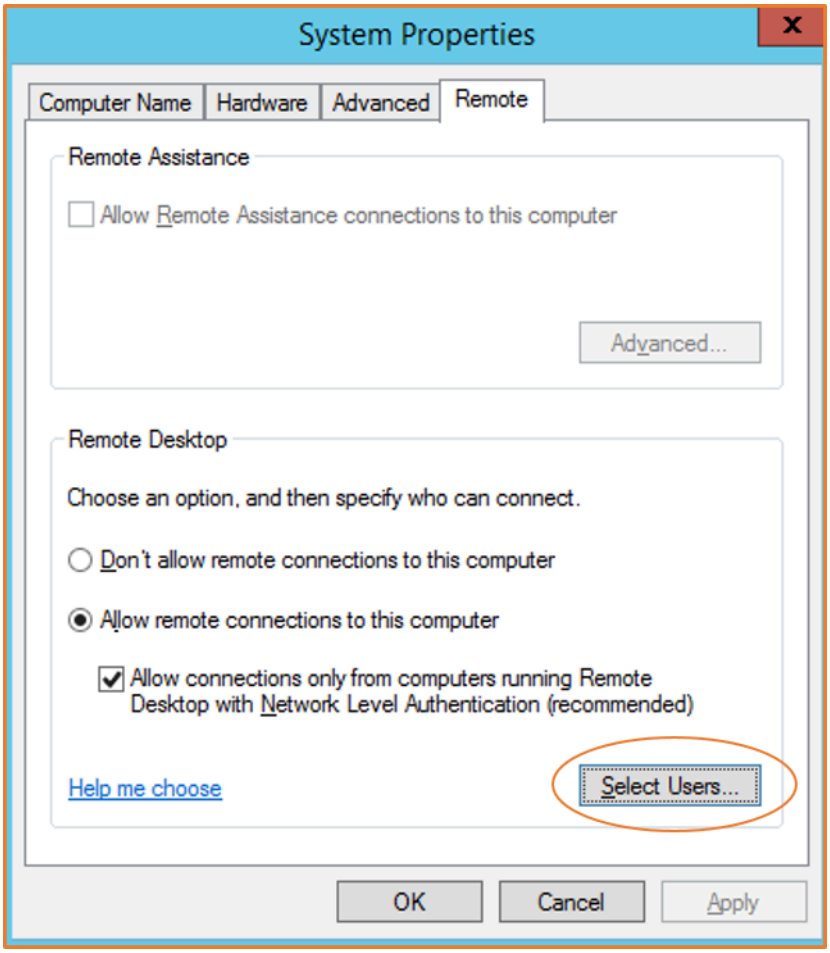
1. Na página Conectar-se a uma instância, escolha Baixar arquivo de área de trabalho remota. Quando o download do arquivo terminar, escolha Cancelar para retornar à página Instâncias. O arquivo RDP é baixado para a sua pasta `Downloads`.
2. Execute `mstsc.exe` para abrir o cliente RDP.
3. Expanda Mostrar opções, escolha Abrir e selecione o arquivo .rdp na pasta `Downloads`.
4. Por padrão, Computador é o nome DNS IPv4 público da instância, e Nome de usuário é a conta do administrador. Em vez disso, para se conectar à instância usando IPv6, substitua o nome DNS IPv4 público da instância pelo endereço IPv6. Analise as configurações padrão e altere-as conforme necessário.

5. Selecione Conectar. Se você receber um aviso de que o publicador da conexão remota é desconhecido, selecione Conectar para continuar.
6. Digite a senha que você salvou anteriormente e selecione OK.
7. Por causa da natureza de certificados autoassinados, talvez você receba um aviso indicando que não foi possível autenticar o certificado de segurança. Execute um destes procedimentos:
   - Se você confia no certificado, escolha Sim para realizar a conexão com a instância.
   - [Windows] Antes de continuar, compare a impressão digital do certificado com o valor no log do sistema para confirmar a identidade do computador remoto. Escolha Visualizar certificado e, em seguida, escolha Impressão digital na guia Detalhes. Compare esse valor com o valor de `RDPCERTIFICATE-THUMBPRINT` em Ações, Monitorar e solucionar problemas e Obter log do sistema.
   - [Mac OS X] Antes de continuar, compare a impressão digital do certificado com o valor no log do sistema para confirmar a identidade do computador remoto. Escolha Mostrar certificado, expanda Detalhes e selecione Impressões digitais de SHA1. Compare esse valor com o valor de `RDPCERTIFICATE-THUMBPRINT` em Ações, Monitorar e solucionar problemas e Obter log do sistema.
8. Se a conexão RDP tiver êxito, o cliente RDP exibirá a tela de login do Windows e, em seguida, a área de trabalho do Windows. Se, em vez disso, você receber uma mensagem de erro, consulte the section called “O Remote Desktop não pode se conectar ao computador remoto”. Ao finalizar a conexão RDP, será possível fechar o cliente RDP.

Configurar contas de usuário

Depois de se conectar à instância pelo RDP, recomendamos que você execute as seguintes tarefas:

- Altere a senha de administrador do valor padrão. É possível alterar a senha enquanto estiver conectado à instância, assim como faria em qualquer outro computador executando o Windows Server.
- Crie outro usuário com privilégios de administrador na instância. Essa é uma proteção no caso de você esquecer a senha de administrador ou ter um problema com a conta de administrador. O novo usuário deve ter permissão para acessar a instância remotamente. Abra System Properties (Propriedades do sistema clicando com o botão direito do mouse no ícone This PC (Este PC) no desktop do Windows ou no Explorador de Arquivos e selecione Properties (Propriedades). Escolha Remote settings (Configurações remotas) e escolha Select Users (Selecionar usuários) para adicionar o usuário ao grupo Remote Desktop Users (Usuários de Desktop Remoto).



Conectar a uma instância do Windows usando o Fleet Manager

É possível usar o Fleet Manager, um recurso do AWS Systems Manager, para se conectar a instâncias do Windows usando o Remote Desktop Protocol (RDP) e exibir até quatro instâncias do Windows na mesma página no Console de gerenciamento da AWS. É possível se conectar à primeira instância no Fleet Manager Remote Desktop diretamente da página Instâncias no console do Amazon EC2. Para obter mais informações sobre o Fleet Manager, consulte Conectar-se a uma instância gerenciada usando o Remote Desktop no Guia do usuário doAWS Systems Manager.

Não é necessário permitir especificamente o tráfego RDP de entrada do seu endereço IP se você usa o Fleet Manager para se conectar. O Fleet Manager trata disso para você.

Pré-requisitos

Antes de tentar se conectar a uma instância usando o Fleet Manager, você deve configurar seu ambiente. Para obter mais informações, consulte Como configurar seu ambiente no Guia do usuário do AWS Systems Manager.

Conectar-se a uma instância do Windows usando o Fleet Manager

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 Conectar.
4. Na guia Cliente RDP, em Tipo de conexão, escolha Conectar usando o Fleet Manager.
5. Escolha Fleet Manager: área de trabalho remota. Isso abre a página Fleet Manager Remote Desktop no console do AWS Systems Manager.
6. Insira suas credenciais e, em seguida, selecione Conectar.
7. Se a conexão RDP ftiver êxito, o Fleet Manager exibirá a área de trabalho do Windows. Ao finalizar a sessão, escolha Ações, Encerrar sessão.

Para obter mais informações, consulte Conectar a uma instância gerenciada pelo Windows Server usando o Remote Desktop no Guia do usuário do AWS Systems Manager.

Transferir arquivos para uma instância do Windows usando o RDP

É possível trabalhar com sua instância Windows da mesma forma que trabalharia com qualquer servidor Windows. Por exemplo, é possível transferir arquivos entre uma instância do Windows e o computador local usando o recurso de compartilhamento de arquivos local do software Microsoft Remote Desktop Connection (RDP). É possível acessar arquivos locais em unidades de disco rígido, unidades de DVD, unidades de mídia portáteis e unidades de rede mapeadas.

Para acessar arquivos locais das instâncias do Windows, é necessário habilitar o recurso de compartilhamento de arquivos local mapeando a unidade de sessão remota para a unidade local. As etapas são um pouco diferentes, dependendo se o sistema operacional do computador local for Windows ou macOS X.

Para obter mais informações sobre os pré-requisitos para conexão usando o RDP, consulte Pré-requisitos.

Windows

Para mapear a unidade de sessão remota para sua unidade local em seu computador Windows local

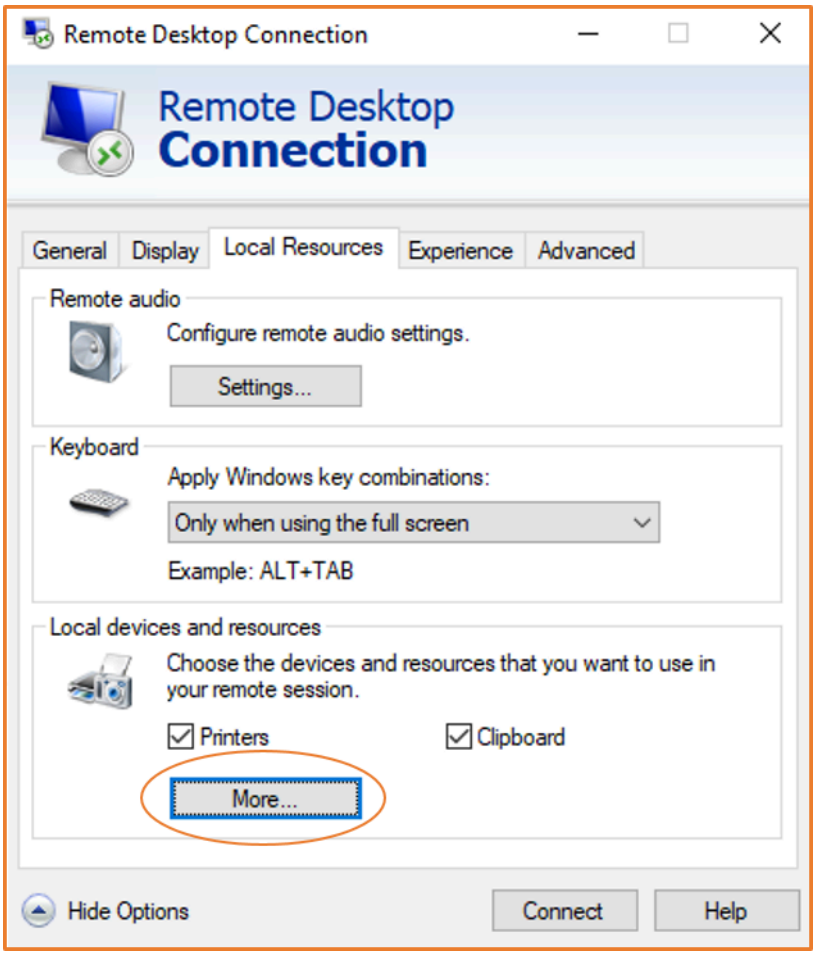
1. Abra o cliente de Conexão de Desktop Remoto.

2. Selecione Exibir opções.
3. Adicione o nome do host da instância ao campo Computador e o nome de usuário ao campo Nome de usuário da seguinte forma:

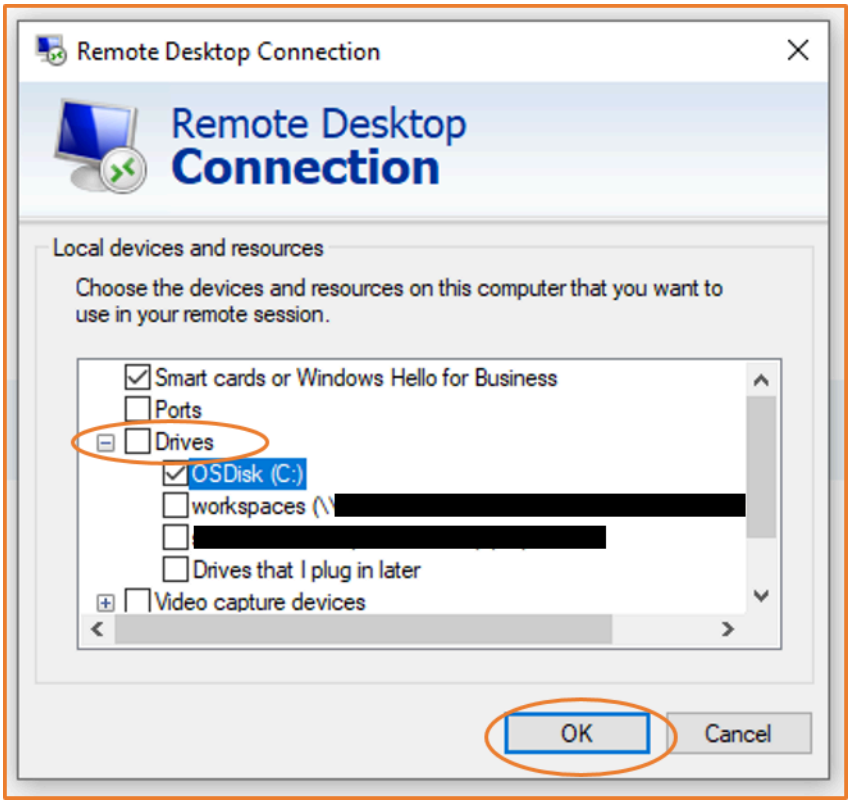
   a. Em Connection settings (Configurações de conexão), escolha Open... (Aberto) e busque o arquivo de atalho RDP baixado do console do Amazon EC2. O arquivo contém o nome do host DNS IPv4 público que identifica a instância e o nome de usuário do Administrador.

   b. Selecione o arquivo selecione Open (Abrir). Os campos Computer (Computador) e User name (Nome de usuário) são preenchidos com os valores do arquivo de atalho RDP.

   c. Escolha Salvar.
4. Selecione a guia Local Resources (Recursos locais).
5. Em Local Devices and resources (Dispositivos e recursos locais), escolha More... (Mais...).



6. Abra Drives (Unidades) e selecione a unidade local à qual mapear sua instância do Windows.
7. Escolha OK.

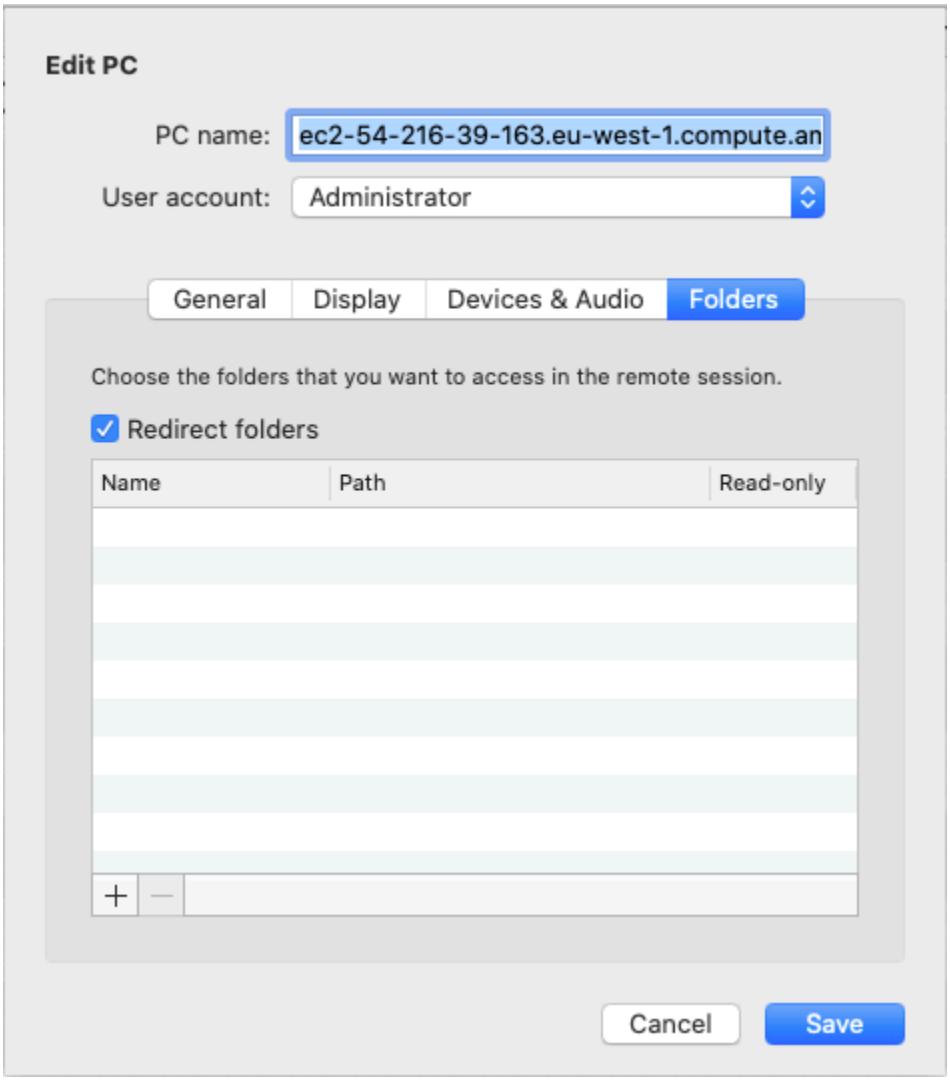


8. Selecione Connect (Conectar) para se conectar à sua instância do Windows.

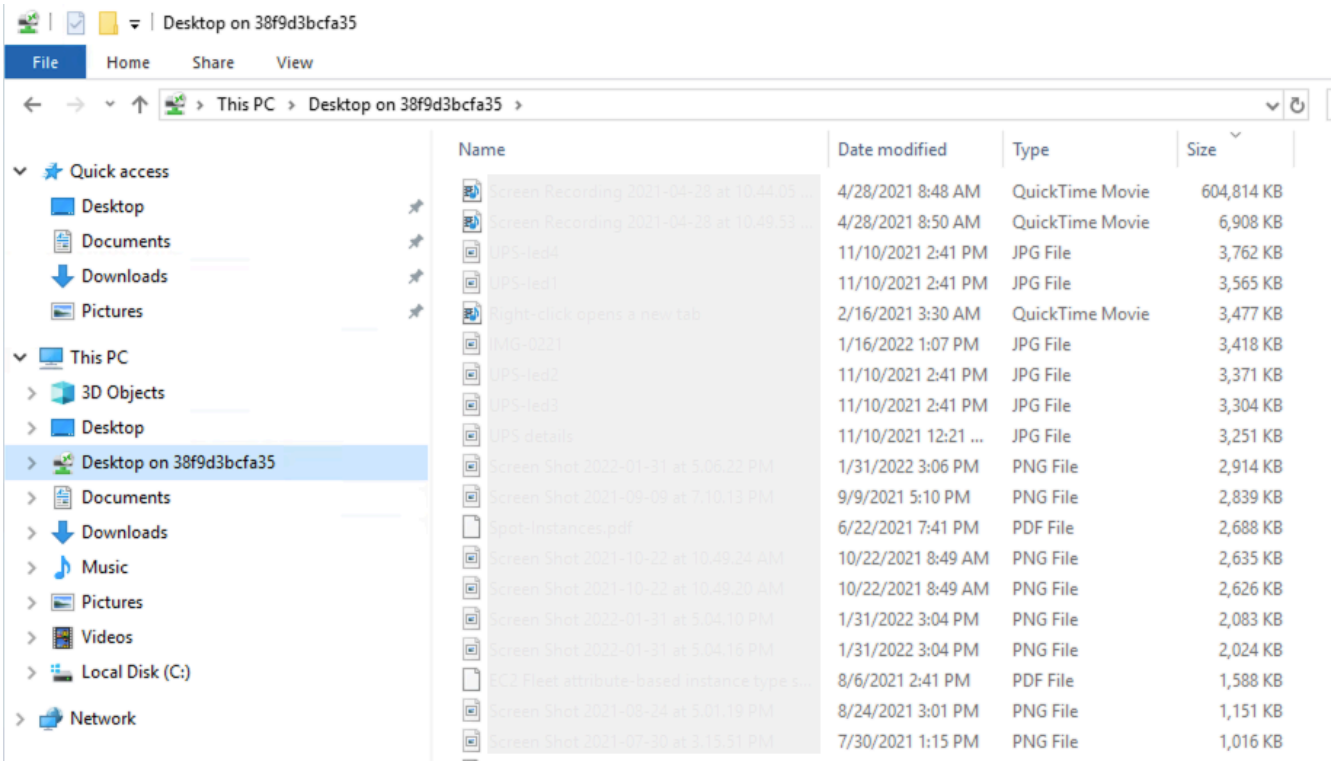
macOS X

Para mapear a unidade de sessão remota à pasta local em seu computador macOS X local

1. Abra o cliente de Conexão de Desktop Remoto.
2. Navegue até o arquivo RDP que você baixou do console do Amazon EC2 (ao se conectar inicialmente à instância) e arraste para o cliente Conexão de desktop remoto.
3. Clique com o botão direito do mouse no arquivo RDP e escolha Edit (Editar).
4. Selecione a guia Pastas e a caixa de seleção Redirecionar pastas.



5. Selecione o ícone + no canto inferior esquerdo, navegue até a pasta a ser mapeada e escolha Open (Abrir). Repita esta etapa para cada pasta a ser mapeada.
6. Escolha Salvar.
7. Selecione Connect (Conectar) para se conectar à sua instância do Windows. Você deverá inserir a senha.
8. Na instância, no Explorador de arquivos, expanda This PC (Este computador) e encontre a pasta compartilhada em que é possível acessar seus arquivos locais. Na captura de tela seguinte, a pasta Desktop no computador local foi mapeada para a unidade de sessão remota na instância.



Para obter mais informações sobre como disponibilizar dispositivos locais para uma sessão remota em um computador Mac, consulte Introdução ao cliente no Mac.

Conectar-se a uma instância do Amazon EC2 usando o Gerenciador de Sessões

O Session Manager é um recurso totalmente gerenciado do AWS Systems Manager para gerenciar suas instâncias do Amazon EC2 por meio de um shell interativo baseado no navegador com um clique ou por meio da AWS CLI. É possível usar o Gerenciador de sessões para iniciar uma sessão com uma instância na sua conta. Depois que a sessão for iniciada, você poderá executar comandos interativos na instância como faria para qualquer outro tipo de conexão. Para obter mais informações sobre o Gerenciador de sessões, consulte Gerenciador de sessões do AWS Systems Manager no Guia do usuário do AWS Systems Manager.

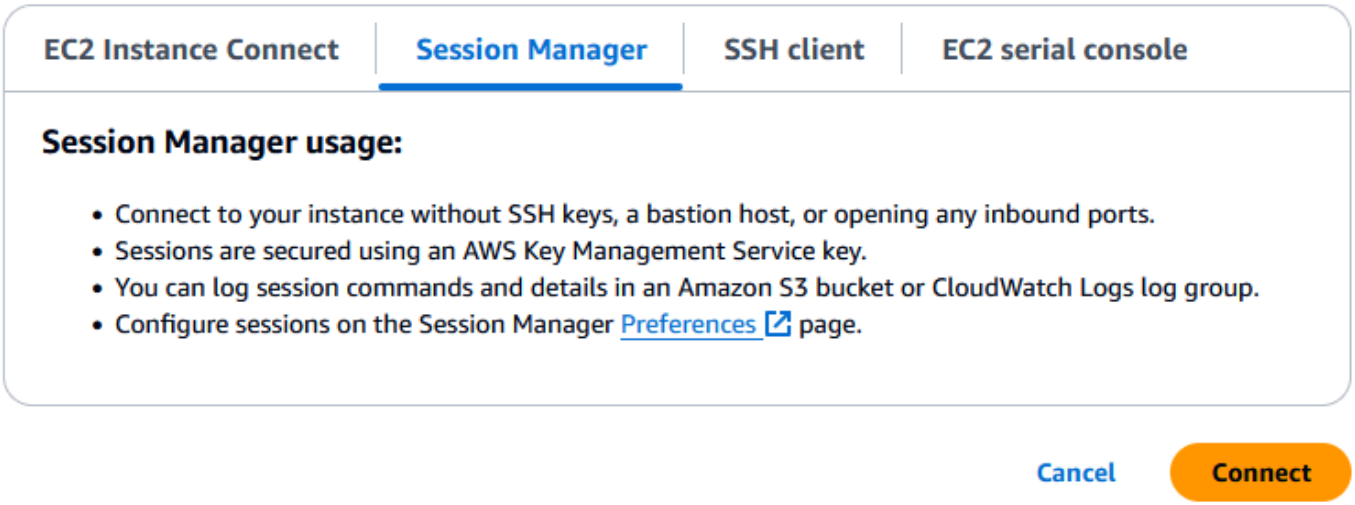
Pré-requisitos

Antes de tentar se conectar a uma instância usando o Gerenciador de Sessões, conclua as etapas de configuração necessárias. Por exemplo, a instância deve ser gerenciada pelo SSM e ter um

perfil do IAM com a política AmazonSSMManagedInstanceCore. Para mais informações, consulte Configurar o Session Manager.

Para se conectar a uma instância do Amazon EC2 usando o Gerenciador de Sessões no console do Amazon EC2

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância e escolha Connect (Conectar).
4. No método de conexão, escolha Gerenciador de Sessões.
5. Escolha Conectar para iniciar a sessão.



Solução de problemas

Se você receber um erro informando que você não tem autorização para executar uma ou mais ações do Gerenciador de Sessões (`ssm:command-name`), você precisará atualizar suas políticas para poder iniciar sessões no console do Amazon EC2. Para obter mais informações e instruções, consulte Início rápido de políticas padrão do IAM para o gerenciador de sessões no Guia do usuário doAWS Systems Manager.

Conecte-se à sua instância Linux usando um endereço IP público e o EC2 Instance Connect

O Amazon EC2 Instance Connect fornece uma forma segura de conexão com as instâncias do Linux com o Secure Shell (SSH). Com o EC2 Instance Connect, você usa políticas do AWS Identity

and Access Management (IAM) e principais para controlar o acesso de SSH às suas instâncias, eliminando a necessidade de compartilhar e gerenciar as chaves de SSH. Todas as solicitações de conexão usando o EC2 Instance Connect são registradas no AWS CloudTrail para que você possa auditar as solicitações de conexão.

É possível usar o EC2 Instance Connect para se conectar às instâncias usando o console do Amazon EC2 ou um cliente SSH da sua escolha.

Ao conectar-se a uma instância usando o EC2 Instance Connect, a API do EC2 Instance Connect envia por push uma chave pública SSH para os metadados da instância, onde ela permanece por 60 segundos. A política do IAM anexada ao usuário autoriza o usuário a enviar por push a chave pública para os metadados da instância. O daemon SSH usa `AuthorizedKeysCommand` e `AuthorizedKeysCommandUser`, que são configurados quando o EC2 Instance Connect é instalado, para procurar a chave pública dos metadados da instância para autenticação e conectar você à instância.

> **Tip**
>
> O EC2 Instance Connect é uma das opções para se conectar a instâncias do Linux. Para obter outras opções, consulte Conectar-se à instância do Linux usando SSH. Para se conectar a uma instância do Windows, consulte Conectar-se à instância do Windows no usando RDP.

Preços

O EC2 Instance Connect está disponível sem custo adicional.

Disponibilidade de regiões

O EC2 Instance Connect está disponível em todas as Regiões da AWS, exceto na região Ásia-Pacífico (Malásia). Ele não é compatível em zonas locais.

Conteúdo

- Tutorial: Concluir a configuração necessária para se conectar à sua instância usando o EC2 Instance Connect
- Pré-requisitos para o EC2 Instance Connect
- Conceder permissões do IAM para o EC2 Instance Connect
- Instalar o EC2 Instance Connect nas suas instâncias do EC2

- Conectar-se à instância do Linux usando EC2 Instance Connect
- Desinstalar o EC2 Instance Connect

Para obter uma postagem de blog que discute como melhorar a segurança de bastion hosts usando o EC2 Instance Connect, consulte Proteção dos seus bastion hosts com o Amazon EC2 Instance Connect.

Tutorial: Concluir a configuração necessária para se conectar à sua instância usando o EC2 Instance Connect

Para se conectar à sua instância usando o EC2 Instance Connect no console do Amazon EC2, primeiro é necessário concluir a configuração de pré-requisito que permitirá que você se conecte com sucesso à sua instância. O objetivo deste tutorial é orientar você pelas tarefas de conclusão da configuração de pré-requisitos.

Visão geral do tutorial

Nesse tutorial, você deverá concluir as seguintes quatro tarefas:

- Tarefa 1: conceder as permissões necessárias para usar o EC2 Instance Connect

  Primeiro, você criará uma política do IAM que contenha as permissões do IAM que permitem que você envie uma chave pública para os metadados da instância. Você anexará essa política à sua identidade (usuário, grupo de usuários ou perfil) do IAM para que sua identidade do IAM receba essas permissões.
- Tarefa 2: permitir tráfego de entrada do serviço EC2 Instance Connect para a instância

  Em seguida, você criará um grupo de segurança que permita o tráfego do EC2 Instance Connect para sua instância. Isso é necessário quando você usa o EC2 Instance Connect no console do Amazon EC2 para se conectar à sua instância.
- Tarefa 3: iniciar sua instância

  Em seguida, você iniciará uma instância do EC2 usando uma AMI pré-instalada com o EC2 Instance Connect e adicionará o grupo de segurança que criou na etapa anterior.
- Tarefa 4: conectar à sua instância

  Por fim, você usará o EC2 Instance Connect no console do Amazon EC2 para se conectar à sua instância. Se você conseguir se conectar, poderá ter certeza de que a configuração de pré-requisito concluída nas Tarefas 1, 2 e 3 foi bem-sucedida.

Tarefa 1: conceder as permissões necessárias para usar o EC2 Instance Connect

Ao conectar-se a uma instância usando o EC2 Instance Connect, a API do EC2 Instance Connect envia por push uma chave pública SSH para os metadados da instância, onde ela permanece por 60 segundos. É necessário ter uma política do IAM anexada à sua identidade do IAM (usuário, grupo de usuários ou função) para fornecer a permissão necessária para enviar por push a chave pública para os metadados da instância.

Objetivo da tarefa

Você criará a política do IAM que concede a permissão necessária para enviar por push a chave pública para a instância. A ação específica a ser permitida é `ec2-instance-connect:SendSSHPublicKey`. Você também deve permitir a ação `ec2:DescribeInstances` para poder visualizar e selecionar sua instância no console do Amazon EC2.

Depois de criar a política, você anexará a política à sua identidade do IAM (usuário, grupo de usuários ou perfil) para que sua identidade do IAM receba as permissões.

Você criará uma política configurada da seguinte forma:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": "ec2-instance-connect:SendSSHPublicKey",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:DescribeInstances",
            "Resource": "*"
        }
    ]
}
```

> **Important**
>
> A política do IAM criada neste tutorial é uma política altamente permissiva. Ela permite que você se conecte a qualquer instância usando qualquer nome de usuário da AMI. Estamos usando essa política altamente permissiva para manter o tutorial simples e focado nas configurações específicas que este tutorial está ensinando. No entanto, em um ambiente de produção, recomendamos que sua política do IAM seja configurada para fornecer permissões com privilégios mínimos. Para obter exemplos de políticas do IAM, consulte Conceder permissões do IAM para o EC2 Instance Connect.

Para criar e anexar uma política do IAM que permita a você usar o EC2 Instance Connect para se conectar às suas instâncias

1. Crie primeiro a política do IAM
   a. Abra o console do IAM em https://console.aws.amazon.com/iam/.
   b. No painel de navegação, escolha Policies.
   c. Selecione Criar política.
   d. Na página Especificar permissão, faça o seguinte:
      i. Em Serviço, escolha EC2 Instance Connect.
      ii. Em Ações permitidas, no campo de pesquisa, comece a digitar **send** para mostrar as ações relevantes e selecione SendSSHPublicKey.
      iii. Em Recursos, escolha Todos. Para um ambiente de produção, recomendamos especificar a instância pelo ARN, mas, neste tutorial, você está permitindo todas as instâncias.
      iv. Escolha Add more permissions (Adicionar mais permissões).
      v. Em Serviço, escolha EC2.
      vi. Em Ações permitidas, no campo de pesquisa, comece a digitar **describein** para mostrar as ações relevantes e selecione DescribeInstances.
      vii. Escolha Próximo.
   e. Na página Revisar e criar, faça o seguinte:
      i. Em Policy Name (Nome da política), digite um nome para a política.
      ii. Escolha Criar política.

2. Em seguida, anexe a política à sua identidade

   a. No console do IAM, no painel de navegação, escolha Policies (Políticas).

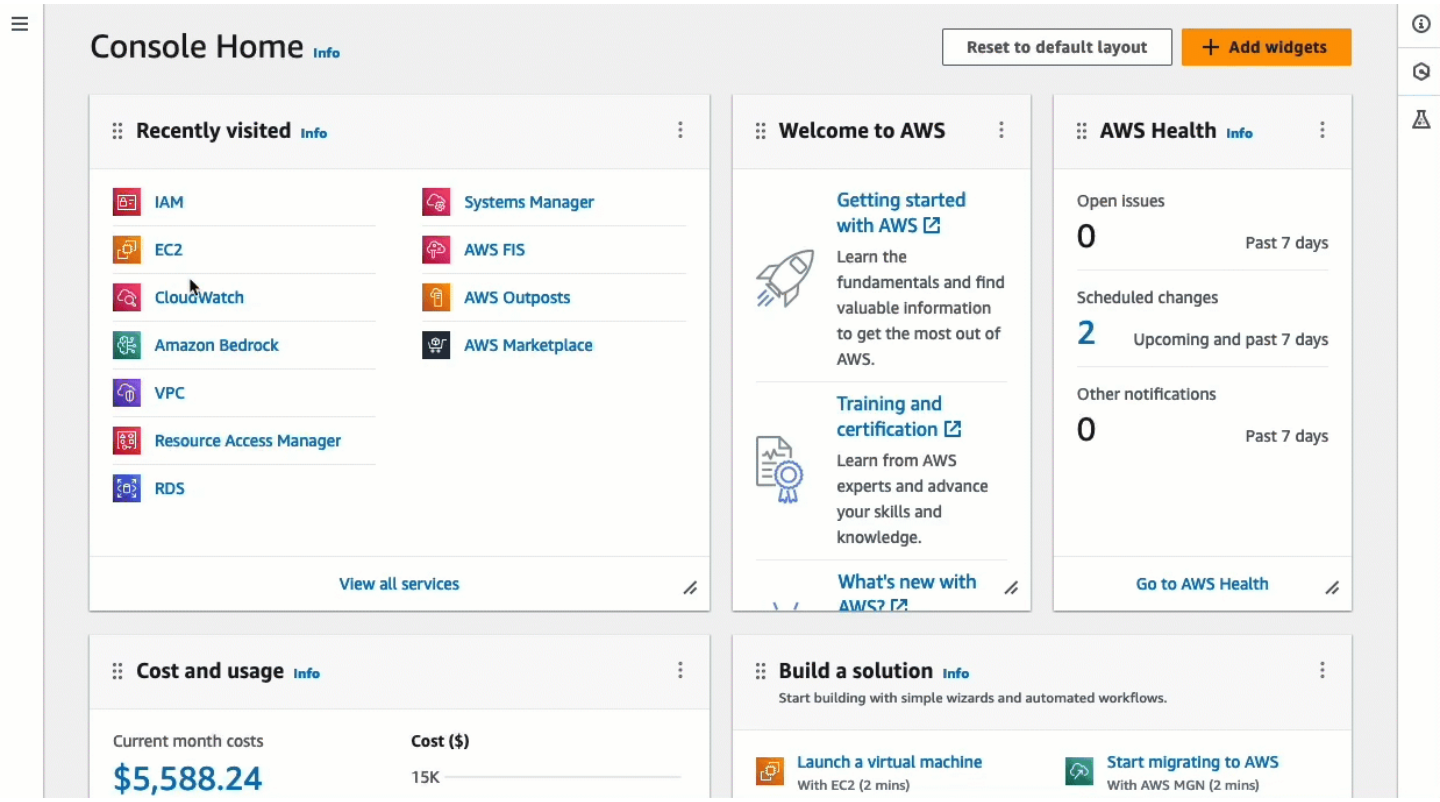
   b. Na lista de políticas, selecione o botão de seleção ao lado do nome da política que você criou. É possível usar a caixa de pesquisa para filtrar a lista de políticas.

   c. Clique em Actions (Ações) e em Attach (Associar).

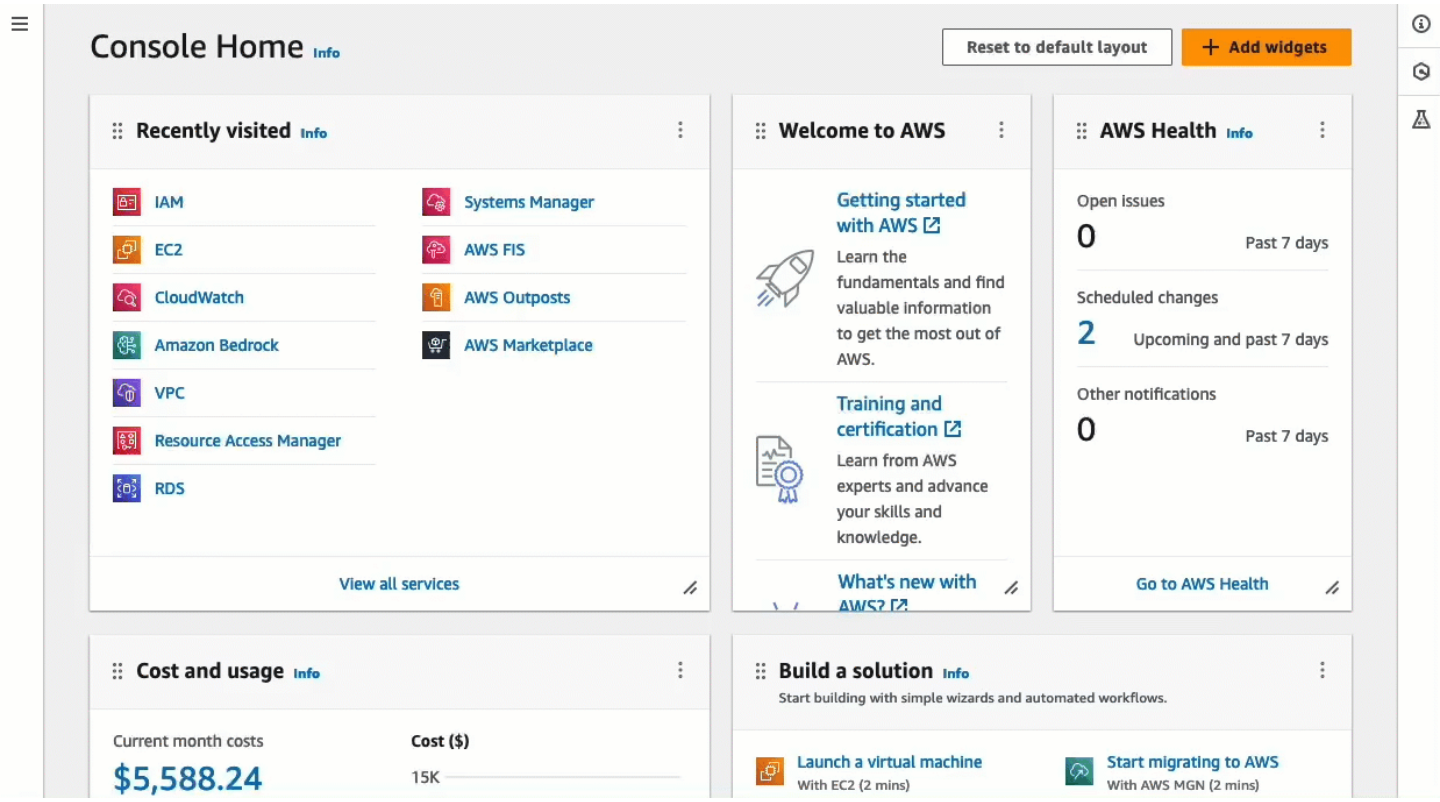
   d. Em Entidades do IAM, marque a caixa de seleção ao lado da sua identidade (usuário, grupo de usuários ou perfil). É possível usar a caixa de pesquisa para filtrar a lista de identidades.

   e. Escolha Anexar política.

Visualizar uma animação: criar uma política do IAM



Visualizar uma animação: anexar uma política do IAM



Tarefa 2: permitir tráfego de entrada do serviço EC2 Instance Connect para a instância

Quando você usa o EC2 Instance Connect no console do Amazon EC2 para se conectar a uma instância, o tráfego que deve ser permitido para chegar à instância é o tráfego do serviço do EC2 Instance Connect. Isso é diferente de se conectar do seu computador local a uma instância; nesse caso, você deverá permitir o tráfego do seu computador local para sua instância. Para permitir o tráfego do EC2 Instance Connect, é necessário criar um grupo de segurança que permita tráfego SSH de entrada da faixa de endereços IP para o serviço do EC2 Instance Connect.

A AWS usa listas de prefixos para gerenciar intervalos de endereços IP. Os nomes das listas de prefixos do EC2 Instance Connect são os seguintes, com a *`região`* substituída pelo código da região:

- Nome da lista de prefixos IPv4: `com.amazonaws.`*`region`*`.ec2-instance-connect`
- Nome da lista de prefixos IPv6: `com.amazonaws.`*`region`*`.ipv6.ec2-instance-connect`

Objetivo da tarefa

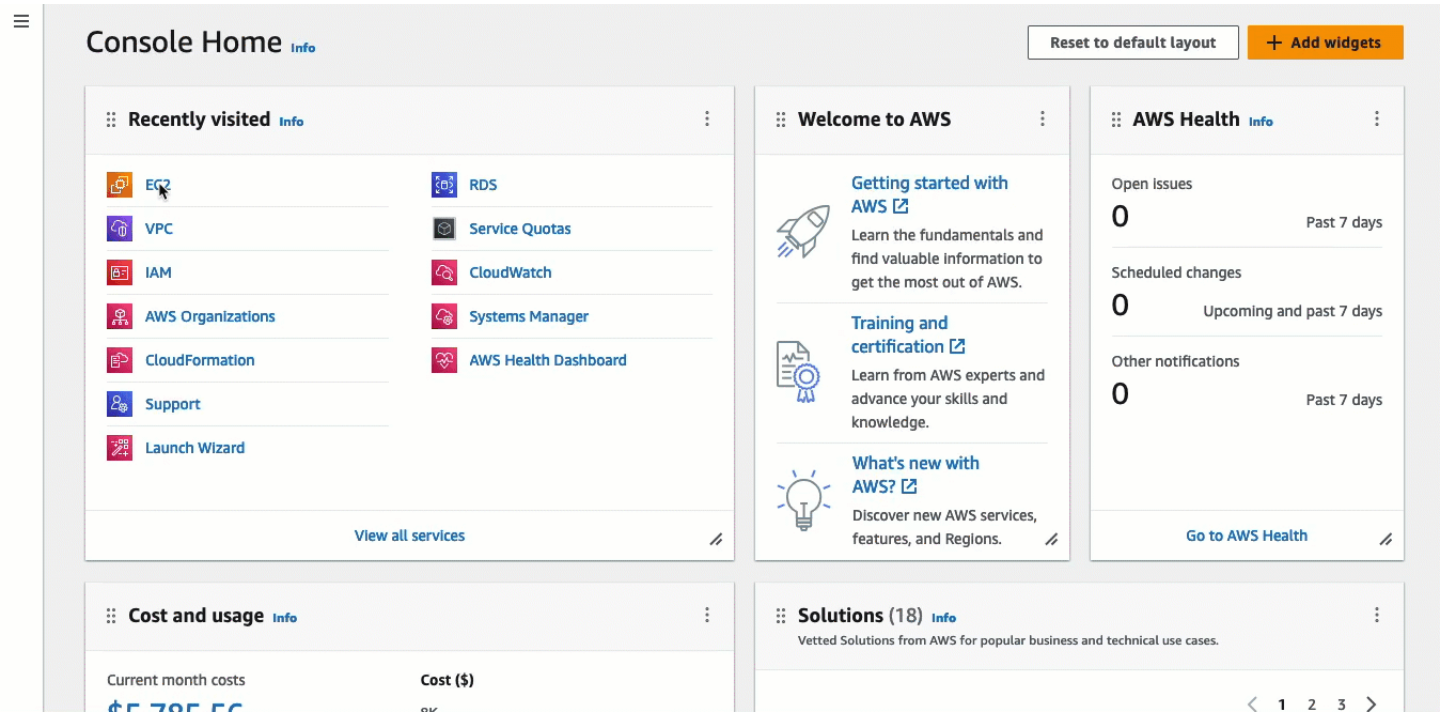
Você criará um grupo de segurança que permite tráfego SSH de entrada na porta 22 da lista de prefixos IPv4 na região em que sua instância está localizada.

Para criar um grupo de segurança que permita tráfego de entrada do serviço do EC2 Instance Connect para sua instância

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 Criar grupo de segurança.
4. Em Basic details (Detalhes básicos), faça o seguinte:
   a. Em Nome do grupo de segurança, insira um nome que faça sentido para o grupo de segurança.
   b. Em Descrição, insira uma descrição para o grupo de segurança.
5. Em Regras de entrada, faça o seguinte:
   a. Escolha Adicionar regra.
   b. Para Tipo, escolha SSH.
   c. Em Origem, mantenha a opção Personalizada.
   d. No campo ao lado de Origem, selecione a lista de prefixos do EC2 Instance Connect.

      Por exemplo, se sua instância estiver localizada na região Leste dos EUA (Norte da Virgínia) (`us-east-1`) e seus usuários se conectarão ao seu endereço IPv4 público, escolha a seguinte lista de prefixos: com.amazonaws.us-east-1.ec2-instance-connect
6. Escolha Criar grupo de segurança.

Visualizar uma animação: criar um grupo de segurança



Tarefa 3: iniciar sua instância

Ao iniciar uma instância, especifique uma AMI que contenha as informações necessárias para iniciá-la. É possível optar por iniciar uma instância com ou sem o EC2 Instance Connect pré-instalado. Nessa tarefa, especificamos uma AMI que é fornecida pré-instalada com o EC2 Instance Connect.

Se você iniciar sua instância sem o EC2 Instance Connect pré-instalado e quiser usar o EC2 Instance Connect para se conectar à sua instância, precisará executar etapas adicionais de configuração. Essas etapas estão fora do escopo deste tutorial.

Objetivo da tarefa

Você iniciará uma instância com a AMI do Amazon Linux 2023, que é fornecida pré-instalada com o EC2 Instance Connect. Você também especificará o grupo de segurança que criou anteriormente para poder usar o EC2 Instance Connect no console do Amazon EC2 para se conectar à sua instância. Como você usará o EC2 Instance Connect para se conectar à sua instância, que envia uma chave pública aos metadados da sua instância, não será necessário especificar uma chave SSH ao executar sua instância.

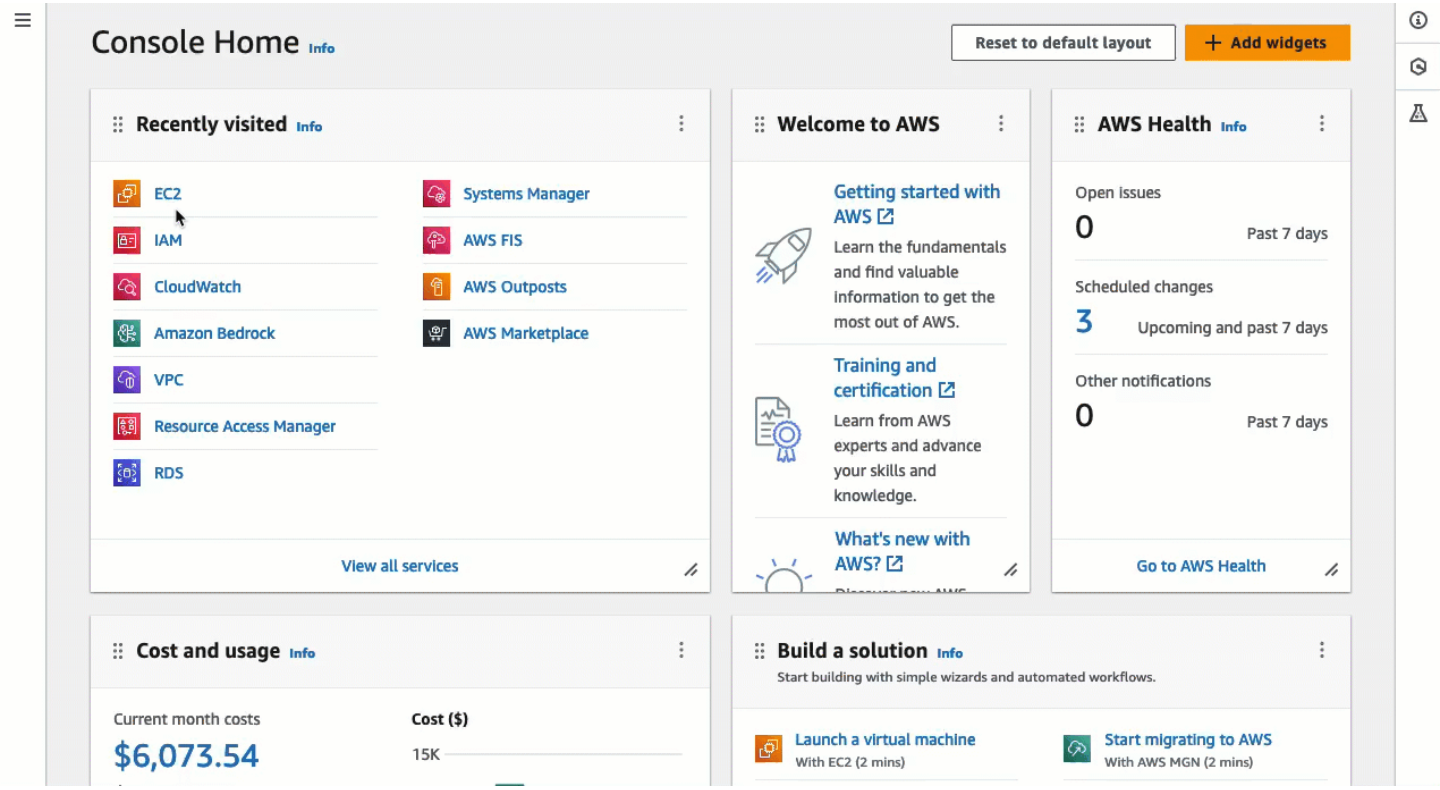
Para iniciar uma instância que pode usar o EC2 Instance Connect no console do Amazon EC2 para conexão

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 da AWS atual será exibida (por exemplo, Irlanda). Selecione uma região na qual a instância será iniciada. Essa escolha é importante porque você criou um grupo de segurança que permite tráfego para uma região específica. Por isso, é necessário selecionar a mesma região na qual a instância será executada.
3. No painel do console do Amazon EC2, selecione Launch instance (Executar instância).
4. (Opcional) Em Name and tags (Nome e tags), para Name (Nome), insira um nome descritivo para a instância.
5. Em Imagens de aplicações e sistemas operacionais (imagem de máquina da Amazon), escolha Início rápido. O Amazon Linux é selecionado por padrão. Em Imagem de máquina da Amazon (AMI), a opção AMI do Amazon Linux 2023 é selecionada por padrão. Mantenha a seleção padrão para essa tarefa.
6. Em Tipo de instância, para Tipo de instância, mantenha a seleção padrão ou escolha um tipo de instância diferente.
7. Em Par de chaves (login), em Nome do par de chaves, escolha Continuar sem um par de chaves (não recomendado). Quando você usa o EC2 Instance Connect para se conectar a uma instância, o EC2 Instance Connect envia um par de chaves para os metadados da instância, e é esse par de chaves que é usado para a conexão.
8. Em Network settings (Configurações de rede), faça o seguinte:
   a. Em Atribuir IP público automaticamente, mantenha a opçaõ Habilitar.

      > **Note**
      >
      > Para usar o EC2 Instance Connect no console do Amazon EC2 para se conectar a uma instância, a instância deve ter um endereço IPv4 público ou IPv6.

   b. Em Firewall (grupos de segurança), escolha Selecionar grupo de segurança existente.
   c. Em Grupos de segurança comuns, escolha o grupo de segurança criado anteriormente.
9. No painel Resumo painel, escolha Iniciar instância.

Visualizar uma animação: iniciar sua instância



Tarefa 4: conectar à sua instância

Ao conectar-se a uma instância usando o EC2 Instance Connect, a API do EC2 Instance Connect envia por push uma chave pública SSH para os metadados da instância, onde ela permanece por 60 segundos. O daemon SSH usa `AuthorizedKeysCommand` e `AuthorizedKeysCommandUser` para procurar a chave pública nos metadados da instância para autenticação e conectar você à instância.

Objetivo da tarefa

Nessa tarefa, você se conectará à sua instância usando o EC2 Instance Connect no console do Amazon EC2. Se você concluiu os pré-requisitos das Tarefas 1, 2 e 3, a conexão deverá ser bem-sucedida.

Etapas para se conectar à sua instância

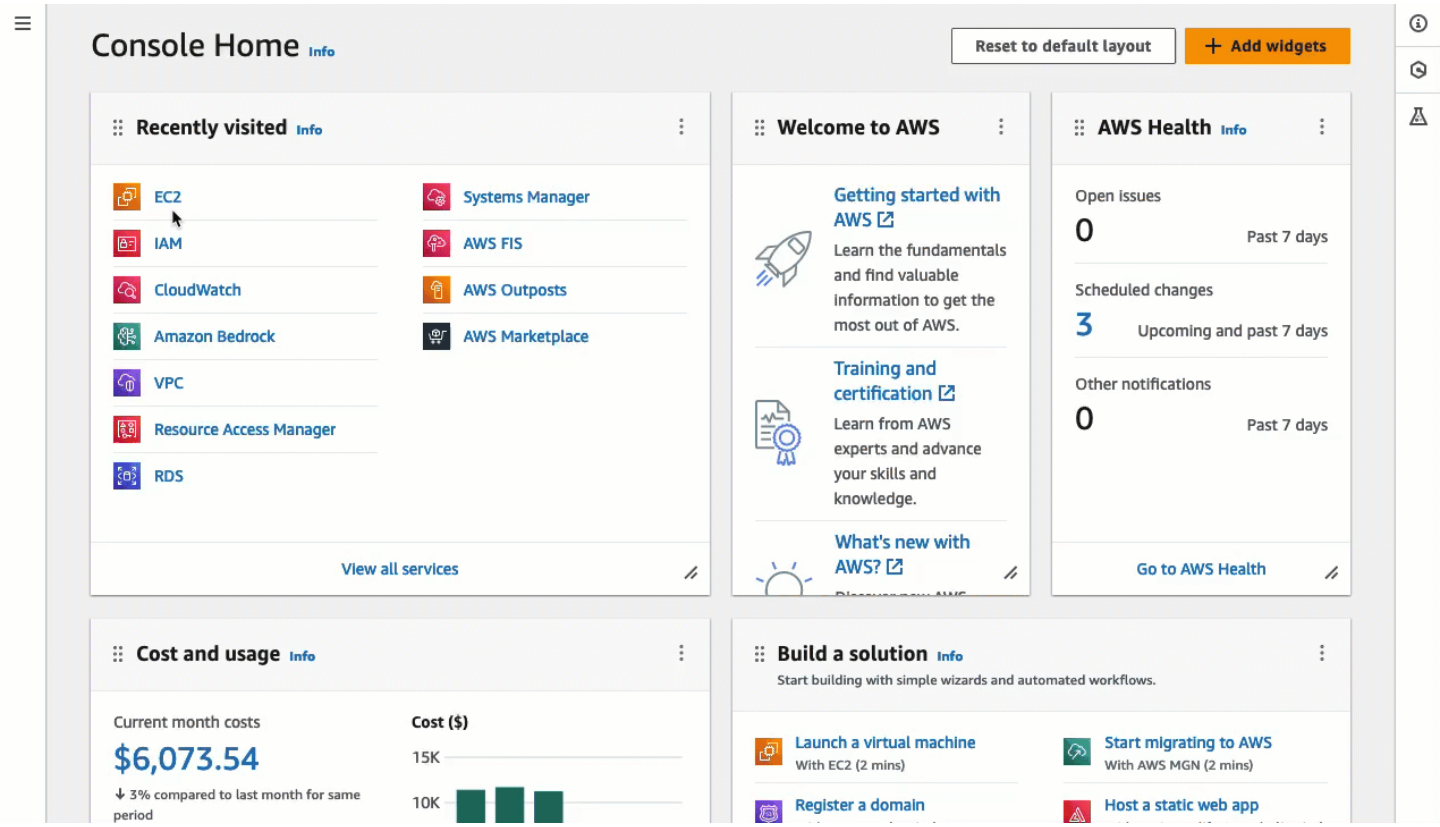
Use as etapas a seguir para se conectar à sua instância. Para visualizar uma animação dessas etapas, consulte Visualizar uma animação: conectar à sua instância.

Para conectar uma instância usando o EC2 Instance Connect no console do Amazon EC2

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 da AWS atual será exibida (por exemplo, Irlanda). Selecione a região na qual a instância está localizada.
3. No painel de navegação, escolha Instâncias.
4. Selecione a instância e escolha Conectar.
5. Escolha a guia EC2 Instance Connect.
6. Escolha Conectar usando um IP público.
7. Selecione Conectar.

   Uma janela de terminal abrirá no navegador e você estará conectado à sua instância.

Visualizar uma animação: conectar à sua instância



Pré-requisitos para o EC2 Instance Connect

Veja a seguir os pré-requisitos para a instalação e o uso do EC2 Instance Connect:

- Instalar o EC2 Instance Connect
- Garantir a conectividade da rede
- Permitir tráfego SSH de entrada
- Conceder permissões
- Instalar um cliente SSH no computador local
- Atender a requisitos de nome de usuário

Instalar o EC2 Instance Connect

Para usar o EC2 Instance Connect para se conectar a uma instância, a instância deve ter o EC2 Instance Connect instalado. É possível iniciar a instância usando uma AMI que é fornecida pré-instalada com o EC2 Instance Connect ou instalar o EC2 Instance Connect em instâncias que são iniciadas com AMIs compatíveis. Para obter mais informações, consulte Instalar o EC2 Instance Connect nas suas instâncias do EC2.

Garantir a conectividade da rede

As instâncias podem ser configuradas para permitir que os usuários conectem-se à sua instância pela Internet ou por meio do endereço IP privado da instância. Dependendo de como seus usuários forem conectar-se à sua instância usando o EC2 Instance Connect, será necessário configurar o seguinte acesso à rede:

- Se os usuários forem se conectar à sua instância pela Internet, a instância deverá ter um endereço público IPv4 ou IPv6 e estar em uma sub-rede pública com uma rota para a Internet. Se você não modificou sua sub-rede pública padrão, ela contém uma rota para a Internet somente para IPv4, e não para IPv6. Para obter mais informações, consulte Habilitar o acesso à internet usando gateways da internet no Guia do usuário do Amazon VPC.
- Caso seus usuários forem se conectar à sua instância por meio do endereço IPv4 privado da instância, você deverá estabelecer uma conectividade de rede privada com sua VPC por meio do AWS Direct Connect, do AWS Site-to-Site VPN ou do emparelhamento da VPC, para que os usuários possam acessar o endereço IP privado da instância.

Se a instância não tiver um endereço IPv4 público ou um endereço IPv6 e você preferir não configurar o acesso à rede como descrito acima, considere o EC2 Instance Connect Endpoint como uma alternativa ao EC2 Instance Connect. Com o EC2 Instance Connect Endpoint, você pode se conectar a uma instância usando SSH ou RDP mesmo que a instância não tenha um endereço

um IPv4 público ou um endereço IPv6. Para obter mais informações, consulte Conectar-se à sua instância do Linux usando o console do Amazon EC2.

Permitir tráfego SSH de entrada

Ao usar o console do Amazon EC2 para se conectar a uma instância

Quando usuários se conectam a uma instância usando o console do Amazon EC2 o tráfego que deve ser permitido para chegar à instância é o tráfego do serviço do EC2 Instance Connect. O serviço é identificado por intervalos de endereços IP específicos, que a AWS gerencia por meio de listas de prefixos. Você deve criar um grupo de segurança que permita tráfego de SSH de entrada do serviço do EC2 Instance Connect. Para configurar isso, para a regra de entrada, no campo ao lado de Origem, selecione a lista de prefixos do EC2 Instance Connect.

A AWS fornece diferentes listas de prefixo gerenciadas para endereços IPv4 e IPv6 para cada região. Os nomes das listas de prefixos do EC2 Instance Connect são os seguintes, com a *região* substituída pelo código da região:

- Nome da lista de prefixos IPv4: `com.amazonaws.region.ec2-instance-connect`
- Nome da lista de prefixos IPv6: `com.amazonaws.region.ipv6.ec2-instance-connect`

Para obter instruções sobre a criação do grupo de segurança, consulte Tarefa 2: permitir tráfego de entrada do serviço EC2 Instance Connect para a instância. Para obter mais informações, consulte AWS-managed prefix lists disponíveis no Guia do usuário do Amazon VPC.

Ao usar a CLI ou SSH para conectar a uma instância

Certifique-se de que o grupo de segurança associado à sua instância permita tráfego SSH de entrada na porta 22 a partir do seu endereço IP ou da rede. O grupo de segurança padrão para a VPC não permite o tráfego SSH de entrada por padrão. O grupo de segurança criado pelo assistente de inicialização de instâncias permite o tráfego SSH de entrada por padrão. Para obter mais informações, consulte Regras para se conectar a instâncias pelo computador.

Conceder permissões

Você deve conceder as permissões necessárias a cada usuário do IAM que usará o EC2 Instance Connect para se conectar a uma instância. Para obter mais informações, consulte Conceder permissões do IAM para o EC2 Instance Connect.

Instalar um cliente SSH no computador local

Caso os usuários utilizem SSH para se conectar, eles devem garantir que o computador local tenha um cliente SSH.

É muito provável que o computador local do usuário tenha um cliente SSH instalado por padrão. É possível verificar se existe um cliente SSH digitando ssh na linha de comando. Se o computador local não reconhecer o comando, será preciso instalar um cliente SSH. Para obter informações sobre como instalar um cliente SSH no Linux ou macOS X, consulte http://www.openssh.com. Para obter informações sobre como instalar um cliente SSH no Windows 10, consulte OpenSSH no Windows.

Não haverá necessidade de instalar um cliente SSH em um computador local se os usuários só usarem o console do Amazon EC2 para se conectarem a uma instância.

Atender a requisitos de nome de usuário

Quando o EC2 Instance Connect for usado para conexão com uma instância, o nome de usuário deverá atender aos seguintes requisitos:

- Primeiro caractere: deve ser uma letra (`A-Z` ou `a-z`), um dígito (`0-9`) ou um sublinhado (`_`)
- Caracteres subsequentes: podem ser letras (`A-Z`, `a-z`), dígitos (`0-9`) ou os seguintes caracteres: `@ . _ -`
- Tamanho mínimo: 1 caractere
- Tamanho máximo: 31 caracteres

Conceder permissões do IAM para o EC2 Instance Connect

Para se conectar a uma instância usando o EC2 Instance Connect, é necessário criar uma política do IAM que conceda permissões aos usuários para as ações e condições a seguir:

- Ação `ec2-instance-connect:SendSSHPublicKey`: concede permissão para enviar por push a chave pública a uma instância.
- Condição `ec2:osuser`: especifica o nome do usuário do sistema operacional que pode enviar por push a chave pública a uma instância. Use o nome de usuário padrão da AMI que você usou para iniciar a instância. O nome de usuário padrão para o AL2023 e o Amazon Linux 2 é `ec2-user` e, para o Ubuntu, é `ubuntu`.
- Ação `ec2:DescribeInstances`: exigida ao usar o console do EC2, pois o wrapper chama essa ação. Os usuários talvez já tenham permissão para chamar essa ação a partir de outra política.

- Ação `ec2:DescribeVpcs`: necessário ao se conectar a um endereço IPv6.

Considere restringir o acesso a instâncias do EC2 específicas. Caso contrário, todas as entidades principais do IAM com permissão para ação `ec2-instance-connect:SendSSHPublicKey` poderão conectar a todas as instâncias do EC2. É possível restringir o acesso especificando ARNs de recursos ou usando tags de recurso como chaves de condição.

Para obter mais informações, consulte Ações, recursos e chaves de condição para o Amazon EC2 Instance Connect.

Para obter informações sobre a criação de políticas do IAM, consulte Criação de políticas do IAM, no Manual do usuário do IAM.

Permitir que os usuários conectem-se a instâncias específicas

A política do IAM a seguir concede permissão para se conectar a instâncias específicas, identificadas por seus ARNs de recursos.

No exemplo de política do IAM a seguir, as ações e condições abaixo são especificadas:

- A ação `ec2-instance-connect:SendSSHPublicKey` concede aos usuários permissão para se conectar a duas instâncias, especificadas pelos ARNs do recurso. Para conceder aos usuários permissão para se conectar a todas as instâncias do EC2, substitua os ARNs do recurso pelo curinga `*`.
- A condição `ec2:osuser` concede permissão para se conectar às instâncias somente se o nome do *`ami-user`* for especificado durante a conexão.
- A ação `ec2:DescribeInstances` é especificada para conceder permissão aos usuários que usarão o console para se conectar às suas instâncias. Caso seus usuários utilizem somente um cliente SSH para se conectar às suas instâncias, é possível omitir `ec2:DescribeInstances`. Observe que as ações da API `ec2:Describe*` não oferecem suporte a permissões no nível do recurso. Portanto, o caractere curinga `*` é necessário no elemento `Resource`.
- A ação `ec2:DescribeVpcs` é especificada para conceder permissão aos usuários que usarão o console para se conectar às suas instâncias usando um endereço IPv6. Se seus usuários usarão somente um endereço IPv4, você pode omitir `ec2:DescribeVpcs`. Observe que as ações da API `ec2:Describe*` não oferecem suporte a permissões no nível do recurso. Portanto, o caractere curinga `*` é necessário no elemento `Resource`.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": "ec2-instance-connect:SendSSHPublicKey",
            "Resource": [
                "arn:aws:ec2:us-
east-1:111122223333:instance/i-1234567890abcdef0",
                "arn:aws:ec2:us-east-1:111122223333:instance/i-0598c7d356eba48d7"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:osuser": "ami-username"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeVpcs"
            ],
            "Resource": "*"
        }
    ]
}
```

Permitir que os usuários conectem-se a instâncias com tags específicas

O controle de acesso por atributo (ABAC) é uma estratégia de autorização que define permissões de acordo com tags que podem ser anexadas a usuários e a recursos da AWS. É possível usar tags de recurso para controlar o acesso a uma instância. Para obter mais informações sobre como usar tags para controlar o acesso aos recursos da AWS, consulte Controle do acesso aos recursos da AWS no Guia do usuário do IAM.

No exemplo de política do IAM a seguir, a ação `ec2-instance-connect:SendSSHPublicKey` concede aos usuários permissão para se conectar a qualquer instância (indicada pelo curinga `*` no

ARN do recurso), desde que a instância tenha uma tag de recurso com key=`tag-key` e value=`tag-value`.

A ação `ec2:DescribeInstances` é especificada para conceder permissão aos usuários que usarão o console para se conectar às suas instâncias. Caso seus usuários usem somente um cliente SSH para se conectarem às suas instâncias, será possível omitir `ec2:DescribeInstances`. Observe que as ações da API `ec2:Describe*` não oferecem suporte a permissões no nível do recurso. Portanto, o caractere curinga `*` é necessário no elemento `Resource`.

A ação `ec2:DescribeVpcs` é especificada para conceder permissão aos usuários que usarão o console para se conectar às suas instâncias usando um endereço IPv6. Se seus usuários usarão somente um endereço IPv4, você pode omitir `ec2:DescribeVpcs`. Observe que as ações da API `ec2:Describe*` não oferecem suporte a permissões no nível do recurso. Portanto, o caractere curinga `*` é necessário no elemento `Resource`.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": "ec2-instance-connect:SendSSHPublicKey",
            "Resource": "arn:aws:ec2:us-east-1:111122223333:instance/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/tag-key": "tag-value"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeVpcs"
            ],
            "Resource": "*"
        }
    ]
}
```

Instalar o EC2 Instance Connect nas suas instâncias do EC2

Para conexão com uma instância do Linux usando o EC2 Instance Connect, a instância deve ter o EC2 Instance Connect instalado. Instalar o EC2 Instance Connect configura o daemon SSH na instância.

Para obter mais informações sobre o pacote do EC2 Instance Connect, consulte aws/aws-ec2-instance-connect-config no site do GitHub.

> **Note**
>
> Se você definiu as configurações de `AuthorizedKeysCommand` e `AuthorizedKeysCommandUser` para a autenticação SSH, a instalação do EC2 Instance Connect não as atualizará. Consequentemente, não é possível usar o EC2 Instance Connect.

Pré-requisitos de instalação

Antes de instalar o EC2 Instance Connect, verifique se você atende aos pré-requisitos a seguir.

- Verifique se a instância usa algum dos seguintes recursos:
  - Amazon Linux 2 anterior à versão 2.0.20190618 *
  - AMI mínima do AL2023 ou AMI otimizada para o Amazon ECS
  - CentOS Stream 8 e 9
  - macOS Sonoma anterior à versão 14.2.1, Ventura anterior à versão 13.6.3 e Monterey anterior à versão 12.7.2 *
  - Red Hat Enterprise Linux (RHEL) 8 e 9
  - Ubuntu 16.04 e 18.04 *

  > **Tip**
  >
  > * Para Amazon Linux 2, macOS e Ubuntu: se você iniciou sua instância usando uma versão posterior às listadas acima, o EC2 Instance Connect vem pré-instalado e nenhuma instalação manual é necessária.

- Verifique os pré-requisitos gerais para o EC2 Instance Connect.

  Para obter mais informações, consulte Pré-requisitos para o EC2 Instance Connect.

- Verifique os pré-requisitos para se conectar à sua instância usando um cliente SSH em sua máquina local.

  Para obter mais informações, consulte Conectar-se à instância do Linux usando SSH.

- Obtenha o ID da instância.

  É possível obter o ID da instância usando o console do Amazon EC2 (na coluna ID da instância). Se preferir, é possível usar o comando describe-instances (AWS CLI) ou Get-EC2Instance (AWS Tools for Windows PowerShell).

Instalar manualmente o EC2 Instance Connect

> **Note**
>
> Se você iniciar a instância usando uma das AMIs a seguir, o EC2 Instance Connect estará pré-instalado e será possível ignorar este procedimento:
>
> - AMI padrão do AL2023
> - Amazon Linux 2 2.0.20190618 ou posterior
> - macOS Sonoma 14.2.1 ou posterior
> - macOS Ventura 13.6.3 ou posterior
> - macOS Monterey 12.7.2 ou posterior
> - Ubuntu 20.04 ou posterior

Use um dos procedimentos a seguir para instalar o EC2 Instance Connect, dependendo do sistema operacional da instância.

Amazon Linux 2

Para instalar o EC2 Instance Connect em uma instância aberta com Amazon Linux 2

1. Conecte-se à sua instância usando SSH.

   Substitua o exemplo de valores no seguinte comando pelos seus valores: Use o par de chaves SSH atribuído à sua instância ao abri-la e o nome do usuário padrão da AMI usada para abrir a instância. Para o Amazon Linux 2, o nome do usuário padrão é `ec2-user`.

```
$ ssh -i my_ec2_private_key.pem ec2-user@ec2-a-b-c-d.us-
west-2.compute.amazonaws.com
```

Para obter mais informações sobre como se conectar à sua instância, consulte Conectar-se à instância do Linux usando um cliente SSH.

2. Instale o pacote EC2 Instance Connect na sua instância.

```
[ec2-user ~]$ sudo yum install ec2-instance-connect
```

Deverão estar visíveis três novos scripts na pasta `/opt/aws/bin/`:

```
eic_curl_authorized_keys
eic_parse_authorized_keys
eic_run_authorized_keys
```

3. (Opcional) Verifique se o EC2 Instance Connect foi instalando com êxito na sua instância.

```
[ec2-user ~]$ sudo less /etc/ssh/sshd_config
```

O EC2 Instance Connect foi instalado com êxito se as linhas `AuthorizedKeysCommand` e `AuthorizedKeysCommandUser` contiverem os seguintes valores:

```
AuthorizedKeysCommand /opt/aws/bin/eic_run_authorized_keys %u %f
AuthorizedKeysCommandUser ec2-instance-connect
```

- O `AuthorizedKeysCommand` define o script `eic_run_authorized_keys` para buscar as chaves nos metadados da instância
- `AuthorizedKeysCommandUser` O define o usuário do sistema como `ec2-instance-connect`

> **Note**
>
> Se você tiver previamente configurado `AuthorizedKeysCommand` e `AuthorizedKeysCommandUser`, a instalação do EC2 Instance Connect não mudará os valores e você não poderá usar o EC2 Instance Connect.

CentOS

Para instalar o EC2 Instance Connect em uma instância executada com o CentOS

1. Conecte-se à sua instância usando SSH.

   Substitua o exemplo de valores no seguinte comando pelos seus valores: Use o par de chaves SSH atribuído à sua instância ao abri-la e o nome do usuário padrão da AMI usada para abrir a instância. Para o CentOS, o nome de usuário padrão é `centos` ou `ec2-user`.

   ```
   $ ssh -i my_ec2_private_key.pem centos@ec2-a-b-c-d.us-
   west-2.compute.amazonaws.com
   ```

   Para obter mais informações sobre como se conectar à sua instância, consulte Conectar-se à instância do Linux usando um cliente SSH.

2. Se você usar um proxy HTTP ou HTTPS, defina o `http_proxy` ou as variáveis de ambiente `https_proxy` na sessão do shell atual.

   Se você não estiver usando um proxy, ignore esta etapa.

   - Para um servidor de proxy HTTP, execute os seguintes comandos:

     ```
     $ export http_proxy=http://hostname:port
     $ export https_proxy=http://hostname:port
     ```

   - Para um servidor de proxy HTTPS, execute os seguintes comandos:

     ```
     $ export http_proxy=https://hostname:port
     $ export https_proxy=https://hostname:port
     ```

3. Instale o pacote do EC2 Instance Connect na sua instância executando os comandos a seguir.

   Os arquivos de configuração do EC2 Instance Connect para CentOS são fornecidos em um pacote do Red Hat Package Manager (RPM), com pacotes do RPM diferentes para CentOS 8 e CentOS 9 e para tipos de instância executados em Intel/AMD (x86_64) ou ARM (AArch64).

   Use o bloco de comando para a arquitetura do seu sistema operacional e de CPU.

- CentOS 8

  Intel/AMD (x86_64)

  ```
  [ec2-user ~]$ mkdir /tmp/ec2-instance-connect
  [ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-
  west-2.s3.us-west-2.amazonaws.com/latest/linux_amd64/ec2-instance-
  connect-2.0.0-5.rhel8.x86_64.rpm -o /tmp/ec2-instance-connect/ec2-instance-
  connect.rpm
  [ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
  west-2.amazonaws.com/latest/linux_amd64/ec2-instance-connect-
  selinux-2.0.0-5.noarch.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect-
  selinux.rpm
  [ec2-user ~]$ sudo yum install -y /tmp/ec2-instance-connect/ec2-instance-
  connect.rpm /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
  ```

  ARM (AArch64)

  ```
  [ec2-user ~]$ mkdir /tmp/ec2-instance-connect
  [ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-
  west-2.s3.us-west-2.amazonaws.com/latest/linux_arm64/ec2-instance-
  connect-2.0.0-5.rhel8.aarch64.rpm -o /tmp/ec2-instance-connect/ec2-instance-
  connect.rpm
  [ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
  west-2.amazonaws.com/latest/linux_arm64/ec2-instance-connect-
  selinux-2.0.0-5.noarch.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect-
  selinux.rpm
  [ec2-user ~]$ sudo yum install -y /tmp/ec2-instance-connect/ec2-instance-
  connect.rpm /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
  ```

- CentOS 9

  Intel/AMD (x86_64)

  ```
  [ec2-user ~]$ mkdir /tmp/ec2-instance-connect
  [ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-
  west-2.s3.us-west-2.amazonaws.com/latest/linux_amd64/ec2-instance-
  connect-2.0.0-5.rhel9.x86_64.rpm -o /tmp/ec2-instance-connect/ec2-instance-
  connect.rpm
  [ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
  west-2.amazonaws.com/latest/linux_amd64/ec2-instance-connect-
  ```

```
selinux-2.0.0-5.noarch.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect-
selinux.rpm
[ec2-user ~]$ sudo yum install -y /tmp/ec2-instance-connect/ec2-instance-
connect.rpm /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
```

ARM (AArch64)

```
[ec2-user ~]$ mkdir /tmp/ec2-instance-connect
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-
west-2.s3.us-west-2.amazonaws.com/latest/linux_arm64/ec2-instance-
connect-2.0.0-5.rhel9.aarch64.rpm -o /tmp/ec2-instance-connect/ec2-instance-
connect.rpm
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
west-2.amazonaws.com/latest/linux_arm64/ec2-instance-connect-
selinux-2.0.0-5.noarch.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect-
selinux.rpm
[ec2-user ~]$ sudo yum install -y /tmp/ec2-instance-connect/ec2-instance-
connect.rpm /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
```

Deverá estar visível o seguinte novo script na pasta `/opt/aws/bin/`:

```
eic_run_authorized_keys
```

4. (Opcional) Verifique se o EC2 Instance Connect foi instalando com êxito na sua instância.

   - Para o CentOS 8:

     ```
     [ec2-user ~]$ sudo less /lib/systemd/system/sshd.service.d/ec2-instance-
     connect.conf
     ```

   - Para o CentOS 9:

     ```
     [ec2-user ~]$ sudo less /etc/ssh/sshd_config.d/60-ec2-instance-connect.conf
     ```

   O EC2 Instance Connect foi instalado com êxito se as linhas `AuthorizedKeysCommand` e `AuthorizedKeysCommandUser` contiverem os seguintes valores:

   ```
   AuthorizedKeysCommand /opt/aws/bin/eic_run_authorized_keys %u %f
   AuthorizedKeysCommandUser ec2-instance-connect
   ```

- O `AuthorizedKeysCommand` define o script `eic_run_authorized_keys` para buscar as chaves nos metadados da instância
- `AuthorizedKeysCommandUser` O define o usuário do sistema como `ec2-instance-connect`

> **Note**
>
> Se você tiver previamente configurado `AuthorizedKeysCommand` e `AuthorizedKeysCommandUser`, a instalação do EC2 Instance Connect não mudará os valores e você não poderá usar o EC2 Instance Connect.

macOS

Para instalar o EC2 Instance Connect em uma instância executada com o macOS

1. Conecte-se à sua instância usando SSH.

   Substitua o exemplo de valores no seguinte comando pelos seus valores: Use o par de chaves SSH atribuído à sua instância ao abri-la e o nome do usuário padrão da AMI usada para abrir a instância. Para instâncias macOS, o nome de usuário padrão é `ec2-user`.

   ```
   $ ssh -i my_ec2_private_key.pem ec2-user@ec2-a-b-c-d.us-
   west-2.compute.amazonaws.com
   ```

   Para obter mais informações sobre como se conectar à sua instância, consulte Conectar-se à instância do Linux usando um cliente SSH.

2. Atualize o Homebrew usando o seguinte comando. A atualização listará o software que o Homebrew conhece. O pacote do EC2 Instance Connect é fornecido via Homebrew em instâncias do macOS. Para obter mais informações, consulte Atualizar o sistema operacional e o software em instâncias Mac do Amazon EC2.

   ```
   [ec2-user ~]$ brew update
   ```

3. Instale o pacote EC2 Instance Connect na sua instância. Isso instalará o software e configurará o SSHD para usá-lo.

```
[ec2-user ~]$ brew install ec2-instance-connect
```

Deverá estar visível o seguinte novo script na pasta `/opt/aws/bin/`:

```
eic_run_authorized_keys
```

4. (Opcional) Verifique se o EC2 Instance Connect foi instalando com êxito na sua instância.

```
[ec2-user ~]$ sudo less /etc/ssh/sshd_config.d/60-ec2-instance-connect.conf
```

O EC2 Instance Connect foi instalado com êxito se as linhas `AuthorizedKeysCommand` e `AuthorizedKeysCommandUser` contiverem os seguintes valores:

```
AuthorizedKeysCommand /opt/aws/bin/eic_run_authorized_keys %u %f
AuthorizedKeysCommandUser ec2-instance-connect
```

- O `AuthorizedKeysCommand` define o script `eic_run_authorized_keys` para buscar as chaves nos metadados da instância
- `AuthorizedKeysCommandUser` O define o usuário do sistema como `ec2-instance-connect`

> **Note**
>
> Se você tiver previamente configurado `AuthorizedKeysCommand` e `AuthorizedKeysCommandUser`, a instalação do EC2 Instance Connect não mudará os valores e você não poderá usar o EC2 Instance Connect.

RHEL

Para instalar o EC2 Instance Connect em uma instância executada com o Red Hat Enterprise Linux (RHEL)

1. Conecte-se à sua instância usando SSH.

Substitua o exemplo de valores no seguinte comando pelos seus valores: Use o par de chaves SSH atribuído à sua instância ao abri-la e o nome do usuário padrão da AMI usada para abrir a instância. Para o RHEL, o nome de usuário padrão é `ec2-user` ou `root`.

```
$ ssh -i my_ec2_private_key.pem ec2-user@ec2-a-b-c-d.us-
west-2.compute.amazonaws.com
```

Para obter mais informações sobre como se conectar à sua instância, consulte Conectar-se à instância do Linux usando um cliente SSH.

2. Se você usar um proxy HTTP ou HTTPS, defina o `http_proxy` ou as variáveis de ambiente `https_proxy` na sessão do shell atual.

   Se você não estiver usando um proxy, ignore esta etapa.

   - Para um servidor de proxy HTTP, execute os seguintes comandos:

     ```
     $ export http_proxy=http://hostname:port
     $ export https_proxy=http://hostname:port
     ```

   - Para um servidor de proxy HTTPS, execute os seguintes comandos:

     ```
     $ export http_proxy=https://hostname:port
     $ export https_proxy=https://hostname:port
     ```

3. Instale o pacote do EC2 Instance Connect na sua instância executando os comandos a seguir.

   Os arquivos de configuração do EC2 Instance Connect para RHEL são fornecidos em um pacote do Red Hat Package Manager (RPM), com pacotes do RPM diferentes para RHEL 8 e RHEL 9 e para tipos de instância executados em Intel/AMD (x86_64) ou ARM (AArch64).

   Use o bloco de comando para a arquitetura do seu sistema operacional e de CPU.

   - RHEL 8

     Intel/AMD (x86_64)

     ```
     [ec2-user ~]$ mkdir /tmp/ec2-instance-connect
     [ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-
     west-2.s3.us-west-2.amazonaws.com/latest/linux_amd64/ec2-instance-
     ```

```
connect-2.0.0-5.rhel8.x86_64.rpm -o /tmp/ec2-instance-connect/ec2-instance-
connect.rpm
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
west-2.amazonaws.com/latest/linux_amd64/ec2-instance-connect-
selinux-2.0.0-5.noarch.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect-
selinux.rpm
[ec2-user ~]$ sudo yum install -y /tmp/ec2-instance-connect/ec2-instance-
connect.rpm /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
```

ARM (AArch64)

```
[ec2-user ~]$ mkdir /tmp/ec2-instance-connect
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-
west-2.s3.us-west-2.amazonaws.com/latest/linux_arm64/ec2-instance-
connect-2.0.0-5.rhel8.aarch64.rpm -o /tmp/ec2-instance-connect/ec2-instance-
connect.rpm
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
west-2.amazonaws.com/latest/linux_arm64/ec2-instance-connect-
selinux-2.0.0-5.noarch.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect-
selinux.rpm
[ec2-user ~]$ sudo yum install -y /tmp/ec2-instance-connect/ec2-instance-
connect.rpm /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
```

- RHEL 9

  Intel/AMD (x86_64)

```
[ec2-user ~]$ mkdir /tmp/ec2-instance-connect
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-
west-2.s3.us-west-2.amazonaws.com/latest/linux_amd64/ec2-instance-
connect-2.0.0-5.rhel9.x86_64.rpm -o /tmp/ec2-instance-connect/ec2-instance-
connect.rpm
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
west-2.amazonaws.com/latest/linux_amd64/ec2-instance-connect-
selinux-2.0.0-5.noarch.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect-
selinux.rpm
[ec2-user ~]$ sudo yum install -y /tmp/ec2-instance-connect/ec2-instance-
connect.rpm /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
```

  ARM (AArch64)

```
[ec2-user ~]$ mkdir /tmp/ec2-instance-connect
```

```
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-
west-2.s3.us-west-2.amazonaws.com/latest/linux_arm64/ec2-instance-
connect-2.0.0-5.rhel9.aarch64.rpm -o /tmp/ec2-instance-connect/ec2-instance-
connect.rpm
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
west-2.amazonaws.com/latest/linux_arm64/ec2-instance-connect-
selinux-2.0.0-5.noarch.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect-
selinux.rpm
[ec2-user ~]$ sudo yum install -y /tmp/ec2-instance-connect/ec2-instance-
connect.rpm /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
```

Deverá estar visível o seguinte novo script na pasta `/opt/aws/bin/`:

```
eic_run_authorized_keys
```

4. (Opcional) Verifique se o EC2 Instance Connect foi instalando com êxito na sua instância.

   - Para o RHEL 8:

     ```
     [ec2-user ~]$ sudo less /lib/systemd/system/sshd.service.d/ec2-instance-
     connect.conf
     ```

   - Para o RHEL 9:

     ```
     [ec2-user ~]$ sudo less /etc/ssh/sshd_config.d/60-ec2-instance-connect.conf
     ```

   O EC2 Instance Connect foi instalado com êxito se as linhas `AuthorizedKeysCommand` e `AuthorizedKeysCommandUser` contiverem os seguintes valores:

   ```
   AuthorizedKeysCommand /opt/aws/bin/eic_run_authorized_keys %u %f
   AuthorizedKeysCommandUser ec2-instance-connect
   ```

   - O `AuthorizedKeysCommand` define o script `eic_run_authorized_keys` para buscar as chaves nos metadados da instância
   - `AuthorizedKeysCommandUser` O define o usuário do sistema como `ec2-instance-connect`

> **Note**
>
> Se você tiver previamente configurado `AuthorizedKeysCommand` e `AuthorizedKeysCommandUser`, a instalação do EC2 Instance Connect não mudará os valores e você não poderá usar o EC2 Instance Connect.

Ubuntu

Para instalar o EC2 Instance Connect em uma instância aberta com Ubuntu 16.04 ou posterior

1. Conecte-se à sua instância usando SSH.

   Substitua o exemplo de valores no seguinte comando pelos seus valores: Use o par de chaves SSH atribuído à sua instância quando você a executou e use o nome de usuário padrão da AMI que você usou para iniciar sua instância. Para uma AMI Ubuntu, o nome de usuário é `ubuntu`.

   ```
   $ ssh -i my_ec2_private_key.pem ubuntu@ec2-a-b-c-d.us-
   west-2.compute.amazonaws.com
   ```

   Para obter mais informações sobre como se conectar à sua instância, consulte Conectar-se à instância do Linux usando um cliente SSH.

2. (Opcional) Garanta que sua instância tenha a AMI do Ubuntu mais recente.

   Execute os comandos a seguir para atualizar todos os pacotes na instância.

   ```
   ubuntu:~$ sudo apt-get update
   ```

   ```
   ubuntu:~$ sudo apt-get upgrade
   ```

3. Instale o pacote EC2 Instance Connect na sua instância.

   ```
   ubuntu:~$ sudo apt-get install ec2-instance-connect
   ```

   Deverão estar visíveis três novos scripts na pasta `/usr/share/ec2-instance-connect/`:

```
eic_curl_authorized_keys
eic_parse_authorized_keys
eic_run_authorized_keys
```

4. (Opcional) Verifique se o EC2 Instance Connect foi instalando com êxito na sua instância.

```
ubuntu:~$ sudo less /lib/systemd/system/ssh.service.d/ec2-instance-connect.conf
```

O EC2 Instance Connect foi instalado com êxito se as linhas `AuthorizedKeysCommand` e `AuthorizedKeysCommandUser` contiverem os seguintes valores:

```
AuthorizedKeysCommand /usr/share/ec2-instance-connect/eic_run_authorized_keys %
%u %%f
AuthorizedKeysCommandUser ec2-instance-connect
```

- O `AuthorizedKeysCommand` define o script `eic_run_authorized_keys` para buscar as chaves nos metadados da instância
- `AuthorizedKeysCommandUser` O define o usuário do sistema como `ec2-instance-connect`

> **Note**
>
> Se você tiver previamente configurado `AuthorizedKeysCommand` e `AuthorizedKeysCommandUser`, a instalação do EC2 Instance Connect não mudará os valores e você não poderá usar o EC2 Instance Connect.

Conectar-se à instância do Linux usando EC2 Instance Connect

As instruções a seguir explicam como você pode se conectar a instâncias do Linux usando o EC2 Instance Connect por meio do console do Amazon EC2, da AWS CLI ou de um cliente SSH.

Ao conectar-se a uma instância usando o EC2 Instance Connect por meio do console ou da AWS CLI, a API do EC2 Instance Connect envia automaticamente por push uma chave pública de SSH para os metadados da instância, onde ela permanece por 60 segundos. Uma política do IAM anexada ao seu usuário autoriza esta ação. Se você preferir usar sua própria chave de SSH, será

possível usar um cliente de SSH e enviar explicitamente sua chave de SSH para a instância usando o EC2 Instance Connect.

Considerações

Depois de se conectar a uma instância usando o Instance Connect do EC2, a conexão persiste até que a sessão SSH seja encerrada. A duração da conexão não é determinada pela duração de suas credenciais do IAM. Se as suas credenciais do IAM expirarem, a conexão persistirá. Ao utilizar a experiência do console do Instance Connect do EC2, se as suas credenciais de IAM expirarem, encerre a conexão fechando a página do navegador. Ao usar seu próprio cliente SSH e o Instance Connect do EC2 para enviar sua chave, você pode definir um valor de tempo limite de SSH para encerrar a sessão SSH automaticamente.

Requisitos

Antes de começar, revise todos os pré-requisitos.

Opções de conexão

- Conectar-se usando o console do Amazon EC2
- Conectar-se usando o AWS CLI
- Conectar-se usando sua própria chave e cliente SSH
- Solução de problemas

Conectar-se usando o console do Amazon EC2

É possível se conectar a uma instância usando o EC2 Instance Connect por meio do console do Amazon EC2.

Requisitos

Para se conectar usando o console do Amazon EC2, a instância deve ter um endereço IPv4 público ou IPv6. Se a instância só tiver um endereço IPv4 privado, será possível usar o comando da AWS CLI ec2-instance-connect para se conectar.

Conectar-se a instâncias do Linux usando o console do Amazon EC2

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância e escolha Connect (Conectar).

4. Escolha a guia EC2 Instance Connect.
5. Escolha Conectar usando um IP público.
6. Se houver uma opção, selecione o endereço IP ao qual se conectar. Caso contrário, o endereço IP será selecionado automaticamente.
7. Em Nome de usuário, verifique o nome de usuário.
8. Escolha Conectar para estabelecer uma conexão. Uma janela de terminal no navegador é aberta.

Conectar-se usando o AWS CLI

É possível usar o comando da AWS CLI ec2-instance-connect para se conectar à instância usando um cliente de SSH. O EC2 Instance Connect tenta estabelecer uma conexão usando um endereço IP disponível em uma ordem predefinida, com base no tipo de conexão especificado. Se um endereço IP não estiver disponível, ele tentará automaticamente o próximo, na ordem.

Tipos de conexão

`auto` (padrão)

O EC2 Instance Connect tentará conectar-se usando os endereços IP da instância na ordem a seguir e com o tipo de conexão correspondente:

1. IPv4 público: `direct`
2. IPv4 privado: `eice`
3. IPv6: `direct`

`direct`

O EC2 Instance Connect tentará conectar-se usando os endereços IP da instância na ordem a seguir:

1. IPv4 público
2. IPv6
3. IPv4 privado (não se conecta por meio de um endpoint do EC2 Instance Connect)

`eice`

O EC2 Instance Connect tenta se conectar usando o endereço IPv4 privado da instância e um endpoint do EC2 Instance Connect.

> **Note**
>
> No futuro, podemos mudar o comportamento do tipo de conexão `auto`. Para garantir que o tipo de conexão desejado seja usado, recomendamos que você defina explicitamente o `--connection-type` como `direct` ou `eice`.

Requisitos

É necessário usar a AWS CLI versão 2. Para obter mais informações, consulte Install or update to the latest version of the AWS CLI.

Para se conectar a uma instância usando o ID da instância

Se souber apenas o ID da instância e quiser permitir que o EC2 Instance Connect determine o tipo de conexão a ser usado ao se conectar à sua instância, use o comando da CLI ec2-instance-connect ssh e o ID da instância.

```
aws ec2-instance-connect ssh --instance-id i-1234567890example
```

Para se conectar a uma instância usando o ID da instância e um EC2 Instance Connect Endpoint

Se você quiser conectar-se à sua instância por meio de um EC2 Instance Connect Endpoint, use o comando anterior e também especifique o parâmetro `--connection-type` com o valor `eice`.

```
aws ec2-instance-connect ssh --instance-id i-1234567890example --connection-type eice
```

Para se conectar a uma instância usando o ID da instância e seu próprio arquivo de chave privada

Se você quiser conectar-se à sua instância por meio de um EC2 Instance Connect Endpoint usando sua própria chave privada, especifique o ID da instância e o caminho para o arquivo da chave privada. Não inclua *file://* no caminho. O exemplo a seguir falhará: *file: ///caminho/para/a/chave*.

```
aws ec2-instance-connect ssh --instance-id i-1234567890example --private-key-file /path/to/key.pem
```

> **Tip**
>
> Se receber um erro ao usar esses comandos, verifique se está usando a AWS CLI versão 2, pois o comando `ssh` só está disponível nesta versão principal. Também recomendamos atualizar regularmente para a versão secundária mais recente da AWS CLI versão 2 para acessar os recursos mais recentes. Para obter mais informações, consulte Sobre o AWS CLI versão 2, no Guia do usuário do AWS Command Line Interface.

Conectar-se usando sua própria chave e cliente SSH

É possível usar sua própria chave SSH e conectar-se à sua instância a partir do cliente SSH de sua escolha enquanto usa a API do EC2 Instance Connect. Isso permite que você se beneficie da capacidade do EC2 Instance Connect de enviar por push uma chave pública para a instância. Esse método de conexão funciona para instâncias com endereços IP públicos e privados.

Requisitos

- Requisitos para pares de chaves
  - Tipos com suporte: RSA (OpenSSH e SSH2) e ED25519
  - Tamanhos com suporte: 2048 e 4096.
  - Para obter mais informações, consulte Criar um par de chaves usando uma ferramenta de terceiros e importe a chave pública para o Amazon EC2.
- Quando ocorre uma conexão com uma instância que só tem endereços IP privados, o computador local em que você está iniciando a sessão SSH deve ter conectividade com o endpoint do serviço EC2 Instance Connect (para enviar sua chave pública SSH para a instância), além de conectividade de rede para o endereço IP privado da instância para estabelecer a sessão SSH. O endpoint de serviço do EC2 Instance Connect é acessível pela Internet ou por meio de uma interface virtual pública do Direct Connect. Para se conectar ao endereço IP privado da instância, é possível aproveitar serviços, como Direct Connect, AWS Site-to-Site VPN ou emparelhamento de VPC.

Para se conectar à sua instância usando a própria chave e qualquer cliente SSH

1. (Opcional) Gerar chaves novas chaves SSH privadas e públicas

   É possível gerar novas chaves SSH públicas e privadas, `my_key` e `my_key.pub`, usando o comando a seguir:

   ```
   ssh-keygen -t rsa -f my_key
   ```

2. Envie por push a chave pública do SSH para a instância

   Use o comando send-ssh-public-key para enviar por push a chave pública SSH para a instância. Se você executou sua instância usando o AL2023 ou o Amazon Linux 2, o nome de usuário padrão da AMI é `ec2-user`. Se você executou sua instância usando o Ubuntu, o nome de usuário padrão da AMI é `ubuntu`.

   O exemplo a seguir envia a chave pública para a instância especificada na zona de disponibilidade especificada, para autenticar `ec2-user`.

   ```
   aws ec2-instance-connect send-ssh-public-key \
       --region us-west-2 \
       --availability-zone us-west-2b \
       --instance-id i-001234a4bf70dec41EXAMPLE \
       --instance-os-user ec2-user \
       --ssh-public-key file://my_key.pub
   ```

3. Conecte-se à instância usando a chave privada

   Use o comando ssh para se conectar à instância usando a chave privada antes de a chave pública ser removida dos metadados da instância (você tem 60 segundos antes de ser removida). Especifique a chave privada que corresponde à chave pública, o nome de usuário padrão da AMI usado para iniciar sua instância e o nome DNS público da instância (se estiver se conectando por uma rede privada, especifique o nome DNS privado ou o endereço IP). Adicione a opção `IdentitiesOnly=yes` para garantir que apenas os arquivos na configuração ssh e a chave especificada sejam usados para a conexão.

   ```
   ssh -o "IdentitiesOnly=yes" -i my_key ec2-
   user@ec2-198-51-100-1.compute-1.amazonaws.com
   ```

O exemplo a seguir usa `timeout 3600` para definir que sua sessão SSH seja encerrada após 1 hora. Os processos iniciados durante a sessão podem continuar em execução na sua instância após o término da sessão.

```
timeout 3600 ssh -o “IdentitiesOnly=yes” -i my_key ec2-
user@ec2-198-51-100-1.compute-1.amazonaws.com
```

Solução de problemas

Se você receber um erro ao tentar se conectar à instância, consulte:

- Solucionar problemas de conexão com a instância do Linux do Amazon EC2
- Como solucionar problemas de conexão à minha instância do EC2 usando o EC2 Instance Connect?

Desinstalar o EC2 Instance Connect

Para desabilitar o EC2 Instance Connect, conecte-se à instância do Linux e desinstale o pacote `ec2-instance-connect` que está instalado no SO. Se a configuração `sshd` corresponder ao que foi definido quando você instalou o EC2 Instance Connect, desinstalar o pacote `ec2-instance-connect` também removerá a configuração `sshd`. Se a configuração `sshd` tiver sido modificada após a instalação do EC2 Instance Connect, você deverá atualizá-la manualmente.

Amazon Linux

É possível desinstalar o EC2 Instance Connect no AL2023 e no Amazon Linux 2 2.0.20190618 ou posterior, em que o EC2 Instance Connect está pré-configurado.

Desinstalar o EC2 Instance Connect em uma instância iniciada com o Amazon Linux

1. Conecte-se à sua instância usando SSH. Especifique o par de chaves SSH que você usou para sua instância ao executá-la e o nome de usuário padrão da AMI AL2023 ou Amazon Linux 2, que é `ec2-user`.

   Por exemplo. o comando ssh conecta-se à instância com o nome DNS público `ec2-a-b-c-d.us-west-2.compute.amazonaws.com`, usando o par de chaves `my_ec2_private_key.pem`.

```
$ ssh -i my_ec2_private_key.pem ec2-user@ec2-a-b-c-d.us-
west-2.compute.amazonaws.com
```

2. Desinstale o pacote `ec2-instance-connect` usando o comando yum.

```
[ec2-user ~]$ sudo yum remove ec2-instance-connect
```

Ubuntu

Desinstalar o EC2 Instance Connect em uma instância iniciada com uma AMI do Ubuntu

1. Conecte-se à sua instância usando SSH. Especifique o par de chaves SSH usado para sua instância ao iniciá-la e o nome de usuário padrão da AMI Ubuntu, que é `ubuntu`.

   Por exemplo. o comando ssh conecta-se à instância com o nome DNS público `ec2-a-b-c-d.us-west-2.compute.amazonaws.com`, usando o par de chaves `my_ec2_private_key.pem`.

```
$ ssh -i my_ec2_private_key.pem ubuntu@ec2-a-b-c-d.us-
west-2.compute.amazonaws.com
```

2. Desinstale o pacote `ec2-instance-connect` usando o comando apt-get.

```
ubuntu:~$ sudo apt-get remove ec2-instance-connect
```

Conecte-se às suas instâncias usando um endereço IP privado e o endpoint de conexão da instância do EC2

O EC2 Instance Connect Endpoint permite a você se conectar com segurança a uma instância da Internet sem usar um bastion host ou exigir que sua nuvem privada virtual (VPC) tenha conectividade direta com a Internet.

Benefícios

- É possível se conectar às instâncias sem exigir que elas tenham um endereço IPv4 público ou um endereço IPv6. A AWS cobra por todos os endereços IPv4 públicos, incluindo os endereços

IPv4 públicos associados a instâncias em execução e endereços IP elásticos. Para obter mais informações, consulte a guia Endereço IPv4 público na página de preços da Amazon VPC.

- É possível se conectar às suas instâncias pela Internet sem exigir que sua VPC tenha conectividade direta via gateway da Internet.
- É possível controlar o acesso à criação e ao uso dos endpoints do EC2 Instance Connect para se conectar a instâncias usando políticas e permissões do IAM.
- Todas as tentativas de conexão com suas instâncias, tanto bem quanto malsucedidas, são registradas em log no CloudTrail.

Preços

Não há custo adicional para usar endpoints do EC2 Instance Connect. Se você usar um EC2 Instance Connect Endpoint para se conectar a uma instância em uma zona de disponibilidade diferente, haverá uma cobrança adicional pela transferência de dados entre zonas de disponibilidade.

Conteúdo

- Como funcionam
- Considerações
- Conceder permissões para usar o EC2 Instance Connect Endpoint
- Grupos de segurança para o EC2 Instance Connect Endpoint
- Criar um EC2 Instance Connect Endpoint
- Modificar um endpoint do EC2 Instance Connect
- Excluir um EC2 Instance Connect Endpoint
- Conexão com uma instância do Amazon EC2 usando o EC2 Instance Connect Endpoint
- Registro em log de conexões estabelecidas através do EC2 Instance Connect Endpoint
- Perfil vinculado ao serviço para o EC2 Instance Connect Endpoint
- Cotas para EC2 Instance Connect Endpoint

Como funcionam

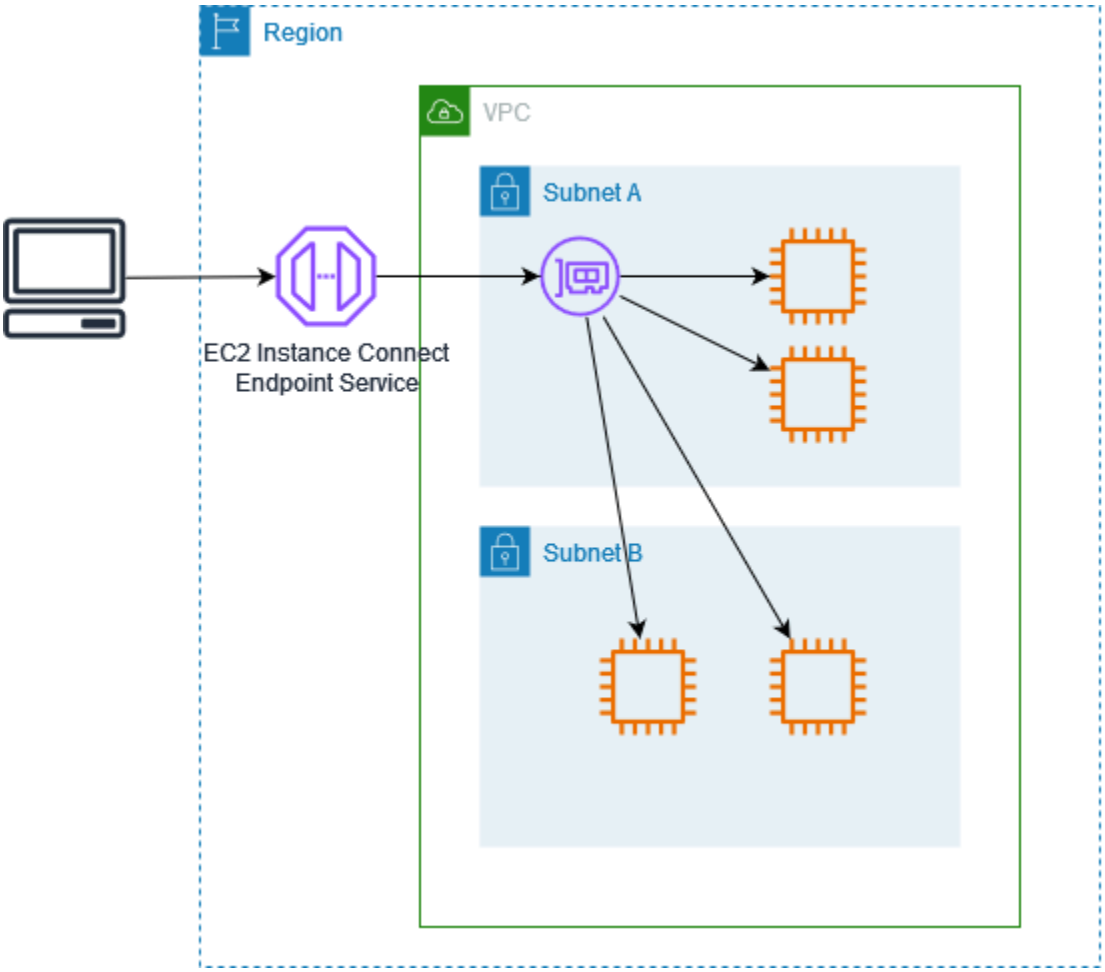
O EC2 Instance Connect Endpoint é um proxy TCP com reconhecimento de identidade. O serviço EC2 Instance Connect Endpoint estabelece um túnel privado do seu computador até o endpoint

usando as credenciais da sua entidade do IAM. O tráfego é autenticado e autorizado antes de chegar à sua VPC.

É possível configurar regras adicionais de grupo de segurança para restringir o tráfego de entrada para suas instâncias. Por exemplo, é possível usar regras de entrada para permitir nas portas de gerenciamento tráfego somente do EC2 Instance Connect Endpoint.

Também é possível configurar regras da tabela de rotas para permitir que o endpoint se conecte a qualquer instância em qualquer sub-rede da VPC.

O diagrama a seguir mostra como um usuário pode se conectar às suas instâncias via Internet usando um EC2 Instance Connect Endpoint. Primeiro, crie um EC2 Instance Connect Endpoint na sub-rede A. Criamos então uma interface de rede para o endpoint na sub-rede, o qual atua como ponto de entrada para o tráfego destinado às suas instâncias na VPC. Se a tabela de rotas da sub-rede B permitir o tráfego da sub-rede A, será possível usar o endpoint para alcançar instâncias na sub-rede B.



Considerações

Antes de começar, considere o seguinte:

- O EC2 Instance Connect Endpoint foi projetado especificamente para casos de uso de tráfego de gerenciamento, e não para transferências de dados de alto volume. A utilização de transferências de dados de alto volume é controlada.
- Você pode criar um EC2 Instance Connect Endpoint para permitir tráfego para uma instância com um endereço IPv4 privado ou um endereço IPv6. O tipo de endereço IP do endpoint deve corresponder ao endereço IP da instância. Você pode criar um endpoint compatível com todos os tipos de endereço IP.
- (Instâncias do Linux) Caso use o próprio par de chaves, será possível usar qualquer AMI do Linux. Caso contrário, a instância deverá ter o EC2 Instance Connect instalado. Para obter informações sobre quais AMIs incluem o EC2 Instance Connect e como instalá-lo em outras AMIs compatíveis, consulte Instalar o EC2 Instance Connect.
- É possível atribuir um grupo de segurança a um EC2 Instance Connect Endpoint. Caso contrário, o grupo de segurança padrão será usado para a VPC. O grupo de segurança de um EC2 Instance Connect Endpoint deve permitir tráfego de saída para as instâncias de destino. Para obter mais informações, consulte Grupos de segurança para o EC2 Instance Connect Endpoint.
- É possível configurar um EC2 Instance Connect Endpoint para preservar os endereços IP de origem dos clientes ao rotear solicitações para as instâncias. Caso contrário, o endereço IP da interface de rede se tornará o endereço IP do cliente para todo o tráfego de entrada.
  - Se você ativar a preservação de IP do cliente, os grupos de segurança das instâncias deverão permitir o tráfego dos clientes. Além disso, as instâncias deverão estar na mesma VPC do EC2 Instance Connect Endpoint.
  - Se você desativar a preservação de IP do cliente, os grupos de segurança das instâncias deverão permitir o tráfego da VPC. Esse é o padrão.
  - A preservação de IP do cliente é compatível somente com EC2 Instance Connect Endpoints IPv4. Para usar preservação de IP do cliente, o tipo de endereço IP do EC2 Instance Connect Endpoint deve ser IPv4. A preservação do IP do cliente não é compatível com o tipo de endereço IP de pilha dupla ou IPv6.
  - Os seguintes tipos de instância não oferecem suporte à preservação do IP do cliente: C1, CG1, CG2, G1, HI1, M1, M2, M3 e T1. Se você ativar a preservação de IP do cliente e tentar se conectar a uma instância com um desses tipos de instância usando o EC2 Instance Connect Endpoint, a conexão falhará.

  - Não há suporte à preservação de IP do cliente quando o tráfego for roteado por meio de um gateway de trânsito.
- Ao criar um EC2 Instance Connect Endpoint, uma função vinculada ao serviço é criada automaticamente para o serviço Amazon EC2 no AWS Identity and Access Management (IAM). O Amazon EC2 usa o perfil vinculado ao serviço para provisionar interfaces de rede em sua conta, que são exigidas ao criar EC2 Instance Connect Endpoints. Para obter mais informações, consulte Perfil vinculado ao serviço para o EC2 Instance Connect Endpoint.
- É possível criar um EC2 Instance Connect Endpoint por VPC e por sub-rede. Para obter mais informações, consulte Cotas para EC2 Instance Connect Endpoint. Se você precisar criar outro EC2 Instance Connect Endpoint em uma zona de disponibilidade diferente na mesma VPC, deverá primeiro excluir o EC2 Instance Connect Endpoint atual. Caso contrário, você receberá um erro de cota.
- Cada EC2 Instance Connect Endpoint pode acomodar até 20 conexões simultâneas.
- A duração máxima de uma conexão TCP estabelecida é 1 hora (3.600 segundos). É possível especificar a duração máxima permitida em uma política do IAM, que pode ser de até 3.600 segundos. Para obter mais informações, consulte Permissões para usar o EC2 Instance Connect Endpoint para se conectar às instâncias.

  A duração da conexão não é determinada pela duração de suas credenciais do IAM. Se suas credenciais do IAM expirarem, a conexão continuará persistindo até que a duração máxima especificada seja atingida. Ao se conectar a uma instância usando a experiência do console de Endpoint do Instance Connect do EC2, defina a duração máxima do túnel (segundos) como um valor menor que a duração das suas credenciais do IAM. Se suas credenciais do IAM expirarem antes do tempo, encerre a conexão com sua instância fechando a página do navegador.

Conceder permissões para usar o EC2 Instance Connect Endpoint

Por padrão, as entidades do IAM não têm permissão para criar, descrever ou modificar os EC2 Instance Connect Endpoints. Um administrador do IAM deve criar políticas do IAM que concedam as permissões necessárias para executar ações específicas nos recursos necessários.

Para obter informações sobre a criação de políticas do IAM, consulte Criação de políticas do IAM, no Manual do usuário do IAM.

Os exemplos de políticas a seguir mostram como é possível controlar as permissões que os usuários têm sobre os EC2 Instance Connect Endpoints.

Exemplos

- Permissões para criar, descrever, modificar e excluir os endpoints do EC2 Instance Connect
- Permissões para usar o EC2 Instance Connect Endpoint para se conectar às instâncias
- Permissões para conectar somente de um intervalo de endereços IP específico

Permissões para criar, descrever, modificar e excluir os endpoints do EC2 Instance Connect

Para criar e modificar um endpoint do EC2 Instance Connect, os usuários precisam de permissões para as seguintes ações:

- `ec2:CreateInstanceConnectEndpoint`
- `ec2:CreateNetworkInterface`
- `ec2:CreateTags`
- `ec2:ModifyInstanceConnectEndpoint`
- `iam:CreateServiceLinkedRole`

Para descrever e excluir EC2 Instance Connect Endpoints, os usuários precisam de permissões para as seguintes ações:

- `ec2:DescribeInstanceConnectEndpoints`
- `ec2:DeleteInstanceConnectEndpoint`

É possível criar uma política que conceda permissão para criar, descrever, modificar e excluir os endpoints do EC2 Instance Connect em todas as sub-redes. Como alternativa, é possível restringir ações para sub-redes especificadas somente especificando os ARNs da sub-rede como o `Resource` permitido ou usando a chave de condição `ec2:SubnetID`. Você também pode usar a chave de condição `aws:ResourceTag` para permitir ou negar explicitamente a criação de endpoints com determinadas tags. Para ter mais informações, consulte Políticas e permissões no IAM, no Guia do usuário do IAM.

Exemplo de política do IAM

No exemplo de política do IAM a seguir, a seção `Resource` concede permissão para criar, modificar e excluir endpoints em todas as sub-redes, especificadas pelo asterisco (`*`). As ações da API `ec2:Describe*` não oferecem suporte a permissões no nível do recurso. Portanto, o caractere curinga `*` é necessário no elemento `Resource`.

Permissões para usar o EC2 Instance Connect Endpoint para se conectar às instâncias

A ação `ec2-instance-connect:OpenTunnel` concede permissão para estabelecer uma conexão TCP com uma instância para se conectar via EC2 Instance Connect Endpoint. É possível especificar o EC2 Instance Connect Endpoint a ser usado. Como alternativa, um `Resource` com um asterisco (*) permite que os usuários usem qualquer EC2 Instance Connect Endpoint disponível. Você também pode restringir o acesso às instâncias com base na presença ou ausência de tags de recurso como chaves de condição.

Condições

- `ec2-instance-connect:remotePort`: a porta na instância que pode ser usada para estabelecer uma conexão TCP. Quando essa chave de condição é usada, tentar conectar-se a uma instância em qualquer outra porta que não seja a especificada na política resultará em falha.
- `ec2-instance-connect:privateIpAddress`: o endereço IP privado de destino associado à instância com a qual você deseja estabelecer uma conexão TCP. É possível especificar um único endereço IP, como `10.0.0.1/32`, ou um intervalo de IPs por meio de CIDRs, como `10.0.1.0/28`. Quando essa chave de condição é usada, tentar conectar-se a uma instância com um endereço IP privado diferente ou fora do intervalo CIDR resultará em falha.
- `ec2-instance-connect:maxTunnelDuration`: a duração máxima de uma conexão TCP estabelecida. A unidade é em segundos, e a duração varia de um mínimo de 1 segundo a um máximo de 3.600 segundos (uma hora). Se a condição não for especificada, a duração padrão será definida como 3.600 segundos (uma hora). A tentativa de conectar-se a uma instância por mais tempo do que a duração especificada na política do IAM ou por mais tempo do que o máximo padrão resultará em falha. A conexão é desconectada após a duração especificada.

  Se `maxTunnelDuration` for especificado na política do IAM e o valor especificado for inferior a 3.600 segundos (o padrão), você deverá especificar `--max-tunnel-duration` no comando ao conectar-se a uma instância. Para obter informações sobre como conectar-se a uma instância, consulte Conexão com uma instância do Amazon EC2 usando o EC2 Instance Connect Endpoint.

Também é possível conceder a um usuário acesso para estabelecer conexões com instâncias com base na presença de tags de recursos no EC2 Instance Connect Endpoint. Para ter mais informações, consulte Políticas e permissões no IAM, no Guia do usuário do IAM.

Para instâncias do Linux, a ação `ec2-instance-connect:SendSSHPublicKey` concede permissão para enviar a chave pública para uma instância. A condição `ec2:osuser` especifica o nome do usuário do SO (sistema operacional) que pode enviar a chave pública para uma instância.

Use o nome de usuário padrão da AMI que você usou para iniciar a instância. Para obter mais informações, consulte Conceder permissões do IAM para o EC2 Instance Connect.

Exemplo de política do IAM

Os exemplos de políticas do IAM apresentados a seguir permitem que uma entidade principal do IAM se conecte a uma instância usando somente o endpoint de conexão da instância do EC2 especificado, que é identificado pelo ID `eice-123456789abcdef` do endpoint especificado. A conexão será estabelecida com êxito somente se todas as condições forem atendidas.

> **Note**
>
> As ações da API `ec2:Describe*` não oferecem suporte a permissões no nível do recurso. Portanto, o caractere curinga `*` é necessário no elemento `Resource`.

Linux

Este exemplo avalia se a conexão com a instância foi estabelecida na porta 22 (SSH), se o endereço IP privado da instância está dentro do intervalo de `10.0.1.0/31` (que compreende `10.0.1.0` e `10.0.1.1`) e `maxTunnelDuration` é menor ou igual a `3600` segundos. A conexão será desconectada após `3600` segundos (1 hora).

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [{
            "Sid": "EC2InstanceConnect",
            "Action": "ec2-instance-connect:OpenTunnel",
            "Effect": "Allow",
            "Resource": "arn:aws:ec2:us-east-1:111122223333:instance-connect-
endpoint/eice-123456789abcdef",
            "Condition": {
                "NumericEquals": {
                    "ec2-instance-connect:remotePort": "22"
                },
                "IpAddress": {
                    "ec2-instance-connect:privateIpAddress": "10.0.1.0/31"
                },
```

```
                "NumericLessThanEquals": {
                    "ec2-instance-connect:maxTunnelDuration": "3600"
                }
            }
        },
        {
            "Sid": "SSHPublicKey",
            "Effect": "Allow",
            "Action": "ec2-instance-connect:SendSSHPublicKey",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ec2:osuser": "ami-username"
                }
            }
        },
        {
            "Sid": "Describe",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceConnectEndpoints"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

Windows

Este exemplo avalia se a conexão com a instância foi estabelecida na porta 3389 (RDP), se o endereço IP privado da instância está dentro do intervalo de `10.0.1.0/31` (que compreende `10.0.1.0` e `10.0.1.1`) e `maxTunnelDuration` é menor ou igual a `3600` segundos. A conexão será desconectada após `3600` segundos (1 hora).

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [{
            "Sid": "EC2InstanceConnect",
```

```
            "Action": "ec2-instance-connect:OpenTunnel",
            "Effect": "Allow",
            "Resource": "arn:aws:ec2:us-east-1:111122223333:instance-connect-
endpoint/eice-123456789abcdef",
            "Condition": {
                "NumericEquals": {
                    "ec2-instance-connect:remotePort": "3389"
                },
                "IpAddress": {
                    "ec2-instance-connect:privateIpAddress": "10.0.1.0/31"
                },
                "NumericLessThanEquals": {
                    "ec2-instance-connect:maxTunnelDuration": "3600"
                }
            }
        },
        {
            "Sid": "Describe",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceConnectEndpoints"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

Permissões para conectar somente de um intervalo de endereços IP específico

O exemplo de política do IAM a seguir permite que uma entidade principal do IAM conecte-se a uma instância, desde que esteja se conectando a partir de um endereço IP dentro do intervalo de endereços IP especificado na política. Se a entidade principal do IAM chamar `OpenTunnel` desde um endereço IP que não esteja dentro de `192.0.2.0/24` (o exemplo de intervalo de endereços IP nesta política), a resposta será `Access Denied`. Para obter mais informações, consulte `aws:SourceIp` no Guia do usuário do IAM.

JSON

```
{
    "Version":"2012-10-17",
```

```
    "Statement": [{
            "Effect": "Allow",
            "Action": "ec2-instance-connect:OpenTunnel",
            "Resource": "arn:aws:ec2:us-east-1:111122223333:instance-connect-
endpoint/eice-123456789abcdef",
            "Condition": {
                "IpAddress": {
                    "aws:SourceIp": "192.0.2.0/24"
                },
                "NumericEquals": {
                    "ec2-instance-connect:remotePort": "22"
                }
            }
        },
        {
            "Sid": "SSHPublicKey",
            "Effect": "Allow",
            "Action": "ec2-instance-connect:SendSSHPublicKey",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ec2:osuser": "ami-username"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceConnectEndpoints"
            ],
            "Resource": "*"
        }
    ]
}
```

Grupos de segurança para o EC2 Instance Connect Endpoint

Um grupo de segurança controla o tráfego que tem permissão para acessar e sair dos recursos aos quais está associado. Por exemplo, negamos tráfego de e para uma instância do Amazon EC2, a menos que seja especificamente permitido pelos grupos de segurança associados à instância.

Os exemplos a seguir mostram como configurar as regras do grupo de segurança para o EC2 Instance Connect Endpoint e as instâncias de destino.

Exemplos

- Regras de grupo de segurança para o EC2 Instance Connect Endpoint
- Regras do grupo de segurança da instância de destino

Regras de grupo de segurança para o EC2 Instance Connect Endpoint

As regras de grupo de segurança para um EC2 Instance Connect Endpoint devem permitir que o tráfego de saída para as instâncias de destino deixem o endpoint. É possível especificar o grupo de segurança da instância ou o intervalo de endereços IPv4 ou iPv6 da VPC como o destino.

O tráfego para o endpoint é proveniente do EC2 Instance Connect Endpoint Service e é permitido independentemente das regras de entrada do grupo de segurança do endpoint. Para controlar quem pode usar o endpoint do EC2 Instance Connect para se conectar a uma instância, use uma política do IAM. Para obter mais informações, consulte Permissões para usar o EC2 Instance Connect Endpoint para se conectar às instâncias.

Exemplo de regra de saída: referência a grupos de segurança

O exemplo a seguir usa referência a grupos de segurança, o que significa que o destino é um grupo de segurança associado às instâncias de destino. Essa regra permite tráfego de saída do endpoint para todas as instâncias que usam esse grupo de segurança.

Protocolo	Destino	Intervalo de portas	Comment
TCP	*ID do grupo de segurança da instância*	22	Permite tráfego SSH de saída para todas as instâncias associadas ao grupo de segurança da instância

Exemplo de regra de saída: intervalo de endereços IPv4

O exemplo a seguir permite tráfego de saída para o intervalo de endereços IPv4 especificado. Os endereços IPv4 de uma instância são atribuídos a partir de sua sub-rede para que você possa usar o intervalo de endereços IPv4 da VPC.

Protocolo	Destino	Intervalo de portas	Comment
TCP	*CIDR IPv4 da VPC*	22	Permite tráfego SSH de saída para a VPC

Exemplo de regra de saída: intervalo de endereços IPv6

O exemplo a seguir permite tráfego de saída para o intervalo de endereços IPv6 especificado. Os endereços IPv6 de uma instância são atribuídos a partir de sua sub-rede para que você possa usar o intervalo de endereços IPv6 da VPC.

Protocolo	Destino	Intervalo de portas	Comment
TCP	*CIDR IPv6 da VPC*	22	Permite tráfego SSH de saída para a VPC

Regras do grupo de segurança da instância de destino

As regras do grupo de segurança para instâncias de destino devem permitir o tráfego de entrada do EC2 Instance Connect Endpoint. É possível especificar o grupo de segurança do endpoint ou um intervalo de endereços IPv4 ou IPv6 como origem. Se você especificar um intervalo de endereços IPv4, a origem dependerá se a preservação do IP do cliente está desativada ou ativada. Para obter mais informações, consulte Considerações.

Como os grupos de segurança são stateful, o tráfego de resposta tem permissão para sair da VPC, independentemente das regras de saída do grupo de segurança da instância.

Exemplo de regra de entrada: referência a grupos de segurança

O exemplo a seguir usa referência a grupos de segurança, o que significa que a origem é o grupo de segurança associado ao endpoint. Essa regra permite tráfego SSH de entrada do endpoint para todas as instâncias que usam esse grupo de segurança, independentemente de a preservação do IP do cliente estar ativada ou desativada. Se não houver outras regras do grupo de segurança de entrada para SSH, as instâncias aceitarão tráfego SSH somente do endpoint.

Protocolo	Origem	Intervalo de portas	Comment
TCP	*ID do grupo de segurança do endpoint*	22	Permite tráfego SSH de entrada dos recursos associados ao grupo de segurança do endpoint

Exemplo de regra de entrada: preservação do IP do cliente desativada

O exemplo a seguir permite tráfego SSH de entrada do intervalo de endereços IPv4 especificado. Como a preservação do IP do cliente está desativada, o endereço IPv4 de origem é o endereço da interface de rede do endpoint. O endereço da interface de rede do endpoint é atribuído a partir de sua sub-rede, então você pode usar o intervalo de endereços IPv4 da VPC para permitir conexões com todas as instâncias na VPC.

Protocolo	Origem	Intervalo de portas	Comment
TCP	*CIDR IPv4 da VPC*	22	Permitir tráfego de entrada SSH da VPC

Exemplo de regra de entrada: preservação do IP do cliente ativada

O exemplo a seguir permite tráfego SSH de entrada do intervalo de endereços IPv4 especificado. Como a preservação do IP do cliente está ativada, o endereço IPv4 de origem é o endereço do cliente.

Protocolo	Origem	Intervalo de portas	Comment
TCP	*Intervalo de endereços IPv4 públicos*	22	Permite tráfego de entrada do intervalo de endereços IPv4 do cliente especificado.

Criar um EC2 Instance Connect Endpoint

É possível criar um EC2 Instance Connect Endpoint para permitir uma conexão segura com suas instâncias.

Considerações

- Sub-redes compartilhadas: é possível criar um EC2 Instance Connect Endpoint em uma sub-rede compartilhada com você. Mas, você não pode usar os EC2 Instance Connect Endpoints que o proprietário da VCP criou em uma sub-rede compartilhada com você.
- Tipos de endereço IP: os EC2 Instance Connect Endpoints são compatíveis com os seguintes tipos de endereço, que devem ser compatíveis com a sub-rede:
  - `ipv4`: conectar somente com instâncias do EC2 que têm endereços IPv4 privados.
  - `dualstack` : conectar com instâncias do EC2 que têm endereços IPv4 privados ou endereços IPv6.
  - `ipv6`: conectar somente com instâncias do EC2 que têm endereços IPv6.

Pré-requisitos

É necessário ter as permissões do IAM exigidas para criar um EC2 Instance Connect Endpoint. Para obter mais informações, consulte Permissões para criar, descrever, modificar e excluir os endpoints do EC2 Instance Connect.

Console

Para criar um EC2 Instance Connect Endpoint

1. Abra o console da Amazon VPC, em https://console.aws.amazon.com/vpc/.
2. No painel de navegação à esquerda, escolha Endpoints.
3. Escolha Criar endpoint e, em seguida, especifique as configurações do endpoint:
   a. (Opcional) Em Tag de nome, insira um nome para o endpoint.
   b. Em Tipo, escolha Endpoint do EC2 Instance Connect.
   c. Em Configurações de rede, em VPC, selecione a VPC que contém as instâncias de destino.

d. (Opcional) Para preservar os endereços IP dos clientes, expanda Configurações adicionais e marque a caixa de seleção Preservar IP dos clientes. Caso contrário, o padrão é usar a interface de rede do endpoint como endereço IP do cliente.

> **Note**
>
> Essa opção está disponível somente quando o tipo de endereço IP do endpoint está configurado como IPv4.

e. (Opcional) Em Grupos de segurança, selecione o grupo de segurança a ser associado ao endpoint. Caso contrário, o grupo de segurança padrão da VPC será usado. Para obter mais informações, consulte Grupos de segurança para o EC2 Instance Connect Endpoint.

f. Em Sub-rede, selecione a sub-rede na qual o endpoint será criado.

g. Em Tipo de endereço IP, escolha o tipo de endereço IP do endpoint. Escolha Pilha dupla se precisar de compatibilidade com conexões IPv4 e IPv6 para suas instâncias. Escolha IPv4 se precisar de compatibilidade com preservação de IP do cliente.

h. (Opcional) Para adicionar uma tag, escolha Adicionar nova tag e insira a chave e o valor da tag.

4. Revise suas configurações e escolha Criar endpoint.

   O estado inicial do endpoint é Pendente. Antes de conectar-se a uma instância usando esse endpoint, aguarde até que o status do endpoint seja Disponível. Isso pode levar alguns minutos.

5. Para se conectar a uma instância usando seu endpoint, consulte Conectar a uma instância.

AWS CLI

Para criar um EC2 Instance Connect Endpoint

Use o comando create-instance-connect-endpoint.

```
aws ec2 create-instance-connect-endpoint \
    --subnet-id subnet-0123456789example
```

Para especificar o tipo de tráfego com que o endpoint é compatível, inclua o parâmetro `--ip-address-type`. Os valores válidos são `ipv4`, `dualstack` ou `ipv6`. A sub-rede deverá

ser compatível com o tipo de endereço IP que você especificar. Quando o parâmetro `--ip-address-type` é omitido, o valor padrão é determinado pelo tipo de endereço IP com que a sub-rede é compatível.

```
aws ec2 create-instance-connect-endpoint \
    --subnet-id subnet-0123456789example \
    --ip-address-type ipv4
```

O seguinte é um exemplo de saída.

```
{
        "OwnerId": "111111111111",
        "InstanceConnectEndpointId": "eice-0123456789example",
        "InstanceConnectEndpointArn": "arn:aws:ec2:us-east-1:111111111111:instance-
connect-endpoint/eice-0123456789example",
        "State": "create-complete",
        "StateMessage": "",
        "DnsName": "eice-0123456789example.0123abcd.ec2-instance-connect-
endpoint.us-east-1.amazonaws.com",
        "FipsDnsName": "eice-0123456789example.0123abcd.fips.ec2-instance-connect-
endpoint.us-east-1.amazonaws.com",
        "NetworkInterfaceIds": [
            "eni-0123abcd"
        ],
        "VpcId": "vpc-0123abcd",
        "AvailabilityZone": "us-east-1a",
        "AvailabilityZoneId": "use1-az4",
        "CreatedAt": "2023-04-07T15:43:53.000Z",
        "SubnetId": "subnet-0123abcd",
        "PreserveClientIp": false,
        "SecurityGroupIds": [
            "sg-0123abcd"
        ],
        "Tags": [],
        "IpAddressType": "ipv4"
}
```

Para monitorar o status da criação

O valor inicial do campo `State` é `create-in-progress`. Antes de se conectar a uma instância usando esse endpoint, aguarde até que o status seja `create-complete`. Use o comando

describe-instance-connect-endpoints para monitorar o status do EC2 Instance Connect Endpoint. O parâmetro `--query` filtra os resultados para o campo `State`.

```
aws ec2 describe-instance-connect-endpoints --instance-connect-endpoint-
ids eice-0123456789example --query InstanceConnectEndpoints[*].State --output text
```

O seguinte é um exemplo de saída.

```
create-complete
```

PowerShell

Para criar um endpoint do EC2 Instance Connect

Use o cmdlet New-EC2InstanceConnectEndpoint.

```
New-EC2InstanceConnectEndpoint -SubnetId subnet-0123456789example
```

Para especificar o tipo de tráfego com que o endpoint é compatível, inclua o parâmetro `-IpAddressType`. Os valores válidos são `ipv4`, `dualstack` ou `ipv6`. A sub-rede deverá ser compatível com o tipo de endereço IP que você especificar. Quando o parâmetro `-IpAddressType` é omitido, o valor padrão é determinado pelo tipo de endereço IP com que a sub-rede é compatível.

```
New-EC2InstanceConnectEndpoint -SubnetId subnet-0123456789example -
IpAddressType ipv4
```

O seguinte é um exemplo de saída.

```
OwnerId                     : 111111111111
InstanceConnectEndpointId   : eice-0123456789example
InstanceConnectEndpointArn  : arn:aws:ec2:us-east-1:111111111111:instance-connect-
endpoint/eice-0123456789example
State                       : create-complete
StateMessage                :
DnsName                     : eice-0123456789example.0123abcd.ec2-instance-connect-
endpoint.us-east-1.amazonaws.com
FipsDnsName                 : eice-0123456789example.0123abcd.fips.ec2-instance-
connect-endpoint.us-east-1.amazonaws.com
NetworkInterfaceIds         : {eni-0123abcd}
VpcId                       : vpc-0123abcd
```

```
AvailabilityZone            : us-east-1a
AvailabilityZoneId          : use1-az4
CreatedAt                   : 4/7/2023 3:43:53 PM
SubnetId                    : subnet-0123abcd
PreserveClientIp            : False
SecurityGroupIds            : {sg-0123abcd}
Tags                        : {}
IpAddressType               : ipv4
```

Para monitorar o status da criação

O valor inicial do campo `State` é `create-in-progress`. Antes de se conectar a uma instância usando esse endpoint, aguarde até que o status seja `create-complete`. Use o cmdlet Get-EC2InstanceConnectEndpoint para monitorar o status do endpoint do EC2 Instance Connect. `.State.Value` filtra os resultados para o campo `State`.

```
(Get-EC2InstanceConnectEndpoint -InstanceConnectEndpointId
 "eice-0123456789example").State.Value
```

O seguinte é um exemplo de saída.

```
create-complete
```

Modificar um endpoint do EC2 Instance Connect

Você pode modificar os endpoints existentes do EC2 Instance Connect usando o AWS CLI ou um SDK. O console do Amazon EC2 não é compatível com a modificação de endpoint.

Antes de começar, você precisa ter as permissões de IAM necessárias. Para obter mais informações, consulte Permissões para criar, descrever, modificar e excluir os endpoints do EC2 Instance Connect.

Parâmetros que você pode modificar

É possível modificar os seguintes parâmetros do endpoint do EC2 Instance Connect:

Grupos de segurança

É possível especificar novos grupos de segurança para o endpoint do EC2 Instance Connect. Os novos grupos de segurança substituem os grupos de segurança atuais.

Ao modificar os grupos de segurança, é necessário especificar:

- Pelo menos um grupo de segurança, mesmo que seja apenas o grupo de segurança padrão na VPC.
- Os IDs dos grupos de segurança, não os nomes.

Tipo de endereço IP

É possível especificar um novo tipo de endereço IP para endpoint do EC2 Instance Connect.

Valores válidos: `ipv4` | `dualstack` | `ipv6`

Preservar a configuração do IP do cliente

Você pode especificar se deseja preservar o endereço IP do cliente como origem.

> **Note**
>
> A preservação do IP do cliente só é suportada em endpoints IPv4 do EC2 Instance Connect. Ao habilitar `PreserveClientIp`, o tipo de endereço IP existente do endpoint deve ser ou `ipv4`, se estiver modificando o tipo de endereço IP na mesma solicitação, o novo valor deve ser `ipv4`.

AWS CLI

Para modificar um endpoint do EC2 Instance Connect

Use o comando modify-instance-connect-endpoint e especifique o endpoint do EC2 Instance Connect e o parâmetro a ser modificado. O exemplo a seguir modifica todos os parâmetros em uma única solicitação.

```
aws ec2 modify-instance-connect-endpoint \
    --instance-connect-endpoint-id eice-0123456789example \
    --security-group-ids sg-0123456789example \
    --ip-address-type dualstack \
    --no-preserve-client-ip
```

O seguinte é um exemplo de saída.

```
{
```

```
    "Return": true
}
```

Para monitorar o status da atualização

Durante a modificação, o status do endpoint do EC2 Instance Connect é alterado para `update-in-progress`. O processo de atualização é executado de forma assíncrona e é concluído com um status `update-complete` ou `update-failed`. O endpoint usa sua configuração antiga até que o status mude para `update-complete`.

Use o comando describe-instance-connect-endpoints para monitorar o status da atualização. O parâmetro `--query` filtra os resultados para o campo `State`.

```
aws ec2 describe-instance-connect-endpoints \
    --instance-connect-endpoint-ids eice-0123456789example \
    --query InstanceConnectEndpoints[*].State --output text
```

O seguinte é um exemplo de saída.

```
update-complete
```

PowerShell

Para modificar um endpoint do EC2 Instance Connect

Use o cmdlet Edit-EC2InstanceConnectEndpoint e especifique o endpoint do EC2 Instance Connect e o parâmetro a ser modificado. O exemplo a seguir modifica todos os parâmetros em uma única solicitação.

```
Edit-EC2InstanceConnectEndpoint `
    -InstanceConnectEndpointId eice-0123456789example `
    -SecurityGroupIds sg-0123456789example `
    -IpAddressType dualstack `
    -PreserveClientIp $false
```

O seguinte é um exemplo de saída.

```
True
```

Para monitorar o status da atualização

Durante a modificação, o status do endpoint do EC2 Instance Connect é alterado para `update-in-progress`. O processo de atualização é executado de forma assíncrona e é concluído com um status `update-complete` ou `update-failed`. O endpoint usa sua configuração antiga até que o status mude para `update-complete`.

Use o comando Get-EC2InstanceConnectEndpoint para monitorar o status da atualização. O `.State.Value` filtra os resultados para o campo `State`.

```
(Get-EC2InstanceConnectEndpoint -InstanceConnectEndpointId
 "eice-0123456789example").State.Value
```

O seguinte é um exemplo de saída.

```
update-complete
```

Excluir um EC2 Instance Connect Endpoint

Quando não precisar mais de um EC2 Instance Connect Endpoint, será possível excluí-lo.

É necessário ter as permissões do IAM exigidas para criar um EC2 Instance Connect Endpoint. Para obter mais informações, consulte Permissões para criar, descrever, modificar e excluir os endpoints do EC2 Instance Connect.

Quando um EC2 Instance Connect Endpoint é excluído via console, ele entra no estado Excluindo. Se a exclusão for bem-sucedida, o endpoint excluído não aparecerá mais. Se houver falha na exclusão, o estado será delete-failed e o campo Mensagem de status fornecerá o motivo da falha.

Quando um EC2 Instance Connect Endpoint é excluído via AWS CLI, ele entra no estado `delete-in-progress`. Se a exclusão for bem-sucedida, ela entrará no estado `delete-complete`. Se exclusão falhar, o estado será `delete-failed` e `StateMessage` fornecerá o motivo da falha.

Console

Para excluir um EC2 Instance Connect Endpoint

1. Abra o console da Amazon VPC, em https://console.aws.amazon.com/vpc/.
2. No painel de navegação à esquerda, escolha Endpoints.

3. Selecione o endpoint.
4. Escolha Actions (Ações), Delete VPC endpoints (Excluir endpoints da VPC).
5. Quando a confirmação for solicitada, insira **`delete`**.
6. Escolha Excluir.

AWS CLI

Para excluir um EC2 Instance Connect Endpoint

Use o comando delete-instance-connect-endpoint e especifique o ID do endpoint do EC2 Instance Connect a ser excluído.

```
aws ec2 delete-instance-connect-endpoint --instance-connect-endpoint-
id eice-03f5e49b83924bbc7
```

O seguinte é um exemplo de saída.

```
{
    "InstanceConnectEndpoint": {
        "OwnerId": "111111111111",
        "InstanceConnectEndpointId": "eice-0123456789example",
        "InstanceConnectEndpointArn": "arn:aws:ec2:us-east-1:111111111111:instance-
connect-endpoint/eice-0123456789example",
        "State": "delete-in-progress",
        "StateMessage": "",
        "NetworkInterfaceIds": [],
        "VpcId": "vpc-0123abcd",
        "AvailabilityZone": "us-east-1d",
        "AvailabilityZoneId": "use1-az2",
        "CreatedAt": "2023-02-07T12:05:37+00:00",
        "SubnetId": "subnet-0123abcd"
    }
}
```

PowerShell

Para excluir um EC2 Instance Connect Endpoint

Use o cmdlet Remove-EC2InstanceConnectEndpoint e especifique o ID do endpoint do EC2 Instance Connect a ser excluído.

```
Remove-EC2InstanceConnectEndpoint -InstanceConnectEndpointId eice-03f5e49b83924bbc7
```

O seguinte é um exemplo de saída.

```
@{
    InstanceConnectEndpoint = @{
        OwnerId = "111111111111"
        InstanceConnectEndpointId = "eice-0123456789example"
        InstanceConnectEndpointArn = "arn:aws:ec2:us-east-1:111111111111:instance-
connect-endpoint/eice-0123456789example"
        State = "delete-in-progress"
        StateMessage = ""
        NetworkInterfaceIds = @()
        VpcId = "vpc-0123abcd"
        AvailabilityZone = "us-east-1d"
        AvailabilityZoneId = "use1-az2"
        CreatedAt = "2023-02-07T12:05:37+00:00"
        SubnetId = "subnet-0123abcd"
    }
}
```

Conexão com uma instância do Amazon EC2 usando o EC2 Instance Connect Endpoint

É possível usar o EC2 Instance Connect Endpoint para se conectar a uma instância do Amazon EC2 compatível com SSH ou RDP.

Pré-requisitos

- É necessário ter a permissão do IAM exigida para criar um EC2 Instance Connect Endpoint. Para obter mais informações, consulte Permissões para usar o EC2 Instance Connect Endpoint para se conectar às instâncias.
- O EC2 Instance Connect Endpoint deve estar em um dos seguintes estados:
  - create-complete para um novo endpoint
  - update-in-progress, update-complete ou update-failed para um endpoint existente que está sendo modificado. Ao modificar um endpoint, ele continua usando sua configuração original até o status mudar para update-complete.

Se a VPC não tiver um EC2 Instance Connect Endpoint, você poderá criar um. Para obter mais informações, consulte Criar um EC2 Instance Connect Endpoint.

- O tipo de endereço IP do EC2 Instance Connect Endpoint deve ser compatível com o tipo de endereço IP da instância. Quando o tipo de endereço IP do endpoint é pilha dupla, ele pode funcionar tanto para endereços IPv4 quanto IPv6.
- (Instâncias do Linux) Para usar o console do Amazon EC2 para se conectar à instância ou para usar a CLI para se conectar e fazer com que o EC2 Instance Connect lide com a chave temporária, a instância deve ter o EC2 Instance Connect instalado. Para obter mais informações, consulte Instalar o EC2 Instance Connect.
- Certifique-se de que o grupo de segurança da instância permita tráfego SSH de entrada do grupo de segurança do EC2 Instance Connect Endpoint. Para obter mais informações, consulte Regras do grupo de segurança da instância de destino.

Opções de conexão

- Conectar-se à sua instância do Linux usando o console do Amazon EC2
- Conectar-se à instância do Linux usando SSH
- Conectar-se à instância do Linux com seu ID da instância usando a AWS CLI
- Conectar-se à sua instância baseada no Windows usando RDP
- Solução de problemas

Conectar-se à sua instância do Linux usando o console do Amazon EC2

É possível se conectar a uma instância usando o console do Amazon EC2 (um cliente baseado em navegador) conforme descrito a seguir.

Conectar-se a instâncias do Linux usando o console do Amazon EC2

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância e escolha Conectar.
4. Escolha a guia EC2 Instance Connect.
5. Em Tipo de conexão, escolha Conectar usando um IP privado.

6. Escolha Endereço IPv4 privado ou Endereço IPv6. As opções estão disponíveis com base nos endereços IP atribuídos à instância. Quando uma opção está esmaecida, ela não tem um endereço IP daquele tipo atribuído a ela.
7. Em EC2 Instance Connect Endpoint, escolha o ID do EC2 Instance Connect Endpoint.

   > **Note**
   >
   > O EC2 Instance Connect Endpoint deve ser compatível com o endereço IP escolhido na etapa anterior. Quando o tipo de endereço IP do endpoint é pilha dupla, ele pode funcionar tanto para endereços IPv4 quanto IPv6. Para obter mais informações, consulte Criar um EC2 Instance Connect Endpoint.

8. Para Nome de usuário, se a AMI que você usou para executar a instância usar um nome de usuário diferente de `ec2-user`, insira o nome de usuário correto.
9. Em Duração máxima do túnel (segundos), insira a duração máxima permitida para a conexão de SSH.

   A duração deve estar em conformidade com qualquer condição `maxTunnelDuration` especificada na política do IAM. Caso não tenha acesso à política do IAM, entre em contato com seu administrador.
10. Selecione Conectar. Isso abrirá uma janela de terminal para sua instância.

Conectar-se à instância do Linux usando SSH

É possível usar o SSH para se conectar à sua instância de Linux e usar o comando `open-tunnel` para estabelecer um túnel privado. É possível usar `open-tunnel` no modo de conexão única ou de conexão múltipla. Você pode especificar o ID da instância, um endereço IPv4 privado ou um endereço IPv6.

Para obter mais informações sobre o uso da AWS CLI para se conectar à sua instância utilizando SSH, consulte Conectar-se usando o AWS CLI.

Os exemplos a seguir usam OpenSSH. É possível usar qualquer outro cliente SSH que ofereça suporte a um modo proxy.

Conexão única

Para permitir somente uma única conexão com uma instância usando SSH e o comando **`open-tunnel`**

Use o `ssh` o comando open-tunnel da AWS CLI da seguinte forma. O comando de proxy `-o` inclui o comando `open-tunnel` que cria o túnel privado para a instância.

```
ssh -i my-key-pair.pem ec2-user@i-1234567890abcdef0 \
    -o ProxyCommand='aws ec2-instance-connect open-tunnel --instance-
id i-1234567890abcdef0'
```

Em:

- `-i`: especifique o par de chaves usado para iniciar a instância.
- *ec2-user*@*i-1234567890abcdef0*: especifique o nome do usuário da AMI que foi usada para iniciar a instância e o ID da instância. Para instâncias com um endereço IPv6, você deve especificar o endereço IPv6 em vez do ID da instância.
- `--instance-id`: especifique o ID da instância à qual se conectar. Como alternativa, especifique `%h`, que extrai o ID da instância do usuário. Para instâncias com um endereço IPv6, substitua `--instance-id` *i-1234567890abcdef0* por `--private-ip-address` *2001:db8::1234:5678:1.2.3.4*.

Conexão múltipla

Para permitir várias conexões a uma instância, primeiro execute o comando open-tunnel da AWS CLI para começar a escutar novas conexões de TCP, e depois use o `ssh` para criar uma nova conexão de TCP e um túnel privado para sua instância.

Para permitir várias conexões com sua instância usando SSH e o comando **`open-tunnel`**

1. Execute o comando a seguir para começar a escutar novas conexões de TCP na porta especificada em sua máquina local.

   ```
   aws ec2-instance-connect open-tunnel \
       --instance-id i-1234567890abcdef0 \
       --local-port 8888
   ```

   Saída esperada:

   ```
   Listening for connections on port 8888.
   ```

2. Em uma nova janela de terminal, execute o comando `ssh` a seguir para criar uma nova conexão de TCP e um túnel privado para sua instância.

```
ssh -i my-key-pair.pem ec2-user@localhost -p 8888
```

Saída esperada: na primeira janela do terminal, você verá o seguinte:

```
[1] Accepted new tcp connection, opening websocket tunnel.
```

Também será possível ver o seguinte:

```
[1] Closing tcp connection.
```

Conectar-se à instância do Linux com seu ID da instância usando a AWS CLI

Se você souber apenas o ID da sua instância, poderá usar o comando ec2-instance-connect ssh da AWS CLI para se conectar à sua instância usando um cliente SSH. Para obter mais informações, consulte Conectar-se usando o AWS CLI.

Pré-requisitos

- Instale a AWS CLI versão 2 e configure-a usando suas credenciais. Para obter mais informações, consulte Instalar ou atualizar para a versão mais recente da AWS CLI e Configurar a AWS CLI no Guia do usuário da AWS Command Line Interface.
- Como alternativa, abra AWS CloudShell e execute os comandos da AWS CLI em seu shell pré-autenticado.

Para se conectar a uma instância usando o ID da instância e um EC2 Instance Connect Endpoint

Se você souber apenas o ID da instância, use o comando ec2-instance-connect ssh da CLI e especifique o comando `ssh`, o ID da instância e o parâmetro `--connection-type` com o valor `eice` para usar um EC2 Instance Connect Endpoint. Se a instância tiver apenas um endereço IPv6, você deverá incluir também o parâmetro `--instance-ip` com o endereço IPv6.

- Se a instância tiver um endereço IPv4 privado (ela também pode ter um endereço IPv6), use o seguinte comando e os seguintes parâmetros:

```
aws ec2-instance-connect ssh \
    --instance-id i-1234567890example \
    --os-user ec2-user \
```

```
    --connection-type eice
```

- Se a instância tiver apenas um endereço IPv6, inclua o parâmetro `--instance-ip` com o endereço IPv6:

```
aws ec2-instance-connect ssh \
    --instance-id i-1234567890example \
    --instance-ip 2001:db8::1234:5678:1.2.3.4 \
    --os-user ec2-user \
    --connection-type eice
```

> **Tip**
>
> Se receber um erro ao usar esse comando, verifique se está usando a versão 2 da AWS CLI. O parâmetro `ssh` apenas está disponível para o AWS CLI versão 2. Para obter mais informações, consulte Sobre o AWS CLI versão 2, no Guia do usuário do AWS Command Line Interface.

Conectar-se à sua instância baseada no Windows usando RDP

É possível usar o Remote Desktop Protocol (RDP) no EC2 Instance Connect Endpoint para se conectar a uma instância do Windows sem um endereço IPv4 público ou nome de DNS público.

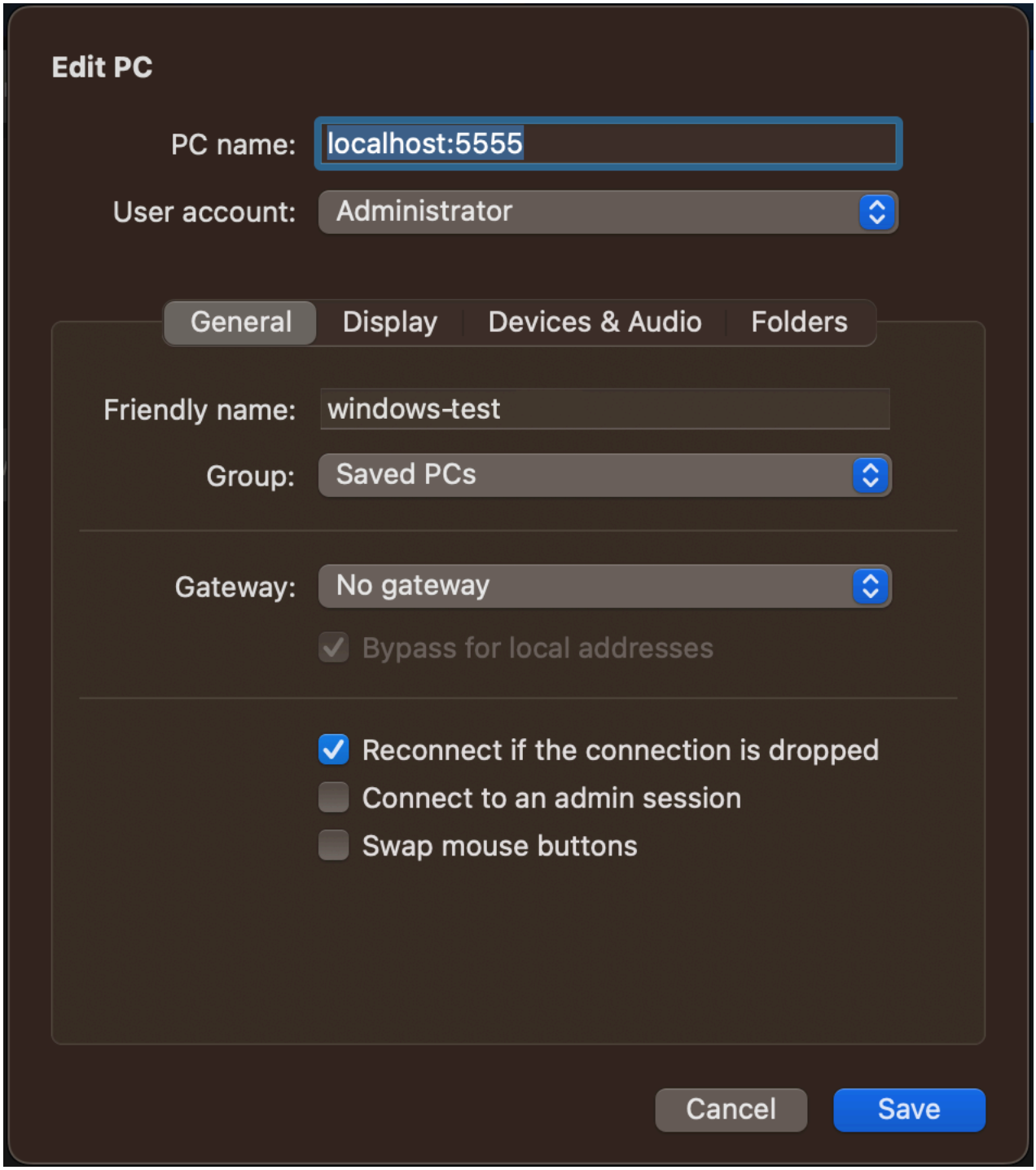
Para se conectar à sua instância do Windows usando um cliente RDP

1. Conclua as etapas 1 a 8 em Conectar-se à sua instância baseada no Windows usando RDP. Após fazer o download do arquivo da área de trabalho RDP na Etapa 8, você receberá uma mensagem Não foi possível se conectar, o que é esperado porque a instância não tem um endereço IP público.
2. Execute o comando a seguir para estabelecer um túnel privado para a VPC na qual a instância está localizada. A `--remote-port` deve ser `3389`, pois o RDP usa a porta 3389 por padrão.

```
aws ec2-instance-connect open-tunnel \
    --instance-id i-1234567890abcdef0 \
    --remote-port 3389 \
    --local-port any-port
```

3. Na sua pasta Downloads, localize o arquivo de área de trabalho de RDP que você baixou e arraste-o para a janela do cliente RDP.
4. Clique com o botão direito do mouse no arquivo de área de trabalho de RDP e escolha Editar.
5. Na janela Editar computador, para Nome do computador (a instância à qual se conectar), insira `localhost:`*`local-port`*, em que *`local-port`* usa o mesmo valor especificado na Etapa 2, e, em seguida, escolha Salvar.

   Observe que a captura de tela a seguir da janela Editar PC é do Microsoft Remote Desktop em um Mac. Se você estiver usando um cliente Windows, a janela pode ser diferente.



6. No cliente RDP, clique com o botão direito do mouse no PC (que você acabou de configurar) e escolha Conectar para se conectar à sua instância.
7. No prompt, insira a senha descriptografada da conta do administrador.

Solução de problemas

Use as informações a seguir para ajudar a diagnosticar e corrigir problemas que podem ser encontrados ao usar o EC2 Instance Connect Endpoint para se conectar a uma instância.

Não é possível conectar-se à sua instância

A seguir estão motivos comuns pelos quais você pode não conseguir se conectar à sua instância.

- Grupos de segurança: verifique os grupos de segurança atribuídos ao EC2 Instance Connect Endpoint e à sua instância. Para obter mais informações sobre as regras necessárias de grupo de segurança, consulte Grupos de segurança para o EC2 Instance Connect Endpoint.
- Estado da instância:^verifique se a instância está no estado `running`.
- Par de chaves: se o comando que você está usando para se conectar exigir uma chave privada, verifique se sua instância tem uma chave pública e se você tem a chave privada correspondente.
- Permissões do IAM: verifique se você tem as permissões do IAM necessárias. Para obter mais informações, consulte Conceder permissões para usar o EC2 Instance Connect Endpoint.

Para obter mais dicas de solução de problemas para instâncias do Linux, consulte Solucionar problemas de conexão com a instância do Linux do Amazon EC2. Para obter dicas de solução de problemas para instâncias do Windows, consulte the section called “Problemas de RDP com instâncias do Windows”.

ErrorCode: AccessDeniedException

Se você receber um erro `AccessDeniedException` e a condição `maxTunnelDuration` estiver especificada na política do IAM, certifique-se de especificar o parâmetro `--max-tunnel-duration` ao conectar-se a uma instância. Para obter mais informações sobre esse parâmetro, consulte open-tunnel na Referência de comandos da AWS CLI.

Registro em log de conexões estabelecidas através do EC2 Instance Connect Endpoint

É possível registrar em log operações de recursos e auditar conexões estabelecidas através do EC2 Instance Connect Endpoint com logs do AWS CloudTrail.

Para obter mais informações sobre o uso do AWS CloudTrail com o Amazon EC2, consulte Registro em log das chamadas de API do Amazon EC2 usando o AWS CloudTrail.

Registro em log de chamadas da API do EC2 Instance Connect Endpoint com o AWS CloudTrail

As operações de recursos do EC2 Instance Connect Endpoint são registradas em log no CloudTrail como eventos de gerenciamento. Quando as seguintes chamadas de API são executadas, a atividade é registrada como um evento do CloudTrail no Histórico de eventos:

- `CreateInstanceConnectEndpoint`
- `DescribeInstanceConnectEndpoints`
- `DeleteInstanceConnectEndpoint`

Você pode exibir, pesquisar e baixar eventos recentes em sua Conta da AWS. Para obter mais informações, consulte Visualizar eventos com o histórico de eventos CloudTrail no Guia do usuário do AWS CloudTrail.

Use o AWS CloudTrail para auditar usuários que se conectam a uma instância usando o EC2 Instance Connect Endpoint

As tentativas de conexão a instâncias por meio do EC2 Instance Connect Endpoint são registradas em log no CloudTrail no Histórico de eventos. Quando uma conexão a uma instância é iniciada por meio de um EC2 Instance Connect Endpoint, a conexão é registrada em log como um evento de gerenciamento do CloudTrail com `eventName` de `OpenTunnel`.

É possível criar regras do Amazon EventBridge que direcionem o evento do CloudTrail para um destino. Para saber mais, consulte o Guia do Usuário do Amazon EventBridge.

Veja a seguir o exemplo de um evento de gerenciamento `OpenTunnel` que foi registrado em log no CloudTrail.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "ABCDEFGONGNOMOOCB6XYTQEXAMPLE",
        "arn": "arn:aws:iam::1234567890120:user/IAM-friendly-name",
        "accountId": "123456789012",
        "accessKeyId": "ABCDEFGUKZHNAW4OSN2AEXAMPLE",
        "userName": "IAM-friendly-name"
    },
    "eventTime": "2023-04-11T23:50:40Z",
    "eventSource": "ec2-instance-connect.amazonaws.com",
```

```
    "eventName": "OpenTunnel",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "1.2.3.4",
    "userAgent": "aws-cli/1.15.61 Python/2.7.10 Darwin/16.7.0 botocore/1.10.60",
    "requestParameters": {
        "instanceConnectEndpointId": "eici-0123456789EXAMPLE",
        "maxTunnelDuration": "3600",
        "remotePort": "22",
        "privateIpAddress": "10.0.1.1"
    },
    "responseElements": null,
    "requestID": "98deb2c6-3b3a-437c-a680-03c4207b6650",
    "eventID": "bbba272c-8777-43ad-91f6-c4ab1c7f96fd",
    "readOnly": false,
    "resources": [{
        "accountId": "123456789012",
        "type": "AWS::EC2::InstanceConnectEndpoint",
        "ARN": "arn:aws:ec2:us-east-1:123456789012:instance-connect-endpoint/
eici-0123456789EXAMPLE"
    }],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```

Perfil vinculado ao serviço para o EC2 Instance Connect Endpoint

O Amazon EC2 usa perfis vinculados ao serviço do AWS Identity and Access Management (IAM). Um perfil vinculado ao serviço é um tipo especial de perfil do IAM vinculado diretamente ao Amazon EC2. Os perfis vinculados a serviços são predefinidas pelo Amazon EC2 e incluem todas as permissões que o Amazon EC2 requer para chamar outros Serviços da AWS em seu nome. Para obter mais informações, consulte Perfis vinculados ao serviço no Guia do usuário do IAM.

Permissões de perfil vinculado ao serviço para o EC2 Instance Connect Endpoint

O Amazon EC2 usa o AWSServiceRoleForEC2InstanceConnect para gerenciar as interfaces de rede em sua conta que são exigidas pelo EC2 Instance Connect Endpoint.

O perfil vinculado ao serviço AWSServiceRoleForEC2InstanceConnect confia nos seguintes serviços para assumir o perfil:

- `ec2-instance-connect.amazonaws.com`

O perfil vinculado ao serviço AWSServiceRoleForEC2InstanceConnect utiliza a seguinte política gerenciada:

- Ec2InstanceConnectEndpoint

Para visualizar as permissões para esta política gerenciada, consulte Ec2InstanceConnectEndpoint na Referência de políticas gerenciadas da AWS.

Criar um perfil vinculado ao serviço para um EC2 Instance Connect Endpoint

Você não precisa criar manualmente esse perfil vinculado ao serviço. Quando você cria um EC2 Instance Connect Endpoint, o Amazon EC2 cria o perfil vinculado ao serviço por você.

Editar um perfil vinculado ao serviço para o EC2 Instance Connect Endpoint

O EC2 Instance Connect Endpoint não permite editar o perfil vinculado ao serviço AWSServiceRoleForEC2InstanceConnect.

Excluir um perfil vinculado ao serviço para um EC2 Instance Connect Endpoint

Se você não precisar mais usar o EC2 Instance Connect Endpoint, é recomendável excluir o perfil vinculado ao serviço AWSServiceRoleForEC2InstanceConnect.

Antes de excluir o perfil vinculado ao serviço, é necessário excluir todos os recursos do EC2 Instance Connect Endpoint.

Para excluir o perfil vinculado ao serviço, consulte Exclusão de um perfil vinculado ao serviço no Guia do usuário do IAM.

Você deve configurar permissões para que uma entidade do IAM (um usuário, grupo ou função) crie, edite ou exclua um perfil vinculado a serviço. Para ter mais informações, consulte Permissões de perfil vinculado a serviços no Guia do usuário do IAM.

Cotas para EC2 Instance Connect Endpoint

Sua Conta da AWS tem cotas padrão para cada serviço da AWS, que anteriormente eram chamadas de limites. A menos que especificado de outra forma, cada cota é específica da região.

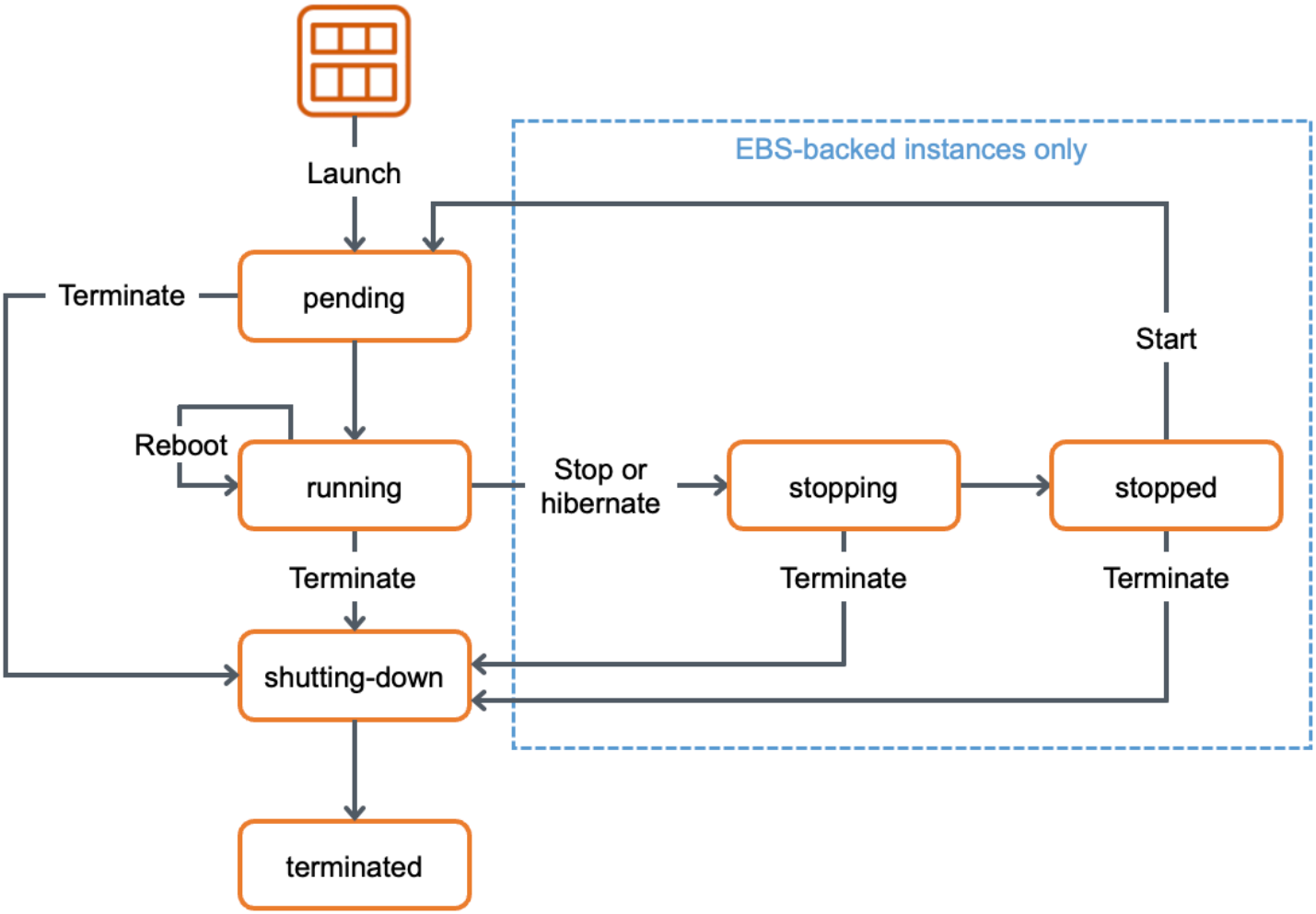
Sua Conta da AWS tem as seguintes cotas relacionadas ao EC2 Instance Connect Endpoint.

Nome	Padrão	Ajustável
Número máximo de endpoints do EC2 Instance Connect por Conta da AWS Região da AWS	5	Não
Número máximo de endpoints do EC2 Instance Connect por VPC	1	Não
Número máximo de endpoints do EC2 Instance Connect por sub-rede	1	Não
Número máximo de conexões simultâneas por endpoint do Instance Connect do EC2	20	Não

Alterações do estado de instâncias do Amazon EC2

Uma instância do Amazon EC2 passa por diferentes estados do momento em que você a inicia até seu encerramento.

A ilustração a seguir representa as transições entre os estados da instância.



Você poderá receber notificações quando as instâncias mudarem de estado. Para obter mais informações, consulte the section called “Eventos de alteração de estado”.

Faturamento por estado da instância

A tabela apresentada a seguir fornece uma breve descrição de cada estado da instância e indica se o uso da instância é faturado. Alguns recursos da AWS, como volumes do Amazon EBS e endereços IP elásticos, incorrem em cobranças independentemente do estado da instância. Para obter mais informações, consulte Evitar cobranças inesperadas no Manual do usuário do AWS Billing.

Estado da instância	Descrição	Faturamento para uso da instância
`pending`	A instância está se preparando para entrar no estado `running`. Uma instância entra no estado `pending` quando ela é executada ou quando é iniciada após estar no estado `stopped`.	Não faturado
`running`	A instância está em execução e pronta para uso.	Faturado
`stopping`	A instância está se preparando para ser interrompida.	Não faturado **Note** Caso hiberne uma instância, você será cobrado enquanto a instância estiver no estado `stopping`.
`stopped`	A instância está desativada e não pode ser usada. A instância pode ser iniciada a qualquer momento.	Não faturado
`shutting-down`	A instância está se preparando para ser encerrada.	Não faturado
`terminated`	A instância foi permanentemente excluída e não pode ser iniciada.	Não faturado

Estado da instância	Descrição	Faturamento para uso da instância
		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 . Visão geral de instâncias reservadas para o Amazon EC2

Instâncias pendentes

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`. É possível se conectar à instância em execução e usá-la da forma como usaria um computador bem à sua frente.

Assim que sua instância fizer a transição para o estado `running`, você será cobrado por cada segundo, com o mínimo de um minuto, que mantiver a instância em execução, mesmo se a instância permanecer ociosa e você não se conectar a ela.

Instâncias interrompidas

Se sua instância falhar na verificação de status ou não estiver executando suas aplicações como esperado, e se o volume do dispositivo raiz de sua instância for um volume do Amazon EBS, será possível 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`. Você não é cobrado pelas taxas de uso ou transferência de dados da sua instância quando ela é `stopped`. Cobranças são geradas pelo armazenamento de qualquer volume do Amazon EBS. Quando sua instância estiver no estado `stopped`, será possível modificar determinados atributos da instância, inclusive o tipo de instância.

Quando você inicia a instância, ela entra no estado `pending` e é movida para um novo computador host (embora em alguns casos ela permaneça no host atual). Quando você interrompe e inicia instância, perde todos os dados nos volumes de armazenamento de instância anexados ao 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 permanece associado à sua instância. Se sua instância tiver um endereço IPv6, ela reterá o endereço IPv6.

Toda vez que você faz a transição de uma instância de `stopped` para `running`, a cobrança é feita por segundo quando a instância está em execução, com no mínimo um minuto por início de instância.

Para obter mais detalhes sobre como interromper e iniciar instâncias, consulte Início e interrupção de instâncias do Amazon EC2.

Instâncias hibernadas

Ao hibernar uma instância, sinalizamos para o sistema operacional para executar hibernação (suspend-to-disk), o que salva o conteúdo da memória da instância (RAM) no volume raiz do Amazon EBS. Persistimos o volume raiz do Amazon EBS e todos os volumes de dados do Amazon EBS da instância anexados. Quando você inicia a instância, o volume raiz do Amazon EBS é restaurado para seu estado anterior, e o conteúdo da RAM é recarregado. Os volumes de dados anexados anteriormente são reanexados e a instância conserva seu ID de instância.

Quando você hiberna a instância, ela entra no estado `stopping` e, em seguida, no estado `stopped`. Não cobramos pelo uso de uma instância hibernada quando ela está no estado `stopped`, mas cobramos quando ela está no estado `stopping`, ao contrário de quando você interrompe uma instância sem hiberná-la. Não cobramos pelo uso de taxas de transferência de dados, mas cobramos pelo armazenamento de qualquer volume do Amazon EBS, incluindo armazenamento dos dados da RAM.

Quando você inicia a instância hibernada, ela entra no estado `pending` e a movemos para um novo computador host (embora em alguns casos, ela permaneça no host atual).

Sua instância retém o endereço IPv4 privado, o que significa que um endereço IP elástico associado ao endereço IPv4 privado ou à interface de rede ainda estará associado à sua instância. Se sua instância tiver um endereço IPv6, ela reterá o endereço IPv6.

Para obter mais informações, consulte Hibernar sua instância do Amazon EC2.

Instâncias de reinicialização

É possível reinicializar sua instância usando o console do Amazon EC2, uma ferramenta da linha de comando e a API do Amazon EC2. Recomendamos que você use o Amazon EC2 para reinicializar sua instância em vez de executar o comando de reinicialização do sistema operacional pela sua instância.

A reinicialização de uma instância equivale a reinicialização de um sistema operacional. A instância permanece no mesmo computador host e mantém seu nome DNS público, endereço IP privado e todos os dados em seus volumes de armazenamento de instância. Normalmente demora alguns minutos para a reinicialização ser concluída, mas o tempo necessário para reinicialização depende da configuração da instância.

Reiniciar uma instância não inicia uma novo período de faturamento de instância; o faturamento por segundo continua sem a cobrança mínima de um minuto.

Para obter mais informações, consulte Reinicializar uma instância do Amazon EC2.

Instâncias encerradas

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. Também é possível 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 baseada no Amazon EBS é compatível com o atributo `InstanceInitiatedShutdownBehavior`, que controla se a instância é interrompida ou encerrada quando você inicia o desligamento de dentro da própria instância (por exemplo, ao usar o comando shutdown no Linux). O comportamento padrão é interromper a instância. É possível 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. Por padrão, o volume raiz é excluído, enquanto os demais volumes do EBS são preservados.

Para obter mais informações, consulte Encerramento de instâncias do Amazon EC2.

Diferenças entre os estados de instâncias

A tabela a seguir resume as principais diferenças entre reinicialização, parada, hibernação e encerramento da sua instância.

Característica	Reinicializar	Parar/iniciar (somente instâncias baseadas no Amazon EBS)	Hibernação (somente instâncias baseadas no Amazon EBS)	Encerrar
Computador host	A instância permanece no mesmo computador host.	Nós movemos a instância para um novo computador host (embora em alguns casos, ela permaneça no host atual).	Nós movemos a instância para um novo computador host (embora em alguns casos, ela permaneça no host atual).	Nenhum
Endereço IPv4 privado	A instância mantém seu endereço IPv4 privado.	A instância mantém seu endereço IPv4 privado.	A instância mantém seu endereço IPv4 privado.	Nenhum
Endereço IPv4 público	A instância mantém seu endereço IPv4 público.	A instância obtém um novo endereço IPv4 público, a menos que tenha uma interface de rede secundária ou um endereço IPv4 privado secundário associado a	A instância obtém um novo endereço IPv4 público, a menos que tenha uma interface de rede secundária ou um endereço IPv4 privado secundári	Nenhum

Característica	Reinicializar	Parar/iniciar (somente instâncias baseadas no Amazon EBS)	Hibernação (somente instâncias baseadas no Amazon EBS)	Encerrar
		um endereço IP elástico.	o associado a um endereço IP elástico.	
Endereço IP elástico (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	A instância mantém seu endereço IPv6	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 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

Característica	Reinicializar	Parar/iniciar (somente instâncias baseadas no Amazon EBS)	Hibernação (somente instâncias baseadas no Amazon EBS)	Encerrar
Faturamento	O momento de faturamento da instância não sofre alterações.	As cobranças de uma instância são interrompidas assim que o estado mudar para `stopping`. Toda vez que uma instância faz a transição de `stopped` para `running`, nós iniciamos um novo período, cobrando o mínimo de um minuto toda vez que você inicia a instância.	Você incorre em cobranças quando a instância está no estado `stopping`, mas não incorre em cobranças quando a instância está no estado `stopped`. Toda vez que uma instância faz a transição de `stopped` para `running`, nós iniciamos um novo período, cobrando o mínimo de um minuto toda vez que você inicia a instância.	Você deixa de incorrer em cobranças para uma instância assim que o estado é alterado para `shutting-down` .

Comandos de desligamento do sistema operacional sempre encerram uma instância com volume raiz do tipo armazenamento de instância. É possível controlar se os comandos de desligamento do sistema operacional devem interromper ou encerrar uma instância com volume raiz do EBS. Para obter mais informações, consulte Alterar comportamento de desligamento iniciado da instância.

Início e interrupção de instâncias do Amazon EC2

Você pode interromper e reiniciar a instância se o volume raiz for um volume do Amazon EBS. Quando você interrompe uma instância, ela é desligada. Quando você inicia uma instância, ela é normalmente migrada para um novo computador host subjacente e recebe um novo endereço IPv4 público.

Uma parada de instância pode ser iniciada pelo usuário (quando você interrompe manualmente a instância) ou iniciada pela AWS (em resposta a um evento de parada programada quando a AWS detecta uma falha irreparável do host subjacente da sua instância).

Para interrupções iniciadas pelo usuário, recomendamos usar o console do Amazon EC2, a CLI ou a API em vez de executar o comando de interrupção do sistema operacional na instância. Ao usar o Amazon EC2, se a instância não for desligada de maneira limpa em alguns minutos, o Amazon EC2 realizará um desligamento forçado. Além disso, o AWS CloudTrail cria um registro de API de quando a instância foi interrompida.

Este tópico descreve como realizar uma interrupção iniciada pelo usuário. Para obter informações sobre uma interrupção realizada pelo AWS, consulte Gerenciamento das instâncias do Amazon EC2 agendadas para interrupção ou desativação.

Quando você interrompe uma instância, ela não é excluída. Se você decidir que não necessita mais de uma instância, pode encerrá-la. Para obter mais informações, consulte Encerramento de instâncias do Amazon EC2. Se você quiser hibernar uma instância para salvar o conteúdo da memória da instância (RAM), consulte Hibernar sua instância do Amazon EC2. Para obter distinções entre as ações do ciclo de vida da instância, consulte. Diferenças entre os estados de instâncias

Conteúdo

- Como funciona a inicialização e a interrupção de uma instância do EC2
- Métodos para parar uma instância
- Início e interrupção manuais das instâncias
- Parar e iniciar instâncias automaticamente
- Localizar todas as instâncias em execução e interrompidas
- Encontrar os horários de execução inicial e mais recente
- Habilitar a proteção contra interrupção para as instâncias do EC2

Como funciona a inicialização e a interrupção de uma instância do EC2

Quando você interrompe uma instância do Amazon EC2, as alterações são registradas no nível do sistema operacional (SO) da instância, alguns recursos são perdidos e outros persistem. Quando você inicia uma instância, as alterações são registradas no nível da instância.

Tópicos

- O que acontece quando você interrompe uma instância
- O que acontece quando você inicia uma instância
- Teste a resposta da aplicação para interromper e iniciar
- Custos relacionados ao início e à interrupção de uma instância

O que acontece quando você interrompe uma instância

Veja a seguir o que normalmente acontece quando você interrompe uma instância usando o método de parada padrão. Observe que alguns aspectos podem variar dependendo do método de parada usado.

Alterações registradas no nível do sistema operacional

- A solicitação da API envia um evento de pressionamento de botão ao convidado.
- Vários serviços do sistema são interrompidos como resultado do evento de pressionamento de botão. O desligamento normal do sistema operacional é acionado pelo evento de pressionamento do botão de desligamento de ACPI do hipervisor.
- O desligamento de ACPI é iniciado.
- A instância será desligada quando o processo de desligamento normal do sistema operacional terminar. Não existe um tempo de desligamento configurável para o SO.
- Se o sistema operacional da instância não for desligado de forma limpa em alguns minutos, um desligamento forçado será executado.
- A execução da instância é interrompida.
- O estado da instância muda para `stopping` e depois para `stopped`.
- [Auto Scaling] Se a instância estiver em um grupo do Auto Scaling, quando ela estiver em qualquer estado do Amazon EC2 diferente de `running` ou se o status das verificações de status mudar para `impaired`, o Amazon EC2 Auto Scaling considerará a instância como não íntegra e a substituirá. Para obter mais informações, consulte Health checks for instances in an Auto Scaling group no Amazon EC2 Auto Scaling User Guide.
- [Instâncias do Windows] Quando você interrompe e inicia uma instância do Windows, o agente de inicialização executa tarefas na instância, como alterar as letras das unidades de quaisquer volumes do Amazon EBS anexados. Para obter mais informações sobre esses padrões e como é possível alterá-los, consulte the section called “EC2Launch v2”.

Recursos perdidos

- Dados armazenados na RAM.
- Dados armazenados nos volumes de armazenamento de instância.
- O endereço IPv4 público que o Amazon EC2 atribuiu automaticamente à instância quando ela foi iniciada. Para manter um endereço IPv4 público que nunca muda, é possível associar um endereço IP elástico à instância.

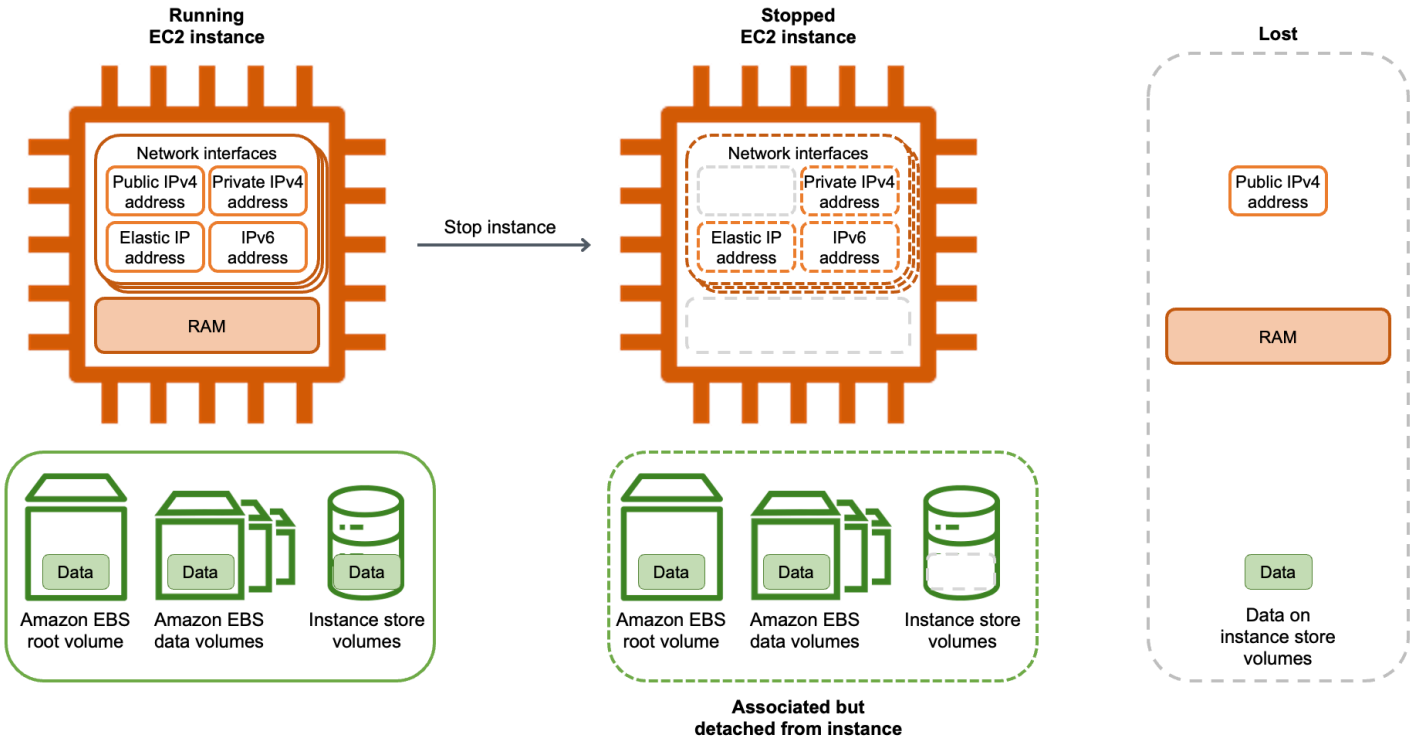
Recursos que persistem

- Qualquer volume raiz e de dados do Amazon EBS que esteja anexado.
- Dados armazenados em volumes do Amazon EBS.
- Qualquer interface de rede anexada.

  Uma interface de rede inclui os seguintes recursos, que também persistem:

  - Endereços IPv4 privados.
  - Endereços IPv6.
  - O endereço IP elástico a ser associado à instância. Observe que, quando a instância for interrompida, você será cobrado pelos endereços IP elásticos associados.

O diagrama a seguir ilustra o que é perdido e o que persiste quando uma instância do Amazon EC2 é interrompida. O diagrama é dividido em três partes: a primeira parte, chamada Instância do EC2 em execução, mostra a instância no estado `running` com seus recursos. A segunda parte, chamada Instância do EC2 parada, mostra a instância no estado `stopped` com os recursos que persistem. A terceira parte, chamada Perdido, mostra os recursos que são perdidos quando a instância é interrompida.



Para obter informações sobre o que acontece quando você interrompe uma instância do Mac, consulte Parar ou terminar a instância do Mac no Amazon EC2.

O que acontece quando você inicia uma instância

- Na maioria dos casos, a instância é migrada para um novo computador host subjacente (embora em alguns casos, como quando uma instância está alocada a um host em uma configuração de Host dedicado, ela permaneça no host atual).
- Os volumes e interfaces de rede do EBS associados são reconectados à instância.
- O Amazon EC2 atribui um novo endereço IPv4 público à instância se ela estiver configurada para receber um endereço IPv4 público, a menos que tenha uma interface de rede secundária ou um endereço IPv4 privado secundário associado a um endereço IP elástico.
- 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 no início se não houver capacidade suficiente para a instância. Se você receber um erro de capacidade ao iniciar uma instância em um grupo de posicionamento que já tenha instâncias em execução, interrompa todas as instâncias no grupo de posicionamento e inicie-as novamente. Iniciar as instâncias pode migrá-las para o hardware com capacidade para todas as instâncias solicitadas.

Teste a resposta da aplicação para interromper e iniciar

É possível usar o AWS Fault Injection Service para testar como suas aplicações respondem quando sua instância é interrompida e iniciada. Para saber mais, consulte o Guia do usuário do AWS Fault Injection Service.

Custos relacionados ao início e à interrupção de uma instância

Os custos a seguir estão associados à interrupção e inicialização de uma instância.

Interrupção: assim que o estado de uma instância muda para `shutting-down` ou `terminated`, as cobranças pela instância deixam de ser feitas. Você não é cobrado pelas taxas de uso ou transferência de dados para instâncias interrompidas. No entanto, cobranças são aplicáveis para armazenar volumes de armazenamento do Amazon EBS.

Inicialização: toda vez que você inicia uma instância interrompida, cobramos o mínimo de um minuto pelo uso. Após um minuto, você será cobrado apenas pelos segundos que usar. Por exemplo, se você executar uma instância por 20 segundos e, em seguida, interrompê-la, será cobrado por um minuto completo. Se você executar uma instância por 3 minutos e 40 segundos, você será cobrado exatamente por 3 minutos e 40 segundos de uso.

Métodos para parar uma instância

Há quatro maneiras de realizar uma parada iniciada pelo usuário: parada padrão, parada com ignorar o desligamento do sistema operacional, parada forçada e parada forçada com ignorar o desligamento do sistema operacional. A tabela a seguir compara as principais diferenças entre os métodos de parada:

Método de parada	Objetivo principal	Caso de uso	Comando da CLI
Parada padrão	Desligamento normal da instância com tentativa de desligamento normal do sistema operacional.	Parada típica de uma instância.	`aws ec2 stop-instances \ --instance-id i-1234567890abcdef0`

Método de parada	Objetivo principal	Caso de uso	Comando da CLI
Parada com ignorar o desligamento do sistema operacional	Ignora o desligamento normal do sistema operacional ao parar uma instância.	Quando ignorar o desligamento normal do sistema operacional é necessário.	`aws ec2 stop-instances \ --instance-id i-1234567890abcdef0 \ --skip-os-shutdown`
Forçar a parada	Resolve instâncias travadas. Tenta primeiro uma parada padrão; se a instância não para, interrompe a instância à força.	Quando a instância está travada no estado `stopping`.	`aws ec2 stop-instances \ --instance-id i-1234567890abcdef0 \ --force`
Forçar a parada com ignorar o desligamento do sistema operacional	Força a parada e ignora o desligamento normal do sistema operacional ao parar uma instância.	Quando forçar a parada e ignorar o desligamento normal do sistema operacional são necessários.	`aws ec2 stop-instances \ --instance-id i-1234567890abcdef0 \ --force \ --skip-os-shutdown`

Para obter instruções sobre como usar cada método, consulte:

- Parar uma instância com um desligamento normal do sistema operacional

- Parar uma instância e ignorar o desligamento normal do sistema operacional
- Forçar a interrupção de uma instância

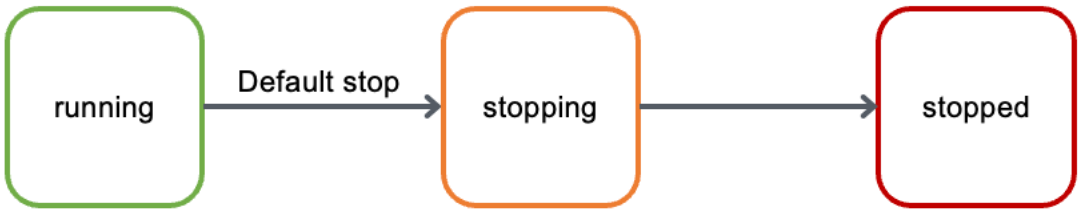
Métodos de parada:

- Parada padrão
- Parada com ignorar o desligamento do sistema operacional
- Forçar a parada
- Forçar a parada com ignorar o desligamento do sistema operacional

As seções a seguir fornecem informações mais detalhadas sobre os quatro métodos diferentes de parada iniciada pelo usuário.

Parada padrão

O método de parada padrão é a maneira padrão de parar uma instância. Quando você emite o comando StopInstances, a instância faz a transição do estado `running` para `stopping` e, finalmente, para `stopped`, conforme ilustrado no diagrama a seguir:



Objetivo: desligamento normal da instância com tentativa de desligamento normal do sistema operacional.

Impacto nos dados: preserva os dados no volume raiz e nos volumes de dados do EBS. Os dados no volume de armazenamento de instância são perdidos.

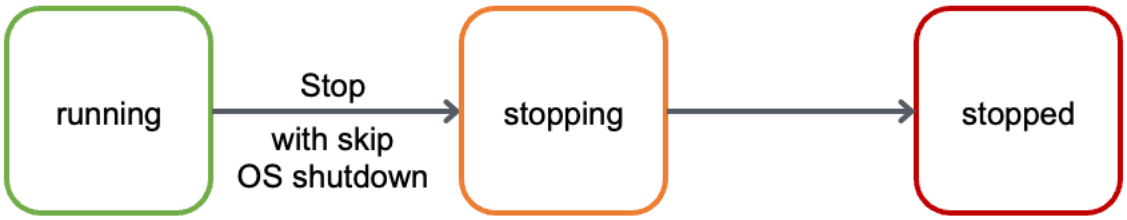
Quando usar: a primeira tentativa de parada em paradas típicas.

> **Note**
>
> Se você já tentou realizar uma parada com ignorar desligamento do sistema operacional, uma tentativa subsequente de parada padrão durante a mesma sessão de transição de estado não executará um desligamento normal do sistema operacional. Ignorar o

desligamento normal do sistema operacional é uma ação irreversível para a sessão atual da instância.

Parada com ignorar o desligamento do sistema operacional

Quando é necessário ignorar o desligamento normal do sistema operacional, o método de parada com ignorar desligamento do sistema operacional pode ser usado para parar uma instância e ignorar o desligamento normal do sistema operacional, conforme ilustrado no diagrama a seguir:



Warning

Ignorar o desligamento normal do sistema operacional pode resultar em perda ou corrompimento de dados (por exemplo, conteúdo da memória não transferido para o disco ou perda de E/S em andamento) ou em scripts de desligamento ignorados.

Objetivo: ignorar o desligamento normal do sistema operacional ao parar uma instância.

Impacto nos dados: pode resultar em perda ou corrompimento de dados. O conteúdo da memória pode não ser transferido para o disco e as operações de E/S em andamento podem ser perdidas. Pode ignorar scripts de desligamento.

Quando usar: quando é necessário ignorar o desligamento normal do sistema operacional. Se usada enquanto uma parada padrão com desligamento normal do sistema operacional estiver em andamento, o desligamento normal do sistema operacional será ignorado.

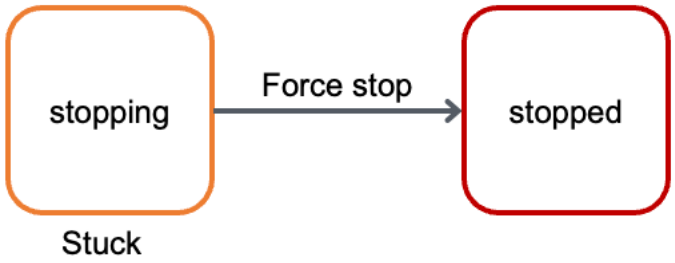
Note

Ignorar o desligamento normal do sistema operacional é uma ação irreversível para a sessão de transição de estado atual da instância. Uma tentativa de parada padrão subsequente durante esta sessão não tentará um desligamento normal do sistema operacional.

Forçar a parada

O método de forçar a parada é usado para lidar com instâncias que estão presas no estado `stopping`. Normalmente, uma instância fica paralisada devido a um problema de hardware subjacente (indicado por uma falha na verificação do status do sistema).

O método de parada forçada primeiro tenta realizar uma parada padrão. Se a instância permanecer presa no estado `stopping`, o parâmetro `force` encerrará a instância à força e fará a transição da instância para o estado `stopped`, conforme indicado no diagrama a seguir:



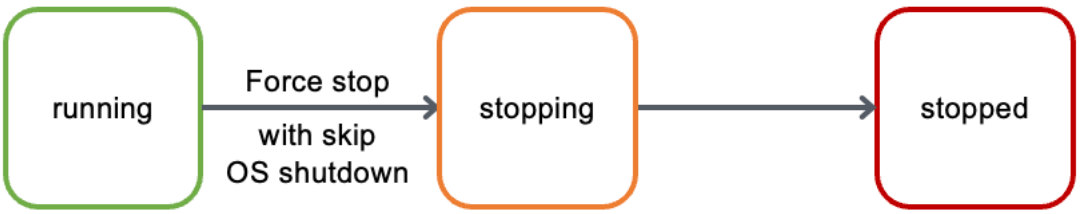
Objetivo: lida com instâncias bloqueadas no estado `stopping`. Tenta primeiro uma parada padrão. Se a instância não for interrompida, ela será desligada à força.

Impacto nos dados: tenta primeiro uma parada padrão, mas se a parada forçada continuar, isso pode causar perda ou corrompimento de dados. Em casos raros, resulta em gravações pós-parada em volumes do EBS ou em outros recursos compartilhados.

Quando usar: segunda tentativa de parada quando uma instância permanece travada após uma parada padrão. Para obter mais informações, consulte Solucionar problemas de interrupção de instâncias do Amazon EC2.

Forçar a parada com ignorar o desligamento do sistema operacional

Quando forçar a parada e ignorar o desligamento normal do sistema operacional são necessários, o método de forçar a parada com ignorar desligamento do sistema operacional pode ser usado para levar uma instância ao estado `stopped`, conforme ilustrado no diagrama a seguir:



Objetivo: combina forçar a parada com ignorar o desligamento normal do sistema operacional ao parar uma instância.

Impacto nos dados: ignorar o desligamento do sistema operacional pode resultar em perda ou corrompimento de dados. O conteúdo da memória pode não ser transferido para o disco e as operações de E/S em andamento podem ser perdidas. Pode ignorar scripts de desligamento. Se a parada forçada ocorrer, ela poderá causar perda ou corrompimento adicional de dados. Em casos raros, resulta em gravações pós-parada nos volumes do EBS ou em outros recursos compartilhados.

Quando usar: quando você quer ter certeza de que sua instância será interrompida e deseja ignorar o desligamento normal do sistema operacional. Se usada enquanto uma parada padrão com desligamento normal do sistema operacional estiver em andamento, o desligamento normal do sistema operacional será ignorado.

Início e interrupção manuais das instâncias

É possível iniciar e parar instâncias baseadas no Amazon EBS (instâncias com volumes-raiz do EBS). Não é possível iniciar e parar instâncias com um volume-raiz de armazenamento de instância.

Ao usar o método padrão para parar uma instância, uma tentativa de desligamento normal do sistema operacional (SO) é feita. É possível ignorar o desligamento normal do sistema operacional; no entanto, isso pode colocar em risco a integridade dos dados.

> **Warning**
>
> Quando você interrompe uma instância, os dados em todos os volumes de armazenamento de instâncias são apagados. Antes de interromper uma instância, verifique se você copiou todos os dados necessários dos volumes de armazenamento de instância para um armazenamento persistente, como o Amazon EBS ou o Amazon S3.

[Instâncias do Linux] Usar o comando halt do sistema operacional de uma instância não inicia um desligamento. Se você usar o comando halt, a instância não será encerrada; em vez disso, ela colocará a CPU em HLT, o que suspende a operação da CPU. A instância permanece em execução.

Você pode iniciar um desligamento usando os comandos shutdown ou poweroff do sistema operacional. Quando você usa um comando do sistema operacional, a instância é interrompida por padrão. É possível alterar esse comportamento. Para obter mais informações, consulte Alterar comportamento de desligamento iniciado da instância.

> **Note**
>
> Se você interrompeu uma instância baseada no Amazon EBS e ela aparentar estar "presa" no estado `stopping`, será possível interrompê-la à força. Para obter mais informações, consulte Solucionar problemas de interrupção de instâncias do Amazon EC2.

Métodos de interrupção e execução

- Parar uma instância com um desligamento normal do sistema operacional
- Parar uma instância e ignorar o desligamento normal do sistema operacional
- Iniciar uma instância

Parar uma instância com um desligamento normal do sistema operacional

É possível parar uma instância usando o método de parada padrão, que inclui uma tentativa de desligamento normal do sistema operacional. Para obter mais informações, consulte Parada padrão.

Console

Para parar uma instância usando o método padrão

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação à esquerda, escolha Instâncias e, em seguida, selecione a instância.
3. Escolha Estado da instância e Parar instância. Se a opção estiver desabilitada, significa que a instância já está interrompida ou que o volume raiz é um armazenamento de instância.
4. Quando a confirmação for solicitada, escolha Parar. Pode demorar alguns minutos para que a instância pare.

AWS CLI

Para parar uma instância usando o método padrão

Use o comando stop-instances.

```
aws ec2 stop-instances --instance-ids i-1234567890abcdef0
```

PowerShell

Para parar uma instância usando o método padrão

Use o cmdlet Stop-EC2Instance.

```
Stop-EC2Instance -InstanceId i-1234567890abcdef0
```

Parar uma instância e ignorar o desligamento normal do sistema operacional

É possível ignorar o desligamento normal do sistema operacional ao parar uma instância. Para obter mais informações, consulte Parada com ignorar o desligamento do sistema operacional.

> **Warning**
>
> Ignorar o desligamento normal do sistema operacional pode resultar em perda ou corrompimento de dados (por exemplo, conteúdo da memória não transferido para o disco ou perda de E/S em andamento) ou em scripts de desligamento ignorados.

Console

Para parar uma instância e ignorar o desligamento normal do sistema operacional

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 Instance state (Estado da instância) e Stop instance (Interromper instância).
4. Em Ignorar desligamento do sistema operacional, marque a caixa de seleção Ignorar desligamento do sistema operacional. Se você não vir essa opção no console, isso significa que ela ainda não está disponível no console na região atual. No entanto, você pode acessar esse recurso usando a AWS CLI ou o SDK, ou até mesmo experimentar outra região no console.
5. Escolha Parar.

AWS CLI

Para parar uma instância e ignorar o desligamento normal do sistema operacional

Use o comando stop-instances com `--skip-os-shutdown`.

```
aws ec2 stop-instances \
    --instance-ids i-1234567890abcdef0 \
    --skip-os-shutdown
```

PowerShell

Para parar uma instância e ignorar o desligamento normal do sistema operacional

Use o cmdlet Stop-EC2Instance com `-SkipOsShutdown $true`.

```
Stop-EC2Instance `
    -InstanceId i-1234567890abcdef0 `
    -SkipOsShutdown $true
```

Iniciar uma instância

Você pode iniciar uma instância parada.

Console

Para iniciar uma instância

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação à esquerda, selecione Instâncias.
3. Selecione a instância e escolha Estado da instância e Iniciar instância.

   Pode demorar alguns minutos para que a instância entre no estado `running`.

AWS CLI

Para iniciar uma instância

Use o comando start-instances.

```
aws ec2 start-instances --instance-ids i-1234567890abcdef0
```

PowerShell

Para iniciar uma instância

Use o cmdlet Start-EC2Instance.

```
Start-EC2Instance -InstanceId i-1234567890abcdef0
```

Parar e iniciar instâncias automaticamente

É possível automatizar a interrupção e o início de instâncias com os seguintes serviços:

Instance Scheduler na AWS

É possível usar o Instance Scheduler na AWS para automatizar o início e a interrupção de instâncias do EC2. Para obter mais informações, consulte How do I use Instance Scheduler with CloudFormation to schedule EC2 instances? (Como uso o Instance Scheduler com o CloudFormation para agendar instâncias do EC2?) Observe que se aplicam outras cobranças.

AWS Lambda e uma regra do Amazon EventBridge

É possível usar o Lambda e uma regra do EventBridge para interromper e iniciar suas instâncias em um agendamento. Para obter mais informações, consulte Como usar o Lambda para interromper e iniciar instâncias do Amazon EC2 em intervalos regulares?

Amazon EC2 Auto Scaling

Para garantir que você tenha o número correto de instâncias do Amazon EC2 disponíveis para lidar com a carga de uma aplicação, crie grupos do Auto Scaling. O Amazon EC2 Auto Scaling garante que sua aplicação sempre tenha a capacidade certa para lidar com a demanda de tráfego e economiza custos ao iniciar instâncias somente quando elas são necessárias. Observe que o Amazon EC2 Auto Scaling encerra, em vez de interromper, instâncias desnecessárias. Para configurar grupos do Auto Scaling, consulte Começar a usar o Amazon EC2 Auto Scaling.

Localizar todas as instâncias em execução e interrompidas

É possível localizar todas as instâncias em execução e interrompidas em todas as Regiões da AWS em uma única página na Visualização Global do Amazon EC2. Isso é útil especialmente para inventariar e localizar instâncias esquecidas. Para obter informações sobre como usar o Visualização Global , consulte Visualizar recursos entre regiões usando a Visualização Global da AWS.

Como alternativa, você pode executar um comando ou cmdlet em cada região na qual tenha instâncias.

AWS CLI

Para obter o número de instâncias do EC2 em uma região

Use o seguinte comando describe-instances para contar as instâncias na região atual. Você precisa executar esse comando em cada região na qual tenha instâncias.

```
aws ec2 describe-instances \
    --region us-east-2 \
    --query "length(Reservations[].Instances[])"
```

O seguinte é um exemplo de saída.

```
27
```

Para obter um resumo de informações sobre suas instâncias do EC2 em uma região

Use o seguinte comando describe-instances. Você precisa executar esse comando em cada região na qual tenha instâncias.

```
aws ec2 describe-instances \
    --region us-east-2 \
    --query "Reservations[].Instances[].[InstanceId,InstanceType,PrivateIpAddress]"
 \
    --output table
```

O seguinte é um exemplo de saída.

```
-------------------------------------------------------------
|                   DescribeInstances                       |
+---------------------+---------------+-----------------+
|  i-0e3e777f4362f1bf7|  t2.micro     |  10.0.12.9      |
|  i-09453945dcf1529e9|  t2.micro     |  10.0.143.213   |
|  i-08fd74f3f1595fdbd|  m7i.4xlarge  |  10.0.1.103     |
+---------------------+---------------+-----------------+
```

PowerShell

Para obter o número de instâncias do EC2 em uma região

Use o cmdlet Get-EC2Instance.

```
(Get-EC2Instance -Region us-east-2).Instances.Length
```

O seguinte é um exemplo de saída.

```
27
```

Para obter um resumo de informações sobre suas instâncias do EC2 em uma região

Use o cmdlet Get-EC2Instance. Você precisa executar esse comando em cada região na qual tenha instâncias.

```
(Get-EC2Instance).Instances | Select InstanceId, InstanceType, PrivateIpAddress
```

O seguinte é um exemplo de saída.

```
InstanceId          InstanceType PrivateIpAddress
----------          ------------ ----------------
i-0e3e777f4362f1bf7 t2.micro     10.0.12.9
i-09453945dcf1529e9 t2.micro     10.0.143.213
i-08fd74f3f1595fdbd m7i.4xlarge  10.0.1.103
```

Encontrar os horários de execução inicial e mais recente

Quando você descreve uma instância, o horário de execução dela é o mais recente. Depois que você interrompe e inicia uma instância, o horário de execução reflete o horário de início da nova instância. Para descobrir o horário de execução inicial de uma instância, mesmo depois de interrompê-la e iniciá-la, consulte a hora em que a interface de rede primária foi anexada à instância.

Console

Para localizar o horário mais recente de inicialização

Selecione a instância e encontre Hora de inicialização em Detalhes da instância na guia Detalhes.

Para encontrar a hora inicial de inicialização

Selecione a instância e encontre a interface de rede primária (o índice do dispositivo é 0) em Interfaces de rede na guia Rede.

AWS CLI

Para encontrar os horários inicial e mais recente de inicialização

Use o seguinte comando describe-instances para exibir o horário inicial de inicialização e o horário mais recente de inicialização da instância especificada.

```
aws ec2 describe-instances \
    --instance-id i-1234567890abcdef0 \
    --query 'Reservations[].Instances[].
{InstanceID:InstanceId,InitialLaunch:NetworkInterfaces[0].Attachment.AttachTime,LastLaunch:L
```

O seguinte é um exemplo de saída.

```
[
    {
        "InstanceID": "i-1234567890abcdef0",
        "InitialLaunch": "2024-04-19T00:47:08+00:00",
        "LastLaunch": "2024-05-27T06:24:06+00:00"
    }
]
```

PowerShell

Para localizar o horário mais recente de inicialização

Use o cmdlet Get-EC2Instance.

```
(Get-EC2Instance -InstanceId i-1234567890abcdef0).Instances.LaunchTime
```

O seguinte é um exemplo de saída.

```
Monday, May 27, 2024 6:24:06 AM
```

Para encontrar a hora inicial de inicialização

Use o cmdlet Get-EC2Instance.

```
(Get-EC2Instance -
InstanceId i-1234567890abcdef0).Instances.NetworkInterfaces.Attachment.AttachTime
```

O seguinte é um exemplo de saída.

```
Friday, April 19, 2024 12:47:08 AM
```

Habilitar a proteção contra interrupção para as instâncias do EC2

Para impedir que uma instância seja interrompida acidentalmente, habilite a proteção contra interrupção da instância. A proteção contra interrupção também protege a instância contra término acidental.

O atributo `DisableApiStop` da API `ModifyInstanceAttribute` do Amazon EC2 controla se a instância pode ser interrompida usando o console do Amazon EC2, a AWS CLI ou a API do Amazon EC2. É possível definir o valor desse atributo ao executar a instância, enquanto a instância estiver em execução ou quando a instância for interrompida.

Considerações

- Habilitar a proteção contra interrupção não impede que você interrompa acidentalmente uma instância iniciando um desligamento da instância com um comando do sistema operacional, como shutdown ou poweroff.
- Habilitar a proteção contra interrupção não impede que a AWS interrompa a instância quando houver um evento programado para interromper a instância.
- Habilitar a proteção contra interrupção não impede que Amazon EC2 Auto Scaling termine uma instância quando ela não estiver íntegra ou durante eventos de redução da escala horizontal. É possível controlar se um grupo do Auto Scaling pode encerrar uma instância específica ao reduzir a escala horizontalmente usando a proteção contra redução da escala da instância na horizontal.
- A proteção contra interrupção não só impede que a instância seja interrompida acidentalmente, mas também previne o término acidental durante o uso do console, da AWS CLI ou da API. No entanto, isso não define automaticamente o atributo `DisableApiTermination`. Observe que, quando o atributo `DisableApiStop` é definido como `false`, o atributo `DisableApiTermination` é usado para determinar se a instância pode ser encerrada usando o console, a AWS CLI ou a API. Para obter mais informações, consulte Encerramento de instâncias do Amazon EC2.
- Não é possível habilitar a proteção contra interrupções para uma instância cujo volume raiz seja um armazenamento de instância.
- Não é possível habilitar a proteção contra interrupção para instâncias spot.
- A API do Amazon EC2 segue um modelo de consistência eventual quando você habilita ou desabilita a proteção contra interrupção. Isso significa que o resultado da execução de comandos

para definir o atributo da proteção contra interrupção poderá não ser imediatamente visível para todos os comandos subsequentes que forem executados. Para obter mais informações, consulte Eventual consistency no Guia do desenvolvedor do Amazon EC2.

Tarefas de proteção contra interrupção

- Habilitar a proteção contra interrupção de uma instância na inicialização
- Habilitar a proteção contra interrupção de uma instância em execução ou interrompida
- Desabilitar a proteção contra interrupção de uma instância em execução ou interrompida

Habilitar a proteção contra interrupção de uma instância na inicialização

É possível habilitar a proteção contra interrupções de uma instância ao inicializá-la.

Console

Como habilitar a proteção contra término de uma instância na inicialização

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel, escolha Executar instância.
3. Configure sua instância no novo assistente de inicialização de instância.
4. Para habilitar a proteção contra interrupções, em Advanced details (Detalhes avançados), em Stop protection (Proteção contra interrupções), escolha Enable (Habilitar).

AWS CLI

Como habilitar a proteção contra término de uma instância na inicialização

Use o comando run-instances para inicializar a instância. Adicione o seguinte parâmetro.

```
--disable-api-stop
```

PowerShell

Como habilitar a proteção contra término de uma instância na inicialização

Use o cmdlet New-EC2Instance para inicializar a instância. Adicione o seguinte parâmetro.

```
-DisableApiStop $true
```

Habilitar a proteção contra interrupção de uma instância em execução ou interrompida

É possível habilitar a proteção contra interrupções de uma instância enquanto a instância estiver em execução ou interrompida.

Console

Para habilitar a proteção contra interrupção de uma instância

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação à esquerda, selecione Instâncias.
3. Selecione a instância e escolha Ações > Configurações da instância > Alterar proteção contra interrupção.
4. Marque a caixa de seleção Habilitar e escolha Salvar.

AWS CLI

Para habilitar a proteção contra interrupção de uma instância

Use o comando modify-instance-attribute.

```
aws ec2 modify-instance-attribute \
    --instance-id i-1234567890abcdef0 \
    --disable-api-stop
```

PowerShell

Para habilitar a proteção contra interrupção de uma instância

Use o cmdlet Edit-EC2InstanceAttribute.

```
Edit-EC2InstanceAttribute `
    -InstanceId i-1234567890abcdef0 `
    -DisableApiStop $true
```

Desabilitar a proteção contra interrupção de uma instância em execução ou interrompida

Desabilite a proteção contra interrupções de uma instância em execução ou interrompida usando um dos métodos a seguir.

Console

Para desabilitar a proteção contra interrupção de uma instância em execução ou interrompida

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação à esquerda, selecione Instâncias.
3. Selecione a instância e escolha Actions (Ações), Instance Settings (Configurações da instância) e Change Termination Protection (Alterar proteção contra interrupção).
4. Desmarque a caixa de seleção Habilitar e escolha Salvar.

AWS CLI

Para desabilitar a proteção contra interrupção de uma instância em execução ou interrompida

Use o comando modify-instance-attribute.

```
aws ec2 modify-instance-attribute \
    --instance-id i-1234567890abcdef0 \
    --no-disable-api-stop
```

PowerShell

Para desabilitar a proteção contra interrupção de uma instância

Use o cmdlet Edit-EC2InstanceAttribute.

```
Edit-EC2InstanceAttribute `
    -InstanceId i-1234567890abcdef0 `
    -DisableApiStop $false
```

Hibernar sua instância do Amazon EC2

Ao hibernar uma instância, o Amazon EC2 indica a realização da hibernação (suspend-to-disk) ao sistema operacional. A hibernação salva os conteúdos da memória da instância (RAM) para o volume raiz do Amazon Elastic Block Store (Amazon EBS). O Amazon EC2 persiste o volume raiz do EBS e todos os volumes de dados do EBS anexados. Quando a instância é iniciada:

- O volume raiz do EBS é restaurado para seu estado anterior

- Os conteúdos da RAM são recarregados
- Os processos que estavam em execução anteriormente na instância são retomados
- Os volumes de dados anexados anteriormente são reanexados e a instância conserva seu ID de instância.

É possível hibernar uma instância apenas se ela estiver habilitada para hibernação e atender aos pré-requisitos de hibernação.

Se uma instância ou aplicação levar muito tempo para o bootstrap e criar um espaço de memória para se tornar totalmente produtivo, será possível usar a hibernação para preaquecer a instância. Para pré-aquecer a instância:

1. Execute-a com a hibernação habilitada.
2. Coloque-a em um estado desejado.
3. Deixe-a em hibernação para que ela fique pronta para ser retomada no estado desejado sempre que necessário.

Você não terá cobranças pelo uso de uma instância em hibernação quando ela estiver no estado `stopped` ou pela transferência de dados quando o conteúdo da RAM for transferido para o volume raiz do EBS. Você terá cobranças pelo armazenamento de quaisquer volumes do EBS, incluindo o armazenamento de conteúdo da RAM.

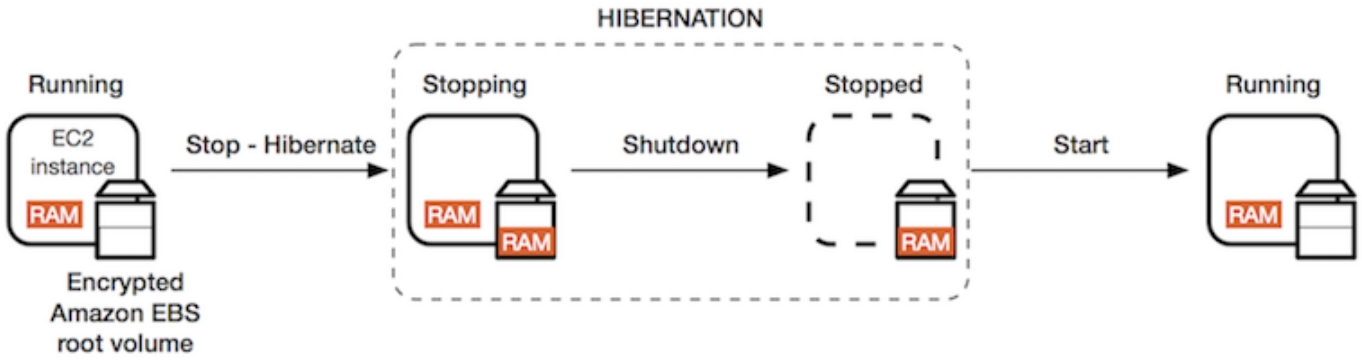
Se não precisar mais de uma instância, é possível encerrá-la a qualquer momento, incluindo quando ela está em um estado `stopped` (em hibernação). Para obter mais informações, consulte Encerramento de instâncias do Amazon EC2.

Conteúdo

- Como a hibernação de instâncias do Amazon EC2 funciona
- Pré-requisitos para a hibernação de instância do EC2
- Configurar uma AMI para oferecer suporte à hibernação
- Habilitar a hibernação para uma instância do Amazon EC2
- Desabilitar o KASLR em uma instância (apenas Ubuntu)
- Hibernar uma instância do Amazon EC2
- Iniciar um instância do Amazon EC2 em hibernação
- Solucionar problemas de hibernação de instâncias do Amazon EC2

Como a hibernação de instâncias do Amazon EC2 funciona

O diagrama a seguir mostra uma visão geral básica do processo de hibernação para instâncias do EC2.



O que acontece quando uma instância é colocada em hibernação

Quando uma instância é colocada em hibernação, o seguinte acontece:

- O instância entrará no estado `stopping`. O Amazon EC2 sinaliza o sistema operacional para realizar a hibernação (suspend-to-disk). A hibernação congela todos os processos, salva o conteúdo da RAM no volume raiz do EBS e, depois, executa um desligamento normal.
- Quando o desligamento é concluído, a instância muda para o estado `stopped`.
- Todos os volumes do EBS permanecem anexados à instância, e seus dados são mantidos, incluindo o conteúdo salvo da RAM.
- Todos os volumes de armazenamento de instâncias do Amazon EC2 permanecem associados à instância, mas os dados nos volumes de armazenamento de instância são perdidos.
- Na maioria dos casos, a instância é migrada para um novo computador host subjacente quando ele é iniciado. Isso também acontece ao interromper e iniciar uma instância.
- Quando a instância é iniciada, ela é carregada e o sistema operacional lê o conteúdo da RAM no volume raiz do EBS antes de descongelar os processos para retomar ao seu estado.
- A instância retém seus endereços IPv4 privados e todos os endereços IPv6. Quando a instância é iniciada, ela continua a reter os endereços IPv4 privados e todos os endereços IPv6.
- O Amazon EC2 libera o endereço IPv4 público. Quando a instância é iniciada, o Amazon EC2 atribui a ela um novo endereço IPv4 público.
- A instância retém os endereços IP elásticos associados. Você é cobrado por todos os endereços IP elásticos associados a uma instância em hibernação.

Para obter informações sobre como a hibernação difere da reinicialização, da interrupção e do encerramento, consulte Diferenças entre os estados de instâncias.

Limitações

- Quando você hiberna uma instância, os dados em todos os volumes de armazenamento de instâncias são perdidos.
- (Instâncias do Linux) Não é possível hibernar uma instância do Linux com mais de 150 GiB de RAM.
- (Instâncias do Windows) Não é possível hibernar uma instância do Windows com mais de 16 GiB de RAM.
- Enquanto sua instância está hibernando, você não pode modificá-la. Isso é diferente para uma instância parada que não está hibernando, na qual você pode modificar certos atributos, como o tipo ou o tamanho da instância.
- Se você criar um snapshot ou uma AMI a partir de uma instância que está hibernada ou que tenha hibernação habilitada, talvez não consiga se conectar a uma nova instância iniciada a partir da AMI ou de uma AMI criada pelo snapshot.
- (Apenas instâncias spot) Se o Amazon EC2 colocar sua instância spot em hibernação, somente o Amazon EC2 poderá reiniciá-la. Se você mesmo colocar a instância spot em hibernação (hibernação iniciada pelo usuário), poderá reiniciá-la. Uma instância spot colocada em hibernação só poderá ser reiniciada se houver capacidade disponível e se o preço spot for menor ou igual ao preço máximo especificado.
- Não é possível hibernar uma instância que está em um grupo do Auto Scaling ou é usada pelo Amazon ECS. Se sua instância estiver em um grupo do Auto Scaling, e você tentar hiberná-la, o serviço Amazon EC2 Auto Scaling marcará a instância interrompida como não íntegra e poderá encerrá-la e executar uma instância substituta. Para obter mais informações, consulte Health checks for instances in an Auto Scaling group no Amazon EC2 Auto Scaling User Guide.
- Não é possível efetuar a hibernação de uma instância configurada para inicializar no modo UEFI com o UEFI Secure Boot habilitado.
- Se você hibernar uma instância que foi executada em um Reserva de capacidade, o Reserva de capacidade não garante que a instância hibernada possa retornar depois de tentar iniciá-la.
- Você não pode hibernar uma instância que usa um kernel abaixo de 5.10 se o modo Federal Information Processing Standard (FIPS) estiver ativado.
- Não oferecemos suporte à manutenção de uma instância em hibernação por mais de 60 dias. Para manter a instância por mais que 60 dias, inicie, interrompa e inicialize a instância em hibernação.

- Atualizamos constantemente nossa plataforma com atualizações e patches de segurança, o que entra em conflito com instâncias em hibernação. Notificamos você sobre as atualizações críticas que exijam uma inicialização das instâncias em hibernação para que você possa executar um desligamento ou uma reinicialização para aplicar as atualizações e os patches de segurança necessários.

Considerações sobre colocar uma instância spot em hibernação

- Se você colocar em hibernação a instância spot, poderá reiniciá-la, desde que haja capacidade disponível e o preço spot seja menor ou igual ao preço máximo especificado.
- Se o Amazon EC2 colocar a instância spot em hibernação:
  - Somente o Amazon EC2 poderá reiniciar a instância.
  - O Amazon EC2 reinicia a instância spot que foi colocada em hibernação quando a capacidade fica disponível por um preço spot igual ou inferior ao preço máximo especificado por você.
  - Dois minutos antes que o Amazon EC2 coloque a instância spot em hibernação, você receberá um aviso de interrupção.

  Para obter mais informações, consulte Interrupções de instâncias spot.

Pré-requisitos para a hibernação de instância do EC2

É possível habilitar o suporte à hibernação para uma instância sob demanda ou uma instância spot ao iniciá-la. Não é possível habilitar a hibernação em uma instância existente, esteja ela em execução ou parada. Para obter mais informações, consulte Habilitar hibernação da instância.

Requisitos para hibernar uma instância

- Regiões da AWS
- AMIs
- Famílias de instâncias
- Tamanho da instância RAM
- Tipo do volume de raiz
- Tamanho do volume raiz
- Criptografia do volume raiz
- Tipo de volume do EBS
- Solicitações de instância Spot

Regiões da AWS

É possível usar a hibernação com instâncias em todas as Regiões da AWS.

AMIs

É necessário usar uma AMI do HVM que ofereça suporte à hibernação. As seguintes AMIs oferecem suporte para hibernação:

AMIs do Linux

AMIs para tipos de instância Intel e AMD

- AMI do AL2023 lançada em 20/09/2023 ou posteriormente [1]
- AMI do Amazon Linux 2 lançada em 29/08/2019 ou posterior
- AMI do Amazon Linux 2018.03 lançada em 16/11/2018 ou posterior
- AMI do CentOS versão 8 [2] (uma configuração adicional é necessária)
- AMI do Fedora versão 34 ou posterior [2] (uma configuração adicional é necessária)
- AMI do Red Hat Enterprise Linux (RHEL) 9 [2] (uma configuração adicional é necessária)
- AMI do Red Hat Enterprise Linux (RHEL) 8 [2] (uma configuração adicional é necessária)
- AMI do Ubuntu 22.04.2 LTS (Jammy Jellyfish) lançada com o número de série 20230303 ou posterior [3]
- AMI do Ubuntu 20.04 LTS (Focal Fossa) lançada com o número de série 20210820 ou posterior [3]
- AMI do Ubuntu 18.04 LTS (Bionic Beaver) lançada com o número de série 20190722.1 ou posterior [3] [5]
- AMI do Ubuntu 16.04 LTS (Xenial Xerus) [3] [4] [5] (uma configuração adicional é necessária)

AMIs para tipos de instância Graviton

- AMI do AL2023 (ARM de 64 bits) lançada em 01/07/2024 ou posteriormente [1]
- AMI do Amazon Linux 2 (Arm de 64 bits) lançada em 20/6/2024 ou posterior
- AMI do Ubuntu 22.04.2 LTS (ARM de 64 bits) (Jammy Jellyfish) lançada com o número de série 20240701 ou posterior [3]
- AMI do Ubuntu 20.04 LTS (ARM de 64 bits) (Focal Fossa) lançada com o número de série 20240701 ou posterior [3]

[1] Para a AMI mínima do AL2023, é necessária uma configuração adicional.

[2] Para CentOS, Fedora e Red Hat Enterprise Linux, a hibernação é compatível apenas com instâncias baseadas em Nitro.

[3] Recomendamos desabilitar o KASLR em instâncias com o Ubuntu 22.04.2 LTS (Jammy Jellyfish), Ubuntu 20.04 LTS (Focal Fossa), Ubuntu 18.04 LTS (Bionic Beaver) e Ubuntu 16.04 LTS (Xenial Xerus). Para obter mais informações, consulte Desabilitar o KASLR em uma instância (apenas Ubuntu).

[4] Para a AMI do Ubuntu 16.04 LTS (Xenial Xerus), a hibernação não é compatível com os tipos de instância `t3.nano`. Nenhum patch será disponibilizado porque o Ubuntu (Xenial Xerus) encerrou o suporte em abril de 2021. Se quiser usar os tipos de instância `t3.nano`, recomendamos que você atualize para a AMI do Ubuntu 22.04.2 LTS (Jammy Jellyfish), a AMI do Ubuntu 20.04 LTS (Focal Fossa) ou a AMI do Ubuntu 18.04 LTS (Bionic Beaver).

[5] O suporte ao Ubuntu 18.04 LTS (Bionic Beaver) e Ubuntu 16.04 LTS (Xenial Xerus) chegou ao fim da vida útil.

Para configurar sua AMI para oferecer suporte à hibernação, consulte Configurar uma AMI para oferecer suporte à hibernação.

O suporte para outras versões do Ubuntu e outros sistemas operacionais será disponibilizado em breve.

AMIs do Windows

- AMI do Windows Server 2022 lançada em 13/09/2023 ou posterior.
- AMI do Windows Server 2019 lançada em 11/09/2019 ou posterior.
- AMI do Windows Server 2016 lançada em 11/09/2019 ou posterior.
- AMI do Windows Server 2012 R2 lançada em 11/09/2019 ou posterior.
- AMI do Windows Server 2012 lançada em 11/09/2019 ou posterior.

Famílias de instâncias

É necessário usar uma família de instâncias que ofereça suporte à hibernação. No entanto, não há suporte a instâncias bare metal.

- Uso geral: M3, M4, M5, M5a, M5ad, M5d, M6a, M6g, M6gd, M6i, M6id, M6idn, M6in, M7a, M7g, M7gd, M7i, M7i-flex, M8a, M8azn, M8g, M8gb, M8gd, M8gn, M8i, M8i-flex, T2, T3, T3a, T4g
- Otimizadas para computação: C3, C4, C5, C5d, C6a, C6g, C6gd, C6gn, C6i, C6id, C6in, C7a, C7g, C7gd, C7gn, C7i, C7i-flex, C8a, C8g, C8gb, C8gd, C8gn, C8i, C8i-flex
- Otimizadas para memória: R3, R4, R5, R5a, R5ad, R5d, R6a, R6g, R6gd, R6idn, R6in, R7a, R7g, R7gd, R7i, R7iz, R8a, R8g, R8gb, R8gd, R8gn, R8i, R8i-flex, X2gd, X8aedz, X8i
- Otimizadas para armazenamento: I3, I3en, I4g, I7i, I7ie, I8g, I8ge, Im4gn, Is4gen

Console

Para obter os tipos de instância que oferecem suporte à hibernação

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Instance Types (Tipos de instância).
3. Adicione o filtro Suporte à hibernação sob demanda = true.
4. (Opcional) Adicione filtros para ampliar o escopo de tipos específicos de instância de interesse.

AWS CLI

Para obter os tipos de instância que oferecem suporte à hibernação

Use o comando describe-instance-types. Observe que os tipos de instância disponíveis variam de acordo com a região.

```
aws ec2 describe-instance-types \
    --filters Name=hibernation-supported,Values=true \
    --query "InstanceTypes[*].[InstanceType]" \
    --output text | sort
```

PowerShell

Para obter os tipos de instância que oferecem suporte à hibernação

Use o cmdlet Get-EC2InstanceType. Observe que os tipos de instância disponíveis variam de acordo com a região.

```
(Get-EC2InstanceType `
```

```
    -Filter @{Name="hibernation-supported"; Values="true"}).InstanceType | Sort-
Object
```

Tamanho da instância RAM

Instâncias Linux: devem ter menos de 150 GiB.

Instâncias Windows: devem ser inferiores ou iguais a 16 GiB. Para colocar uma instância T3 ou T3a em hibernação, recomendamos pelo menos 1 GiB de RAM.

Tipo do volume de raiz

O volume raiz deve ser um volume do EBS, e não um volume de armazenamento de instâncias.

Tamanho do volume raiz

O volume raiz deve ser grande o suficiente para armazenar o conteúdo da RAM e acomodar o uso esperado, por exemplo, sistema operacional ou aplicações. Quando você habilita a hibernação, é alocado espaço no volume raiz no lançamento para armazenar a RAM.

Criptografia do volume raiz

O volume raiz deve ser criptografado para garantir a proteção do conteúdo confidencial existente na memória no momento da hibernação. Quando os dados da RAM são movidos para o volume raiz do EBS, eles sempre são criptografados. A criptografia do volume raiz é imposta na execução da instância.

Use uma das três opções a seguir para garantir que o volume raiz seja um volume criptografado do EBS:

- Criptografia do EBS por padrão: é possível habilitar a criptografia do EBS por padrão para garantir que todos os novos volumes do EBS criados na sua conta da AWS sejam criptografados. Dessa forma, você habilita a hibernação para suas instâncias sem especificar a intenção da criptografia na execução da instância. Para obter mais informações, consulte Habilitar criptografia por padrão.
- Criptografia EBS de uma “única etapa”: é possível iniciar instâncias do EC2 criptografadas com suporte de EBS a partir de uma AMI não criptografada e, ao mesmo tempo, habilitar a hibernação. Para obter mais informações, consulte Usar criptografia com AMIs com EBS.
- AMI criptografada: é possível habilitar a criptografia do EBS usando uma AMI criptografada para iniciar sua instância. Se a sua AMI não tiver um snapshot raiz criptografado, será possível copiá-

lo para uma nova AMI e solicitar a criptografia. Para obter mais informações, consulte Criptografar uma imagem não criptografada durante a cópia e Copiar um AMI.

Tipo de volume do EBS

Os volumes do EBS devem usar um dos seguintes tipos de volume do EBS:

- SSD para uso geral (`gp2` e `gp3`)
- IOPS provisionado SSD (`io1` e `io2`)

Se você escolher um tipo de volume SSD de IOPS Provisionado SSD, você deverá provisionar o volume do EBS com as IOPS apropriadas para alcançar a performance ideal para hibernação. Para obter mais informações, consulte Tipos de volumes do Amazon EBS no Guia do usuário do Amazon EC2.

Solicitações de instância Spot

Os seguintes requisitos se aplicam a instâncias spot:

- O tipo de solicitação da instância spot deve ser `persistent`.
- Não é possível especificar um grupo de execução na solicitação de instância spot.

Configurar uma AMI para oferecer suporte à hibernação

As seguintes AMIs do Linux podem oferecer suporte à hibernação de uma instância do Amazon EC2, desde que você conclua as etapas adicionais de configuração descritas nesta seção.

Configurações adicionais são necessárias para:

- AMI do AL2023 mínima lançada em 20/09/2023 ou posteriormente
- AMI do Amazon Linux 2 mínima lançada em 29/08/2019 ou posterior
- Amazon Linux 2 lançado antes de 29/08/2019
- Amazon Linux lançado antes de 16/11/2018
- CentOS versão 8 ou posterior
- Fedora versão 34 ou posterior
- Red Hat Enterprise Linux versão 8 ou 9
- Ubuntu 20.04 LTS (Focal Fossa) liberado antes do número de série 20210820

- Ubuntu 18.04 (Bionic Beaver) lançado antes do número de série 20190722.1
- Ubuntu 16.04 (Xenial Xerus)

Para as AMIs do Linux e do Windows que oferecem suporte à hibernação e para as quais nenhuma configuração adicional é necessária, consulte AMIs.

Para obter mais informações, consulte Update instance software on your Amazon Linux 2 instance.

AMI do AL2023 mínima lançada em 20/09/2023 ou posteriormente

Para configurar uma AMI do AL2023 mínima lançada em 20/09/2023 ou posteriormente e permitir hibernação

1. Instale o pacote `ec2-hibinit-agent` dos repositórios.

```
[ec2-user ~]$ sudo dnf install ec2-hibinit-agent
```

2. Reinicie o serviço .

```
[ec2-user ~]$ sudo systemctl start hibinit-agent
```

AMI do Amazon Linux 2 mínima lançada em 29/08/2019 ou posterior

Para configurar uma AMI do Amazon Linux 2 mínima lançada antes de 29/08/2019 para permitir hibernação

1. Instale o pacote `ec2-hibinit-agent` dos repositórios.

```
[ec2-user ~]$ sudo yum install ec2-hibinit-agent
```

2. Reinicie o serviço .

```
[ec2-user ~]$ sudo systemctl start hibinit-agent
```

Amazon Linux 2 lançado antes de 29/08/2019

Como configurar uma AMI do Amazon Linux 2 lançada antes de 29/08/2019 para suportar hibernação

1. Atualize o kernel para `4.14.138-114.102` ou posterior.

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

2. Instale o pacote `ec2-hibinit-agent` dos repositórios.

```
[ec2-user ~]$ sudo yum install ec2-hibinit-agent
```

3. Reinicialize a instância.

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

4. Confirme se a versão do kernel está atualizada para `4.14.138-114.102` ou posterior.

```
[ec2-user ~]$ uname -a
```

5. Interrompa a instância e crie uma AMI. Para obter mais informações, consulte Criação de uma AMI baseada no Amazon EBS.

Amazon Linux lançado antes de 16/11/2018

Para configurar uma AMI do Amazon Linux lançada antes de 16/11/2018 para oferecer suporte à hibernação

1. Atualize o kernel para `4.14.77-70.59` ou posterior.

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

2. Instale o pacote `ec2-hibinit-agent` dos repositórios.

```
[ec2-user ~]$ sudo yum install ec2-hibinit-agent
```

3. Reinicialize a instância.

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

4. Confirme se a versão do kernel está atualizada para `4.14.77-70.59` ou maior.

```
[ec2-user ~]$ uname -a
```

5. Interrompa a instância e crie uma AMI. Para obter mais informações, consulte Criação de uma AMI baseada no Amazon EBS.

CentOS versão 8 ou posterior

Para configurar uma AMI do CentOS versão 8 ou posterior para suportar hibernação

1. Atualize o kernel para `4.18.0-305.7.1.el8_4.x86_64` ou posterior.

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

2. Instale o repositório Fedora Extra Packages for Enterprise Linux (EPEL).

```
[ec2-user ~]$ sudo yum install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
```

3. Instale o pacote `ec2-hibinit-agent` dos repositórios.

```
[ec2-user ~]$ sudo yum install ec2-hibinit-agent
```

4. Habilite o agente de hibernação para iniciar na inicialização.

```
[ec2-user ~]$ sudo systemctl enable hibinit-agent.service
```

5. Reinicialize a instância.

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

6. Confirme se a versão do kernel está atualizada para `4.18.0-305.7.1.el8_4.x86_64` ou posterior.

```
[ec2-user ~]$ uname -a
```

Fedora versão 34 ou posterior

Para configurar uma AMI do Fedora versão 34 ou posterior para suportar hibernação

1. Atualize o kernel para `5.12.10-300.fc34.x86_64` ou posterior.

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

2. Instale o pacote `ec2-hibinit-agent` dos repositórios.

```
[ec2-user ~]$ sudo dnf install ec2-hibinit-agent
```

3. Habilite o agente de hibernação para iniciar na inicialização.

```
[ec2-user ~]$ sudo systemctl enable hibinit-agent.service
```

4. Reinicialize a instância.

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

5. Confirme se a versão do kernel está atualizada para `5.12.10-300.fc34.x86_64` ou posterior.

```
[ec2-user ~]$ uname -a
```

Red Hat Enterprise Linux versão 8 ou 9

Para configurar uma AMI do Red Hat Enterprise Linux 8 ou 9 para suportar hibernação

1. Atualize o kernel para `4.18.0-305.7.1.el8_4.x86_64` ou posterior.

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

2. Instale o repositório Fedora Extra Packages for Enterprise Linux (EPEL).

   Versão 8 da RHEL:

```
[ec2-user ~]$ sudo yum install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
```

Versão 9 da RHEL:

```
[ec2-user ~]$ sudo yum install https://dl.fedoraproject.org/pub/epel/epel-release-latest-9.noarch.rpm
```

3. Instale o pacote `ec2-hibinit-agent` dos repositórios.

```
[ec2-user ~]$ sudo yum install ec2-hibinit-agent
```

4. Habilite o agente de hibernação para iniciar na inicialização.

```
[ec2-user ~]$ sudo systemctl enable hibinit-agent.service
```

5. Reinicialize a instância.

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

6. Confirme se a versão do kernel está atualizada para `4.18.0-305.7.1.el8_4.x86_64` ou posterior.

```
[ec2-user ~]$ uname -a
```

Ubuntu 20.04 LTS (Focal Fossa) liberado antes do número de série 20210820

Para configurar uma AMI do Ubuntu 20.04 LTS (Focal Fossa) lançada antes do número de série 20210820 para ser compatível com hibernação

1. Atualize o linux-aws-kernel para `5.8.0-1038.40` ou posterior, e grub2 para `2.04-1ubuntu26.13` ou posterior.

```
[ec2-user ~]$ sudo apt update
[ec2-user ~]$ sudo apt dist-upgrade
```

2. Reinicialize a instância.

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

3. Confirme se a versão do kernel está atualizada para `5.8.0-1038.40` ou posterior.

```
[ec2-user ~]$ uname -a
```

4. Confirme se a versão do grub2 está atualizada para `2.04-1ubuntu26.13` ou posterior.

```
[ec2-user ~]$ dpkg --list | grep grub2-common
```

Ubuntu 18.04 (Bionic Beaver) lançado antes do número de série 20190722.1

Para configurar uma AMI do Ubuntu 18.04 LTS lançada antes do número de série 20190722.1 para suportar hibernação

1. Atualize o kernel para `4.15.0-1044` ou posterior.

```
[ec2-user ~]$ sudo apt update
[ec2-user ~]$ sudo apt dist-upgrade
```

2. Instale o pacote `ec2-hibinit-agent` dos repositórios.

```
[ec2-user ~]$ sudo apt install ec2-hibinit-agent
```

3. Reinicialize a instância.

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

4. Confirme se a versão do kernel está atualizada para `4.15.0-1044` ou posterior.

```
[ec2-user ~]$ uname -a
```

Ubuntu 16.04 (Xenial Xerus)

Para configurar o Ubuntu 16.04 LTS para ser compatível com a hibernação, é necessário instalar o pacote do kernel linux-aws-hwe versão 4.15.0-1058-aws ou posterior e o agente ec2-hibint.

> **Important**
>
> O pacote do kernel `linux-aws-hwe` é totalmente compatível com o Canonical. O suporte padrão para o Ubuntu 16.04 LTS terminou em abril de 2021, e o pacote não recebe mais atualizações regulares. No entanto, ele receberá atualizações de segurança adicionais até

que o suporte de Manutenção de segurança estendida termine em 2024. Para obter mais informações, consulte Amazon EC2 Hibernation for Ubuntu 16.04 LTS now available no blog do Canonical Ubuntu.
Recomendamos que você atualize para a AMI do Ubuntu 20.04 LTS (Focal Fossa) ou a AMI do Ubuntu 18.04 LTS (Bionic Beaver).

Como configurar uma AMI do Ubuntu 16.04 LTS para que seja compatível com a hibernação

1. Atualize o kernel para `4.15.0-1058-aws` ou posterior.

```
[ec2-user ~]$ sudo apt update
[ec2-user ~]$ sudo apt install linux-aws-hwe
```

2. Instale o pacote `ec2-hibinit-agent` dos repositórios.

```
[ec2-user ~]$ sudo apt install ec2-hibinit-agent
```

3. Reinicialize a instância.

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

4. Confirme se a versão do kernel está atualizada para `4.15.0-1058-aws` ou posterior.

```
[ec2-user ~]$ uname -a
```

Habilitar a hibernação para uma instância do Amazon EC2

Para colocar uma instância em hibernação, é necessário habilitá-la para hibernação ao iniciar a instância.

Important

Não é possível habilitar ou desabilitar a hibernação para uma instância depois de executá-la.

Tarefas

- Habilitar a hibernação de uma instância sob demanda

- Para habilitar a hibernação de instâncias spot
- Visualizar se uma instância está habilitada para hibernação

Habilitar a hibernação de uma instância sob demanda

É possível habilitar a hibernação das instâncias sob demanda.

Console

Para habilitar a hibernação de uma instância sob demanda

1. Siga o procedimento para iniciar uma instância, mas não inicie a instância até concluir as etapas a seguir para habilitar a hibernação.
2. Para habilitar a hibernação, configure os seguintes campos no assistente de inicialização da instância:

   a. Em Application and OS Images (Amazon Machine Image) (Imagens de aplicações e sistemas operacionais [imagem de máquina da Amazon]), selecione uma AMI com suporte à hibernação. Para obter mais informações, consulte AMIs.

   b. Em Instance type (Tipo de instância), selecione um tipo de instância compatível. Para obter mais informações, consulte Famílias de instâncias.

   c. Em Configure storage (Configurar armazenamento), escolha Advanced (Avançado) (à direita) e especifique estas informações para o volume raiz:

      - Para Size (GiB) (Tamanho (GiB)), insira o tamanho do volume raiz do EBS. O volume deve ser grande o suficiente para armazenar o conteúdo da RAM e acomodar o uso esperado.
      - Em Volume Type (Tipo de volume), selecione um tipo de volume do EBS compatível: SSD de uso geral (`gp2` e `gp3`) ou SSD de IOPS provisionadas (`io1` e `io2`).
      - Em Encrypted (Criptografado), escolha Yes (Sim). Se você tiver habilitado a criptografia por padrão nessa região da AWS, a opção Yes (Sim) estará selecionada.
      - Para KMS key (Chave do KMS), selecione a chave de criptografia para o volume. Se tiver habilitado a criptografia por padrão nessa região da AWS, a criptografia padrão será selecionada.

      Para obter mais informações sobre os pré-requisitos para o volume raiz, consulte Pré-requisitos para a hibernação de instância do EC2.

d. Expanda Advanced details (Detalhes avançados) e, em Stop - Hibernate behavior (Interromper: comportamento de hibernação), escolha Enable (Habilitar).

3. No painel Summary (Resumo), analise a configuração da instância e selecione Launch instance (Iniciar instância). Para obter mais informações, consulte Executar uma instância do EC2 usando o assistente de inicialização de instâncias no console.

AWS CLI

Para habilitar a hibernação de uma instância sob demanda

Use o comando run-instances para executar uma instância. Especifique os parâmetros do volume raiz do EBS usando o parâmetro `--block-device-mappings file://mapping.json` e habilite a hibernação usando o parâmetro `--hibernation-options Configured=true`.

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --instance-type m5.large \
    --block-device-mappings file://mapping.json \
    --hibernation-options Configured=true \
    --count 1 \
    --key-name MyKeyPair
```

Especifique o seguinte em `mapping.json`.

```
[
    {
        "DeviceName": "/dev/xvda",
        "Ebs": {
            "VolumeSize": 30,
            "VolumeType": "gp2",
            "Encrypted": true
        }
    }
]
```

O valor para `DeviceName` deve corresponder ao nome do dispositivo raiz associado à AMI. Para localizar o nome do dispositivo raiz, use o comando describe-images.

```
aws ec2 describe-images --image-id ami-0abcdef1234567890
```

Se você habilitou a criptografia por padrão nesta região da AWS, é possível omitir `"Encrypted": true`.

PowerShell

Para habilitar a hibernação de uma instância sob demanda

Use o comando New-EC2Instance para executar uma instância. Especifique o volume raiz do EBS definindo primeiro o mapeamento do dispositivo de bloco e adicionando-o ao comando usando o parâmetro `-BlockDeviceMappings`. Habilite a hibernação usando o parâmetro `-HibernationOptions_Configured $true`.

```
$ebs_encrypt = New-Object Amazon.EC2.Model.BlockDeviceMapping
$ebs_encrypt.DeviceName = "/dev/xvda"
$ebs_encrypt.Ebs = New-Object Amazon.EC2.Model.EbsBlockDevice
$ebs_encrypt.Ebs.VolumeSize = 30
$ebs_encrypt.Ebs.VolumeType = "gp2"
$ebs_encrypt.Ebs.Encrypted = $true

New-EC2Instance `
    -ImageId ami-0abcdef1234567890 `
    -InstanceType m5.large `
    -BlockDeviceMappings $ebs_encrypt `
    -HibernationOptions_Configured $true `
    -MinCount 1 `
    -MaxCount 1 `
    -KeyName MyKeyPair
```

O valor para `DeviceName` deve corresponder ao nome do dispositivo raiz associado à AMI. Para localizar o nome do dispositivo raiz, use o comando Get-EC2Image.

```
Get-EC2Image -ImageId ami-0abcdef1234567890
```

Se você habilitou a criptografia por padrão nesta região da AWS, poderá omitir o `Encrypted = $true` do mapeamento do dispositivo de bloco.

Para habilitar a hibernação de instâncias spot

É possível habilitar a hibernação das instâncias spot. Para obter mais informações sobre a hibernação de instâncias spot ao ocorrer uma interrupção, consulte Interrupções de instâncias spot.

Console

Para habilitar a hibernação de uma instância spot

1. Siga o procedimento para solicitar uma instância spot usando o assistente de inicialização de instâncias, mas não inicie a instância até concluir as etapas a seguir para habilitar a hibernação.
2. Para habilitar a hibernação, configure os seguintes campos no assistente de inicialização da instância:

   a. Em Application and OS Images (Amazon Machine Image) (Imagens de aplicações e sistemas operacionais [imagem de máquina da Amazon]), selecione uma AMI com suporte à hibernação. Para obter mais informações, consulte AMIs.

   b. Em Instance type (Tipo de instância), selecione um tipo de instância compatível. Para obter mais informações, consulte Famílias de instâncias.

   c. Em Configure storage (Configurar armazenamento), escolha Advanced (Avançado) (à direita) e especifique estas informações para o volume raiz:

      - Para Size (GiB) (Tamanho (GiB)), insira o tamanho do volume raiz do EBS. O volume deve ser grande o suficiente para armazenar o conteúdo da RAM e acomodar o uso esperado.
      - Em Volume Type (Tipo de volume), selecione um tipo de volume do EBS compatível: SSD de uso geral (`gp2` e `gp3`) ou SSD de IOPS provisionadas (`io1` e `io2`).
      - Em Encrypted (Criptografado), escolha Yes (Sim). Se você tiver habilitado a criptografia por padrão nessa região da AWS, a opção Yes (Sim) estará selecionada.
      - Para KMS key (Chave do KMS), selecione a chave de criptografia para o volume. Se tiver habilitado a criptografia por padrão nessa região da AWS, a criptografia padrão será selecionada.

      Para obter mais informações sobre os pré-requisitos para o volume raiz, consulte Pré-requisitos para a hibernação de instância do EC2.

   d. Expanda Detalhes avançados e, além de preencher os campos para configurar uma instância spot, faça o seguinte:

      i. Em Tipo de solicitação, escolha Persistente.

ii. Em Comportamento de interrupção, escolha Hibernar. Ou então, em Comportamento de parar - hibernar, escolha Habilitar. Ambos os campos habilitam a hibernação da instância spot. Você só precisa configurar um deles.

3. No painel Resumo, analise a configuração da instância e selecione Iniciar instância. Para obter mais informações, consulte Executar uma instância do EC2 usando o assistente de inicialização de instâncias no console.

AWS CLI

Para habilitar a hibernação de uma instância spot

Use o comando run-instances para executar uma instância spot. Especifique os parâmetros do volume raiz do EBS usando o parâmetro `--block-device-mappings file://mapping.json` e habilite a hibernação usando o parâmetro `--hibernation-options Configured=true`. O tipo de solicitação da instância spot (`SpotInstanceType`) deve ser `persistent`.

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --instance-type c4.xlarge \
    --block-device-mappings file://mapping.json \
    --hibernation-options Configured=true \
    --count 1 \
    --key-name MyKeyPair
    --instance-market-options
        {
           "MarketType":"spot",
           "SpotOptions":{
              "MaxPrice":"1",
              "SpotInstanceType":"persistent"
            }
        }
```

Especifique os parâmetros do volume raiz do EBS no `mapping.json` como se segue.

```
[
    {
        "DeviceName": "/dev/xvda",
        "Ebs": {
            "VolumeSize": 30,
```

```
            "VolumeType": "gp2",
            "Encrypted": true
        }
    }
]
```

O valor para `DeviceName` deve corresponder ao nome do dispositivo raiz associado à AMI. Para localizar o nome do dispositivo raiz, use o comando describe-images.

```
aws ec2 describe-images --image-id ami-0abcdef1234567890
```

Se você habilitou a criptografia por padrão nesta região da AWS, é possível omitir `"Encrypted": true`.

PowerShell

Para habilitar a hibernação de uma instância spot

Use o comando New-EC2Instance para solicitar uma instância spot. Especifique o volume raiz do EBS definindo primeiro o mapeamento do dispositivo de bloco e adicionando-o ao comando usando o parâmetro `-BlockDeviceMappings`. Habilite a hibernação usando o parâmetro `-HibernationOptions_Configured $true`.

```
$ebs_encrypt = New-Object Amazon.EC2.Model.BlockDeviceMapping
$ebs_encrypt.DeviceName = "/dev/xvda"
$ebs_encrypt.Ebs = New-Object Amazon.EC2.Model.EbsBlockDevice
$ebs_encrypt.Ebs.VolumeSize = 30
$ebs_encrypt.Ebs.VolumeType = "gp2"
$ebs_encrypt.Ebs.Encrypted = $true

New-EC2Instance `
    -ImageId ami-0abcdef1234567890 `
    -InstanceType m5.large `
    -BlockDeviceMappings $ebs_encrypt `
    -HibernationOptions_Configured $true `
    -MinCount 1 `
    -MaxCount 1 `
    -KeyName MyKeyPair `
    -InstanceMarketOption @(
        MarketType = spot;
        SpotOptions @{
        MaxPrice = 1;
        SpotInstanceType = persistent}
```

```
    )
```

O valor para `DeviceName` deve corresponder ao nome do dispositivo raiz associado à AMI. Para localizar o nome do dispositivo raiz, use o comando Get-EC2Image.

```
Get-EC2Image -ImageId ami-0abcdef1234567890
```

Se você habilitou a criptografia por padrão nesta região da AWS, poderá omitir o `Encrypted = $true` do mapeamento do dispositivo de bloco.

Visualizar se uma instância está habilitada para hibernação

É possível verificar se uma instância está habilitada para hibernação.

Console

Para visualizar se uma instância está habilitada para hibernação

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância e, na guia Details (Detalhes), na seção Instance details (Detalhes da instância), verifique Stop-hibernate behavior (Interromper - comportamento de hibernação). Enabled (Habilitada) indica que a instância está habilitada para hibernação.

AWS CLI

Para visualizar se uma instância está habilitada para hibernação

Use o comando describe-instances e especifique o parâmetro `--filters "Name=hibernation-options.configured,Values=true"` para filtrar as instâncias que estão habilitadas para hibernação.

```
aws ec2 describe-instances \
    --filters "Name=hibernation-options.configured,Values=true"
```

O campo da saída a seguir indica que a instância está habilitada para hibernação.

```
"HibernationOptions": {
    "Configured": true
```

```
}
```

PowerShell

Para visualizar se uma instância está habilitada para hibernação

Use o cmdlet Get-EC2Instance e filtre as instâncias que estão habilitadas para hibernação.

```
(Get-EC2Instance `
    -Filter @{Name="hibernation-options.configured"; Values="true"}).Instances
```

Desabilitar o KASLR em uma instância (apenas Ubuntu)

Para executar a hibernação em uma instância recém-executada com o Ubuntu 16.04 LTS (Xenial Xerus), o Ubuntu 18.04 LTS (Bionic Beaver) lançado com o número de série 20190722.1 ou posterior ou o Ubuntu 20.04 LTS (Focal Fossa) lançado com o número de série 20210820 ou posterior, recomendamos desabilitar o KASLR (Kernel Address Space Layout Randomization). No Ubuntu 16.04 LTS, Ubuntu 18.04 LTS ou Ubuntu 20.04 LTS, o KASLR é habilitado por padrão.

O KASLR é um recurso de segurança do kernel padrão do Linux que ajuda a mitigar as ramificações de e a exposição e às vulnerabilidades de acesso à memória ainda não descobertas por randomização do valor base do endereço do kernel. Com o KASLR habilitado, há uma possibilidade de a instância não ser retomada depois de ter estado em hibernação.

Para saber mais sobre o KASLR, consulte Recursos do Ubuntu.

Para desabilitar o KASLR em uma instância executada com o Ubuntu

1. Conecte-se à sua instância usando SSH. Para obter mais informações, consulte Conectar-se à instância do Linux usando SSH.
2. Abra o arquivo `/etc/default/grub.d/50-cloudimg-settings.cfg` com seu editor de preferência. Edite a linha `GRUB_CMDLINE_LINUX_DEFAULT` para anexar a opção `nokaslr` no final, conforme mostrado no exemplo a seguir.

   ```
   GRUB_CMDLINE_LINUX_DEFAULT="console=tty1 console=ttyS0
    nvme_core.io_timeout=4294967295 nokaslr"
   ```
3. Salve o arquivo e saia do editor.
4. Execute o comando a seguir para recompilar a configuração do grub.

```
sudo update-grub
```

5. Reinicialize a instância.

```
sudo reboot
```

6. Execute o seguinte comando para confirmar que `nokaslr` foi adicionado.

```
cat /proc/cmdline
```

A saída do comando deve incluir a opção `nokaslr`.

Hibernar uma instância do Amazon EC2

Será possível iniciar a hibernação em uma instância sob demanda ou de uma instância spot se a instância for baseada em EBS, estiver habilitada para hibernação e atender aos pré-requisitos para hibernação. Se uma instância não puder hibernar com sucesso, ocorrerá um desligamento normal.

Console

Para hibernar 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 e escolha Instance state (Estado da instância) e Hibernate instance (Hibernar instância). Se Hibernate instance (Hibernar instância) estiver desabilitado, a instância já estará em hibernação ou interrompida ou não poderá ser hibernada. Para obter mais informações, consulte Pré-requisitos para a hibernação de instância do EC2.
4. Quando a confirmação for solicitada, escolha Hibernate (Hibernar). Pode demorar alguns minutos para que a instância hiberne. O estado da instância primeiro muda para Interrompendo e, em seguida, muda para Interrompido quando a instância tiver hibernado.

AWS CLI

Para hibernar uma instância

Use o comando stop-instances e especifique o parâmetro `--hibernate`.

```
aws ec2 stop-instances \
    --instance-ids i-1234567890abcdef0 \
    --hibernate
```

PowerShell

Para hibernar uma instância

Use o cmdlet Stop-EC2Instance.

```
Stop-EC2Instance `
    -InstanceId i-1234567890abcdef0 `
    -Hibernate $true
```

É possível verificar se a hibernação foi iniciada em uma instância.

Console

Para visualizar se a hibernação foi iniciada em 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, na guia Detalhes, na seção Detalhes da instância), verifique o valor de Mensagem de transição de estado.

   Client.UserInitiatedHibernate: hibernação iniciada pelo usuário indica que você iniciou a hibernação da instância sob demanda ou da instância spot.

AWS CLI

Para visualizar se a hibernação foi iniciada em uma instância

Use o comando describe-instances e especifique o filtro `state-reason-code` para ver as instâncias nas quais a hibernação foi iniciada.

```
aws ec2 describe-instances \
    --filters "Name=state-reason-code,Values=Client.UserInitiatedHibernate"
```

O campo da saída a seguir indica que a hibernação foi iniciada na instância sob demanda ou na instância spot.

```
"StateReason": {
    "Code": "Client.UserInitiatedHibernate"
}
```

PowerShell

Para visualizar se a hibernação foi iniciada em uma instância

Use o cmdlet Get-EC2Instance e especifique o filtro `state-reason-code` para ver as instâncias nas quais a hibernação foi iniciada.

```
Get-EC2Instance `
    -Filter @{Name="state-reason-code";Value="Client.UserInitiatedHibernate"}
```

Iniciar um instância do Amazon EC2 em hibernação

Inicie uma instância em hibernação da mesma maneira como faria em uma instância interrompida.

Para instâncias spot, se o Amazon EC2 colocou a instância em hibernação, só Amazon EC2 poderá reiniciá-la. Você só poderá reiniciar uma instância spot em hibernação se tiver sido você que a colocou em hibernação. Instâncias spot colocadas em hibernação só poderão ser reiniciadas se houver capacidade disponível e se o preço spot for menor ou igual ao preço máximo especificado.

Console

Para iniciar um instância em hibernação

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione uma instância em hibernação e escolha Instance state (Estado da instância) e Start instance (Iniciar instância). Pode demorar alguns minutos para que a instância entre no estado `running`. Durante esse tempo, as verificações de status da instância mostram a instância em um estado de falha até que a instância seja iniciada.

AWS CLI

Para iniciar um instância em hibernação

Use o comando start-instances.

```
aws ec2 start-instances --instance-ids i-1234567890abcdef0
```

PowerShell

Para iniciar um instância em hibernação

Use o cmdlet Start-EC2Instance.

```
Start-EC2Instance -InstanceId i-1234567890abcdef0
```

Solucionar problemas de hibernação de instâncias do Amazon EC2

Use estas informações para ajudar a diagnosticar e corrigir problemas que podem ser encontrados ao hibernar uma instância.

Problemas de hibernação

- Não é possível hibernar imediatamente após a execução
- A transição de stopping para stopped demora muito tempo, e o estado da memória não é restaurado depois da execução
- A instância está "presa" no estado stopping
- Não é possível iniciar a instância spot imediatamente após a hibernação
- Falha ao retomar instâncias spot

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.

Após iniciar a execução, aguarde cerca de dois minutos para instâncias do Linux e cerca de cinco minutos para instâncias do Windows para hiberná-las.

A transição de stopping para stopped demora muito tempo, e o estado da memória não é restaurado depois da execução

Quando demora muito tempo para que a instância em hibernação faça a transição do estado `stopping` para `stopped`, e se o estado da memória não é restaurado depois da execução, isso pode indicar que a hibernação não foi configurada corretamente.

Instâncias do Linux

Verifique o log do sistema da instância e procure as mensagens relacionadas à hibernação. Para acessar o log do sistema, conecte-se 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 para a hibernação de instância do EC2. Se você usou sua própria AMI do Linux, certifique-se de seguir as instruções para Configurar uma AMI para oferecer suporte à hibernação.

Windows Server 2016 e posterior

Verifique o log de execução do EC2 e procure mensagens relacionadas à hibernação. Para acessar o log de execução do EC2, conecte-se à instância e abra o arquivo `C:\ProgramData\Amazon\EC2-Windows\Launch\Log\Ec2Launch.log` em um editor de texto. Se você estiver usando EC2Launch v2, abra `C:\ProgramData\Amazon\EC2Launch\log\agent.log`.

> **Note**
>
> Por padrão, o Windows oculta os arquivos e as pastas sob `C:\ProgramData`. Para visualizar os diretórios e os arquivos do EC2, insira o caminho no Windows Explorer ou altere as propriedades da pasta para visualizar os arquivos e as pastas ocultos.

Localize as linhas do log para hibernação. Se as linhas do log indicarem uma falha ou se não houver linhas no log, muito provavelmente terá ocorrido uma falha na configuração da hibernação na execução.

Por exemplo, a seguinte mensagem indica que a hibernação falhou na configuração: `Message: Failed to enable hibernation.` Se a mensagem de erro incluir valores ASCII decimais, será possível converter os valores ASCII em texto simples para ler a mensagem de erro completa.

Se a linha do log contiver `HibernationEnabled: true`, a hibernação terá sido configurada com êxito.

Windows Server 2012 R2 e anteriores

Verifique o log de configuração do EC2 e procure mensagens relacionadas à hibernação. Para acessar o log de configuração do EC2, conecte-se à instância e abra o arquivo `C:\Program Files\Amazon\Ec2ConfigService\Logs\Ec2ConfigLog.txt` em um editor de texto. Localize as linhas do log para `SetHibernateOnSleep`. Se as linhas do log indicarem uma falha ou se não houver linhas no log, muito provavelmente terá ocorrido uma falha na configuração da hibernação na execução.

Por exemplo, a seguinte mensagem indica que o volume raiz da instância não é grande o suficiente: `SetHibernateOnSleep: Failed to enable hibernation: Hibernation failed with the following error: There is not enough space on the disk.`

Se a linha do log for `SetHibernateOnSleep: HibernationEnabled: true`, a hibernação terá sido configurada com êxito.

Tamanho da instância do Windows

Se você estiver usando uma instância do Windows T3 ou T3a com menos de 1 GiB de RAM, tente aumentar o tamanho da instância para uma que tenha pelo menos 1 GiB de RAM.

A instância está "presa" no estado stopping

Se você tiver hibernado sua instância e ela aparentar estar "presa" no estado `stopping`, será possível interrompê-la à força. Para obter mais informações, consulte Solucionar problemas de interrupção de instâncias do Amazon EC2.

Não é possível iniciar a instância spot imediatamente após a hibernação

Se você tentar iniciar uma instância spot até dois minutos após colocá-la em hibernação, poderá receber o seguinte erro:

`You failed to start the Spot Instance because the associated Spot Instance request is not in an appropriate state to support start.`

Aguarde cerca de dois minutos para as instâncias do Linux e cerca de cinco minutos para as instâncias do Windows e tente iniciar a instância novamente.

Falha ao retomar instâncias spot

Se a instância spot foi colocada em hibernação com sucesso, mas não foi possível retomá-la e, em vez disso, ela foi reinicializada (uma nova inicialização em que o estado de hibernação não é retido), talvez os dados do usuário contivessem o seguinte script:

```
/usr/bin/enable-ec2-spot-hibernation
```

Remova esse script do campo Dados de usuário no modelo de inicialização e solicite uma nova instância spot.

Observe que, mesmo havendo falha ao retomar a instância, se o estado de hibernação não for preservado, a instância ainda poderá ser iniciada da mesma forma que aconteceria se ela estivesse no estado `stopped`.

Reinicializar uma instância do Amazon EC2

Reinicializar a instância equivale a reinicializar o sistema operacional. Na maioria dos casos, leva apenas alguns minutos para reinicializar sua instância.

Quando você reinicializa uma instância, ela mantém o seguinte:

- Nome DNS público (IPv4)
- Endereço IPv4 privado
- Endereço IPv4 público
- Endereço IPv6 (se aplicável)
- Todos os dados em seus volumes de armazenamento de instância

A reinicialização de uma instância não inicia um novo período de faturamento de instância, ao contrário de interromper e iniciar uma instância (que inicia um novo período de faturamento com uma cobrança mínima de um minuto).

A reinicialização da instância pode ser iniciada pelo usuário (quando você a reinicializa manualmente) ou iniciada pela AWS (para recuperação automática da instância ou em resposta a um evento de reinicialização programado para manutenção necessária, por exemplo, para aplicar atualizações que exijam reinicialização).

Para reinicializações iniciadas pelo usuário, recomendamos usar o console do Amazon EC2, a CLI ou a API em vez de executar o comando de reinicialização do sistema operacional na instância. Ao usar o Amazon EC2, se a instância não for desligada de maneira limpa em alguns minutos, o Amazon EC2 realizará uma reinicialização forçada. Além disso, o AWS CloudTrail cria um registro de API de quando a instância foi reinicializada.

Este tópico descreve como realizar uma reinicialização iniciada pelo usuário. Para obter informações sobre reinicializações realizadas pela AWS, consulte Recuperação automática de instâncias e Gerenciamento das instâncias do Amazon EC2 agendadas para reinicialização.

> **Important**
>
> Se houver atualizações sendo instaladas em sua instância, recomendamos não reiniciar ou fechar sua instância usando o console do Amazon EC2 ou a linha de comando até que todas as atualizações estejam instaladas. Ao usar o console ou a linha de comando Amazon EC2 para reinicializar ou fechar sua instância, há risco que sua instância seja reinicializada forçadamente. Uma "hard reboot" enquanto as atualizações estão sendo instaladas poderia colocar suas instâncias em um estado instável.

Console

Como reinicializar 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 Instance State (Estado da instância), Reboot instance (Reinicializar a instância).
4. Escolha Reboot (Reinicializar) quando a confirmação for solicitada.

   A instância permanecerá no estado `running`.

AWS CLI

Para reinicializar uma instância

Use o comando reboot-instances.

```
aws ec2 reboot-instances --instance-ids i-1234567890abcdef0
```

PowerShell

Como reinicializar uma instância

Use o cmdlet Restart-EC2Instance.

```
Restart-EC2Instance -InstanceId i-1234567890abcdef0
```

Para executar um experimento controlado de injeção de falha

É possível usar o AWS Fault Injection Service para testar como suas aplicações respondem quando sua instância é reinicializada. Para obter mais informações, consulte o Guia do usuário da AWS Fault Injection Service.

Encerramento de instâncias do Amazon EC2

Warning

O encerramento de uma instância é permanente e irreversível.
Depois de encerrar uma instância, não será mais possível se conectar a ela e ela não poderá ser recuperada. Todos os volumes anexados do Amazon EBS configurados para serem excluídos no encerramento também serão excluídos permanentemente e não poderão ser recuperados. Todos os dados armazenados em volumes de armazenamento de instância serão perdidos permanentemente. Para obter mais informações, consulte Como funciona o encerramento de uma instância.
Antes de encerrar uma instância, certifique-se de ter feito backup de todos os dados que você precise reter após o encerramento no armazenamento persistente.

É possível excluir sua instância quando não precisar mais dela. Isso é chamado de encerrar sua instância. Assim que o estado de uma instância mudar para `shutting-down` ou para `terminated`, não haverá mais custos para essa instância.

Não é possível conectar-se a uma instância ou iniciá-la depois de interrompê-la. No entanto, é possível executar novas instâncias usando a mesma AMI.

Se você preferir interromper ou hibernar a instância, consulte Início e interrupção de instâncias do Amazon EC2 ou Hibernar sua instância do Amazon EC2. Para obter mais informações, consulte Diferenças entre os estados de instâncias.

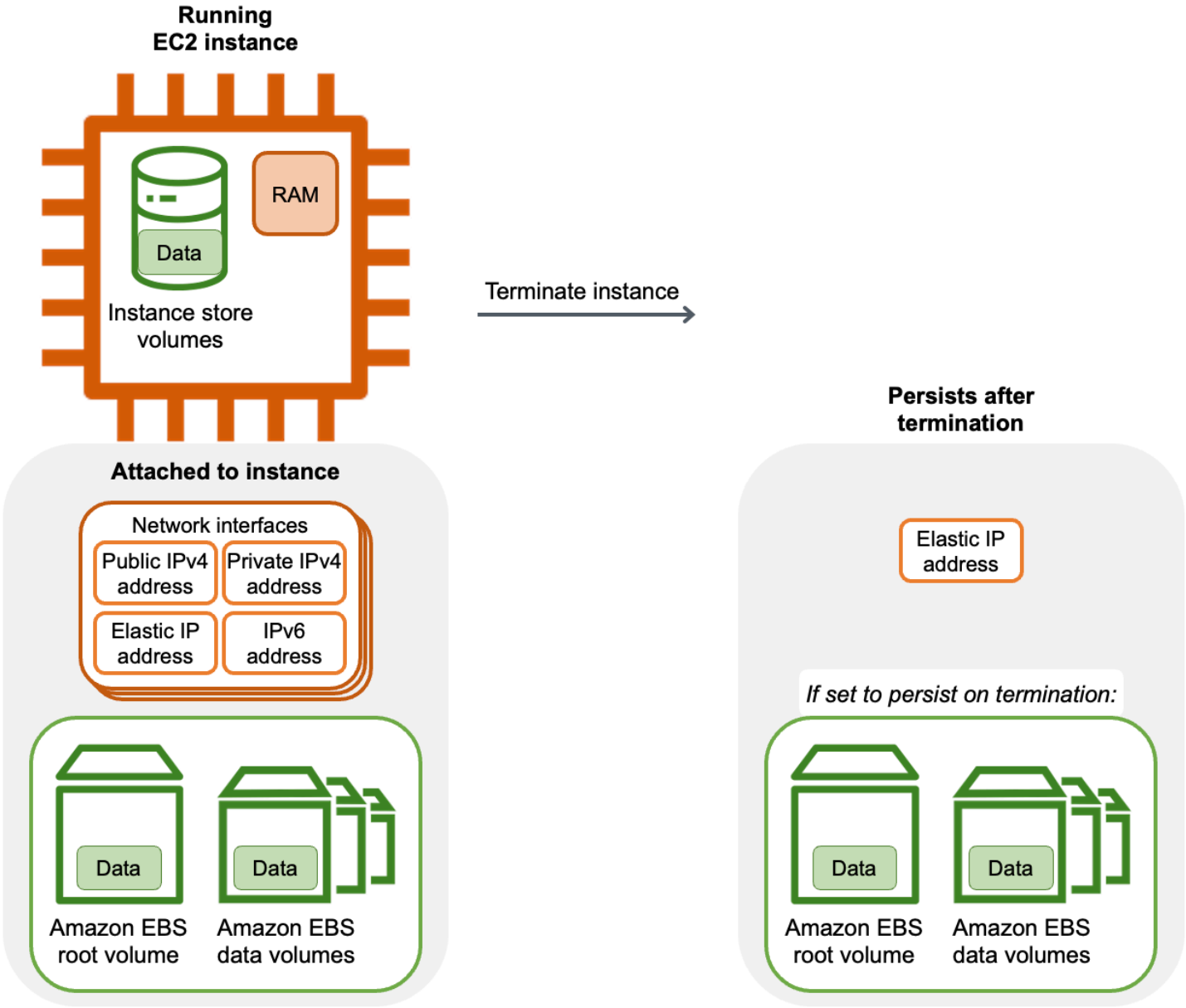
Conteúdo

- Como funciona o encerramento de uma instância
- Métodos para encerrar uma instância
- Encerrar uma instância com um desligamento normal do sistema operacional
- Encerrar uma instância e ignorar o desligamento normal do sistema operacional
- Solucionar problemas de encerramento da instância
- Alterar proteção contra encerramento de instância
- Alterar comportamento de desligamento iniciado da instância
- Preservação de dados quando uma instância for encerrada

Como funciona o encerramento de uma instância

Quando você encerra uma instância, as alterações são registradas no nível do sistema operacional (SO) da instância, alguns recursos são perdidos e outros persistem.

O diagrama apresentado a seguir mostra o que é perdido e o que persiste quando uma instância do Amazon EC2 é encerrada. Quando uma instância é encerrada, os dados em quaisquer volumes de armazenamento de instância e os dados armazenados na RAM da instância são apagados. Todos os endereços IP elásticos associados à instância são desanexados. Para os volumes raiz e volumes de dados do Amazon EBS, o resultado depende da configuração Excluir no encerramento definida para cada volume.



Considerações

- Persistência de dados
  - Volumes do armazenamento de instância: todos os dados são excluídos permanentemente quando a instância é encerrada.
  - Volume raiz do EBS:
    - Quando anexado na inicialização, é excluído por padrão quando a instância é encerrada.
    - Quando anexado após a inicialização, persiste por padrão quando a instância é encerrada.
  - Volumes de dados do EBS:

  - Quando anexados na inicialização usando o console: persistem por padrão quando a instância é encerrada.
  - Quando anexados na inicialização usando a CLI: excluídos por padrão quando a instância é encerrada.
  - Quando anexados após a inicialização usando o console ou a CLI: persistem por padrão quando a instância é encerrada.

    > **Note**
    >
    > Quaisquer volumes que não forem excluídos após o encerramento da instância continuarão incorrendo em cobranças. É possível alterar a configuração para que um volume seja excluído ou persista após o encerramento da instância. Para obter mais informações, consulte Preservação de dados quando uma instância for encerrada.

- Proteção contra encerramento acidental
  - Para evitar que uma instância seja encerrada acidentalmente por alguém, habilite a proteção contra encerramento.
  - Para controlar se uma instância é interrompida ou encerrada quando o desligamento é iniciado usando a instância, altere o comportamento de desligamento iniciado pela instância.
- Scripts de desativação: se você executar um script no encerramento da instância, ela poderá sofrer uma interrupção anormal, pois não há como garantir que os scripts de desativação serão executados. O Amazon EC2 tenta desativar uma instância de forma limpa corretamente e executar quaisquer scripts de desativação do sistema. No entanto, determinados eventos (como falhas de hardware) podem impedir que esses scripts de desativação do sistema sejam executados.
- Instâncias bare metal: as instâncias bare metal x86 não oferecem suporte à desativação cooperativa.

O que acontece quando você encerra uma instância

Alterações registradas no nível do sistema operacional

- A solicitação da API envia um evento de pressionamento de botão ao convidado.
- Vários serviços do sistema são interrompidos como resultado do evento de pressionamento de botão. O desligamento normal do sistema é fornecido pelo systemd (Linux) ou pelo processo do sistema (Windows). O desligamento normal é acionado pelo evento de pressionamento do botão de desligamento de ACPI do hipervisor.

- O desligamento de ACPI é iniciado.
- A instância será desativada após o término do processo de desativação normal. Não existe um tempo de desligamento configurável para o SO. A instância permanece visível no console por um curto período e depois a entrada é excluída automaticamente.

Recursos perdidos

- Dados armazenados nos volumes de armazenamento de instância.
- Volume raiz do EBS se o atributo `DeleteOnTermination` estiver definido como `true`.
- Volumes de dados do EBS (anexados no lançamento ou após) se o atributo `DeleteOnTermination` estiver definido como `true`.

Recursos que persistem

- Volume raiz do EBS se o atributo `DeleteOnTermination` estiver definido como `false`.
- Volumes de dados do EBS (anexados no lançamento ou após) se o atributo `DeleteOnTermination` estiver definido como `false`.

Teste da resposta da aplicação ao encerramento da instância

É possível usar o AWS Fault Injection Service para testar como suas aplicações respondem quando sua instância é encerrada. Para saber mais, consulte o Guia do usuário do AWS Fault Injection Service.

Métodos para encerrar uma instância

> **Warning**
>
> O encerramento de uma instância é permanente e irreversível.
> Depois de encerrar uma instância, não será mais possível se conectar a ela e ela não poderá ser recuperada. Todos os volumes anexados do Amazon EBS configurados para serem excluídos no encerramento também serão excluídos permanentemente e não poderão ser recuperados. Todos os dados armazenados em volumes de armazenamento de instância serão perdidos permanentemente. Para obter mais informações, consulte Como funciona o encerramento de uma instância.

Antes de encerrar uma instância, certifique-se de ter feito backup de todos os dados que você precise reter após o encerramento no armazenamento persistente.

Existem quatro maneiras de realizar um encerramento de instância iniciado pelo usuário: encerramento padrão, encerramento com ignorar desligamento do sistema operacional, encerramento forçado e encerramento forçado com ignorar desligamento do sistema operacional. A tabela a seguir compara as principais diferenças entre os métodos de encerramento:

Note

Não será possível encerrar uma instância se a proteção contra encerramento estiver ativada. Para obter mais informações, consulte Alterar proteção contra encerramento de instância.

Método de encerramento	Objetivo principal	Caso de uso	Comando da CLI
Encerramento padrão	Desligamento normal da instância com tentativa de desligamento normal do sistema operacional.	Encerramento de instância típico.	`aws ec2 terminate-instances \ --instance-id i-1234567890abcdef0`
Encerrar com ignorar desligamento do sistema operacional	Ignora o desligamento normal do sistema operacional ao encerrar uma instância.	Quando ignorar o desligamento normal do sistema operacional é necessário.	`aws ec2 terminate-instances \ --instance-id i-1234567890abcdef0 \ --skip-os-shutdown`

Método de encerramento	Objetivo principal	Caso de uso	Comando da CLI
Forçar finalização	Resolve instâncias travadas. Tenta primeiro um encerramento padrão; se a instância não conseguir encerrar, encerra-a à força.	Quando a instância está travada no estado `shutting-down` .	`aws ec2 terminate-instances \ --instance-id i-1234567890abcdef0 \ --force`
Encerrar à força com ignorar o encerramento do sistema operacional	A força encerra e ignora o encerramento normal do sistema operacional ao encerrar uma instância.	Quando é necessário encerrar o sistema à força e ignorar o encerramento normal do sistema operacional.	`aws ec2 terminate-instances \ --instance-id i-1234567890abcdef0 \ --force \ --skip-os-shutdown`

Para obter instruções sobre como usar cada método, consulte:

- Encerrar uma instância com um desligamento normal do sistema operacional
- Encerrar uma instância e ignorar o desligamento normal do sistema operacional
- Encerrar uma instância à força

Encerrar uma instância com um desligamento normal do sistema operacional

É possível encerrar uma instância usando o método de parada padrão, que inclui uma tentativa de desligamento normal do sistema operacional. Para obter mais informações, consulte Métodos para encerrar uma instância.

Console

Para encerrar uma instância usando o método de encerramento padrão

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 Estado da instância e Encerrar instância.
4. Quando a confirmação for solicitada, escolha Encerrar (excluir).
5. Após encerrar uma instância, ela permanecerá visível por um breve período, com um estado de `terminated`.

   Se o encerramento apresentar falhas ou se uma instância encerrada permanecer visível por mais do que algumas horas, consulte Instância encerrada ainda sendo exibida.

AWS CLI

Para encerrar uma instância usando o método de encerramento padrão

Use o comando terminate-instances.

```
aws ec2 terminate-instances --instance-ids i-1234567890abcdef0
```

PowerShell

Para encerrar uma instância usando o método de encerramento padrão

Use o cmdlet Remove-EC2Instance.

```
Remove-EC2Instance -InstanceId i-1234567890abcdef0
```

Encerrar uma instância e ignorar o desligamento normal do sistema operacional

É possível ignorar o desligamento normal do sistema operacional ao encerrar uma instância. Para obter mais informações, consulte Métodos para encerrar uma instância.

Console

Para encerrar uma instância e ignorar o desligamento normal do sistema operacional

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 Estado da instância e Encerrar instância.
4. Em Ignorar desligamento do sistema operacional, marque a caixa de seleção Ignorar desligamento do sistema operacional. Se você não vir essa opção no console, isso significa que ela ainda não está disponível no console na região atual. No entanto, você pode acessar esse recurso usando a AWS CLI ou o SDK, ou até mesmo experimentar outra região no console.
5. Escolha Encerrar (excluir).
6. Após encerrar uma instância, ela permanecerá visível por um breve período, com um estado de `terminated`.

   Se o encerramento apresentar falhas ou se uma instância encerrada permanecer visível por mais do que algumas horas, consulte Instância encerrada ainda sendo exibida.

AWS CLI

Para encerrar uma instância e ignorar o desligamento normal do sistema operacional

Use o comando terminate-instances com `--skip-os-shutdown`.

```
aws ec2 terminate-instances \
    --instance-ids i-1234567890abcdef0 \
    --skip-os-shutdown
```

PowerShell

Para encerrar uma instância e ignorar o desligamento normal do sistema operacional

Use o cmdlet Remove-EC2Instance com `-SkipOsShutdown $true`.

```
Remove-EC2Instance `
    -InstanceId i-1234567890abcdef0 `
    -SkipOsShutdown $true
```

Solucionar problemas de encerramento da instância

O solicitante deve ter permissão para chamar `ec2:TerminateInstances`. Para obter mais informações, consulte Exemplos de políticas para trabalhar com instâncias.

Se você encerrar a instância e outra instância for iniciada, provavelmente você configurou a escalabilidade automática por meio de um recurso como o Frota do EC2 ou o Amazon EC2 Auto Scaling. Para obter mais informações, consulte Instâncias executadas ou encerradas automaticamente.

> **Note**
>
> Não será possível encerrar uma instância se a proteção contra encerramento estiver ativada. Para obter mais informações, consulte Alterar proteção contra encerramento de instância.

Se sua instância permanecer nesse estado `shutting-down` por mais tempo do que o normal, você pode tentar forçar o encerramento. Se permanecer no estado `shutting-down`, ele deverá ser limpo (encerrado) por processos automatizados dentro do serviço Amazon EC2. Para obter mais informações, consulte Encerramento atrasado da instância.

Alterar proteção contra encerramento de instância

Para evitar que sua instância seja encerrada acidentalmente usando a API do Amazon EC2, independentemente de você chamar `TerminateInstances` diretamente ou usar outra interface, como o console do Amazon EC2, habilite a proteção contra encerramento da instância. O atributo `DisableApiTermination` controla se a instância pode ser encerrada. Por padrão, a proteção contra encerramento está desabilitada para sua instância. É possível definir o valor desse atributo ao inicializar a instância ou enquanto a instância estiver em execução ou interrompida.

O atributo `DisableApiTermination` não impede que você encerre uma instância ao iniciar o desligamento nela (por exemplo, usando um comando do sistema operacional para o desligamento do sistema) quando o atributo `InstanceInitiatedShutdownBehavior` está definido como `terminate`. Para obter mais informações, consulte Alterar comportamento de desligamento iniciado da instância.

Considerações

- Habilitar a proteção contra encerramento não impede que a AWS encerre a instância quando há um evento programado para encerrá-la.

- Habilitar a proteção contra encerramento não impede que Amazon EC2 Auto Scaling encerre uma instância quando ela não estiver íntegra ou durante eventos de redução horizontal da escala. É possível controlar se um grupo do Auto Scaling pode encerrar uma instância específica ao escalar usando a proteção contra redução horizontal da escala da instância. É possível controlar se um grupo do Auto Scaling pode encerrar instâncias não íntegras suspendendo o processo de escala ReplaceUnhealthy.
- Você não pode habilitar a proteção contra encerramento para Instâncias spot.

Console

Para habilitar a proteção contra encerramento de uma instância no momento da inicialização

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel, escolha Executar instância.
3. Expanda Advanced details (Detalhes avançados). Em Proteção contra encerramento, selecione Habilitar.
4. Quando acabar de especificar os detalhes da instância, escolha Iniciar instância.

Para alterar a proteção contra encerramento de uma instância

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Instances (Instâncias).
3. Selecione a instância.
4. Selecione Ações, Configurações da instância e Alterar proteção contra encerramento.
5. Em Proteção contra encerramento, selecione ou desmarque Habilitar.
6. Escolha Salvar.

AWS CLI

Para habilitar a proteção contra encerramento de uma instância

Use o comando modify-instance-attribute.

```
aws ec2 modify-instance-attribute \
    --instance-id i-1234567890abcdef0 \
    --disable-api-termination
```

Para desabilitar a proteção contra encerramento de uma instância

Use o comando modify-instance-attribute.

```
aws ec2 modify-instance-attribute \
    --instance-id i-1234567890abcdef0 \
    --no-disable-api-termination
```

PowerShell

Para habilitar a proteção contra encerramento de uma instância

Use o cmdlet Edit-EC2InstanceAttribute.

```
Edit-EC2InstanceAttribute `
    -InstanceId i-1234567890abcdef0 `
    -DisableApiTermination $true
```

Para desabilitar a proteção contra encerramento de uma instância

Use o cmdlet Edit-EC2InstanceAttribute.

```
Edit-EC2InstanceAttribute `
    -InstanceId i-1234567890abcdef0 `
    -DisableApiTermination $false
```

Encerramento de múltiplas instâncias com proteção contra encerramento

Se você encerrar múltiplas instâncias em diversas zonas de disponibilidade usando a mesma solicitação e uma ou mais das instâncias especificadas estiverem habilitadas para a proteção contra encerramento, a solicitação falhará e apresentará os seguintes resultados:

- As instâncias especificadas que estão na mesma zona de disponibilidade que a instância protegida não estão terminadas.
- As instâncias especificadas que estão em zonas de disponibilidade diferentes, em que nenhuma outra instância especificada está protegida, estão terminadas corretamente.

Exemplo

Suponha que você tenha as quatro instâncias apresentadas a seguir em duas zonas de disponibilidade.

Instância	Availability Zone	Encerrar proteção
Instância 1	AZ A	`Disabled`
Instância 2		`Disabled`
Instância 3	AZ B	`Enabled`
Instância 4		`Disabled`

Se você tentar terminar todas essas instâncias na mesma solicitação, a solicitação relatará falha com os seguintes resultados:

- A Instância 1 e a Instância 2 foram encerradas com êxito porque nenhuma das instâncias está habilitada para a proteção contra encerramento.
- A Instância 3 e a Instância 4 não são encerradas porque a Instância 3 está habilitada para a proteção contra encerramento.

Alterar comportamento de desligamento iniciado da instância

> **Warning**
>
> O encerramento de uma instância é permanente e irreversível.
> Depois de encerrar uma instância, não será mais possível se conectar a ela e ela não poderá ser recuperada. Todos os volumes anexados do Amazon EBS configurados para serem excluídos no encerramento também serão excluídos permanentemente e não poderão ser recuperados. Todos os dados armazenados em volumes de armazenamento de instância serão perdidos permanentemente. Para obter mais informações, consulte Como funciona o encerramento de uma instância.
> Antes de encerrar uma instância, certifique-se de ter feito backup de todos os dados que você precise reter após o encerramento no armazenamento persistente.

Por padrão, ao iniciar um desligamento de uma instância baseada no Amazon EBS (usando comandos como shutdown ou poweroff), a instância será interrompida. É possível alterar esse comportamento usando o atributo `InstanceInitiatedShutdownBehavior` para a instância de forma que, em vez de ser desligada, ela seja encerrada. É possível atualizar esse atributo enquanto a instância estiver sendo executada ou interrompida.

O comando halt não inicia um desligamento. Se ele for usado, a instância não será encerrada. Em vez disso, ele colocará a CPU em `HLT` e a instância permanecerá em execução.

> **Note**
>
> O `InstanceInitiatedShutdownBehavior` atributo só se aplica quando você executa um desligamento a partir do sistema operacional da instância em si. Ele não se aplica quando você interrompe uma instância usando a API `StopInstances` ou o console do Amazon EC2.

Console

Alterar o comportamento de desligamento iniciado 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.
4. Escolha Actions (Ações), Instance settings (Configurações da instância), Change shutdown behavior (Alterar comportamento de desativação).

   O comportamento de desligamento exibe o comportamento atual.
5. Para alterar o comportamento, em Comportamento de desligamento, selecione Interromper ou Encerrar.
6. Escolha Salvar.

AWS CLI

Alterar o comportamento de desligamento iniciado da instância

Use o comando modify-instance-attribute.

```
aws ec2 modify-instance-attribute \
    --instance-id i-1234567890abcdef0 \
    --instance-initiated-shutdown-behavior terminate
```

PowerShell

Alterar o comportamento de desligamento iniciado da instância

Use o cmdlet Edit-EC2InstanceAttribute.

```
Edit-EC2InstanceAttribute `
    -InstanceId i-1234567890abcdef0 `
    -InstanceInitiatedShutdownBehavior terminate
```

Preservação de dados quando uma instância for encerrada

Quando uma instância do Amazon EC2 é encerrada, é possível preservar os dados nos volumes de armazenamento da instância ou nos volumes do Amazon EBS. Este tópico explica como garantir que seus dados persistam além do encerramento da instância.

Como o encerramento da instância afeta os volumes raiz e de dados

Volumes de armazenamento de instâncias

Quando uma instância é encerrada, os volumes de armazenamento de instância são excluídos automaticamente e os dados são perdidos. Para preservar esses dados além do tempo de vida da instância, antes de encerrá-la, copie manualmente os dados para um armazenamento persistente, como um volume do Amazon EBS, um bucket do Amazon S3 ou um sistema de arquivos do Amazon EFS. Para obter mais informações, consulte Opções de armazenamento para as instâncias do Amazon EC2.

Volumes do Amazon EBS

Quando uma instância é encerrada, os volumes do EBS são excluídos ou preservados, dependendo do valor do atributo `DeleteOnTermination` para cada volume:

- Sim (console) / `true` (CLI): o volume é excluído quando a instância é encerrada.
- Não (console) / `false` (CLI): o volume é preservado quando a instância é encerrada. Os volumes preservados continuam a incorrer em cobranças.

> **Note**
>
> Depois que uma instância é encerrada, é possível criar um snapshot do volume preservado ou anexá-lo a outra instância. Para evitar incorrer em cobranças, exclua o volume.

Comportamento de exclusão padrão para volumes do EBS

O valor `DeleteOnTermination` padrão difere dependendo do tipo de volume, se o volume foi anexado na inicialização ou depois e do método (console ou CLI) usado para anexá-lo:

Tipo de volume	Anexado quando	Método para anexar	Comportamento padrão no encerramento da instância
Volume raiz	Na inicialização	Console ou CLI	Excluir
Volume raiz	Após a inicialização	Console ou CLI	Preservar
Volume de dados	Na inicialização	Console	Preservar
Volume de dados	Na inicialização	CLI	Excluir
Volume de dados	Após a inicialização	Console e CLI	Preservar

Verificar as configurações de persistência do volume

O valor padrão na inicialização de um volume do EBS é determinado pelo atributo `DeleteOnTermination` definido na AMI. É possível alterar o valor na inicialização da instância substituindo a configuração da AMI. Recomendamos verificar a configuração padrão do atributo `DeleteOnTermination` após iniciar uma instância.

Para verificar se um volume do Amazon EBS será excluído no encerramento 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.

4. Escolha a guia Armazenamento.
5. Em Dispositivos de bloco, role para a direita para verificar a coluna Excluir no encerramento.
   - Se Sim, o volume será excluído quando a instância for encerrada.
   - Se Não, o volume não será excluído quando a instância for encerrada. Quaisquer volumes não excluídos continuarão incorrendo em cobranças.

Alteração do volume raiz para persistir na inicialização

É possível alterar atributo `DeleteOnTermination` de um volume do EBS ao inicializar uma instância. O procedimento a seguir também pode ser usado para um volume de dados.

Console

Para alterar o volume-raiz de uma instância para que persista na inicialização

1. Siga o procedimento para executar uma instância, mas não execute a instância até concluir as etapas a seguir para alterar o volume raiz a ser mantido.
2. No painel Configurar armazenamento, escolha Avançado.
3. Em Volumes do EBS, expanda as informações do volume raiz.
4. Em Excluir no encerramento, escolha Não.
5. No painel Resumo, analise a configuração da instância e selecione Iniciar instância. Para obter mais informações, consulte Executar uma instância do EC2 usando o assistente de inicialização de instâncias no console.

AWS CLI

Para alterar o volume-raiz de uma instância para que persista na inicialização

Use o comando run-instances para alterar o valor de `DeleteOnTermination` no mapeamento de dispositivos de blocos.

Adicione a opção `--block-device-mappings`:

```
--block-device-mappings file://mapping.json
```

Em `mapping.json`, especifique o nome do dispositivo (por exemplo, `/dev/sda1` ou `/dev/xvda`), e em `DeleteOnTermination`, especifique `false`.

```
[
  {
    "DeviceName": "device_name",
    "Ebs": {
      "DeleteOnTermination": false
    }
  }
]
```

PowerShell

Para alterar o volume-raiz de uma instância para que persista na inicialização

Use o cmdlet New-EC2Instance para alterar o valor de `DeleteOnTermination` no mapeamento de dispositivos de blocos.

Adicione a opção `-BlockDeviceMapping`:

```
-BlockDeviceMapping $bdm
```

Em `bdm`, especifique o nome do dispositivo (por exemplo, `/dev/sda1` ou `/dev/xvda`), e em `DeleteOnTermination`, especifique `false`.

```
$ebd = New-Object -TypeName Amazon.EC2.Model.EbsBlockDevice
$ebd.DeleteOnTermination = false
$bdm = New-Object -TypeName Amazon.EC2.Model.BlockDeviceMapping
$bdm.DeviceName = "/dev/sda1"
$bdm.Ebs = $ebd
```

Alteração do volume raiz de uma instância em execução para persistir

É possível alterar o volume raiz do EBS de uma instância em execução para que ele persista. O procedimento a seguir também pode ser usado para um volume de dados.

AWS CLI

Para alterar o volume-raiz para que persista

Use o comando modify-instance-attribute.

```
aws ec2 modify-instance-attribute \
```

```
    --instance-id i-1234567890abcdef0  \
    --block-device-mappings file://mapping.json
```

Em `mapping.json`, especifique o nome do dispositivo (por exemplo, `/dev/sda1` ou `/dev/xvda`), e em `--DeleteOnTermination`, especifique `false`.

```
[
  {
    "DeviceName": "device_name",
    "Ebs": {
      "DeleteOnTermination": false
    }
  }
]
```

PowerShell

Para alterar o volume-raiz para que persista

Use o cmdlet Edit-EC2InstanceAttribute.

Adicione a opção `-BlockDeviceMapping`:

```
-BlockDeviceMapping $bdm
```

Em `bdm`, especifique o nome do dispositivo (por exemplo, `/dev/sda1` ou `/dev/xvda`), e em `DeleteOnTermination`, especifique `false`.

```
$ebd = New-Object -TypeName Amazon.EC2.Model.EbsBlockDevice
$ebd.DeleteOnTermination = false
$bdm = New-Object -TypeName Amazon.EC2.Model.BlockDeviceMapping
$bdm.DeviceName = "/dev/sda1"
$bdm.Ebs = $ebd
```

Desativação da instância

A instância é programada para ser desativada quando a AWS detecta uma falha irreparável do hardware subjacente que hospeda a instância. O tipo de volume raiz da instância determina o comportamento da desativação da instância:

- Se o volume raiz da instância for um volume do Amazon EBS, a instância será interrompida e você poderá iniciá-la novamente a qualquer momento. Iniciar a instância interrompida migra-a para o novo hardware.
- Se o volume raiz da instância for um volume de armazenamento de instância, a instância será encerrada e não poderá ser usada novamente.

Para obter mais informações sobre os tipos de eventos de instância, consulte Eventos programados para instâncias do Amazon EC2.

Tópicos

- Identificar instâncias programadas para desativação
- Ações a serem executadas para instâncias baseadas em EBS programadas para desativação
- Ações a serem executadas para instâncias com armazenamento de instâncias programadas para desativação

Identificar instâncias programadas para desativação

Se a sua instância estiver programada para desativação, você receberá um e-mail antes do evento com o ID e a data de desativação da instância. Você também pode verificar se há instâncias programadas para desativação.

> **Important**
>
> Se uma instância estiver programada para desativação, recomendamos que você aja o mais rápido possível, pois talvez a instância já esteja inacessível. Para obter mais informações, consulte Check if your instance is reachable.

Opções para identificar instâncias programadas para desativação

- Monitore o e-mail dos contatos da conta
- Verificar suas instâncias

Monitore o e-mail dos contatos da conta

Se uma instância estiver programada para desativação, o contato principal da conta e o contato de operações receberão um e-mail antes do evento. Esse e-mail inclui o ID da instância e a data

de desativação programada. Para mais informações, consulte Update the primary contact for your AWS account e Update the alternate contacts for your AWS account no Guia de referência do AWS Gerenciamento de contas.

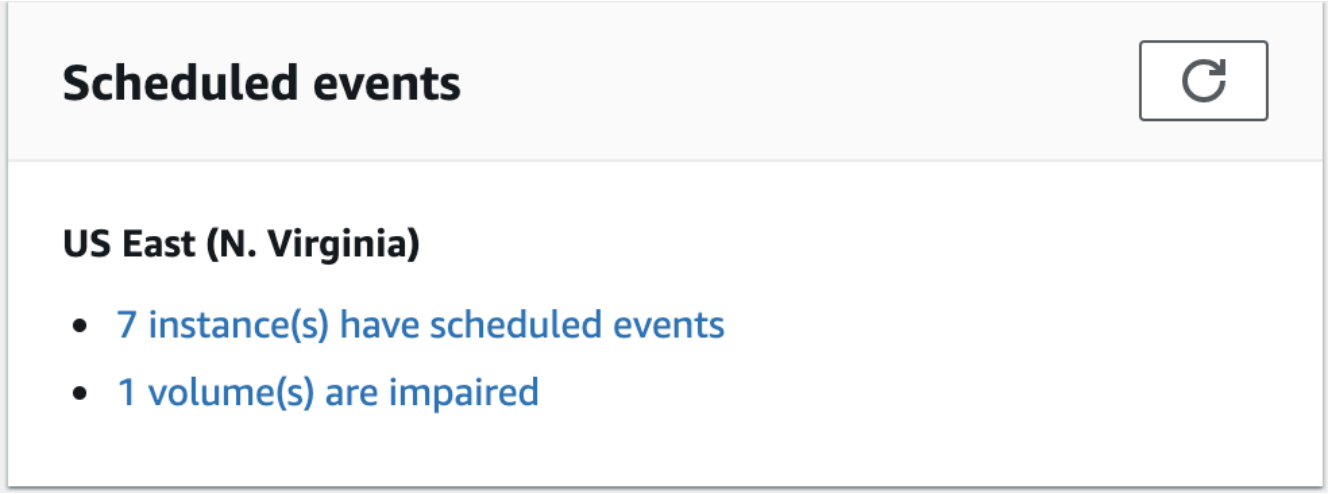
Verificar suas instâncias

Se você usar uma conta de e-mail que não verifica regularmente, poderá perder uma notificação de desativação da instância. Você pode verificar a qualquer momento se alguma de suas instâncias está programada para ser desativada.

Console

Para identificar instâncias programadas para desativação

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha EC2 Dashboard (Painel do EC2). Em Scheduled events (Eventos agendados), é possível ver os eventos associados a volumes e instâncias do Amazon EC2, organizados por região.



3. Se você tiver uma instância com um evento agendado listado, selecione o link abaixo do nome da região para acessar a página Events (Eventos).
4. A página Events (Eventos) lista todos os recursos com eventos associados a eles. Para visualizar as instâncias que estão agendadas para desativação, selecione Instance resources (Recursos da instância) na primeira lista de filtros e, em seguida, Instance stop or retirement (Interrupção ou desativação de instância) na segunda lista de filtros.
5. Se os resultados do filtro mostrarem que uma instância está agendada para desativação, selecione-a e anote a data e a hora do campo Start time (Hora de início) no painel de detalhes. Essa é a data de desativação da instância.

AWS CLI

Para encontrar instâncias programadas para desativação

Use o seguinte comando describe-instance-status. Repita o procedimento em cada região na qual você tenha instâncias em execução.

```
aws ec2 describe-instance-status --filters Name=event.code,Values=instance-
retirement
```

PowerShell

Para encontrar instâncias programadas para desativação

Use o cmdlet Get-EC2InstanceStatus. Repita o procedimento em cada região na qual você tenha instâncias em execução.

```
Get-EC2InstanceStatus -Filter @{Name="event.code"; Values="instance-retirement"}
```

Ações a serem executadas para instâncias baseadas em EBS programadas para desativação

Para preservar os dados em sua instância sendo desativada, é possível executar uma das ações a seguir. É importante que você execute essa ação antes da data de desativação da instância, para evitar períodos de desativação e perda de dados imprevistos.

Para instâncias do Linux, se você não tiver certeza se a instância é baseada no EBS ou no armazenamento de instâncias, consulte Volumes raiz para as instâncias do Amazon EC2.

Verifique se sua instância está acessível

Quando você for notificado de que sua instância está programada para desativação, recomendamos que execute a seguinte ação o mais rápido possível:

- Verifique se sua instância está acessível conectando-se ou fazendo ping na instância.
- Se sua instância estiver acessível, planeje interromper/iniciar a instância em um momento apropriado antes da data de desativação programada, quando o impacto for mínimo. Para obter mais informações sobre como interromper e iniciar sua instância e o que esperar quando a

instância é interrompida, como o efeito em endereços IP elásticos, públicos e privados associados à instância, consulte Início e interrupção de instâncias do Amazon EC2. Observe que os dados em volumes de armazenamento de instâncias são perdidos quando você interrompe e inicia sua instância.

- Se sua instância estiver inacessível, você deverá agir imediatamente e executar uma interrupção/inicialização para recuperar sua instância.
- Se preferir encerrar sua instância, planeje fazê-lo o mais rápido possível, para que você pare de receber cobranças pela instância.

Crie um backup da sua instância

Crie uma AMI baseada em EBS em sua instância para que você tenha um backup. Para garantir a integridade dos dados, interrompa a instância antes de criar a AMI. Espere a data de desativação agendada para a interrupção da instância ou interrompa a instância por conta própria antes dessa data. É possível iniciar a instância novamente a qualquer momento. Para obter mais informações, consulte Criação de uma AMI baseada no Amazon EBS.

Execute uma instância de substituição

Depois de criar uma AMI a partir da sua instância, é possível usar a AMI para iniciar uma instância de substituição. No console do Amazon EC2, selecione sua nova AMI e escolha Iniciar instância a partir da AMI. Configure os parâmetros da sua instância e escolha Iniciar instância. Para obter mais informações sobre cada campo, consulte Executar uma instância do EC2 usando o assistente de inicialização de instâncias no console.

Ações a serem executadas para instâncias com armazenamento de instâncias programadas para desativação

Para preservar os dados em sua instância sendo desativada, é possível executar uma das ações a seguir. É importante que você execute essa ação antes da data de desativação da instância, para evitar períodos de desativação e perda de dados imprevistos.

> **Warning**
>
> Se o volume raiz da instância for de armazenamento de instância e a data de desativação for atingida, a instância será encerrada, tornando impossível recuperar tanto a instância quanto qualquer dado que estivesse armazenado nela. Independentemente do tipo de volume raiz

da instância, os dados nos volumes de armazenamento de instância são perdidos quando a instância é desativada, mesmo que os volumes estejam anexados a uma instância com volume raiz do EBS.

Verifique se sua instância está acessível

Quando você for notificado de que sua instância está programada para desativação, recomendamos que execute a seguinte ação o mais rápido possível:

- Verifique se sua instância está acessível conectando-se ou fazendo ping na instância.
- Se sua instância estiver inacessível, é provável que haja muito pouco que possa ser feito para recuperá-la. Para obter mais informações, consulte Solucionar problemas de uma instância inacessível do Amazon EC2. A AWS encerrará a instância na data de desativação programada, portanto, para uma instância inacessível, é possível encerrar a instância por conta própria.

Execute uma instância de substituição

Crie uma AMI baseada no Amazon S3 usando as ferramentas da AMI na sua instância, conforme descrito em Criação de uma AMI baseada no Amazon S3. No console do Amazon EC2, selecione sua nova AMI e escolha Iniciar instância a partir da AMI. Configure os parâmetros da sua instância e escolha Iniciar instância. Para obter mais informações sobre cada campo, consulte Executar uma instância do EC2 usando o assistente de inicialização de instâncias no console.

Converta sua instância em uma instância baseada em EBS

Transfira seus dados para um volume do EBS, obtenha um snapshot do volume e crie a AMI a partir do snapshot. É possível executar uma instância de substituição a partir da nova AMI. Para obter mais informações, consulte Conversão da AMI baseada no Amazon S3 em uma AMI baseada no EBS.

Recuperação automática de instâncias

Important

Esta seção descreve como configurar proativamente os mecanismos de recuperação em uma instância do EC2. Esses mecanismos de recuperação são projetados para restaurar a disponibilidade da instância quando a AWS detecta um problema subjacente de hardware

ou software que faz com que a verificação de status do sistema falhe. Se você estiver tendo problemas para acessar sua instância, consulte Solução de problemas de instâncias do EC2.

Caso a AWS detecte que uma instância não está disponível devido a um problema de hardware ou software subjacente, há dois mecanismos que podem restaurar automaticamente a disponibilidade da instância : a recuperação automática simplificada e a recuperação baseada em ações do Amazon CloudWatch. A restauração da disponibilidade da instância também é conhecida como recuperação da instância.

Durante o processo de recuperação da instância, a AWS tentará mover sua instância do host com o problema de hardware ou software subjacente para um host diferente. Caso obtenha êxito, o processo de recuperação aparecerá para a instância como uma reinicialização não planejada. É possível verificar se a recuperação da instância ocorreu.

Se o processo de recuperação não for obtive êxito, a instância poderá continuar em execução no host com o problema subjacente de hardware ou software. Nesse caso será necessária uma intervenção manual. Se a instância se tornar inacessível ou se a verificação de status do sistema continuar a falhar, recomendamos que você pare e inicie manualmente a instância. Quando você inicia uma instância, ela é normalmente migrada para um novo computador host subjacente. No entanto, ao contrário da recuperação automática de instâncias, na qual a instância retém seu endereço IPv4 público, uma instância reinicializada recebe um endereço IPv4 público, a menos que tenha um endereço IP elástico.

Para se beneficiar dos mecanismos de recuperação automática, eles devem ser configurados com antecedência em uma instância antes que uma verificação do status do sistema indique falha. Por padrão, a recuperação automática simplificada é habilitada durante a execução da instância. Como opção, é possível configurar a recuperação baseada em ações do Amazon CloudWatch após a execução. Ter um desses mecanismos configurado torna sua instância mais resiliente.

A recuperação automática simplificada e a recuperação baseada em ações do Amazon CloudWatch só estão disponíveis em instâncias com suporte. Para obter mais informações, consulte Requisitos para a habilitação da recuperação automática simplificada e Requisitos para a habilitação da recuperação baseada em ações do CloudWatch.

⚠ Warning

Quando a AWS recupera sua instância de um problema subjacente de hardware ou software, tenha em mente as seguintes consequências: os dados armazenados na memória volátil

(RAM) serão perdidos e o tempo de atividade do sistema operacional recomeçará do zero. Além disso, com a recuperação baseada em ações do CloudWatch, os dados nos volumes de armazenamento de instância também serão perdidos. Para ajudar a se proteger contra a perda de dados, recomendamos que você crie regularmente backups de dados importantes. Para obter mais informações sobre as práticas recomendadas de backup e recuperação de instâncias do EC2, consulte Práticas recomendadas do Amazon EC2.
Os mecanismos automáticos de recuperação de instâncias são projetados para instâncias individuais. Para obter orientação sobre como criar um sistema resiliente, consulte Crie um sistema resiliente.

Tópicos

- Conceitos principais da recuperação automática de instâncias
- Diferenças entre a recuperação automática simplificada e a recuperação baseada em ações do CloudWatch
- Crie um sistema resiliente
- Verificar se ocorreu a recuperação automática da instância
- Configurar a recuperação automática simplificada em uma instância do Amazon EC2
- Configurar recuperação baseada em ação do CloudWatch em uma instância do EC2

Conceitos principais da recuperação automática de instâncias

A recuperação automática de instâncias é um atributo do Amazon EC2 que restaura automaticamente a disponibilidade da instância quando ocorrem falhas subjacentes de hardware ou software, aprimorando a resiliência e a confiabilidade de suas instâncias do EC2.

A seguir estão os principais conceitos da recuperação automática de instâncias:

Opções de configuração

Dois mecanismos podem ser configurados para oferecer suporte à recuperação automática de instâncias:

- Recuperação automática simplificada: habilitada por padrão em instâncias com suporte.
- Recuperação baseada em ações do CloudWatch: requer configuração manual nas instâncias com suporte.

Verificações de status de sistema

As verificações de status do sistema monitoram automaticamente a infraestrutura da AWS na qual sua instância do EC2 é executada.

- Se a verificação do status do sistema falhar, a AWS inicia a recuperação automática da instância, que tenta migrar a instância afetada para um hardware diferente.
- Uma falha na verificação do status do sistema indica um problema com o hardware ou o software do host, e não um problema com a instância em si. A recuperação automática de instâncias pode recuperar uma instância que falhe na verificação do status do sistema. No entanto, a recuperação automática de instâncias não funcionará se somente a verificação do status da instância falhar.
- Para ver as diferenças entre as verificações de status da instância e do sistema, consulte Tipos de verificações de status.

Exemplos de problemas subjacentes de hardware ou software

Os problemas de hardware ou software que podem causar a falha na verificação do status do sistema incluem perda de conectividade de rede, perda de energia do sistema, problemas de software no host físico e problemas de hardware no host físico que afetam a acessibilidade da rede.

Características das instâncias recuperadas

Uma instância recuperada é idêntica à instância original, exceto pelos elementos que são perdidos.

Elementos preservados:

- ID da instância
- seus endereços IP públicos, privados e elásticos;
- Metadados da instância
- Grupo de posicionamento
- volumes do EBS associados.
- Zona de disponibilidade

Elementos perdidos:

- Dados armazenados na memória volátil (RAM)

- Dados armazenados em volumes de armazenamento de instâncias (aplicável somente à recuperação baseada em ações do CloudWatch)
- O tempo de atividade do sistema operacional é redefinido para zero

Monitoramento de verificações de status do sistema com o CloudWatch

A métrica StatusCheckFailed_System no CloudWatch indica se uma verificação de status do sistema foi aprovada ou falhou.

Valores da métrica:

- 0: a verificação de status do sistema foi aprovada.
- 1: a verificação de status do sistema falhou.

Eventos no Health Dashboard

Durante as tentativas automáticas de recuperação da instância, a AWS envia eventos para seu Health Dashboard com base no mecanismo de recuperação configurado e no resultado:

- Recuperação automática simplificada
  - Evento de êxito: `AWS_EC2_SIMPLIFIED_AUTO_RECOVERY_SUCCESS`
  - Evento de falha: `AWS_EC2_SIMPLIFIED_AUTO_RECOVERY_FAILURE`
- Recuperação baseada em ações do CloudWatch
  - Evento de êxito: `AWS_EC2_INSTANCE_AUTO_RECOVERY_SUCCESS`
  - Evento de falha: `AWS_EC2_INSTANCE_AUTO_RECOVERY_FAILURE`

Diferenças entre a recuperação automática simplificada e a recuperação baseada em ações do CloudWatch

A tabela a seguir compara as principais diferenças entre a recuperação automática simplificada e a recuperação baseada em ações do CloudWatch.

Ponto de comparação	Recuperação automática simplificada	Recuperação baseada em ações do CloudWatch
Configuração	Habilitada por padrão nas instâncias com suporte	Requer configuração manual dos alarmes e ações do CloudWatch

Ponto de comparação	Recuperação automática simplificada	Recuperação baseada em ações do CloudWatch
Flexibilidade	Comportamento fixo de recuperação gerenciado pela AWS	Ações e condições personalizáveis
Notificação	Notificações básicas por meio do Health Dashboard	Notificações personalizáveis por meio do SNS
Tamanho da instância metal	Excluído	Incluído
Volumes de armazenamento de instância anexados na execução.	Sem suporte para instâncias que anexam volumes de armazenamento de instância na execução	Com suporte em tipos de instância selecionados. Observe que os dados nos volumes de armazenamento de instância são perdidos durante a recuperação da instância.
Tempo de recuperação	Tentativa de recuperação padrão	Tentativas de recuperação mais rápidas do que a recuperação automática simplificada
O problema do host é solucionado durante a migração	A migração pode ser cancelada, e a instância permanece no host original	A migração continua para um novo host
Custo	Sem custo adicional	Pode incorrer em cobranças do CloudWatch

Crie um sistema resiliente

Embora a recuperação automática simplificada e a recuperação baseada em ações do CloudWatch sejam eficazes para manter a disponibilidade de instâncias individuais, a AWS recomenda a implementação de uma arquitetura de alta disponibilidade que permita o failover do tráfego para instâncias íntegras.

Para conseguir isso, considere usar serviços da AWS como o Elastic Load Balancing (que distribui o tráfego de entrada em várias instâncias do EC2) e o Amazon EC2 Auto Scaling (que ajusta automaticamente o número de instâncias com base na demanda e na integridade).

Para obter mais informações sobre a criação de um sistema resiliente e tolerante a falhas com instâncias do EC2, consulte os recursos a seguir:

- De volta ao básico: projetando para falhas com o EC2 no canal AWS do YouTube
- Arquitetura de recuperação de desastres (DR) na AWS, parte I: estratégias de recuperação na nuvem no site do Blog de Arquitetura da AWS.
- Guia do usuário de Application Load Balancers
- Guia do usuário do Amazon EC2 Auto Scaling
- REL11-BP02 failover para recursos íntegros no Pilar de confiabilidade do AWS Well-Architected Framework

Verificar se ocorreu a recuperação automática da instância

Se sua instância parecer ter ficado offline e, em seguida, reiniciou inesperadamente, ela pode ter passado por uma recuperação automática de instância em resposta a um problema subjacente de hardware ou software. É possível verificar isso verificando os eventos de recuperação automática de instâncias no seu Health Dashboard. Você também pode verificar se um problema subjacente de hardware ou software foi detectado em sua instância verificando a métrica StatusCheckFailed_System do Amazon CloudWatch.

Verifique se há eventos no Health Dashboard

Quando ocorre uma tentativa automática de recuperação da instância, a AWS envia eventos para o seu Health Dashboard. O evento específico depende do mecanismo de recuperação configurado e se a tentativa obteve êxito ou falhou.

Para verificar os eventos de recuperação automática de instâncias no Health Dashboard

1. Abra o Health Dashboard em https://phd.aws.amazon.com/phd/home#/.
2. Procure pelos eventos associados à recuperação automática de instâncias. A presença desses eventos pode confirmar se ocorreu uma tentativa de recuperação automática da instância e seu resultado.

    - Recuperação automática simplificada

    - Evento de êxito: `AWS_EC2_SIMPLIFIED_AUTO_RECOVERY_SUCCESS`
    - Evento de falha: `AWS_EC2_SIMPLIFIED_AUTO_RECOVERY_FAILURE`
- Recuperação baseada em ações do CloudWatch
    - Evento de êxito: `AWS_EC2_INSTANCE_AUTO_RECOVERY_SUCCESS`
    - Evento de falha: `AWS_EC2_INSTANCE_AUTO_RECOVERY_FAILURE`

Monitore as verificações de status do sistema com o CloudWatch

É possível verificar se um problema subjacente de hardware ou software foi detectado em sua instância observando a métrica StatusCheckFailed_System no CloudWatch. O valor da métrica indica se a verificação do status do sistema foi aprovada (sem problemas de hardware ou software) ou falhou (problema de hardware ou software).

Para verificar se um problema subjacente de hardware ou software foi detectado

1. Abra o console do CloudWatch na página Métricas, em https://console.aws.amazon.com/cloudwatch/home?#metricsV2.
2. Verifique se você está na mesma região que a instância do EC2.
3. Cole a métrica a seguir no campo de pesquisa Métricas e pressione Enter.

   ```
   StatusCheckFailed_System
   ```
4. Escolha EC2 > Métricas por instância.
5. Na tabela, marque a caixa de seleção ao lado da instância que você deseja verificar.
6. Altere o período da consulta para o momento em que você suspeita que o evento de recuperação ocorreu.
7. Escolha a guia Métricas em gráfico e, em StatusCheckFailed_System, faça o seguinte:

   a. Em Estatística, escolha Média, Máximo ou Mínimo.
   b. Em Período, escolha 1 minuto.
8. Verifique o valor de StatusCheckFailed_System.

   - Valor 0: a verificação de status do sistema foi aprovada, indicando que não há nenhum problema subjacente de hardware ou software.
   - Valor 1: a verificação de status do sistema falhou, indicando um problema subjacente de hardware ou software.

Para obter mais informações, consulte Recuperação automática de instâncias.

Configurar a recuperação automática simplificada em uma instância do Amazon EC2

> **Important**
>
> Esta seção descreve como configurar proativamente os mecanismos de recuperação em uma instância do EC2. Esses mecanismos de recuperação são projetados para restaurar a disponibilidade da instância quando a AWS detecta um problema subjacente de hardware ou software que faz com que a verificação de status do sistema falhe. Se você estiver tendo problemas para acessar sua instância, consulte Solução de problemas de instâncias do EC2.

Se a AWS detectar que uma instância não está disponível devido a um problema subjacente de hardware ou software, a recuperação automática simplificada pode restaurar automaticamente a disponibilidade da instância movendo a instância do host com o problema subjacente para um host diferente.

Se ocorrer uma recuperação automática simplificada, a AWS enviará um dos eventos a seguir ao seu AWS Health Dashboard, dependendo do resultado:

- Evento de êxito: `AWS_EC2_SIMPLIFIED_AUTO_RECOVERY_SUCCESS`
- Evento de falha: `AWS_EC2_SIMPLIFIED_AUTO_RECOVERY_FAILURE`

Para ser notificado sobre esses eventos, é possível configurar as notificações. Para obter mais informações, consulte Criação da sua primeira configuração de notificação no Notificações de Usuários da AWS no Guia do usuário do Notificações de Usuários da AWS. Você também pode usar as regras do Amazon EventBridge para monitorar os eventos de recuperação automática simplificados.

A recuperação automática simplificada é habilitada por padrão em todas as instâncias com suporte durante a execução da instância. No entanto, ela só poderá operar se uma instância estiver no estado `running`, se não houver eventos de serviço listados no AWS Health Dashboard e se houver capacidade disponível para o tipo de instância. Em algumas situações, como interrupções significativas, restrições de capacidade podem causar falhas nas tentativas de recuperação. Para obter mais informações, consulte the section called “Solução de problemas de falhas da recuperação automática simplificada”.

É possível desabilitar a recuperação automática simplificada durante ou após o lançamento e reabilitá-la posteriormente, caso necessário.

> **Warning**
>
> Quando a AWS recupera sua instância de um problema subjacente de hardware ou software, tenha em mente as seguintes consequências: os dados armazenados na memória volátil (RAM) serão perdidos e o tempo de atividade do sistema operacional recomeçará do zero. Para ajudar a se proteger contra a perda de dados, recomendamos que você crie regularmente backups de dados importantes. Para obter mais informações sobre as práticas recomendadas de backup e recuperação de instâncias do EC2, consulte Práticas recomendadas do Amazon EC2.
>
> Os mecanismos automáticos de recuperação de instâncias são projetados para instâncias individuais. Para obter orientação sobre como criar um sistema resiliente, consulte Crie um sistema resiliente.

Conteúdo

- Requisitos para a habilitação da recuperação automática simplificada
- Configurar a recuperação automática simplificada
- Solução de problemas de falhas da recuperação automática simplificada

Requisitos para a habilitação da recuperação automática simplificada

A recuperação automática simplificada pode ser habilitada em instâncias que atendam aos seguintes critérios:

Tipos de instância

- Uso geral: A1, M3, M4, M5, M5a, M5n, M5zn, M6a, M6g, M6i, M6in, M7a, M7g, M7i, M7i-flex, M8a, M8azn, M8g, M8gb, M8gn, M8i, M8i-flex, T1, T2, T3, T3a, T4g
- Otimizadas para computação: C3, C4, C5, C5a, C5n, C6a, C6g, C6gn, C6i, C6in, C7a, C7g, C7gn, C7i, C7i-flex, C8a, C8g, C8gb, C8gn, C8i, C8i-flex
- Otimizadas para memória: R3, R4, R5, R5a, R5b, R5n, R6a, R6g, R6i, R6in, R7a, R7g, R7i, R7iz, R8a, R8g, R8gb, R8gn, R8i, R8i-flex, U-3tb1, U-6tb1, U-9tb1, U-12tb1, U-18tb1, U-24tb1, U7i-6tb, U7i-8tb, U7i-12tb, U7in-16tb, U7in-24tb, U7in-32tb, U7inh-32tb, X1, X1e, X2iezn, X8g, X8i

- Computação acelerada: G3, G5g, Inf1, P3, VT1
- Computação de alta performance: Hpc6a, Hpc7a, Hpc7g, Hpc8a

Locação

- Compartilhada
- Instância Dedicada

Para obter mais informações, consulte Instâncias dedicadas do Amazon EC2.

Limitações

Não há suporte para a recuperação automática simplificada para instâncias com as características a seguir:

- Tamanho da instância: `metal` instâncias
- Locação: host dedicado. Para hosts dedicados, use a recuperação automática de host dedicado em vez disso.
- Armazenamento: instâncias com volumes de armazenamento de instância
- Rede: instâncias usando um adaptador de malha elástica
- Ajuste de escala automático: instâncias que fazem parte de um grupo do Auto Scaling
- Manutenção: instâncias que estejam passando por um evento de manutenção programada no momento

Configurar a recuperação automática simplificada

A recuperação automática simplificada é ativada por padrão quando você executa uma instância compatível. É possível definir o comportamento de recuperação automática como `disabled` durante ou após a inicialização da instância.

A configuração `default` não habilita a recuperação automática simplificada para uma instância sem suporte.

Console

Para desabilitar a recuperação automática simplificada na inicialização

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias) e Launch Instance (Iniciar instância).

3. Na seção Detalhes avançados, em Recuperação automática de instâncias, escolha Desabilitado.
4. Defina as configurações de execução da instância restantes conforme necessário e, em seguida, inicie a instância.

Para desabilitar a recuperação automática simplificada após a inicialização

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância, escolha Actions (Ações), Instance Settings (Configurações da instância) e selecione Change auto-recovery Behavior (Alterar o comportamento da recuperação automática).
4. Escolha Off (Desativar) e, em seguida, escolha Save (Salvar).

Para habilitar a recuperação automática simplificada após a inicialização

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância, escolha Actions (Ações), Instance Settings (Configurações da instância) e selecione Change auto-recovery Behavior (Alterar o comportamento da recuperação automática).
4. Escolha Padrão e depois Save (Salvar).

AWS CLI

Para desabilitar a recuperação automática simplificada na inicialização

Use o comando run-instances com a opção `--maintenance-options`.

```
--maintenance-options AutoRecovery=Disabled
```

Para desabilitar a recuperação automática simplificada após a inicialização

Use o comando modify-instance-maintenance-options.

```
aws ec2 modify-instance-maintenance-options \
    --instance-id i-1234567890abcdef0 \
```

```
    --auto-recovery disabled
```

Para habilitar a recuperação automática simplificada após a inicialização

Use o comando modify-instance-maintenance-options.

```
aws ec2 modify-instance-maintenance-options \
    --instance-id i-1234567890abcdef0 \
    --auto-recovery default
```

PowerShell

Para desabilitar a recuperação automática simplificada na inicialização

Use o cmdlet New-EC2Instance.

```
-MaintenanceOptions_AutoRecovery Disabled
```

Para desabilitar a recuperação automática simplificada após a inicialização

Use o cmdlet Edit-EC2InstanceMaintenanceOption.

```
Edit-EC2InstanceMaintenanceOption `
    -InstanceId i-1234567890abcdef0 `
    -AutoRecovery Disabled
```

Para habilitar a recuperação automática simplificada após a inicialização

Use o cmdlet Edit-EC2InstanceMaintenanceOption.

```
Edit-EC2InstanceMaintenanceOption `
    -InstanceId i-1234567890abcdef0 `
    -AutoRecovery Enabled
```

Solução de problemas de falhas da recuperação automática simplificada

Se a recuperação automática simplificada falhar ao recuperar a sua instância, considere os problemas a seguir:

- Os eventos de serviço da AWS estão em execução

A recuperação automática simplificada não opera durante eventos de serviço no AWS Health Dashboard. Talvez você não receba notificações de falha de recuperação para esses eventos. Para obter as informações mais recentes sobre a disponibilidade do serviço, consulte a página de status do serviço.

- Capacidade insuficiente

  Há temporariamente hardware de substituição insuficiente para migrar a instância.

- Número máximo de tentativas diárias de recuperação atingido

  A instância alcançou a franquia diária máxima de tentativas de recuperação. Sua instância poderá ser subsequentemente retirada se a recuperação automática falhar e se for determinado que uma degradação do hardware é a causa-raiz da falha original da verificação do status do sistema.

Se a falha na verificação de status do sistema da instância persistir apesar de várias tentativas de recuperação, consulte Solução de problemas em instâncias com falha nas verificações de status para obter mais informações.

Configurar recuperação baseada em ação do CloudWatch em uma instância do EC2

> **Important**
>
> Esta seção descreve como configurar proativamente os mecanismos de recuperação em uma instância do EC2. Esses mecanismos de recuperação são projetados para restaurar a disponibilidade da instância quando a AWS detecta um problema subjacente de hardware ou software que faz com que a verificação de status do sistema falhe. Se você estiver tendo problemas para acessar sua instância, consulte Solução de problemas de instâncias do EC2.

Se o AWS detectar que uma instância está indisponível devido a um problema subjacente de hardware ou software, a recuperação baseada em ações do CloudWatch pode restaurar automaticamente a disponibilidade da instância movendo-a do host com o problema subjacente para um host diferente.

Se a recuperação baseada em ações do CloudWatch ocorrer, a AWS enviará um dos eventos a seguir para o seu AWS Health Dashboard, dependendo do resultado:

- Evento de êxito: `AWS_EC2_INSTANCE_AUTO_RECOVERY_SUCCESS`
- Evento de falha: `AWS_EC2_INSTANCE_AUTO_RECOVERY_FAILURE`

É possível configurar a recuperação baseada em ações do CloudWatch para adicionar ações de recuperação aos alarmes do Amazon CloudWatch. A recuperação baseada em ações do CloudWatch funciona com a métrica `StatusCheckFailed_System`. A recuperação baseada em ações do CloudWatch fornece granularidade de tempo de resposta de recuperação a cada minuto e notificações do Amazon Simple Notification Service (Amazon SNS) sobre as ações e os resultados da recuperação. Essas opções de configuração permitem tentativas de recuperação mais rápidas com controle mais granular sobre a resposta do evento de falha na verificação de status do sistema em comparação com a recuperação automática simplificada. Para obter mais informações sobre as opções disponíveis do CloudWatch, consulte Verificações de status para as instâncias.

No entanto, a recuperação baseada em ações do CloudWatch só pode operar se uma instância estiver no estado `running`, se não houver eventos de serviço listados no AWS Health Dashboard, e se houver capacidade disponível para o tipo de instância. Em algumas situações, como interrupções significativas, restrições de capacidade podem causar falhas nas tentativas de recuperação. Para obter mais informações, consulte the section called “Solução de problemas”.

> **Warning**
>
> Quando a AWS recupera sua instância devido a um problema subjacente de hardware ou software, esteja ciente das seguintes consequências: os dados armazenados na memória volátil (RAM) e nos volumes de armazenamento de instância serão perdidos, e o tempo de atividade do sistema operacional recomeçará do zero. Para ajudar a se proteger contra a perda de dados, recomendamos que você crie regularmente backups de dados importantes. Para obter mais informações sobre as práticas recomendadas de backup e recuperação de instâncias do EC2, consulte Práticas recomendadas do Amazon EC2.
>
> Os mecanismos automáticos de recuperação de instâncias são projetados para instâncias individuais. Para obter orientação sobre como criar um sistema resiliente, consulte Crie um sistema resiliente.

Conteúdo

- Requisitos para a habilitação da recuperação baseada em ações do CloudWatch
- Configurar a recuperação baseada em ações do CloudWatch

- Solução de problemas de falha da recuperação baseada em ações do CloudWatch

Requisitos para a habilitação da recuperação baseada em ações do CloudWatch

A recuperação baseada em ações do CloudWatch pode ser habilitada em instâncias que atendam aos critérios a seguir:

Tipos de instância

- Uso geral: A1, M3, M4, M5, M5a, M5n, M5zn, M6a, M6g, M6i, M6in, M7a, M7g, M7i, M7i-flex, M8a, M8azn, M8g, M8gb, M8gn, M8i, M8i-flex, T1, T2, T3, T3a, T4g
- Otimizadas para computação: C3, C4, C5, C5a, C5n, C6a, C6g, C6gn, C6i, C6in, C7a, C7g, C7gn, C7i, C7i-flex, C8a, C8g, C8gb, C8gn, C8i, C8i-flex
- Otimizadas para memória: R3, R4, R5, R5a, R5b, R5n, R6a, R6g, R6i, R6in, R7a, R7g, R7i, R7iz, R8a, R8g, R8gb, R8gn, R8i, R8i-flex, U-3tb1, U-6tb1, U-9tb1, U-12tb1, U-18tb1, U-24tb1, U7i-6tb, U7i-8tb, U7i-12tb, U7in-16tb, U7in-24tb, U7in-32tb, U7inh-32tb, X1, X1e, X2idn, X2iedn, X2iezn, X8g, X8i
- Computação acelerada: G3, G5g, Inf1, P3, VT1
- Computação de alta performance: Hpc6a, Hpc7a, Hpc7g, Hpc8a
- Instâncias Metal: qualquer uma das instâncias acima com o tamanho da instância metal.
- Se volumes de armazenamento de instância forem adicionados na inicialização: então, há suporte somente para os tipos de instância a seguir: M3, C3, R3, X1, X1e, X2idn, X2iedn

Locação

- Compartilhada
- Instância Dedicada

  Para obter mais informações, consulte Instâncias dedicadas do Amazon EC2.

Limitações

Não há suporte para a recuperação baseada em ações do CloudWatch em instâncias com as características a seguir:

- Locação: host dedicado. Para hosts dedicados, use a Recuperação automática de host dedicado em vez disso.
- Rede: instâncias usando um adaptador de malha elástica

- Ajuste de escala automático: instâncias que fazem parte de um grupo do Auto Scaling
- Manutenção: instâncias que estejam passando por um evento de manutenção programada no momento

Encontrar um tipo de instância compatível

É possível visualizar os tipos de instância que oferecem suporte à recuperação baseada em ação do CloudWatch.

Console

Para visualizar os tipos de instância que oferecem suporte à recuperação baseada em ações do CloudWatch

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. Na barra de filtros, adicione o filtro Suporte a recuperação automática = true. A tabela de Tipos de instâncias exibe todos os tipos de instâncias que oferecem suporte à recuperação baseada em ações do CloudWatch.
4. (Opcional) Adicione filtros para ampliar o escopo de tipos específicos de instância de interesse.

AWS CLI

Para visualizar os tipos de instância que oferecem suporte à recuperação baseada em ações do CloudWatch

Use o comando describe-instance-types com o filtro `auto-recovery-supported`.

```
aws ec2 describe-instance-types \
    --filters Name=auto-recovery-supported,Values=true \
    --query "InstanceTypes[*].[InstanceType]" \
    --output text | sort
```

PowerShell

Para visualizar os tipos de instância que oferecem suporte à recuperação baseada em ações do CloudWatch

Use o cmdlet Get-EC2InstanceType com o filtro `auto-recovery-supported`.

```
Get-EC2InstanceType `
    -Filter @{Name="auto-recovery-supported";Values="true"} | `
    Select InstanceType | Sort-Object InstanceType
```

Configurar a recuperação baseada em ações do CloudWatch

Para configurar a recuperação baseada em ações do CloudWatch para uma instância do EC2, crie um alarme do CloudWatch que monitore a métrica `StatusCheckFailed_System` para a instância especificada. Defina o alarme para ser acionado quando o valor da métrica for 1, indicando uma falha na verificação do status do sistema. Configure a ação do alarme para recuperar automaticamente a instância quando acionada.

É possível configurar o alarme usando o console do Amazon EC2 ou o console do CloudWatch. Para obter instruções, consulte Adicionar ações de recuperação a alarmes do Amazon CloudWatch neste guia do usuário, ou Adição de ações de recuperação aos alarmes do Amazon CloudWatch no Guia do usuário do Amazon CloudWatch.

Solução de problemas de falha da recuperação baseada em ações do CloudWatch

Se a recuperação baseada em ações do CloudWatch falhar ao recuperar a sua instância, considere os problemas a seguir:

- Os eventos de serviço da AWS estão em execução

  A recuperação baseada em ações do CloudWatch não opera durante eventos de serviço no AWS Health Dashboard. Talvez você não receba notificações de falha de recuperação para esses eventos. Para obter as informações mais recentes sobre a disponibilidade do serviço, consulte a página de status do serviço.
- Capacidade insuficiente

  Há temporariamente hardware de substituição insuficiente para migrar a instância.
- Número máximo de tentativas diárias de recuperação atingido

  A instância alcançou a franquia diária máxima de tentativas de recuperação. Sua instância poderá ser subsequentemente retirada se a recuperação automática falhar e se for determinado que uma degradação do hardware é a causa-raiz da falha original da verificação do status do sistema.

Se a falha na verificação de status do sistema da instância persistir apesar de várias tentativas de recuperação, consulte Solução de problemas em instâncias com falha nas verificações de status para obter mais informações.

Usar metadados da instância para gerenciar a instância do EC2

Os metadados da instância são dados sobre sua instância que é possível usar para configurar ou gerenciar a instância em execução. Os metadados de instância incluem o seguinte:

Propriedades de metadados de instância

As propriedades dos metadados de instância são divididas em categorias, por exemplo, nome do host, eventos e grupos de segurança.

Dados dinâmicos

Os dados dinâmicos são metadados que são gerados quando a instância é executada, como um documento de identidade de instância. Para obter mais informações, consulte Categorias de dados dinâmicos.

Dados do usuário

Você também pode usar os metadados de instância para acessar os dados do usuário que você especificou ao executar a instância. Por exemplo, é possível especificar parâmetros para configurar a instância ou incluir um script simples. Além disso, é possível criar AMIs genéricas e usar dados do usuário para modificar os arquivos de configuração fornecidos no momento da inicialização. Por exemplo, se você executar servidores Web para diversas pequenas empresas, todos eles poderão usar a mesma AMI genérica e recuperar o conteúdo de um bucket do Amazon S3 que você especificar nos dados do usuário na execução. Para adicionar um novo cliente a qualquer momento, crie um bucket para o cliente, adicione seu conteúdo e inicie a AMI com o nome exclusivo do bucket fornecido ao código nos dados do usuário. Se você executar várias instâncias usando a mesma chamada `RunInstances`, os dados do usuário estarão disponíveis para todas as instâncias nessa reserva. Cada instância que integra a mesma reserva tem um número de `ami-launch-index` exclusivo, permitindo que você escreva código que controle o que as instâncias farão. Por exemplo, o primeiro host pode se eleger como o nó original em um cluster. Para obter um exemplo detalhado de inicialização da AMI, consulte Identificar cada instância executada em uma única solicitação.

> **Important**
>
> Embora você só possa acessar os metadados de instância e os dados do usuário de dentro da própria instância, os dados não são protegidos por autenticação ou métodos de criptografia. Qualquer usuário que tenha acesso direto à instância e, potencialmente, qualquer software em execução na instância, pode visualizar seus metadados. Portanto, você não deve armazenar dados confidenciais, como senhas ou chaves de criptografia de longa duração, como dados de usuário.

Conteúdo

- Categorias de metadados da instância
- Categorias de dados dinâmicos
- Acessar metadados de instância para uma instância do EC2
- Configurar as opções de serviço de metadados de instância
- Executar comandos ao iniciar uma instância do EC2 com entrada de dados do usuário
- Identificar cada instância executada em uma única solicitação

Categorias de metadados da instância

As propriedades de metadados de instância são divididas em categorias. Para recuperar as propriedades dos metadados de instância, especifique a categoria na solicitação. Os metadados serão retornados na resposta.

Quando novas categorias forem lançadas, uma nova compilação de metadados de instância será criada com um novo número de versão. Na tabela a seguir, a coluna Version when category was released (Versão quando a categoria foi lançada) especifica a versão da compilação quando uma categoria de metadados de instância foi lançada. Para evitar ter que atualizar seu código sempre que o Amazon EC2 lançar uma nova compilação de metadados de instância, use `latest` em vez do número da versão em suas solicitações de metadados. Para obter mais informações, consulte Obter as versões disponíveis dos metadados da instância.

Quando o Amazon EC2 libera uma nova categoria de metadados de instância, os metadados de instância da nova categoria podem não estar disponíveis para instâncias existentes. Com instâncias basedas em Nitro, será possível recuperar metadados de instâncias somente para as categorias que

estavam disponíveis na execução. Para instâncias com o hipervisor Xen, é possível interromper e iniciar a instância para atualizar as categorias que estão disponíveis para a instância.

A tabela a seguir lista as categorias de metadados da instância. Alguns dos nomes de categoria incluem espaços reservados para dados exclusivos da instância. Por exemplo, *mac* representa o endereço MAC para a interface de rede. É necessário substituir os espaços reservados pelos valores reais ao recuperar os metadados da instância.

Categoria	Descrição	Versão quando a categoria foi lançada
`ami-id`	O ID da AMI usada para executar a instância.	1,0
`ami-launch-index`	Se você executar várias instâncias usando a mesma chamada `RunInstances` , esse valor indicará a ordem de execução de cada instância. O valor da primeira instância executada é 0. Se você executar instâncias usando uma frota do Auto Scaling ou do EC2, esse valor será sempre 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 `unknown`.	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 `ancestor-amis` .	10/10/2007

Categoria	Descrição	Versão quando a categoria foi lançada
`autoscaling/target-lifecycle-state`	Valor mostrando o estado de destino do ciclo de vida do Auto Scaling para o qual uma instância do Auto Scaling está fazendo a transição. Presente quando a instância faz a transição para um dos estados de destino do ciclo de vida após 10 de março de 2022. Valores possíveis: `Detached | InService | Standby | Terminated | Warmed:Hibernated | Warmed:Running | Warmed:Stopped | Warmed:Terminated` . Consulte Retrieve the target lifecycle state through instance metadata (Recuperar o estado de destino do ciclo de vida por meio de metadados da instância) no Guia do usuário do Amazon EC2 Auto Scaling.	15/07/2021
`block-device-mapping/ami`	O dispositivo virtual que contém o sistema de arquivos de inicialização/raiz.	15/12/2007

Categoria	Descrição	Versão quando a categoria foi lançada
`block-device-mapping/ebsN`	Os dispositivos virtuais associados a quaisquer volumes do Amazon EBS. Os volumes do Amazon EBS estarão disponíveis somente em metadados se estiverem presentes no momento da execução ou quando a instância foi iniciada pela última vez. O N indica o índice do volume do Amazon EBS (como `ebs1` ou `ebs2`).	15/12/2007
`block-device-mapping/ephemeral N`	Os dispositivos virtuais para qualquer volume de armazenamento de instâncias não NVMe. O N indica o índice de cada volume. O número dos volumes de armazenamento de instâncias no mapeamento de dispositivos de blocos pode não corresponder ao número real de volumes de armazenamento de instâncias da instância. O tipo de instância determina o número de volumes de armazenamento de instâncias que estão disponíveis para uma instância. Se o número de volumes de armazenamento de instâncias em um mapeamento de dispositivos de blocos exceder o número disponível para uma instância, os volumes de armazenamento de instâncias adicionais serão ignorados.	15/12/2007

Categoria	Descrição	Versão quando a categoria foi lançada
`block-device-mapping/root`	Os dispositivos virtuais ou as partições associadas aos dispositivos raiz, ou as partições no dispositivo virtual, onde o sistema de arquivos raiz (/ ou C:) está associado à instância específica.	15/12/2007
`block-device-mapping/swap`	Os dispositivos virtuais associados a `swap`. Nem sempre presente.	15/12/2007
`events/maintenance/history`	Se houver eventos de manutenção da instância concluídos ou cancelados, contém uma string JSON com informações sobre os eventos.	17/08/2018
`events/maintenance/scheduled`	Se houver eventos de manutenção da instância ativos, contém uma string JSON com informações sobre os eventos. Para obter mais informações, consulte Visualizar eventos programados que afetam as instâncias do Amazon EC2.	17/08/2018

Categoria	Descrição	Versão quando a categoria foi lançada
`events/recommendations/rebalance`	O tempo aproximado, em UTC, quando a notificação de recomendação de rebalance amento da instância do EC2 é emitida para a instância. Veja a seguir um exemplo dos metadados para esta categoria: `{"noticeTime": "2020-11-05T08:22:00Z"}` . Esta categoria só está disponível após a emissão da notificação. Para obter mais informações, consulte Recomendações de rebalanceamento de instâncias do EC2.	2020-10-27
`hostname`	Se a instância do EC2 estiver usando a nomenclatura baseada em IP (IPBN), esse é o hostname DNS de IPv4 privado da instância . Se a instância do EC2 estiver usando nomenclatura baseada em recursos (RBN), esse é o RBN. 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). Para obter mais informações sobre IPBN e RBN, consulte Nomes de host e domínios de instâncias do EC2.	1,0

Categoria	Descrição	Versão quando a categoria foi lançada
`iam/info`	Se houver uma função do IAM associada à instância, conterá informações sobre a última vez que o perfil de instância foi atualizado, incluindo a data LastUpdated, InstanceProfileArn e InstanceProfileId. Caso contrário, não estará presente.	12/01/2012
`iam/security-credentials/role-name`	Se houver uma função do IAM associada à instância, *`role-name`* será o nome da função, e *`role-name`* conterá as credenciais de segurança temporárias associadas à função (para obter mais informações, consulte Recuperar credenciais de segurança dos metadados da instância). Caso contrário, não estará presente.	12/01/2012
`identity-credentials/ec2/info`	Informações sobre as credenciais no `identity-credentials/ec2/security-credentials/ec2-instance` .	23/05/2018

Categoria	Descrição	Versão quando a categoria foi lançada
`identity-credentials/ec2/security-credentials/ec2-instance`	As credenciais do perfil de identidade da instância que permitem que o software na instância se identifique para a AWS para oferecer suporte a recursos como o EC2 Instance Connect e à Configuração padrão de gerenciamento de host do AWS Systems Manager. Essas credenciais não têm políticas anexadas, portanto, não têm permissões adicionais de APIs da AWS além de identificar a instância para o recurso da AWS. Para obter mais informações, consulte Perfis de identidade da instância para instâncias do Amazon EC2.	23/05/2018
`instance-action`	Notifica a instância que ela deve ser reinicializada em preparação para o empacotamento. Valores válidos: `none` | `shutdown` | `bundle-pending` .	01/09/2008
`instance-id`	O ID dessa instância.	1,0
`instance-life-cycle`	A opção de compra desta instância . Para obter mais informações, consulte Opções de faturamento e compra do Amazon EC2.	01/10/2019

Categoria	Descrição	Versão quando a categoria foi lançada
`instance-type`	O tipo da instância. Para obter mais informações, consulte Tipos de instância do Amazon EC2.	29/08/2007
`ipv6`	O endereço IPv6 da instância. Em casos em que várias interfaces de rede estão presentes, isso se refere ao dispositivo eth0 (o dispositivo cujo número de dispositivo é 0) na interface de rede e o primeiro endereço iPv6 atribuído. Se nenhum endereço IPv6 existir na interface de rede[0], esse item não será definido e gerará uma resposta HTTP 404.	2021-01-03
`kernel-id`	O ID do kernel executado com essa instância, se aplicável.	01/02/2008

Categoria	Descrição	Versão quando a categoria foi lançada
`local-hostname`	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). Se a instância do EC2 estiver usando a nomenclatura baseada em IP (IPBN), esse é o hostname DNS de IPv4 privado da instância. Se a instância do EC2 estiver usando nomenclatura baseada em recursos (RBN), esse é o RBN. Para obter mais informações sobre IPBN, RBN e nomenclatura de instâncias do EC2, consulte Nomes de host e domínios de instâncias do EC2.	19/01/2007
`local-ipv4`	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). Se esta for uma instância somente IPv6, esse item não será definido e gerará uma resposta HTTP 404.	1,0

Categoria	Descrição	Versão quando a categoria foi lançada
`mac`	O endereço Media Access Control (MAC) da instância. Em casos em que várias interfaces de rede estão presentes, isso se refere ao dispositivo eth0 (o dispositivo para o qual o número de dispositivo é 0).	01/01/2011
`metrics/vhostmd`	Não está mais disponível.	01/05/2011
`network/interfaces/macs/mac/device-number`	O número de dispositivo exclusivo associado a essa interface. O número do dispositivo correspon de ao nome do dispositivo; por exemplo, um `device-number` de 2 é para o dispositivo eth2. Essa categoria corresponde aos campos `DeviceIndex` e `device-index` que são usados pelos comandos da API do Amazon EC2 e do EC2 para a AWS CLI.	01/01/2011
`network/interfaces/macs/mac/interface-id`	O ID da interface de rede.	01/01/2011
`network/interfaces/macs/mac/ipv4-associations/public-ip`	Os endereços IPv4 privados que estão associados a cada endereço IP público e estão atribuídos a essa interface.	01/01/2011
`network/interfaces/macs/mac/ipv6s`	Os endereços IPv6 atribuídos à interface.	30/06/2016

Categoria	Descrição	Versão quando a categoria foi lançada
`network/interfaces/macs/mac/ipv6-prefix`	O prefixo IPv6 atribuído à interface de rede.	
`network/interfaces/macs/mac/local-hostname`	O nome de host DNS IPv4 privado da instância. Em casos em que várias interfaces de rede estão presentes, isso se refere ao dispositivo eth0 (o dispositivo para o qual o número de dispositivo é 0). Se esta for uma instância somente IPv6, esse será o nome baseado em recursos. Para obter mais informações sobre IPBN e RBN, consulte Nomes de host e domínios de instâncias do EC2.	19/01/2007
`network/interfaces/macs/mac/local-ipv4s`	Os endereços IPv4 privados associados à interface. Se esta for uma interface de rede somente IPv6, esse item não será definido e gerará uma resposta HTTP 404.	01/01/2011
`network/interfaces/macs/mac/mac`	O endereço MAC da instância.	01/01/2011
`network/interfaces/macs/`*`mac`*`/network-card`	O índice da placa de rede. Alguns tipos de instância suportam várias placas de rede.	01-11-2020

Categoria	Descrição	Versão quando a categoria foi lançada
`network/interfaces/macs/mac/owner-id`	O ID do proprietário da interface de rede. Em ambientes de várias interfaces, um terceiro pode anexar uma interface, como o Elastic Load Balancing . O tráfego em uma interface é sempre cobrado do proprietário da interface.	01/01/2011
`network/interfaces/macs/mac/public-hostname`	O DNS público da interface (IPv4). Essa categoria só será retornada se o atributo `enableDnsHostnames` for definido como `true`. Para acessar mais informações, consulte Atributos de DNS para sua VPC no Guia do usuário da Amazon VPC. Se a instância tiver apenas um endereço IPv6 público e nenhum endereço IPv4 público, esse item não será definido e gerará uma resposta HTTP 404.	01/01/2011
`network/interfaces/macs/mac/public-ipv4s`	Os endereços IP públicos ou os endereços IP elásticos associados à interface. Pode haver vários endereços IPv4 em uma instância.	01/01/2011
`network/interfaces/macs/mac/security-groups`	Grupos de segurança aos quais a interface de rede pertence.	01/01/2011

Categoria	Descrição	Versão quando a categoria foi lançada
`network/interfaces/macs/mac/security-group-ids`	Os IDs dos grupos de segurança aos quais a interface de rede pertence.	01/01/2011
`network/interfaces/macs/mac/subnet-id`	O ID da sub-rede na qual a interface reside.	01/01/2011
`network/interfaces/macs/mac/subnet-ipv4-cidr-block`	O bloco CIDR IPv4 da sub-rede na qual a interface reside.	01/01/2011
`network/interfaces/macs/mac/subnet-ipv6-cidr-blocks`	O bloco CIDR IPv6 da sub-rede na qual a interface reside.	30/06/2016
`network/interfaces/macs/mac/vpc-id`	O ID da VPC na qual a interface reside.	01/01/2011
`network/interfaces/macs/mac/vpc-ipv4-cidr-block`	O bloco CIDR IPv4 principal da VPC.	01/01/2011
`network/interfaces/macs/mac/vpc-ipv4-cidr-blocks`	Os blocos CIDR IPv4 da VPC.	30/06/2016
`network/interfaces/macs/mac/vpc-ipv6-cidr-blocks`	O bloco CIDR IPv6 da VPC na qual a interface reside.	30/06/2016
`placement/availability-zone`	A zona de disponibilidade na qual a instância foi executada.	01/02/2008

Categoria	Descrição	Versão quando a categoria foi lançada
`placement/availability-zone-id`	O ID estático da zona de disponibilidade em que a instância é executada. O ID da zona de disponibilidade é consistente entre as contas. No entanto, pode ser diferente da zona de disponibilidade, que pode variar de acordo com a conta.	01/10/2019
`placement/group-name`	O nome do grupo de posicionamento no qual a instância é executada.	24/08/2020
`placement/host-id`	O ID do host no qual a instância é executada. Aplicável apenas a Hosts dedicados.	24/08/2020
`placement/partition-number`	O número da partição na qual a instância é executada.	24/08/2020
`placement/region`	A região da AWS na qual a instância é executada.	24/08/2020
`product-codes`	AWS Marketplace Os códigos de produtos associados com a instância, se houver.	01/03/2007

Categoria	Descrição	Versão quando a categoria foi lançada
`public-hostname`	O DNS público da instância (IPv4). Essa categoria só será retornada se o atributo `enableDnsHostnames` for definido como `true`. Para acessar mais informações, consulte Atributos de DNS para sua VPC no Guia do usuário da Amazon VPC. Se a instância tiver apenas um endereço IPv6 público e nenhum endereço IPv4 público, esse item não será definido e gerará uma resposta HTTP 404.	19/01/2007
`public-ipv4`	O endereço IPv4 público. Se um endereço IP elástico estiver associado à instância, o valor retornado será o endereço IP elástico.	19/01/2007
`public-keys/0/openssh-key`	Chave pública. Disponível somente se fornecido no momento da execução da instância.	1,0
`ramdisk-id`	O ID do disco de RAM no momento da execução, se aplicável.	10/10/2007
`reservation-id`	O ID da reserva.	1,0

Categoria	Descrição	Versão quando a categoria foi lançada
`security-groups`	Os nomes dos grupos de segurança aplicados à instância. Após a execução, você só pode alterar os grupos de segurança das instâncias. Essas alterações estão refletidas aqui e em network/interfaces/macs/*mac*/security-groups.	1,0
`services/domain`	O domínio dos recursos da AWS para a região.	25/02/2014
`services/partition`	A partição na qual o recurso está. Para regiões padrão da AWS a partição é `aws`. Se você tem recursos em outras partições, a partição é `aws-`*partition name*. Por exemplo, a partição de recursos na região China (Pequim) é `aws-cn`.	20/10/2015
`spot/instance-action`	A ação (hibernar, interromper ou encerrar) e o tempo aproximado, em UTC, em que a ação ocorrerá. Esse item estará presente somente se a instância spot tiver sido marcada para hibernar, interromper ou encerrar. Para obter mais informações, consulte instance-action.	15/11/2016

Categoria	Descrição	Versão quando a categoria foi lançada
`spot/termination-time`	O tempo aproximado, em UTC, no qual o sistema operacional para sua instância spot receberá o sinal de desligamento. Esse item está presente e contém um valor de tempo (por exemplo, 2015-01-05T18:02:00Z) somente se a instância spot tiver sido marcada para término pelo Amazon EC2. O item hora de encerramento não está definido como uma hora se você mesmo encerrou a instância spot. Para obter mais informações, consulte termination-time.	05/11/2014
`system`	O tipo de virtualização subjacente (hipervisor) da instância.	24/09/2022
`tags/instance`	As tags de instância associadas à instância. Somente disponível se você permitir explicitamente acesso a etiquetas em metadados de instância. Para obter mais informações, consulte Habilitar o acesso a tags em metadados da instância.	23/03/2021

Categorias de dados dinâmicos

A tabela a seguir lista as categorias de dados dinâmicos.

Categoria	Descrição	Versão quando a categoria foi lançada
`fws/instance-monitoring`	O valor que mostra se o cliente habilitou o monitoramento de um minuto detalhado no CloudWatch. Valores válidos: `enabled | disabled`	04/04/2009
`instance-identity/document`	O JSON que contém os atributos da instância, como o ID da instância, o endereço IP privado, etc. Consulte Documentos de identidade da instância para instâncias do Amazon EC2.	04/04/2009
`instance-identity/pkcs7`	Usado para verificar a autenticidade e o conteúdo do documentos em relação à assinatura. Consulte Documentos de identidade da instância para instâncias do Amazon EC2.	04/04/2009
`instance-identity/signature`	Os dados que podem ser usados por outras partes para verificar sua origem e autenticidade. Consulte Documentos de identidade da instância para instâncias do Amazon EC2.	04/04/2009

Acessar metadados de instância para uma instância do EC2

É possível acessar os metadados das instâncias do EC2 na própria instância ou no console do EC2, na API, nos SDKs ou na AWS CLI. Para obter as configurações atuais de metadados de instância para uma instância no console ou na linha de comandos, consulte Consultar as opções de metadados da instância para as instâncias existentes.

É possível modificar os dados do usuário das instâncias com um volume raiz do EBS. A instância deve estar no estado interrompido. Para obter instruções para o console, consulte Atualizar os dados do usuário da instância. Para obter um exemplo do Linux que usa a AWS CLI, consulte modify-instance-attribute. Para obter um exemplo do Windows que usa o Tools for Windows PowerShell, consulte the section called “Dados do usuário e Tools for Windows PowerShell”.

> **Note**
>
> Você não será cobrado pelas solicitações HTTP usadas para recuperar os metadados da instância e os dados do usuário.

Considerações sobre o acesso aos metadados da instância

Para evitar problemas com a recuperação de metadados de instância, considere os aspectos a seguir.

Formato do comando

O formato do comando é diferente, dependendo de você usar a versão 1 do serviço de metadados de instância (IMDSv1) ou a versão 2 do serviço de metadados de instância (IMDSv2). Por padrão, você pode usar as duas versões do serviço de metadados de instância. Para exigir o uso do IMDSv2, consulte Use o serviço de metadados de instância para acessar metadados de instância.

Se o IMDSv2 for necessário, o IMDSv1 não funcionará

Se você usa o IMDSv1 e não recebe nenhuma resposta, é provável que o IMDSv2 seja necessário. Para verificar se o IMDSv2 é necessário, selecione a instância para visualizar seus detalhes. O valor de IMDSv2 indica Obrigatório (você deve usar IMDSv2) ou Opcional (é possível usar IMDSv2 ou IMDSv1).

(IMDSv2) Use /latest/api/token para recuperar o token

Emitir solicitações PUT para qualquer caminho específico da versão, por exemplo `/2021-03-23/api/token`, faz com que o serviço de metadados retorne erros 403 Forbidden. Este é o comportamento pretendido.

Versão de metadados

Para evitar ter que atualizar seu código sempre que o Amazon EC2 lançar uma nova compilação de metadados de instância, recomendamos que você use `latest` no caminho em vez do número da versão.

Suporte a IPv6

Para recuperar metadados da instância usando um endereço IPv6, certifique-se de habilitar e usar o endereço IPv6 do IMDS `[fd00:ec2::254]`, em vez do endereço IPv4

`169.254.169.254`. A instância deve ser uma instância baseada em Nitro executada em uma sub-rede com suporte para IPv6.

(Windows) Criar AMIs personalizadas usando o Sysprep do Windows.

Para garantir que o IMDS funcione quando você iniciar uma instância usando uma AMI personalizada do Windows, a AMI deverá ser uma imagem padronizada criada com a ferramenta Sysprep do Windows. Caso contrário, o IMDS não funcionará. Para obter mais informações, consulte Criar uma AMI do Amazon EC2 usando o Sysprep do Windows.

Em um ambiente de contêiner, considere reconfigurar ou aumentar o limite de saltos para 2.

Os SDKs da AWS usam chamadas IMDSv2 por padrão. Caso a chamada do IMDSv2 não receba resposta, alguns AWS SDKs tentam realizar a chamada novamente e, se ainda não tiver sucesso, usam o IMDSv1. Isso pode resultar em um atraso, especialmente em um ambiente de contêiner. Para os AWS SDKs que precisam do IMDSv2, se o limite de saltos for 1 em um ambiente de contêiner, a chamada pode não receber nenhuma resposta, pois acessar o contêiner é considerado um salto de rede adicional.

Para mitigar esses problemas em um ambiente de contêiner, considere alterar a configuração para transferir as configurações (como a Região da AWS) diretamente para o contêiner, ou considere aumentar o limite de saltos para 2. Para obter informações sobre o impacto do limite de saltos, consulte Add defense in depth against open firewalls, reverse proxies, and SSRF vulnerabilities with enhancements to the EC2 Instance Metadata Service. Para obter informações sobre como alterar o limite de saltos, consulte Alterar o limite de salto de resposta PUT.

Limite de pacotes por segundo (PPS)

Há um limite de 1.024 pacotes por segundo (PPS) para serviços que usam endereços locais do link. Esse limite inclui o agregado de consultas ao DNS do Route 53 Resolver, solicitações do Serviço de metadados de instância (IMDS), solicitações do Amazon Time Service Network Time Protocol (NTP) e solicitações do Windows Licensing Service (para instâncias baseadas no Microsoft Windows).

Considerações adicionais sobre acesso aos dados do usuário

- Os dados do usuário são tratados como dados opacos: o que você especifica é o que receberá de volta na recuperação. Cabe à instância interpretar e agir com base nos dados do usuário.
- Os dados do usuário devem ser codificados por base64. Dependendo da ferramenta ou do SDK que você está usando, a codificação base64 pode ser executada para você. Por exemplo:

  - O console do Amazon EC2 pode executar a codificação base64 para você ou aceitar a entrada codificada por base64.
  - A AWS CLI versão 2 executa a codificação base64 de parâmetros binários para você por padrão. A AWS CLI versão 1 executa a codificação base64 do `--user-data` parâmetro para você.
  - O AWS SDK para Python (Boto3) executa a codificação base64 do parâmetro `UserData` para você.
- Os dados do usuário são limitados a 16 KB, na forma bruta, antes de serem codificados em base64. O tamanho de uma string de comprimento n depois que a codificação em base64 for ceil (n/3)*4.
- Os dados do usuário devem ser decodificados em base64 quando você os recupera. Se você recuperar os dados usando o console ou os metadados da instância, eles serão decodificados automaticamente para você.
- Se você interromper uma instância, modificar os dados do usuário e iniciar a instância, os dados do usuário atualizados não serão executados automaticamente quando você iniciar a instância. Com as instâncias do Windows, é possível definir configurações para que os scripts de dados do usuário atualizados sejam executados uma vez quando você inicia a instância ou sempre que você reinicia ou inicia a instância.
- Os dados do usuário são um atributo da instância. Se você criar uma AMI a partir de uma instância, os dados do usuário da instância não serão incluídos na AMI.

Acessar os metadados de instância em uma instância do EC2

Como os metadados da instância estão disponíveis na 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, é possível acessar o endereço IP local de sua instância a partir dos metadados da instância para gerenciar uma conexão com uma aplicação externa.

Todos os itens a seguir são considerados metadados de instância, mas são acessados de maneiras diferentes. Selecione a guia que representa o tipo de metadados de instância que você quer acessar para ver mais informações.

Metadata

As propriedades de metadados de instância são divididas em categorias. Para obter uma descrição de cada categoria de metadados de instância, consult Categorias de metadados da instância.

Para acessar as propriedades de metadados da instância em uma instância em execução, obtenha os dados dos URIs IPv4 ou IPv6 a seguir. Esses endereços IP são endereços locais de link e são válidos apenas a partir da instância. Para obter mais informações, consulte Endereços locais de link.

IPv4

```
http://169.254.169.254/latest/meta-data/
```

IPv6

```
http://[fd00:ec2::254]/latest/meta-data/
```

Dynamic data

Para recuperar dados dinâmicos de uma instância em execução, use um dos seguintes URIs.

IPv4

```
http://169.254.169.254/latest/dynamic/
```

IPv6

```
http://[fd00:ec2::254]/latest/dynamic/
```

Exemplos: acessar com cURL

Os exemplos a seguir usam cURL para recuperar as categorias de identidade de instância de alto nível.

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
```

```
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/dynamic/
instance-identity/
rsa2048
pkcs7
document
signature
dsa2048
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/dynamic/instance-identity/
rsa2048
pkcs7
document
signature
dsa2048
```

Exemplos: acessar com o PowerShell

Os exemplos a seguir usam o PowerShell para recuperar as categorias de identidade de instância de alto nível.

IMDSv2

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-
seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/dynamic/instance-identity/
document
rsa2048
pkcs7
signature
```

IMDSv1

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/dynamic/instance-
identity/
document
rsa2048
pkcs7
```

```
signature
```

Para obter mais informações sobre dados dinâmicos e os exemplos de como recuperá-los, consulte Documentos de identidade da instância para instâncias do Amazon EC2.

User data

Para recuperar os dados do usuário de uma instância, use um dos URIs a seguir. Para recuperar dados do usuário usando o endereço IPv6, você deve habilitá-lo, e a instância deve ser uma instância baseada em Nitro em uma sub-rede compatível com IPv6.

IPv4

```
http://169.254.169.254/latest/user-data
```

IPv6

```
http://[fd00:ec2::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`). Se a instância não tiver dados do usuário, a solicitação retornará `404 - Not Found`.

Exemplos: acessar com cURL para recuperar texto separado por vírgula

Os exemplos a seguir usam cURL para recuperar dados do usuário que foram especificados como texto separado por vírgula.

IMDSv2

```
TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/user-data
1234,john,reboot,true | 4512,richard, | 173,,,
```

IMDSv1

```
curl http://169.254.169.254/latest/user-data
1234,john,reboot,true | 4512,richard, | 173,,,
```

Exemplos: acessar com o PowerShell para recuperar texto separado por vírgula

Os exemplos a seguir usam o PowerShell para recuperar dados do usuário que foram especificados como texto separado por vírgula.

IMDSv2

```
[string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds"
 = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method GET -Uri
 http://169.254.169.254/latest/user-data
1234,john,reboot,true | 4512,richard, | 173,,,
```

IMDSv1

```
Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = Invoke-RestMethod -Headers
 @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} `
-Method PUT -Uri http://169.254.169.254/latest/api/token} -Method GET -uri
 http://169.254.169.254/latest/user-data
1234,john,reboot,true | 4512,richard, | 173,,,
```

Exemplos: acessar com cURL para recuperar um script

Os exemplos a seguir usam cURL para recuperar dados do usuário que foram especificados como um script.

IMDSv2

```
TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-
token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/user-
data
#!/bin/bash
yum update -y
service httpd start
chkconfig httpd on
```

IMDSv1

```
curl http://169.254.169.254/latest/user-data
#!/bin/bash
yum update -y
service httpd start
```

```
chkconfig httpd on
```

Exemplos: acessar com o PowerShell para recuperar um script

Os exemplos a seguir usam o PowerShell para recuperar dados do usuário que foram especificados como um script.

IMDSv2

```
[string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds"
 = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method GET -Uri
 http://169.254.169.254/latest/user-data
<powershell>
$file = $env:SystemRoot + "\Temp\" + (Get-Date).ToString("MM-dd-yy-hh-mm")
New-Item $file -ItemType file
</powershell>
<persist>true</persist>
```

IMDSv1

```
Invoke-RestMethod -uri http://169.254.169.254/latest/user-data
<powershell>
$file = $env:SystemRoot + "\Temp\" + (Get-Date).ToString("MM-dd-yy-hh-mm")
New-Item $file -ItemType file
</powershell>
<persist>true</persist>
```

Consultar as opções de metadados da instância para as instâncias existentes

É possível consultar as opções de metadados da instância para instâncias existentes.

Console

Para consultar as opções de metadados da instância para uma instância existente

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância e confira os seguintes campos:

- IMDSv2: o valor é Obrigatório ou Opcional.
- Permitir etiquetas em metadados de instâncias: o valor é Habilitado ou Desabilitado.

4. Com sua instância selecionada, escolha Ações, Configurações da instância, Modificar opções de metadados da instância.

   A caixa de diálogo mostra se o serviço de metadados da instância está habilitado ou desabilitado para a instância selecionada.

AWS CLI

Para consultar as opções de metadados da instância para uma instância existente

Use o comando describe-instances.

```
aws ec2 describe-instances \
    --instance-id i-1234567898abcdef0 \
    --query 'Reservations[].Instances[].MetadataOptions'
```

PowerShell

Para consultar as opções de metadados da instância para uma instância existente, usando o Tools for PowerShell

Use o cmdlet Get-EC2Instance.

```
(Get-EC2Instance `
    -InstanceId i-1234567898abcdef0).Instances.MetadataOptions
```

Respostas e mensagens de erro

Todos os metadados de instância são retornados como texto (tipo de conteúdo HTTP `text/plain`).

Uma solicitação para um recurso de metadados específico retorna o valor apropriado, ou um código de erro de HTTP `404 - Not Found` se o recurso não estiver disponível.

Uma solicitação de um recurso de metadados geral (o URI termina com /) retorna uma lista de recursos disponíveis, ou um código de erro de HTTP `404 - Not Found` se não houver esse recurso. Os itens da lista estão em linhas separadas que são delimitadas por caracteres de alimentação de linha (ASCII 10).

Se uma solicitação para o IMDSv1 não receber resposta, é provável que o IMDSv2 seja necessário.

Para solicitações realizadas usando o IMDSv2, os seguintes códigos de erro HTTP podem ser retornados:

- `400 - Missing or Invalid Parameters` – a solicitação PUT não é válida.
- `401 - Unauthorized` – a solicitação GET usa um token inválido. A ação recomendada é gerar um novo token.
- `403 - Forbidden`: a solicitação não é permitida ou o IMDS está desativado.
- `404 - Not Found`: o recurso não está disponível ou não existe esse recurso.
- `503`: a solicitação não pôde ser concluída. Repetir a solicitação.

Se o IMDS retornar um erro, o curl imprimirá a mensagem de erro na saída e retornará um código de status de êxito. A mensagem de erro é armazenada na variável `TOKEN`, o que faz com que os comandos de curl que usam o token falhem. Se você chamar o curl com a opção -f, ele retornará um código de status de erro no caso de um erro no servidor de HTTP. Se você habilitar o tratamento de erros, o shell poderá capturar o erro e interromper o script.

Limitação de consulta

Controlamos a utilização de consultas ao IMDS em uma base por instância, e limitamos o número de conexões simultâneas de uma instância com o IMDS.

Se você estiver usando o IMDS para recuperar as credenciais de segurança da AWS, evite consultar as credenciais durante cada transação ou simultaneamente em um número elevado de threads ou processos, pois isso pode levar a uma limitação. Em vez disso, recomendamos que você armazene em cache as credenciais até elas começarem a se aproximar da data de expiração. Para obter mais informações sobre o perfil do IAM e as credenciais de segurança associadas ao perfil, consulte Recuperar credenciais de segurança dos metadados da instância.

Se você ficar limitado ao acessar o IMDS, tente a consulta novamente com uma estratégia de recuo exponencial.

Use o serviço de metadados de instância para acessar metadados de instância

É possível acessar metadados de instância em uma instância em execução usando um dos seguintes métodos:

- Serviço de metadados da instância versão 2 (IMDSv2): um método orientado a sessões

  Para obter exemplos, consulte Exemplos para IMDSv2.
- Serviço de metadados da instância versão 1 (IMDSv1) – um método de solicitação/resposta

  Para obter exemplos, consulte Exemplos para IMDSv1.

Por padrão, é possível usar o IMDSv1 ou o IMDSv2 ou ambos.

É possível configurar o Serviço de metadados de instância (IMDS) em cada instância de modo a aceitar somente chamadas IMDSv2, o que fará com que as chamadas IMDSv1 falhem. Para obter informações sobre como configurar sua instância para usar o IMDSv2, consulte Configurar as opções de serviço de metadados de instância.

Os cabeçalhos `PUT` ou `GET` são exclusivos do IMDSv2. Se esses cabeçalhos estiverem presentes na solicitação, a solicitação será destinada ao IMDSv2. Se nenhum cabeçalho estiver presente, presume-se que a solicitação seja destinada ao IMDSv1.

Para obter uma análise extensa do IMDSv2, consulte Adicionar defesa profunda contra firewalls abertos, proxies reversos e vulnerabilidades SSRF com melhorias no serviço de metadados da instância do EC2.

Tópicos

- Como Serviço de metadados da instância versão 2 funciona
- Usar um AWS SDK compatível
- Exemplos para IMDSv2
- Exemplos para IMDSv1

Como Serviço de metadados da instância versão 2 funciona

O IMDSv2 usa solicitações orientadas a sessão. Com solicitações orientadas a sessão, você cria um token de sessão que define a duração da sessão, que pode ser, no mínimo, um segundo e, no máximo, seis horas. Durante o período especificado, é possível usar o mesmo token de sessão para solicitações subsequentes. Depois que a duração especificada expira, crie um novo token de sessão para uso em solicitações futuras.

> **Note**
>
> Os exemplos nesta seção usam o endereço IPv4 do Serviço de metadados da instância (IMDS): `169.254.169.254`. Se você estiver recuperando metadados de instância para instâncias do EC2 pelo endereço IPv6, certifique-se de habilitar e usar o endereço IPv6: `[fd00:ec2::254]`. O endereço IPv6 do IMDS é compatível com comandos IMDSv2. O endereço IPv6 só é acessível em instâncias baseadas em Nitro em uma sub-rede compatível com IPv6 (pilha dupla ou somente IPv6).

Os exemplos apresentados a seguir usam um script de shell e um IMDSv2 para recuperar os itens de metadados da instância de nível superior. Cada exemplo:

- Cria um token de sessão que dura seis horas (21.600 segundos) usando a solicitação PUT.
- Armazena o cabeçalho do token da sessão em uma variável chamada `TOKEN` (para as instâncias do Linux) ou `token` (para as instâncias do Windows)
- Solicita os itens de metadados de nível superior usando o token

Exemplo do Linux

É possível executar dois comandos separados ou combiná-los.

Comandos separados

Primeiro, gere um token usando o comando a seguir.

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"`
```

Em seguida, use o token para gerar itens de metadados de nível superior usando o comando a seguir.

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/
```

Comandos combinados

É possível armazenar o token e combinar os comandos. O exemplo a seguir combina os dois comandos acima e armazena o cabeçalho do token de sessão em uma variável chamada TOKEN.

> **Note**
>
> Se houver um erro na criação do token, em vez de um token válido, uma mensagem de erro será armazenada na variável e o comando não funcionará.

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-
ec2-metadata-token-ttl-seconds: 21600"` \
 && curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/
```

Depois de criar um token, é possível reutilizá-lo até que ele expire. No comando de exemplo a seguir, que obtém o ID da AMI usada para executar a instância, o token armazenado em `$TOKEN` no exemplo anterior é reutilizado.

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
meta-data/ami-id
```

Exemplo do Windows

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-
seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method GET -
Uri http://169.254.169.254/latest/meta-data/
```

Depois de criar um token, é possível reutilizá-lo até que ele expire. No comando de exemplo a seguir, que obtém o ID da AMI usada para executar a instância, o token armazenado em `$token` no exemplo anterior é reutilizado.

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} `
 -Method GET -uri http://169.254.169.254/latest/meta-data/ami-id
```

Quando você usa o IMDSv2 para solicitar os metadados da instância, a solicitação deve incluir o seguinte:

1. Use uma solicitação PUT para solicitar a inicialização de uma sessão para o serviço de metadados da instância. A solicitação PUT retorna um token que deve ser incluído em solicitações GET

subsequentes para o serviço de metadados da instância. O token é exigido para acessar metadados usando o IMDSv2.

2. Inclua o token em todas as solicitações `GET` para o IMDS. Quando o uso do token está definido como `required`, as solicitações sem um token válido ou com um token expirado recebem um código de erro HTTP `401 - Unauthorized`.
   - O token é uma chave específica da instância. O token não é válido em outras instâncias do EC2 e será rejeitado se você tentar usá-lo fora da instância na qual foi gerado.
   - A solicitação `PUT` deve incluir um cabeçalho que especifique a vida útil (TTL) do token, em segundos, até um máximo de seis horas (21.600 segundos). O token representa uma sessão lógica. O TTL especifica o período de validade do token e, portanto, a duração da sessão.
   - Depois que o token expira, para continuar a acessar os metadados da instância, crie uma nova sessão usando outro `PUT`.
   - É possível optar por reutilizar um token ou criar um novo token para cada solicitação. Para um número pequeno de solicitações, pode ser mais fácil gerar e usar imediatamente um token a cada vez que você precisar acessar o IMDS. Mas, para obter eficiência, é possível especificar uma duração maior para o token e reutilizá-lo, em vez de precisar escrever uma solicitação `PUT` toda vez que precisar solicitar metadados da instância. Não há um limite prático para o número de tokens simultâneos, cada um representando sua própria sessão. No entanto, o IMDSv2 ainda é restringido pela conexão do IMDS e pelos limites de controle de utilização. Para obter mais informações, consulte Limitação de consulta.

Os métodos HTTP `GET` e `HEAD` são permitidos em solicitações de metadados de instâncias do IMDSv2. As solicitações `PUT` serão rejeitadas se contiverem um cabeçalho X-Forwarded-For.

Por padrão, a resposta a solicitações `PUT` tem um limite de saltos de resposta (vida útil) de 1 no nível de protocolo IP. Se você precisar de um limite maior de saltos, é possível ajustar o limite usando o comando modify-instance-metadata-options da AWS CLI. Por exemplo, um limite de saltos maior pode ser necessário para compatibilidade com versões anteriores de serviços de contêiner em execução na instância. Para obter mais informações, consulte Modificar as opções de metadados de instância para as instâncias existentes.

Usar um AWS SDK compatível

Para usar o IMDSv2, as instâncias do EC2 devem usar uma versão do AWS SDK compatível com o uso do IMDSv2. As versões mais recentes de todos os AWS SDKs permitem usar o IMDSv2.

> **Important**
>
> Recomendamos que você se mantenha atualizado com as versões do SDK para acompanhar os recursos, as atualizações de segurança e as dependências subjacentes mais recentes. O uso contínuo de uma versão não compatível do SDK não é recomendado e é feito a seu critério. Para obter mais informações, consulte a Política de manutenção de SDKs e ferramentas da AWS no Guia de referência de SDKs e ferramentas da AWS.

Veja a seguir as versões mínimas que são compatíveis com o uso do IMDSv2:

- AWS CLI: 1.16.289
- AWS Tools for Windows PowerShell: 4.0.1.0
- AWS SDK for .NET: 3.3.634.1
- AWS SDK para C++: 1.7.229
- AWS SDK for Go: 1.25.38
- AWS SDK para Go v2 – 0.19.0
- AWS SDK for Java: 1.11.678
- AWS SDK for Java 2.x: 2.10.21
- AWS SDK para JavaScript em Node.js – 2.722.0
- AWS SDK para Kotlin – 1.1.4
- AWS SDK for PHP: 3.147.7
- AWS SDK para Python (Botocore) – 1.13.25
- AWS SDK para Python (Boto3): 1.12.6
- AWS SDK for Ruby: 3.79.0

Exemplos para IMDSv2

Execute os exemplos a seguir na sua instância do Amazon EC2 para recuperar os metadados da instância para o IMDSv2.

Em instâncias do Windows, é possível usar o Windows PowerShell ou instalar cURL ou wget. Se você instalar uma ferramenta de terceiros em uma instância do Windows, leia a documentação que a acompanha, pois as chamadas e a saída podem ser diferentes do que é descrito aqui.

Exemplos

- Obter as versões disponíveis dos metadados da instância
- Obter itens de metadados de nível superior.
- Obtenção dos valores dos itens de metadados
- Obter a lista de chaves públicas disponíveis
- Mostrar os formatos nos quais a chave pública 0 está disponível
- Obter a chave pública 0 (no formato de chave OpenSSH)
- Obter o ID de sub-rede de uma instância
- Obter as tags de instância de uma instância de uma instância

Obter as versões disponíveis dos metadados da instância

Este exemplo obtém as versões disponíveis dos metadados da instância. Cada versão indica uma compilação de metadados de instância quando novas categorias de metadados de instância foram lançadas. As versões de compilação de metadados de instância não têm correlação com as versões 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.

cURL

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-
aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" 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
...
latest
```

PowerShell

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-
seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/
1.0
2007-01-19
2007-03-01
2007-08-29
2007-10-10
2007-12-15
2008-02-01
2008-09-01
2009-04-04
2011-01-01
2011-05-01
2012-01-12
2014-02-25
2014-11-05
2015-10-20
2016-04-19
...
latest
```

Obter itens de metadados de nível superior.

Este exemplo obtém itens de metadados de nível superior. Para obter mais informações sobre os itens na resposta, consulte Categorias de metadados da instância.

Observe que as tags serão incluídas nessa saída somente se você tiver permitido o acesso. Para obter mais informações, consulte the section called “Habilitar o acesso a tags em metadados da instância”.

cURL

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/
ami-id
ami-launch-index
ami-manifest-path
block-device-mapping/
events/
hostname
iam/
instance-action
instance-id
instance-life-cycle
instance-type
local-hostname
local-ipv4
mac
metrics/
network/
placement/
profile
public-hostname
public-ipv4
public-keys/
reservation-id
security-groups
services/
tags/
```

PowerShell

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/
ami-id
ami-launch-index
ami-manifest-path
block-device-mapping/
```

```
hostname
iam/
instance-action
instance-id
instance-life-cycle
instance-type
local-hostname
local-ipv4
mac
metrics/
network/
placement/
profile
public-hostname
public-ipv4
public-keys/
reservation-id
security-groups
services/
tags/
```

Obtenção dos valores dos itens de metadados

Esses exemplos obtêm os valores de alguns dos itens de metadados de nível superior obtidos no exemplo anterior. Essas solicitações usam o token armazenado que foi criado usando o comando no exemplo anterior. O token não pode estar expirado.

cURL

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/
latest/meta-data/ami-id
ami-0abcdef1234567890
```

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/
latest/meta-data/reservation-id
r-0efghijk987654321
```

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/
latest/meta-data/local-hostname
ip-10-251-50-12.ec2.internal
```

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/
latest/meta-data/public-hostname
ec2-203-0-113-25.compute-1.amazonaws.com
```

PowerShell

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/ami-id
ami-0abcdef1234567890
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/reservation-id
r-0efghijk987654321
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/local-hostname
ip-10-251-50-12.ec2.internal
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/public-hostname
ec2-203-0-113-25.compute-1.amazonaws.com
```

Obter a lista de chaves públicas disponíveis

Este exemplo obtém uma lista de chaves públicas disponíveis.

cURL

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-
aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-
data/public-keys/
0=my-public-key
```

PowerShell

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-
seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/public-keys/
0=my-public-key
```

Mostrar os formatos nos quais a chave pública 0 está disponível

Este exemplo mostra os formatos nos quais a chave pública 0 está disponível.

cURL

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-
aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-
data/public-keys/0/
openssh-key
```

PowerShell

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-
seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
openssh-key
```

Obter a chave pública 0 (no formato de chave OpenSSH)

Este exemplo obtém a chave pública 0 (no formato de chave OpenSSH).

cURL

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-
aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-
data/public-keys/0/openssh-key
ssh-rsa MIICiTCCAfICCQD6m7oRw0uXOjANBgkqhkiG9w0BAQUFADCBiDELMAkGA1UEBhMC
VVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6
b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAd
BgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5jb20wHhcNMTEwNDI1MjA0NTIxWhcN
```

```
MTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYD
VQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25z
b2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFt
YXpvbi5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ
21uUSfwfEvySWtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
rDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzZswY6786m86gpE
Ibb3OhjZnzcvQAaRHhdlQWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4
nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb
FFBjvSfpJIlJ00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp378OD8uTs7fLvjx79LjSTb
NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE my-public-key
```

PowerShell

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-
seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
ssh-rsa MIICiTCCAfICCQD6m7oRw0uXOjANBgkqhkiG9w0BAQUFADCBiDELMAkGA1UEBhMC
VVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6
b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAd
BgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5jb20wHhcNMTEwNDI1MjA0NTIxWhcN
MTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYD
VQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25z
b2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFt
YXpvbi5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ
21uUSfwfEvySWtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
rDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzZswY6786m86gpE
Ibb3OhjZnzcvQAaRHhdlQWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4
nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb
FFBjvSfpJIlJ00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp378OD8uTs7fLvjx79LjSTb
NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE my-public-key
```

Obter o ID de sub-rede de uma instância

Este exemplo obtém o ID de sub-rede para uma instância.

cURL

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-
aws-ec2-metadata-token-ttl-seconds: 21600"` \
```

```
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/network/interfaces/macs/02:29:96:8f:6a:2d/subnet-id
subnet-be9b61d7
```

PowerShell

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method GET -Uri http://169.254.169.254/latest/meta-data/network/interfaces/macs/02:29:96:8f:6a:2d/subnet-id
subnet-be9b61d7
```

Obter as tags de instância de uma instância de uma instância

Se o acesso às tags da instância nos metadados da instância estiver ativado, será possível obter as tags de uma instância nos metadados da instância. Para obter mais informações, consulte Recuperar tags dos metadados da instância.

Exemplos para IMDSv1

Execute os exemplos a seguir na sua instância do Amazon EC2 para recuperar os metadados da instância para o IMDSv1.

Em instâncias do Windows, é possível usar o Windows PowerShell ou instalar cURL ou wget. Se você instalar uma ferramenta de terceiros em uma instância do Windows, leia a documentação que a acompanha, pois as chamadas e a saída podem ser diferentes do que é descrito aqui.

Exemplos

- Obter as versões disponíveis dos metadados da instância
- Obter itens de metadados de nível superior.
- Obtenção dos valores dos itens de metadados
- Obter a lista de chaves públicas disponíveis
- Mostrar os formatos nos quais a chave pública 0 está disponível
- Obter a chave pública 0 (no formato de chave OpenSSH)
- Obter o ID de sub-rede de uma instância

- Obter as tags de instância de uma instância de uma instância

Obter as versões disponíveis dos metadados da instância

Este exemplo obtém as versões disponíveis dos metadados da instância. Cada versão indica uma compilação de metadados de instância quando novas categorias de metadados de instância foram lançadas. As versões de compilação de metadados de instância não têm correlação com as versões 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.

cURL

```
[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
...
latest
```

PowerShell

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/
1.0
2007-01-19
2007-03-01
2007-08-29
2007-10-10
2007-12-15
2008-02-01
```

```
2008-09-01
2009-04-04
2011-01-01
2011-05-01
2012-01-12
2014-02-25
2014-11-05
2015-10-20
2016-04-19
...
latest
```

Obter itens de metadados de nível superior.

Este exemplo obtém itens de metadados de nível superior. Para obter mais informações sobre os itens na resposta, consulte Categorias de metadados da instância.

Observe que as tags serão incluídas nessa saída somente se você tiver permitido o acesso. Para obter mais informações, consulte the section called “Habilitar o acesso a tags em metadados da instância”.

cURL

```
[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/
tags/
```

PowerShell

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/
ami-id
ami-launch-index
ami-manifest-path
block-device-mapping/
hostname
iam/
instance-action
instance-id
instance-type
local-hostname
local-ipv4
mac
metrics/
network/
placement/
profile
public-hostname
public-ipv4
public-keys/
reservation-id
security-groups
services/
tags/
```

Obtenção dos valores dos itens de metadados

Esses exemplos obtêm os valores de alguns dos itens de metadados de nível superior obtidos no exemplo anterior.

cURL

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

```
ami-0abcdef1234567890
```

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/reservation-id
r-0efghijk987654321
```

```
[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
```

PowerShell

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/ami-id
ami-0abcdef1234567890
```

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/reservation-
id
r-0efghijk987654321
```

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/local-
hostname
ip-10-251-50-12.ec2.internal
```

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/public-
hostname
ec2-203-0-113-25.compute-1.amazonaws.com
```

Obter a lista de chaves públicas disponíveis

Este exemplo obtém uma lista de chaves públicas disponíveis.

cURL

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/public-keys/
0=my-public-key
```

PowerShell

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/public-keys/ 0=my-public-key
```

Mostrar os formatos nos quais a chave pública 0 está disponível

Este exemplo mostra os formatos nos quais a chave pública 0 está disponível.

cURL

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/public-keys/0/
openssh-key
```

PowerShell

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
openssh-key
```

Obter a chave pública 0 (no formato de chave OpenSSH)

Este exemplo obtém a chave pública 0 (no formato de chave OpenSSH).

cURL

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
ssh-rsa MIICiTCCAfICCQD6m7oRw0uXOjANBgkqhkiG9w0BAQUFADCBiDELMAkGA1UEBhMC
VVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6
b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAd
BgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5jb20wHhcNMTEwNDI1MjA0NTIxWhcN
MTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYD
VQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25z
b2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFt
YXpvbi5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ
21uUSfwfEvySWtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
rDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzZswY6786m86gpE
Ibb3OhjZnzcvQAaRHhdlQWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4
nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb
FFBjvSfpJIlJ00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp378OD8uTs7fLvjx79LjSTb
```

```
NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE my-public-key
```

PowerShell

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/public-
keys/0/openssh-key
ssh-rsa MIICiTCCAfICCQD6m7oRw0uXOjANBgkqhkiG9w0BAQUFADCBiDELMAkGA1UEBhMC
VVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6
b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAd
BgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5jb20wHhcNMTEwNDI1MjA0NTIxWhcN
MTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYD
VQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25z
b2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFt
YXpvbi5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ
21uUSfwfEvySWtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
rDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzZswY6786m86gpE
Ibb3OhjZnzcvQAaRHhdlQWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4
nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb
FFBjvSfpJIlJ00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp378OD8uTs7fLvjx79LjSTb
NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE my-public-key
```

Obter o ID de sub-rede de uma instância

Este exemplo obtém o ID de sub-rede para uma instância.

cURL

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/network/interfaces/
macs/02:29:96:8f:6a:2d/subnet-id
subnet-be9b61d7
```

PowerShell

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/network/
interfaces/macs/02:29:96:8f:6a:2d/subnet-id
subnet-be9b61d7
```

Obter as tags de instância de uma instância de uma instância

Se o acesso às tags da instância nos metadados da instância estiver ativado, será possível obter as tags de uma instância nos metadados da instância. Para obter mais informações, consulte Recuperar tags dos metadados da instância.

Transição para usar o Serviço de metadados da instância versão 2

Se você deseja configurar suas instâncias para aceitar somente chamadas da versão 2 do serviço de metadados de instância (IMDSv2), recomendamos que use as ferramentas e o caminho de transição apresentados a seguir.

Tópicos

- Ferramentas para fazer a transição para o IMDSv2
- Caminho recomendado para exigir IMDSv2

Ferramentas para fazer a transição para o IMDSv2

As ferramentas a seguir podem ajudar a identificar, monitorar e gerenciar a transição do seu software do IMDSv1 para o IMDSv2. Para obter instruções sobre como usar as ferramentas, consulte Caminho recomendado para exigir IMDSv2.

AWS Software da

As versões mais recentes da AWS CLI e dos AWS SDKs são compatíveis com o IMDSv2. Para usar o IMDSv2, atualize as instâncias do EC2 para usar as versões mais recentes. Para obter as versões mínimas do AWS SDK compatíveis com IMDSv2, consulte Usar um AWS SDK compatível.

Todos os pacotes de software Amazon Linux 2 e Amazon Linux 2023 são compatíveis com o IMDSv2. O Amazon Linux 2023 desabilita o IMDSv1 por padrão.

IMDS Packet Analyzer

O IMDS Packet Analyzer é uma ferramenta de código aberto que identifica e registra as chamadas IMDSv1 durante a fase de inicialização e as operações de runtime da sua instância. Ao analisar esses registros, você pode identificar com precisão o software que faz chamadas do IMDSv1 em suas instâncias e determinar o que precisa ser atualizado para oferecer suporte ao IMDSv2 somente em suas instâncias. É possível executar o IMDS Packet Analyzer em uma

linha de comando ou instalá-lo como um serviço. Para obter mais informações, consulte AWS ImdsPacketAnalyzer no GitHub.

CloudWatch

O CloudWatch fornece as duas métricas a seguir para monitorar suas instâncias:

`MetadataNoToken` – O IMDSv2 usa sessões baseadas em token, enquanto o IMDSv1 não o faz. A métrica `MetadataNoToken` rastreia o número de chamadas para o Serviço de metadados de instância (IMDS) que estão usando o IMDSv1. Rastreando essa métrica até zero, é possível determinar se e quando todo o software foi atualizado para usar o IMDSv2.

`MetadataNoTokenRejected` – Após desabilitar o IMDSv1, é possível usar a métrica do `MetadataNoTokenRejected` para rastrear o número de vezes que uma chamada do IMDSv1 foi tentada e rejeitada. Ao rastrear essa métrica, você pode verificar se o software precisa ser atualizado para usar o IMDSv2.

Para obter mais informações, consulte Métricas de instância.

Inicie APIs

Novas instâncias: use a API RunInstances para executar novas instâncias que exijam o uso do IMDSv2. Para obter mais informações, consulte Configurar opções de metadados da instância para novas instâncias.

Instâncias existentes: use a API ModifyInstanceMetadataOptions para exigir o uso do IMDSv2 nas instâncias existentes. Para obter mais informações, consulte Modificar as opções de metadados de instância para as instâncias existentes.

Novas instâncias lançadas pelos grupos do Auto Scaling: para exigir o uso do IMDSv2 em todas as novas instâncias executadas por grupos do Auto Scaling, seus grupos do Auto Scaling podem usar um modelo de execução ou uma configuração de execução. Quando você cria um modelo de execução ou cria uma configuração de execução, é necessário configurar os parâmetros de `MetadataOptions` para exigir o uso do IMDSv2. O grupo do Auto Scaling inicia novas instâncias usando o novo modelo de execução ou configuração de execução, mas as instâncias existentes não serão afetadas.

Instâncias existentes em um grupo do Auto Scaling: use a API ModifyInstanceMetadataOptions para exigir o uso do IMDSv2 em instâncias existentes, ou encerrar as instâncias e o grupo do Auto Scaling executará novas instâncias de substituição com as configurações das opções de metadados de instância definidas no modelo ou na configuração de execução.

AMIs

As AMIs configuradas com o parâmetro `ImdsSupport` definido como `v2.0` iniciarão instâncias que exigem o IMDSv2 por padrão. O Amazon Linux 2023 está configurado com `ImdsSupport = v2.0`.

Novas AMIs: use o comando da CLI register-image para definir o parâmetro `ImdsSupport` como `v2.0` ao criar uma nova AMI.

AMIs existentes: use o comando da CLI modify-image-attribute para definir o parâmetro `ImdsSupport` como `v2.0` ao modificar uma AMI existente.

Para obter mais informações, consulte Configurar a AMI.

Políticas do IAM e SCPs

É possível usar uma política do IAM ou uma política de controle de serviços (SCP) do AWS Organizations para controlar os usuários como se segue:

- Não é possível iniciar uma instância usando a API RunInstances, a menos que a instância esteja configurada para usar o IMDSv2.
- Não é possível modificar uma instância em execução usando a API ModifyInstanceMetadataOptions para reabilitar o IMDSv1.

A política do IAM ou a SCP devem conter as seguintes chaves de condição do IAM:

- `ec2:MetadataHttpEndpoint`
- `ec2:MetadataHttpPutResponseHopLimit`
- `ec2:MetadataHttpTokens`

Se um parâmetro da chamada de API ou CLI não corresponder ao estado especificado na política que contém a chave de condição, a chamada de API ou CLI falhará com uma resposta `UnauthorizedOperation`.

Além disso, é possível escolher uma camada adicional de proteção para exigir a alteração do IMDSv1 para o IMDSv2. Na camada de gerenciamento de acesso com relação às APIs chamadas por meio de credenciais de função do EC2, é possível usar uma chave de condição nas políticas do IAM ou nas políticas de controle de serviço (SCPs) do AWS Organizations. Especificamente, usando a chave de condição da política `ec2:RoleDelivery` com um valor `2.0` nas políticas do IAM, as chamadas de API feitas com as credenciais do perfil do EC2 obtidas do IMDSv1 receberão uma resposta `UnauthorizedOperation`. A mesma coisa pode ser obtida de forma mais ampla com essa condição exigida por uma SCP. Isso garante que as credenciadas

entregues por meio do IMDSv1 não podem ser realmente usadas para chamar APIs porque todas as chamadas à API que não corresponderem à condição especificada receberão um erro `Unauthorized0peration`.

Para obter exemplos de políticas do IAM, consulte Trabalhar com metadados de instância. Para obter mais informações sobre SCPs, consulte Políticas de controle de serviço no Guia do usuário do AWS Organizations.

Políticas declarativas

Use políticas declarativas (um atributo do AWS Organizations) para definir e aplicar centralmente o IMDSv2 como a versão padrão do IMDS em toda a sua organização. Para ver um exemplo de política, consulte a guia Padrões de metadados da instância na seção Políticas declarativas suportadas no Guia do usuário do AWS Organizations.

Caminho recomendado para exigir IMDSv2

Usando as ferramentas acima, recomendamos o caminho a seguir para fazer a transição para o IMDSv2:

- Etapa 1: identificar instâncias com IMDSv2=opcional e auditar o uso do IMDSv1
- Etapa 2: atualizar o software para o IMDSv2
- Etapa 3: exigir o IMDSv2 nas instâncias
- Etapa 4: definir IMDSv2=obrigatório como padrão
- Etapa 5: impor instâncias que exijam o IMDSv2

Etapa 1: identificar instâncias com IMDSv2=opcional e auditar o uso do IMDSv1

Para avaliar seu escopo de migração do IMDSv2, identifique as instâncias configuradas para permitir o IMDSv1 ou o IMDSv2 e audite as chamadas do IMDSv1.

1. Identifique instâncias configuradas para permitir o IMDSv1 ou o IMDSv2:

   Amazon EC2 console

   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 somente as instâncias que estão configuradas para permitir IMDSv1 ou IMDSv2, adicione o filtro IMDSv2 = opcional.

4. Como alternativa, para ver se o IMDSv2 é opcional ou obrigatório para todas as instâncias, abra a janela Preferências (ícone de engrenagem), ative o IMDSv2 e escolha Confirmar. Isso adiciona a coluna IMDSv2 à tabela Instâncias.

AWS CLI

Use o comando describe-instances e filtre por `metadata-options.http-tokens = optional`, da seguinte forma:

```
aws ec2 describe-instances --filters "Name=metadata-options.http-
tokens,Values=optional" --query "Reservations[*].Instances[*].[InstanceId]" --
output text
```

2. Audite as chamadas do IMDSv1 em cada instância:

   Use a métrica `MetadataNoToken` do CloudWatch. Esta métrica mostra o número de chamadas IMDSv1 para o IMDS em suas instâncias. Para obter mais informações, consulte Métricas de instância.

3. Identifique o software em suas instâncias que fazem chamadas do IMDSv1:

   Use o IMDS Packet Analyzer de código aberto para identificar e registrar chamadas do IMDSv1 durante a fase de inicialização e as operações de runtime da sua instância. Use essas informações para identificar o software a atualizar e preparar suas instâncias para usar somente o IMDSv2. É possível executar o IMDS Packet Analyzer em uma linha de comando ou instalá-lo como um serviço.

Etapa 2: atualizar o software para o IMDSv2

Atualize todos os SDKs, as CLIs e o software que usam credenciais de função em suas instâncias para versões compatíveis com o IMDSv2. Para obter mais informações sobre como atualizar a CLI, consulte Instalação ou atualização para a versão mais recente da AWS CLI no Guia do usuário da AWS Command Line Interface.

Etapa 3: exigir o IMDSv2 nas instâncias

Depois de confirmar que não há chamadas do IMDSv1 por meio da métrica `MetadataNoToken`, configure suas instâncias existentes para exigir o IMDSv2. Além disso, configure todas as novas instâncias para exigir o IMDSv2. Em outras palavras, desative o IMDSv1 em todas as instâncias novas e existentes.

1. Configure as instâncias existentes para exigir o IMDSv2:

   Amazon EC2 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.
   4. Escolha Ações, Configurações da instância e Modificar opções de metadados da instância.
   5. Em IMDSv2, escolha Obrigatório.
   6. Escolha Salvar.

   AWS CLI

   Use o comando modify-instance-metadata-options da CLI para especificar que apenas o IMDSv2 deverá ser usado.

   > **Note**
   >
   > É possível modificar essa configuração em instâncias em execução. A alteração entra em vigor imediatamente sem a necessidade de reiniciar a instância.

   Para obter mais informações, consulte Exigir o uso de IMDSv2.

2. Monitore os problemas após a desativação do IMDSv1:

   1. Rastreie o número de vezes que uma chamada do IMDSv1 foi tentada e rejeitada com a métrica `MetadataNoTokenRejected` do CloudWatch.
   2. Se a métrica `MetadataNoTokenRejected` registrar chamadas do IMDSv1 em uma instância com problemas de software, isso indica que o software precisa ser atualizado para usar o IMDSv2.

3. Configure novas instâncias para exigir o IMDSv2:

   Amazon EC2 console

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

2. Siga estas etapas para executar uma instância.
3. Expanda Detalhes avançados e, para a versão de metadados, escolha somente V2 (token obrigatório).
4. No painel Resumo, analise a configuração da instância e selecione Iniciar instância.

   Para obter mais informações, consulte Configurar a instância na inicialização.

AWS CLI

AWS CLI: use o comando run-instances e especifique que o IMDSv2 é obrigatório.

Etapa 4: definir IMDSv2=obrigatório como padrão

Você pode definir IMDSv2=obrigatório como a configuração padrão no nível da conta ou da organização. Isso garante que todas as instâncias recém-lançadas sejam automaticamente configuradas para exigir o IMDSv2.

1. Definir padrão por conta:

   Amazon EC2 console

   1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
   2. No Painel do EC2, em Atributos da conta, escolha Proteção e segurança de dados.
   3. Em Padrões do IMDS, escolha Gerenciar.
   4. Em Serviço de metadados de instância, escolha Habilitado.
   5. Em Versão de metadados, selecione Apenas V2 (token obrigatório).
   6. Selecione Atualizar.

   AWS CLI

   Use o comando modify-instance-metadata-defaults da CLI e especifique `--http-tokens required` e `--http-put-response-hop-limit 2`.

   Para obter mais informações, consulte Definir o IMDSv2 como o padrão para a conta.
2. Como alternativa, defina o padrão no nível da organização usando uma Política Declarativa:

Use uma política declarativa para definir o padrão da organização para o IMDSv2 como obrigatório. Para ver um exemplo de política, consulte a guia Padrões de metadados da instância na seção Políticas declarativas suportadas no Guia do usuário do AWS Organizations.

Etapa 5: impor instâncias que exijam o IMDSv2

Use as seguintes chaves de condição do IAM ou do SCP para impor o uso do IMDSv2:

- `ec2:MetadataHttpTokens`
- `ec2:MetadataHttpPutResponseHopLimit`
- `ec2:MetadataHttpEndpoint`

Essas chaves de condição controlam o uso de RunInstances, da API ModifyInstanceMetadataOptions e da CLI correspondente. Se uma política for criada, e um parâmetro na chamada à API não corresponder ao estado especificado na política usando a chave de condição, a chamada à API ou à CLI falhará com uma resposta `UnauthorizedOperation`.

Para obter exemplos de políticas do IAM, consulte Trabalhar com metadados de instância.

Limitar o acesso ao serviço de metadados de instância

É possível considerar o uso de regras de firewall local para desabilitar o acesso de alguns ou de todos os processos ao serviço de metadados de instância (IMDS).

Em instâncias baseadas em Nitro, o IMDS pode ser acessado de sua própria rede quando um dispositivo de rede na VPC, como um roteador virtual, encaminha pacotes para o endereço do IMDS e a verificação de origem e de destino padrão na instância está desabilitada. Para evitar que uma fonte externa à VPC acesse o IMDS, recomendamos que você modifique a configuração do dispositivo de rede para descartar pacotes com o endereço IPv4 de destino do IMDS `169.254.169.254` e, se você tiver habilitado o endpoint IPv6, o endereço IPv6 do IMDS `[fd00:ec2::254]`.

Limitar acesso ao IMDS para instâncias do Linux

Usar iptables para limitar o acesso

O exemplo a seguir usa iptables do Linux e seu módulo `owner` para impedir que o servidor Web do Apache (com base no ID de usuário da instalação padrão do `apache`) acesse 169.254.169.254. Ele

usa uma regra de negação para rejeitar todas as solicitações de metadados de instância (IMDSv1 ou IMDSv2) de qualquer processo que execute como esse usuário.

```
$ sudo iptables --append OUTPUT --proto tcp --destination 169.254.169.254 --match owner
 --uid-owner apache --jump REJECT
```

Ou é possível considerar permitir o acesso apenas a usuários ou grupos específicos usando regras de permissão. As regras de permissão podem ser mais fáceis de gerenciar de uma perspectiva de segurança, porque elas exigem que você decida qual software precisa acessar os metadados de instância. Se você usar regras de permissão, haverá menos probabilidade de você permitir acidentalmente que o software acesse o serviço de metadados (que você não queria que tivesse acesso) se você alterar o software ou a configuração posteriormente em uma instância. Também é possível combinar o uso de grupos com regras de permissão, para que você possa adicionar ou remover usuários de um grupo com permissão sem precisar alterar a regra do firewall.

O exemplo a seguir impede o acesso ao IMDS por todos os processos, exceto os processos em execução na conta do usuário `trustworthy-user`.

```
$ sudo iptables --append OUTPUT --proto tcp --destination 169.254.169.254 --match
 owner ! --uid-owner trustworthy-user --jump REJECT
```

> **Note**
>
> - Para usar regras de firewall local, você precisa adaptar os comandos do exemplo anterior para se ajustarem a suas necessidades.
> - Por padrão, as regras de iptables não são persistentes em todas as reinicializações do sistema. Elas podem ser transformadas em persistentes usando recursos do SO não descritos aqui.
> - O módulo `owner` das iptables só corresponderá à associação do grupo se o grupo for o grupo primário de um determinado usuário local. Outros grupos não são correspondidos.

Usar PF ou IPFW para limitar o acesso

Se você estiver usando FreeBSD ou OpenBSD, poderá considerar também o uso de PF ou IPFW. Os exemplos a seguir limitam o acesso ao IMDS apenas ao usuário raiz.

PF

```
$ block out inet proto tcp from any to 169.254.169.254
```

```
$ pass out inet proto tcp from any to 169.254.169.254 user root
```

IPFW

```
$ allow tcp from any to 169.254.169.254 uid root
```

```
$ deny tcp from any to 169.254.169.254
```

> **Note**
>
> A ordem dos comandos PF e IPFW é importante. O padrão de PF e a regra correspondente mais recente, e o padrão de IPFW é a primeira regra correspondente.

Limitar acesso ao IMDS para instâncias do Windows

Usar o firewall do Windows para limitar o acesso

O seguinte PowerShell de exemplo usa o firewall interno do Windows para impedir que o servidor Web do Servidor de informações da Internet (com base no ID de usuário de sua instalação padrão de `NT AUTHORITY\IUSR`) acesse 169.254.169.254. Ele usa uma regra de negação para rejeitar todas as solicitações de metadados de instância (IMDSv1 ou IMDSv2) de qualquer processo que execute como esse usuário.

```
PS C:\> $blockPrincipal = New-Object -TypeName System.Security.Principal.NTAccount ("NT
 AUTHORITY\IUSR")
PS C:\> $BlockPrincipalSID =
 $blockPrincipal.Translate([System.Security.Principal.SecurityIdentifier]).Value
PS C:\> $BlockPrincipalSDDL = "D:(A;;CC;;;$BlockPrincipalSID)"
PS C:\> New-NetFirewallRule -DisplayName "Block metadata service from IIS" -Action
 block -Direction out `
-Protocol TCP -RemoteAddress 169.254.169.254 -LocalUser $BlockPrincipalSDDL
```

Ou é possível considerar permitir o acesso apenas a usuários ou grupos específicos usando regras de permissão. As regras de permissão podem ser mais fáceis de gerenciar de uma perspectiva

de segurança, porque elas exigem que você decida qual software precisa acessar os metadados de instância. Se você usar regras de permissão, haverá menos probabilidade de você permitir acidentalmente que o software acesse o serviço de metadados (que você não queria que tivesse acesso) se você alterar o software ou a configuração posteriormente em uma instância. Também é possível combinar o uso de grupos com regras de permissão, para que você possa adicionar ou remover usuários de um grupo com permissão sem precisar alterar a regra do firewall.

O exemplo a seguir impede o acesso aos metadados da instância por todos os processos em execução como um grupo do SO especificado na variável `blockPrincipal` (neste exemplo, o grupo `Everyone` do Windows), exceto os processos especificados em `exceptionPrincipal` (neste exemplo, um grupo chamado `trustworthy-users`). Especifique as entidades de negação e de permissão porque o Firewall do Windows, ao contrário da regra `! --uid-owner trustworthy-user` nas iptables do Linux, não fornece um mecanismo de atalho para permitir somente uma entidade específica (usuário ou grupo) negando todas as outras.

```
PS C:\> $blockPrincipal = New-Object -TypeName System.Security.Principal.NTAccount
 ("Everyone")
PS C:\> $BlockPrincipalSID =
 $blockPrincipal.Translate([System.Security.Principal.SecurityIdentifier]).Value
PS C:\> $exceptionPrincipal = New-Object -TypeName System.Security.Principal.NTAccount
 ("trustworthy-users")
PS C:\> $ExceptionPrincipalSID =
 $exceptionPrincipal.Translate([System.Security.Principal.SecurityIdentifier]).Value
PS C:\> $PrincipalSDDL = "O:LSD:(D;;CC;;;$ExceptionPrincipalSID)(A;;CC;;;
$BlockPrincipalSID)"
PS C:\> New-NetFirewallRule -DisplayName "Block metadata service for
 $($blockPrincipal.Value), exception: $($exceptionPrincipal.Value)" -Action block -
Direction out `
-Protocol TCP -RemoteAddress 169.254.169.254 -LocalUser $PrincipalSDDL
```

> **Note**
>
> Para usar regras de firewall local, você precisa adaptar os comandos do exemplo anterior para se ajustarem a suas necessidades.

Usar regras de netsh para limitar o acesso

É possível considerar o bloqueio de todos os softwares usando regras de `netsh`, mas essas regras são muito menos flexíveis.

```
C:\> netsh advfirewall firewall add rule name="Block metadata service altogether"
 dir=out protocol=TCP remoteip=169.254.169.254 action=block
```

> **Note**
>
> - Para usar regras de firewall local, você precisa adaptar os comandos do exemplo anterior para se ajustarem a suas necessidades.
> - `netsh`As regras de devem ser definidas em um prompt de comando elevado e não podem ser definidas para negar ou permitir principais específicos.

Configurar as opções de serviço de metadados de instância

O serviço de metadados de instância (IMDS) é executado localmente em cada instância do EC2. As opções de metadados de instância se referem a um conjunto de configurações que controlam a acessibilidade e o comportamento do IMDS em uma instância do EC2.

É possível configurar as seguintes opções de metadados da instância em cada instância:

Serviço de metadados de instância (IMDS): `enabled` | `disabled`

É possível habilitar ou desabilitar o IMDS em uma instância. Quando desabilitado, os metadados da instância não poderão ser acessados por você ou por nenhum outro código.

O IMDS tem dois endpoints em uma instância: IPv4 (`169.254.169.254`) e IPv6 (`[fd00:ec2::254]`). Quando você habilita o IMDS, o endpoint IPv4 é habilitado automaticamente. Se quiser habilitar o endpoint IPv6, você precisará fazer isso explicitamente.

Endpoint IPv6 do IMDS: `enabled` | `disabled`

É possível habilitar explicitamente o endpoint IPv6 do IMDS em uma instância. Quando o endpoint IPv6 estiver habilitado, o endpoint IPv4 permanecerá habilitado. O endpoint IPv6 só é compatível com instâncias baseadas em Nitro em sub-redes compatíveis com IPv6 (pilha dupla ou IPv6 apenas).

Versão de metadados: `IMDSv1 or IMDSv2 (token optional)` | `IMDSv2 only (token required)`

Ao solicitar metadados de instância, as chamadas do IMDSv2 exigem um token. As chamadas do IMDSv1 não exigem um token. É possível configurar uma instância para permitir chamadas do

IMDSv1 ou do IMDSv2 (quando um token for opcional) ou para permitir somente chamadas do IMDSv2 (quando um token for obrigatório).

Limite de salto de resposta de metadados: 1–64

O limite de saltos é o número de saltos de rede que a resposta PUT pode fazer. É possível definir o limite de saltos para um mínimo de 1 e um máximo de 64. Em um ambiente de contêiner, um limite de salto igual a 1 pode gerar problemas. Para obter informações sobre como mitigar esses problemas, consulte as informações sobre ambientes de contêiner em Considerações sobre o acesso aos metadados da instância.

Acesso a tags nos metadados da instância: `enabled` | `disabled`

É possível habilitar ou desabilitar o acesso às tags de uma instância nos metadados de uma instância. Para obter mais informações, consulte Visualizar tags para as instâncias do EC2 usando os metadados de instância.

Para ver a configuração atual de uma instância, consulte Consultar as opções de metadados da instância para as instâncias existentes.

Onde configurar as opções de metadados da instância

É possível configurar as opções de metadados da instância em diferentes níveis, da seguinte forma:

- Conta: você pode definir valores padrão para as opções de metadados da instância por conta para cada Região da AWS. Quando uma instância for executada, as opções de metadados da instância serão definidas automaticamente para os valores na conta. É possível alterar esses valores na execução. Os valores padrão por conta não afetam as instâncias existentes.
- AMI: ao registrar ou modificar uma AMI, é possível definir o parâmetro `imds-support` como `v2.0`. Quando uma instância for executada com essa AMI, a versão dos metadados da instância será definida automaticamente como IMDSv2 e o limite de saltos será definido como 2.
- Instância: você pode alterar todas as opções de metadados de uma instância na execução, substituindo as configurações padrão. Também é possível alterar as opções de metadados da instância após a execução em uma instância em execução ou parada. Observe que as alterações poderão sofrer restrições de uma política do IAM ou SCP.

Para obter mais informações, consulte Configurar opções de metadados da instância para novas instâncias e Modificar as opções de metadados de instância para as instâncias existentes.

Ordem de precedência das opções de metadados da instância

O valor de cada opção de metadados da instância é determinado na inicialização da instância, seguindo uma ordem hierárquica de precedência. A hierarquia, com a maior precedência no topo, é a seguinte:

- Precedência 1: configuração da instância na execução: é possível especificar os valores no modelo de execução ou na configuração da instância. Todos os valores especificados aqui substituirão os valores especificados por conta ou na AMI.
- Precedência 2: configurações da conta: se não houver um valor especificado na inicialização da instância, ele será determinado pelas configurações por conta (que são definidas para cada Região da AWS). As configurações por conta incluem um valor para cada opção de metadados ou não indicam nenhuma preferência.
- Precedência 3: configuração da AMI: se não houver um valor especificado na execução da instância ou por conta, ele será determinado pela configuração da AMI. Isso se aplica somente a `HttpTokens` e `HttpPutResponseHopLimit`.

Cada opção de metadados é avaliada separadamente. É possível configurar a instância com uma combinação de configuração direta da instância, padrões por conta e a configuração da AMI.

A menos que as alterações sejam restringidas por uma política do IAM ou SCP, será possível alterar o valor de qualquer opção de metadados após a execução em uma instância em execução ou parada.

Determinar valores para opções de metadados: exemplo 1

Neste exemplo, uma instância do EC2 é iniciada em uma região na qual `HttpPutResponseHopLimit` está definido como 1 para a conta. A AMI especificada tem `ImdsSupport` definido como `v2.0`. Nenhuma opção de metadados é especificada diretamente na instância na execução. A instância é executada com as seguintes opções de metadados:

```
"MetadataOptions": {
    ...
    "HttpTokens": "required",
    "HttpPutResponseHopLimit": 1,
    ...
```

Esses valores foram determinados da seguinte manneira:

- Nenhuma opção de metadados especificada na execução: durante a execução da instância, não se forneceu valores específicos para as opções de metadados nos parâmetros de execução da instância nem no modelo de execução.
- As configurações da conta têm a próxima precedência: na ausência da definição de valores específicos na execução, as configurações por conta na região terão precedência. Isso significa que os valores padrão configurados por conta serão aplicados. Nesse caso, o `HttpPutResponseHopLimit` foi definido como 1.
- As configurações da AMI têm a última precedência: na ausência de um valor específico definido na inicialização ou no nível da conta para `HttpTokens` (a versão de metadados da instância), a configuração da AMI é aplicada. Nesse caso, a configuração da AMI `ImdsSupport: v2.0` determinou que `HttpTokens` estava definido como `required`. Observe que, embora a configuração da AMI `ImdsSupport: v2.0` tenha sido projetada para definir `HttpPutResponseHopLimit: 2`, ela foi substituída pela configuração no nível da conta `HttpPutResponseHopLimit: 1`, que tem maior precedência.

Determinar valores para opções de metadados: exemplo 2

Neste exemplo, a instância do EC2 é executada com as mesmas configurações do Exemplo 1 anterior, mas com a configuração `HttpTokens` definida como `optional` diretamente na instância na execução. A instância é executada com as seguintes opções de metadados:

```
"MetadataOptions": {
    ...
    "HttpTokens": "optional",
    "HttpPutResponseHopLimit": 1,
    ...
```

O valor de `HttpPutResponseHopLimit` é determinado da mesma forma que no Exemplo 1. No entanto, o valor de `HttpTokens` é determinado da seguinte forma: as opções de metadados configuradas na instância na execução terão precedência. Embora a AMI tenha sido configurada com `ImdsSupport: v2.0` (em outras palavras, `HttpTokens` esteja definido como `required`), o valor especificado na instância na execução (`HttpTokens` definido como `optional`) teve precedência.

Definir a versão de metadados da instância

Quando uma instância é executada, o valor da versão de metadados da instância é `IMDSv1 or IMDSv2 (token optional)` ou `IMDSv2 only (token required)`.

Na execução da instância, é possível especificar manualmente o valor da versão de metadados ou usar o valor padrão. Se você especificar o valor manualmente, ele substituirá todos os padrões. Se você optar por não especificar o valor manualmente, ele será determinado por uma combinação de configurações padrão, conforme descrito na tabela a seguir.

A tabela mostra como a versão dos metadados de uma instância na execução (indicada pela Configuração resultante da instância na coluna 4) é determinada pelas configurações nos diferentes níveis de configuração. A ordem de precedência é da esquerda para a direita, com a primeira coluna tendo a maior precedência, da seguinte maneira:

- Coluna 1: Parâmetro de inicialização: representa a configuração na instância que você especifica manualmente na execução.
- Coluna 2: Padrão por conta: representa a configuração da conta.
- Coluna 3: Padrão da AMI: representa a configuração na AMI.

Parâmetro de execução	Padrão por conta	Padrão da AMI	Configuração resultante da instância
Somente V2 (requer token)	Sem preferência	Somente V2	Somente V2
Somente V2 (requer token)	Somente V2	Somente V2	Somente V2
Somente V2 (requer token)	V1 ou V2	Somente V2	Somente V2
V1 ou V2 (token opcional)	Sem preferência	Somente V2	V1 ou V2
V1 ou V2 (token opcional)	Somente V2	Somente V2	V1 ou V2
V1 ou V2 (token opcional)	V1 ou V2	Somente V2	V1 ou V2
Não definido	Sem preferência	Somente V2	Somente V2

Parâmetro de execução	Padrão por conta	Padrão da AMI	Configuração resultante da instância
Não definido	Somente V2	Somente V2	Somente V2
Não definido	V1 ou V2	Somente V2	V1 ou V2
Somente V2 (requer token)	Sem preferência	nulo	Somente V2
Somente V2 (requer token)	Somente V2	nulo	Somente V2
Somente V2 (requer token)	V1 ou V2	nulo	Somente V2
V1 ou V2 (token opcional)	Sem preferência	nulo	V1 ou V2
V1 ou V2 (token opcional)	Somente V2	nulo	V1 ou V2
V1 ou V2 (token opcional)	V1 ou V2	nulo	V1 ou V2
Não definido	Sem preferência	nulo	V1 ou V2
Não definido	Somente V2	nulo	Somente V2
Não definido	V1 ou V2	nulo	V1 ou V2

Usar chaves de condição do IAM para restringir as opções de metadados da instância

É possível usar chaves de condição do IAM em uma política do IAM ou SCP da seguinte maneira:

- Permitir que uma instância seja executada somente se ela estiver configurada para exigir o uso do IMDSv2
- Restringir o número de saltos permitidos

- Desativar o acesso aos metadados da instância

Tarefas

- Configurar opções de metadados da instância para novas instâncias
- Modificar as opções de metadados de instância para as instâncias existentes

> **Note**
>
> Proceda com cautela e conduza testes cuidadosos antes de fazer qualquer alteração. Anote o seguinte:
>
> - Se você exigir o uso do IMDSv2, as aplicações ou agentes que usam o IMDSv1 para acesso aos metadados da instância falharão.
> - Se você desativar todo o acesso aos metadados da instância, as aplicações ou agentes que contam com o acesso aos metadados da instância para funcionarem falharão.
> - Para IMDSv2, use `/latest/api/token` ao recuperar o token.
> - (Somente para o Windows) Se a versão do PowerShell for uma versão anterior à 4.0, você deverá atualizar para o Windows Management Framework 4.0 para exigir o uso do IMDSv2.

Configurar opções de metadados da instância para novas instâncias

É possível configurar as opções de metadados de instância a seguir em cada instância.

Opções

- Exigir o uso de IMDSv2
- Habilitar os endpoints IPv4 e IPv6 do IMDS
- Desativar o acesso aos metadados da instância
- Permitir acesso a tags em metadados de instância

> **Note**
>
> A configuração dessa opções é definida no nível da conta, diretamente na conta ou usando uma política declarativa. Elas devem ser configuradas em cada Região da AWS onde você

quiser configurar as opções de metadados da instância. O uso de uma política declarativa permite que você aplique as configurações em várias regiões simultaneamente, bem como em várias contas simultaneamente. Quando uma política declarativa está em uso, você não pode modificar as configurações diretamente em uma conta. Este tópico descreve como ajustar as configurações diretamente em uma conta. Para obter informações sobre o uso de políticas declarativas, consulte Políticas declarativas no Guia do usuário do AWS Organizations.

Exigir o uso de IMDSv2

É possível utilizar um dos métodos a seguir para exigir o uso do IMDSv2 nas novas instâncias.

Para exigir o IMDSv2

- Definir o IMDSv2 como o padrão para a conta
- Configurar a instância na inicialização
- Configurar a AMI
- Usar uma política do IAM

Definir o IMDSv2 como o padrão para a conta

É possível definir a versão padrão do serviço de metadados de instância (IMDS) em nível de conta para cada Região da AWS. Isso significa que, quando uma nova instância é executada, a versão dos metadados da instância é definida automaticamente para padrão do nível de conta. No entanto, você pode substituir manualmente o valor na execução ou após a execução. Para obter mais informações sobre como as configurações em nível de conta e as substituições manuais afetam uma instância, consulte Ordem de precedência das opções de metadados da instância.

Note

Definir o padrão no nível de conta não redefine as instâncias existentes. Por exemplo, se você definir o padrão no nível de conta como IMDSv2, as instâncias existentes definidas como IMDSv1 não serão afetadas. Se desejar alterar o valor nas instâncias existentes, altere manualmente o valor nas próprias instâncias.

É possível definir o padrão da conta para a versão dos metadados de instância como IMDSv2 para que todas as novas instâncias na conta sejam iniciadas com o IMDSv2 obrigatório. Nesse caso, o IMDSv1 será desabilitado. Com esse padrão da conta, quando você executar uma instância, os valores padrão da instância serão os seguintes:

- Console: a Versão de metadados estará definida como Somente V2 (requer token) e o Limite de salto de resposta de metadados como 2.
- AWS CLI: `HttpTokens` estará definido como `required` e `HttpPutResponseHopLimit` como 2.

> **Note**
>
> Antes de definir a conta padrão para IMDSv2, certifique-se de que suas instâncias não dependam do IMDSv1. Para obter mais informações, consulte Caminho recomendado para exigir IMDSv2.

Console

Para definir o IMDSv2 como padrão para a conta da região especificada

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Para alterar a Região da AWS, use o seletor de regiões no canto superior direito da página.
3. No painel de navegação, escolha EC2 Dashboard (Painel do EC2).
4. Em Account attributes (Atributos da conta), escolha Data orotection and security (Proteção e segurança de dados).
5. Ao lado de Padrões do IMDS, escolha Gerenciar.
6. Na página Gerenciar padrões do IMDS, faça o seguinte:
   a. Em Serviço de metadados de instância, escolha Habilitado.
   b. Em Metadata version (Versão de metadados), selecione V2 only (token required) (Apenas V2 [token obrigatório]).
   c. Em Limite de salto de resposta de metadados, especifique 2 se suas instâncias forem hospedar contêineres. Caso contrário, selecione Sem preferência. Quando nenhuma preferência é especificada, na inicialização, o valor padrão é 2 se a AMI tiver a configuração `ImdsSupport: v2.0`; caso contrário, o padrão é 1.

d. Selecione Atualizar.

AWS CLI

Para definir o IMDSv2 como padrão para a conta da região especificada

Use o comando modify-instance-metadata-defaults e especifique a região na qual deseja modificar as configurações do IMDS por conta. Inclua `--http-tokens` definido como `required` e `--http-put-response-hop-limit` como 2 se suas instâncias forem hospedar contêineres. Caso contrário, especifique `-1` para não indicar nenhuma preferência. Quando `-1` (nenhuma preferência) é especificada, na inicialização, o valor padrão é 2 se a AMI tiver a configuração `ImdsSupport: v2.0`; caso contrário, o padrão é 1.

```
aws ec2 modify-instance-metadata-defaults \
    --region us-east-1 \
    --http-tokens required \
    --http-put-response-hop-limit 2
```

O seguinte é um exemplo de saída.

```
{
    "Return": true
}
```

Para visualizar as configurações padrão de conta para as opções de metadados de instância para a região especificada

Use o comando get-instance-metadata-defaults e especifique a região.

```
aws ec2 get-instance-metadata-defaults --region us-east-1
```

O seguinte é um exemplo de saída.

```
{
    "AccountLevel": {
        "HttpTokens": "required",
        "HttpPutResponseHopLimit": 2
    },
```

```
    "ManagedBy": "account"
}
```

O campo `ManagedBy` indica a entidade que definiu as configurações. Neste exemplo, `account` indica que as configurações foram definidas diretamente na conta. Um valor de `declarative-policy` significaria que as configurações foram definidas por uma política declarativa. Para obter mais informações, consulte Políticas declarativas no Guia do Usuário do AWS Organizations.

Para definir o IMDSv2 como o padrão para a conta de todas as regiões

Use o comando modify-instance-metadata-defaults para modificar as configurações em nível de conta do IMDS para todas as regiões. Inclua `--http-tokens` definido como `required` e `--http-put-response-hop-limit` como 2 se suas instâncias forem hospedar contêineres. Caso contrário, especifique `-1` para não indicar nenhuma preferência. Quando `-1` (nenhuma preferência) é especificada, na inicialização, o valor padrão é 2 se a AMI tiver a configuração `ImdsSupport: v2.0`; caso contrário, o padrão é 1.

```
echo -e "Region          \t Modified" ; \
echo -e "--------------  \t ---------" ; \
for region in $(
    aws ec2 describe-regions \
        --region us-east-1 \
        --query "Regions[*].[RegionName]" \
        --output text
    );
    do (output=$(
        aws ec2 modify-instance-metadata-defaults \
            --region $region \
            --http-tokens required \
            --http-put-response-hop-limit 2 \
            --output text)
        echo -e "$region        \t $output"
    );
done
```

O seguinte é um exemplo de saída.

```
Region                  Modified
--------------          ---------
ap-south-1              True
eu-north-1              True
```

```
eu-west-3               True
...
```

Para visualizar as configurações padrão de conta para as opções de metadados de instância para todas as regiões

Use o comando get-instance-metadata-defaults.

```
echo -e "Region   \t Level          Hops    HttpTokens" ; \
echo -e "-------------- \t ------------   ----    ----------" ; \
for region in $(
    aws ec2 describe-regions \
        --region us-east-1 \
        --query "Regions[*].[RegionName]" \
        --output text
    );
    do (output=$(
        aws ec2 get-instance-metadata-defaults \
            --region $region \
            --output text)
        echo -e "$region \t $output"
    );
done
```

O seguinte é um exemplo de saída.

```
Region           Level          Hops    HttpTokens
--------------   ------------   ----    ----------
ap-south-1       ACCOUNTLEVEL   2       required
eu-north-1       ACCOUNTLEVEL   2       required
eu-west-3        ACCOUNTLEVEL   2       required
...
```

PowerShell

Para definir o IMDSv2 como padrão para a conta da região especificada

Use o comando Edit-EC2InstanceMetadataDefault e especifique a região na qual deseja modificar as configurações do IMDS por conta. Inclua `-HttpToken` definido como `required` e `-HttpPutResponseHopLimit` como 2 se suas instâncias forem hospedar contêineres. Caso contrário, especifique `-1` para não indicar nenhuma preferência. Quando `-1` (nenhuma

preferência) é especificada, na inicialização, o valor padrão é 2 se a AMI tiver a configuração `ImdsSupport: v2.0`; caso contrário, o padrão é 1.

```
Edit-EC2InstanceMetadataDefault `
    -Region us-east-1 `
    -HttpToken required `
    -HttpPutResponseHopLimit 2
```

O seguinte é um exemplo de saída.

```
True
```

Para visualizar as configurações padrão de conta para as opções de metadados de instância para a região especificada

Use o comando Get-EC2InstanceMetadataDefault e especifique a região.

```
Get-EC2InstanceMetadataDefault -Region us-east-1 | Format-List
```

O seguinte é um exemplo de saída.

```
HttpEndpoint            :
HttpPutResponseHopLimit : 2
HttpTokens              : required
InstanceMetadataTags    :
```

Para definir o IMDSv2 como o padrão para a conta de todas as regiões

Use o cmdlet Edit-EC2InstanceMetadataDefault para modificar as configurações em nível de conta do IMDS para todas as regiões. Inclua `-HttpToken` definido como `required` e `-HttpPutResponseHopLimit` como 2 se suas instâncias forem hospedar contêineres. Caso contrário, especifique `-1` para não indicar nenhuma preferência. Quando `-1` (nenhuma preferência) é especificada, na inicialização, o valor padrão é 2 se a AMI tiver a configuração `ImdsSupport: v2.0`; caso contrário, o padrão é 1.

```
(Get-EC2Region).RegionName | `
    ForEach-Object {
    [PSCustomObject]@{
        Region   = $_
        Modified = (Edit-EC2InstanceMetadataDefault `
```

```
                -Region $_ `
                -HttpToken required `
                -HttpPutResponseHopLimit 2)
    }
} | `
Format-Table Region, Modified -AutoSize
```

Saída esperada

```
Region         Modified
------         --------
ap-south-1         True
eu-north-1         True
eu-west-3          True
...
```

Para visualizar as configurações padrão de conta para as opções de metadados de instância para todas as regiões

Use o cmdlet Get-EC2InstanceMetadataDefault.

```
(Get-EC2Region).RegionName | `
    ForEach-Object {
    [PSCustomObject]@{
        Region = $_
        HttpPutResponseHopLimit = (Get-EC2InstanceMetadataDefault -Region
 $_).HttpPutResponseHopLimit
        HttpTokens              = (Get-EC2InstanceMetadataDefault -Region
 $_).HttpTokens
    }
} | `
Format-Table -AutoSize
```

Exemplo de saída

```
Region         HttpPutResponseHopLimit HttpTokens
------         ----------------------- ----------
ap-south-1                           2 required
eu-north-1                           2 required
eu-west-3                            2 required
...
```

Configurar a instância na inicialização

Quando você inicia uma instância, pode configurá-la para exigir o uso do IMDSv2, configurando os seguintes campos:

- Console do Amazon EC2: defina Metadata version (Versão de metadados) como V2 only (token required) (Apenas V2 [token obrigatório]).
- AWS CLI: defina `HttpTokens` como `required`.

Quando você especificar que o IMDSv2 é obrigatório, também deverá habilitar o endpoint do Serviço de metadados da instância (IMDS) definindo Metadados acessíveis como Habilitado (console) ou `HttpEndpoint` como `enabled` (AWS CLI).

Em um ambiente de contêiner, quando o IMDSv2 for necessário, recomendamos definir o limite de saltos como 2. Para obter mais informações, consulte Considerações sobre o acesso aos metadados da instância.

Console

Como exigir o uso do IMDSv2 em uma nova instância

- Ao executar uma nova instância no console do Amazon EC2, expanda Advanced details (Detalhes avançados) e faça o seguinte:
  - Para Metadata acessible (Metadados acessíveis), escolha Enabled (Habilitado).
  - Em Metadata version (Versão de metadados), selecione V2 only (token required) (Apenas V2 [token obrigatório]).
  - (Ambiente de contêiner) Em Limite de salto de resposta dos metadados, escolha 2.

  Para obter mais informações, consulte Detalhes avançados.

AWS CLI

Como exigir o uso do IMDSv2 em uma nova instância

O exemplo de run-instances a seguir executa uma instância `c6i.large` com `--metadata-options` definido como `HttpTokens=required`. Quando você especifica um valor para `HttpTokens`, você também deve definir `HttpEndpoint` como `enabled`. Como o cabeçalho

de token seguro é definido como `required` para solicitações de recuperação de metadados, é necessário que a instância use o IMDSv2 ao solicitar metadados da instância.

Em um ambiente de contêiner, quando o IMDSv2 for necessário, recomendamos definir o limite de saltos como 2 com `HttpPutResponseHopLimit=2`.

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --instance-type c6i.large \
 ...
    --metadata-options
 "HttpEndpoint=enabled,HttpTokens=required,HttpPutResponseHopLimit=2"
```

PowerShell

Como exigir o uso do IMDSv2 em uma nova instância

O exemplo de Cmdlet New-EC2Instance a seguir inicia uma instância `c6i.large` com `MetadataOptions_HttpEndpoint` definido como `enabled` e o parâmetro `MetadataOptions_HttpTokens` como `required`. Quando você especifica um valor para `HttpTokens`, você também deve definir `HttpEndpoint` como `enabled`. Como o cabeçalho de token seguro é definido como `required` para solicitações de recuperação de metadados, é necessário que a instância use o IMDSv2 ao solicitar metadados da instância.

```
New-EC2Instance `
    -ImageId ami-0abcdef1234567890 `
    -InstanceType c6i.large `
    -MetadataOptions_HttpEndpoint enabled `
    -MetadataOptions_HttpTokens required
```

CloudFormation

Para especificar as opções de metadados de uma instância usando CloudFormation, consulte a propriedade AWS::EC2::LaunchTemplate MetadataOptions no Guia do usuário do AWS CloudFormation.

Configurar a AMI

Ao registrar uma nova AMI ou modificar uma AMI existente, é possível definir o parâmetro `imds-support` como `v2.0`. As instâncias iniciadas a partir dessa AMI terão Metadata version (Versão

de metadados) definido como V2 only (token required) (Apenas V2 [token obrigatório]) (console) ou `HttpTokens` definido como `required` (AWS CLI). Com essas configurações, a instância exige que o IMDSv2 seja usado ao solicitar metadados da instância.

Observe que quando você configura `imds-support` como `v2.0`, as instâncias iniciadas a partir dessa AMI também têm Metadata response hop limit (Limite de saltos na resposta de metadados) (console) ou `http-put-response-hop-limit` (AWS CLI) definido como 2.

> **Important**
>
> Não use esse parâmetro, a menos que seu software AMI ofereça suporte ao IMDSv2. Após definir o valor como `v2.0`, você não poderá desfazer essa ação. A única maneira de "redefinir" sua AMI é criando uma nova AMI a partir do snapshot subjacente.

Para configurar uma nova AMI para o IMDSv2

Use um dos métodos a seguir para configurar uma nova AMI para o IMDSv2.

AWS CLI

O exemplo de register-image a seguir registra uma AMI usando o snapshot especificado de um volume raiz do EBS como `/dev/xvda` de dispositivo. Especifique `v2.0` para o parâmetro `imds-support`, de forma que instâncias iniciadas a partir dessa AMI exijam que o IMDSv2 seja usado ao solicitar metadados da instância.

```
aws ec2 register-image \
    --name my-image \
    --root-device-name /dev/xvda \
    --block-device-mappings DeviceName=/dev/
xvda,Ebs={SnapshotId=snap-0123456789example} \
    --architecture x86_64 \
    --imds-support v2.0
```

PowerShell

O exemplo de Cmdlet Register-EC2Image a seguir registra uma AMI usando o snapshot especificado de um volume raiz do EBS como dispositivo `/dev/xvda`. Especifique `v2.0` para o parâmetro `ImdsSupport`, de forma que instâncias iniciadas a partir dessa AMI exijam que o IMDSv2 seja usado ao solicitar metadados da instância.

```
Register-EC2Image `
    -Name 'my-image' `
    -RootDeviceName /dev/xvda `
    -BlockDeviceMapping  (
    New-Object `
        -TypeName Amazon.EC2.Model.BlockDeviceMapping `
        -Property @{
        DeviceName = '/dev/xvda';
        EBS        = (New-Object -TypeName Amazon.EC2.Model.EbsBlockDevice -Property
 @{
                SnapshotId = 'snap-0123456789example'
                VolumeType = 'gp3'
                } )
        }  ) `
    -Architecture X86_64 `
    -ImdsSupport v2.0
```

Para configurar uma AMI existente para o IMDSv2

Use um dos métodos a seguir para configurar uma AMI para IMDSv2 existente.

AWS CLI

O exemplo de modify-image-attribute a seguir modifica uma AMI existente para IMDSv2 somente. Especifique `v2.0` para o parâmetro `imds-support`, de forma que instâncias iniciadas a partir dessa AMI exijam que o IMDSv2 seja usado ao solicitar metadados da instância.

```
aws ec2 modify-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --imds-support v2.0
```

PowerShell

O exemplo de Cmdlet Edit-EC2ImageAttribute a seguir só modifica uma AMI existente para IMDSv2. Especifique `v2.0` para o parâmetro `imds-support`, de forma que instâncias iniciadas a partir dessa AMI exijam que o IMDSv2 seja usado ao solicitar metadados da instância.

```
Edit-EC2ImageAttribute `
    -ImageId ami-0abcdef1234567890 `
    -ImdsSupport 'v2.0'
```

Usar uma política do IAM

É possível criar uma política do IAM que impeça que os usuários iniciem novas instâncias, a menos que exijam o IMDSv2 na nova instância.

Para impor o uso do IMDSv2 em todas as novas instâncias usando uma política do IAM

Para garantir que os usuários possam executar apenas instâncias que requeiram o uso do IMDSv2 ao solicitar metadados da instância, é possível especificar que a condição para exigir o IMDSv2 deve ser atendida para que uma instância possa ser executada. Para ver um exemplo de política do IAM, consulte Trabalhar com metadados de instância.

Habilitar os endpoints IPv4 e IPv6 do IMDS

O IMDS tem dois endpoints em uma instância: IPv4 (`169.254.169.254`) e IPv6 (`[fd00:ec2::254]`). Quando você habilita o IMDS, o endpoint IPv4 é habilitado automaticamente. O endpoint IPv6 permanece desabilitado mesmo que você inicie uma instância em uma sub-rede IPv6 apenas. Para habilitar o endpoint IPv6, você precisa fazer isso explicitamente. Quando você habilita o endpoint IPv6, o endpoint IPv4 permanece habilitado.

É possível habilitar o endpoint iPv6 ao iniciar a instância ou posteriormente.

Requisitos para habilitação do endpoint iPv6

- O tipo de instância selecionado é uma instância baseada em Nitro.
- A sub-rede selecionada é compatível com IPv6, no qual a sub-rede é de pilha dupla ou IPv6 apenas.

Use um dos métodos a seguir para iniciar uma instância com o endpoint IPv6 do IMDS habilitado.

Console

Para habilitar o endpoint IPv6 do IMDS na inicialização de instância

- Inicie a instância no console do Amazon EC2 com o valor a seguir especificado em Advanced details (Detalhes avançados):
  - Para o endpoint IPv6 de metadados, escolha Habilitado.

Para obter mais informações, consulte Detalhes avançados.

AWS CLI

Para habilitar o endpoint IPv6 do IMDS na inicialização de instância

O exemplo de run-instances a seguir inicia uma instância `c6i.large` com o endpoint IPv6 habilitado para o IMDS. Para habilitar o endpoint IPv6, no parâmetro `--metadata-options`, especifique `HttpProtocolIpv6=enabled`. Quando você especifica um valor para `HttpProtocolIpv6`, você também deve definir `HttpEndpoint` como `enabled`.

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --instance-type c6i.large \
    ...
    --metadata-options "HttpEndpoint=enabled,HttpProtocolIpv6=enabled"
```

PowerShell

Para habilitar o endpoint IPv6 do IMDS na inicialização de instância

O exemplo de Cmdlet New-EC2Instance a seguir inicia uma instância `c6i.large` com o endpoint IPv6 habilitado para IMDS. Para habilitar o endpoint IPv6, especifique `MetadataOptions_HttpProtocolIpv6` como `enabled`. Quando você especifica um valor para `MetadataOptions_HttpProtocolIpv6`, você também deve definir `MetadataOptions_HttpEndpoint` como `enabled`.

```
New-EC2Instance `
    -ImageId ami-0abcdef1234567890 `
    -InstanceType c6i.large `
    -MetadataOptions_HttpEndpoint enabled `
    -MetadataOptions_HttpProtocolIpv6 enabled
```

Desativar o acesso aos metadados da instância

É possível desativar o acesso aos metadados da instância desativando o IMDS ao executar uma instância. É possível ativar o acesso mais tarde reativando o IMDS. Para obter mais informações, consulte Ativar o acesso aos metadados da instância.

Important

É possível desativar o IMDS na execução ou após a execução. Se você desativar o IMDS na execução, os seguintes problemas poderão ocorrer:

- Talvez você não tenha acesso SSH à sua instância. A `public-keys/0/openssh-key`, que é a chave SSH pública da sua instância, não estará acessível porque a chave normalmente é fornecida e acessada nos metadados da instância do EC2.
- Os dados do usuário do EC2 não estarão disponíveis e não serão executados no início da instância. Os dados do usuário do EC2 são hospedados no IMDS. Caso desative o IMDS, você desativará efetivamente o acesso aos dados do usuário.

Para acessar essa funcionalidade, você pode reativar o IMDS após a execução.

Console

Desativar o acesso aos metadados da instância na execução

- Inicie a instância no console do Amazon EC2 com o valor a seguir especificado em Advanced details (Detalhes avançados):
  - Para Metadata acessible (Metadados acessíveis), escolha Disabled (Desabilitado).

Para obter mais informações, consulte Detalhes avançados.

AWS CLI

Desativar o acesso aos metadados da instância na execução

Inicie a instância com `--metadata-options` definido como `HttpEndpoint=disabled`.

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --instance-type c6i.large \
    ...
    --metadata-options "HttpEndpoint=disabled"
```

PowerShell

Desativar o acesso aos metadados da instância na execução

O exemplo de Cmdlet New-EC2Instance a seguir inicia uma instância `MetadataOptions_HttpEndpoint` definida como `disabled`.

```
New-EC2Instance `
    -ImageId ami-0abcdef1234567890 `
    -InstanceType c6i.large `
    -MetadataOptions_HttpEndpoint disabled
```

CloudFormation

Para especificar as opções de metadados de uma instância usando CloudFormation, consulte a propriedade AWS::EC2::LaunchTemplate MetadataOptions no Guia do usuário do CloudFormation.

Permitir acesso a tags em metadados de instância

Por padrão, as tags de instância não podem ser acessadas nos metadados da instância. Para cada instância, permita o acesso explicitamente. Se o acesso for permitido, as chaves de tag da instância devem estar em conformidade com restrições de caracteres específicas, caso contrário, a execução da instância falhará. Para obter mais informações, consulte Habilitar o acesso a tags em metadados da instância.

Modificar as opções de metadados de instância para as instâncias existentes

É possível modificar as opções de metadados da instância para instâncias existentes.

Também é possível criar uma política do IAM que impeça que os usuários modifiquem as opções de metadados em instâncias existentes. Para controlar quais usuários podem modificar as opções de metadados em uma instância, especifique uma política que impeça que todos os usuários que não tenham um perfil especificado usem a API ModifyInstanceMetadataOptions. Para ver um exemplo de política do IAM, consulte Trabalhar com metadados de instância.

> **Note**
>
> Se uma política declarativa foi usada para configurar as opções de metadados da instância, você não poderá modificá-las diretamente na conta. Para obter mais informações, consulte Políticas declarativas no Guia do usuário do AWS Organizations.

Exigir o uso de IMDSv2

Use um dos seguintes métodos para modificar as opções de metadados da instância para exigir que o IMDSv2 seja usado ao solicitar metadados da instância. Quando o IMDSv2 for necessário, o IMDSv1 não poderá ser usado.

> **Note**
>
> Antes de exigir que o IMDSv2 seja usado, certifique-se de que a instância não esteja fazendo chamadas do IMDSv1. A métrica `MetadataNoToken` do CloudWatch rastreia as chamadas do IMDSv1. Quando `MetadataNoToken` registra zero uso do IMDSv1 para uma instância, a instância está pronta para exigir o IMDSv2.

Console

Para exigir o uso do IMDSv2 em 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 sua instância.
4. Escolha Ações, Configurações da instância e Modificar opções de metadados da instância.
5. Na caixa de diálogo Modificar opções de metadados da instância, faça o seguinte:
   a. Em Serviço de metadados de instância, selecione Habilitar.
   b. Em IMDSv2, escolha Obrigatório.
   c. Escolha Salvar.

AWS CLI

Para exigir o uso do IMDSv2 em uma instância existente

Use o comando modify-instance-metadata-options da CLI e defina o parâmetro `http-tokens` como `required`. Quando você especifica um valor para `http-tokens`, você também deve definir `http-endpoint` como `enabled`.

```
aws ec2 modify-instance-metadata-options \
    --instance-id i-1234567890abcdef0 \
    --http-tokens required \
    --http-endpoint enabled
```

PowerShell

Para exigir o uso do IMDSv2 em uma instância existente

Use o cmdlet Edit-EC2InstanceMetadataOption e defina o parâmetro `HttpTokens`como `required`. Quando você especifica um valor para `HttpTokens`, você também deve definir `HttpEndpoint` como `enabled`.

```
(Edit-EC2InstanceMetadataOption `
    -InstanceId i-1234567890abcdef0 `
    -HttpTokens required `
    -HttpEndpoint enabled).InstanceMetadataOptions
```

Restaurar o uso do IMDSv1

Quando o IMDSv2 for necessário, o IMDSv1 não funcionará ao solicitar metadados de instância. Quando o IMDSv2 for opcional, tanto o IMDSv2 quanto o IMDSv1 funcionarão. Portanto, para restaurar o IMDSv1, torne o IMDSv2 opcional usando um dos métodos a seguir.

Console

Para restaurar o uso do IMDSv1 em 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.
4. Escolha Ações, Configurações da instância e Modificar opções de metadados da instância.
5. Na caixa de diálogo Modificar opções de metadados da instância, faça o seguinte:

a. Em Serviço de metadados de instância, certifique-se de que a opção Habilitar esteja selecionada.

b. Em IMDSv2, escolha Opcional.

c. Escolha Salvar.

AWS CLI

Para restaurar o uso do IMDSv1 em uma instância

É possível usar o comando da CLI modify-instance-metadata-options com `http-tokens` definido como `optional` para restaurar o uso de IMDSv1 ao solicitar metadados de instância.

```
aws ec2 modify-instance-metadata-options \
    --instance-id i-1234567890abcdef0 \
    --http-tokens optional \
    --http-endpoint enabled
```

PowerShell

Para restaurar o uso do IMDSv1 em uma instância

É possível usar o cmdlet Edit-EC2InstanceMetadataOption com o `HttpTokens` configurado como `optional` para restaurar o uso do IMDSv1 ao solicitar metadados da instância.

```
(Edit-EC2InstanceMetadataOption `
    -InstanceId i-1234567890abcdef0 `
    -HttpTokens optional `
    -HttpEndpoint enabled).InstanceMetadataOptions
```

Alterar o limite de salto de resposta PUT

Para instâncias existentes, é possível alterar as configurações do limite de saltos de resposta de PUT.

Atualmente, somente os SDKs AWS CLI e AWS oferecem suporte à alteração do limite de salto de resposta PUT.

AWS CLI

Como alterar o limite de salto de resposta PUT

Use o comando modify-instance-metadata-options da CLI e defina o parâmetro `http-put-response-hop-limit` como o número de saltos necessário. No exemplo a seguir, o limite de saltos está definido como 3. Observe que ao especificar um valor para `http-put-response-hop-limit`, também é necessário definir `http-endpoint` como `enabled`.

```
aws ec2 modify-instance-metadata-options \
    --instance-id i-1234567890abcdef0 \
    --http-put-response-hop-limit 3 \
    --http-endpoint enabled
```

PowerShell

Como alterar o limite de salto de resposta PUT

Use o cmdlet Edit-EC2InstanceMetadataOption e defina o parâmetro `HttpPutResponseHopLimit`para o número necessário de saltos. No exemplo a seguir, o limite de saltos está definido como 3. Observe que ao especificar um valor para `HttpPutResponseHopLimit`, também é necessário definir `HttpEndpoint` como `enabled`.

```
(Edit-EC2InstanceMetadataOption `
    -InstanceId i-1234567890abcdef0 `
    -HttpPutResponseHopLimit 3 `
    -HttpEndpoint enabled).InstanceMetadataOptions
```

Habilitar os endpoints IPv4 e IPv6 do IMDS

O IMDS tem dois endpoints em uma instância: IPv4 (`169.254.169.254`) e IPv6 (`[fd00:ec2::254]`). Quando você habilita o IMDS, o endpoint IPv4 é habilitado automaticamente. O endpoint IPv6 permanece desabilitado mesmo que você inicie uma instância em uma sub-rede IPv6 apenas. Para habilitar o endpoint IPv6, você precisa fazer isso explicitamente. Quando você habilita o endpoint IPv6, o endpoint IPv4 permanece habilitado.

É possível habilitar o endpoint iPv6 ao iniciar a instância ou posteriormente.

Requisitos para habilitação do endpoint iPv6

- O tipo de instância selecionado é uma instância baseada em Nitro.

- A sub-rede selecionada é compatível com IPv6, no qual a sub-rede é de pilha dupla ou IPv6 apenas.

Atualmente, apenas a AWS CLI e os SDKs da AWS são compatíveis com a habilitação do endpoint IPv6 do IMDS após a inicialização da instância.

AWS CLI

Para habilitar o endpoint de IPv6 do IMDS para a instância

Use o comando modify-instance-metadata-options da CLI e defina o parâmetro `http-protocol-ipv6` como `enabled`. Observe que ao especificar um valor para `http-protocol-ipv6`, também é necessário definir `http-endpoint` como `enabled`.

```
aws ec2 modify-instance-metadata-options \
 --instance-id i-1234567890abcdef0 \
 --http-protocol-ipv6 enabled \
 --http-endpoint enabled
```

PowerShell

Para habilitar o endpoint de IPv6 do IMDS para a instância

Use o cmdlet Edit-EC2InstanceMetadataOption e defina o parâmetro `HttpProtocolIpv6`como `enabled`. Observe que ao especificar um valor para `HttpProtocolIpv6`, também é necessário definir `HttpEndpoint` como `enabled`.

```
(Edit-EC2InstanceMetadataOption `
    -InstanceId i-1234567890abcdef0 `
    -HttpProtocolIpv6 enabled `
    -HttpEndpoint enabled).InstanceMetadataOptions
```

Ativar o acesso aos metadados da instância

É possível ativar o acesso aos metadados da instância habilitando o endpoint de HTTP do IMDS na sua instância, independentemente da versão do IMDS que esteja sendo usada. É possível reverter essa alteração a qualquer momento desabilitando o endpoint de HTTP.

Use um dos métodos a seguir para ativar o acesso aos metadados da instância em uma instância.

Console

Para ativar o acesso aos metadados 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 sua instância.
4. Escolha Ações, Configurações da instância e Modificar opções de metadados da instância.
5. Na caixa de diálogo Modificar opções de metadados da instância, faça o seguinte:
   a. Em Serviço de metadados de instância, selecione Habilitar.
   b. Escolha Salvar.

AWS CLI

Para ativar o acesso aos metadados da instância

Use o comando modify-instance-metadata-options da CLI e defina o parâmetro `http-endpoint` como `enabled`.

```
aws ec2 modify-instance-metadata-options \
    --instance-id i-1234567890abcdef0 \
    --http-endpoint enabled
```

PowerShell

Para ativar o acesso aos metadados da instância

Use o cmdlet Edit-EC2InstanceMetadataOption e defina o parâmetro `HttpEndpoint`como `enabled`.

```
(Edit-EC2InstanceMetadataOption `
    -InstanceId i-1234567890abcdef0 `
    -HttpEndpoint enabled).InstanceMetadataOptions
```

Desativar o acesso aos metadados da instância

É possível desativar o acesso aos metadados da instância desabilitando o endpoint de HTTP do IMDS na sua instância, independentemente da versão do IMDS que esteja sendo usada. É possível reverte essa alteração a qualquer momento habilitando o HTTP endpoint.

Use um dos métodos a seguir para desativar o acesso aos metadados da instância em uma instância.

Console

Como desabilitar o acesso aos metadados 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 sua instância.
4. Escolha Ações, Configurações da instância e Modificar opções de metadados da instância.
5. Na caixa de diálogo Modificar opções de metadados da instância, faça o seguinte:
   a. Em Serviço de metadados de instância, desmarque Habilitar.
   b. Escolha Salvar.

AWS CLI

Como desabilitar o acesso aos metadados da instância

Use o comando modify-instance-metadata-options da CLI e defina o parâmetro `http-endpoint` como `disabled`.

```
aws ec2 modify-instance-metadata-options \
    --instance-id i-1234567890abcdef0 \
    --http-endpoint disabled
```

PowerShell

Como desabilitar o acesso aos metadados da instância

Use o cmdlet Edit-EC2InstanceMetadataOption e defina o parâmetro `HttpEndpoint`como `disabled`.

```
(Edit-EC2InstanceMetadataOption `
    -InstanceId i-1234567890abcdef0 `
    -HttpEndpoint disabled).InstanceMetadataOptions
```

Permitir acesso a tags em metadados de instância

É possível permitir o acesso a tags em metadados de instância em uma instância em execução ou parada. Para cada instância, permita o acesso explicitamente. Se o acesso for permitido, as chaves de tag da instância devem estar em conformidade com restrições de caracteres específicas, caso contrário, você receberá um erro. Para obter mais informações, consulte Habilitar o acesso a tags em metadados da instância.

Executar comandos ao iniciar uma instância do EC2 com entrada de dados do usuário

Ao iniciar uma instância do Amazon EC2, é possível transferir dados do usuário para a instância que é usada para executar tarefas de configuração automatizadas ou para executar scripts após o início da instância.

Caso tenha interesse em cenários de automação mais complexos, considere usar o CloudFormation. Para obter mais informações, consulte Implantar aplicações no Amazon EC2 com o CloudFormation no Guia do usuário do AWS CloudFormation.

Em instâncias do Linux, é possível transferir dois tipos de dados do usuário para o Amazon EC2, nomeadamente, os scripts de shell e diretivas do cloud-init. Além disso, é possível transferir esses dados para o assistente de inicialização de instâncias como texto simples, como um arquivo (isso é útil para iniciar instâncias com as ferramentas de linha de comando) ou como texto codificado em base64 (para chamadas de API).

Nas instâncias do Windows, os agentes de inicialização gerenciam os scripts de dados do usuário.

Considerações

- 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 devem ser codificados por base64. O console do Amazon EC2 pode executar a codificação base64 para você ou aceitar uma entrada codificada em base64. Se você

recuperar os dados usando o console ou os metadados da instância, eles serão decodificados automaticamente de base64para você.

- Os dados do usuário são limitados a 16 KB, na forma bruta, antes de serem codificados em base64. O tamanho de uma string de comprimento n depois que a codificação em base64 for ceil (n/3)*4.
- Os dados do usuário são um atributo da instância. Se você criar uma AMI a partir de uma instância, os dados do usuário da instância não serão incluídos na AMI.

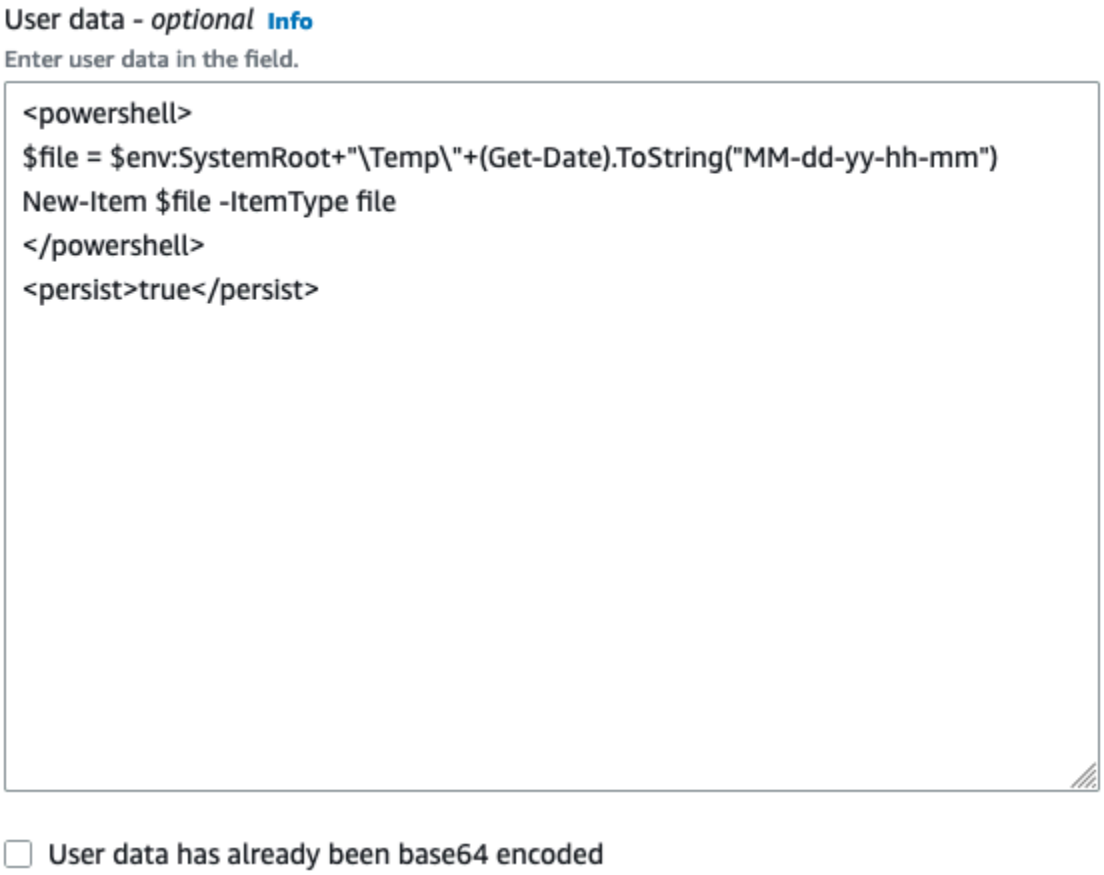
Dados do usuário no Console de gerenciamento da AWS

É possível especificar os dados do usuário da instância ao executar uma instância. Se o volume raiz da instância for um volume do EBS, também é possível parar a instância e atualizar os dados de usuário.

Especificar os dados do usuário da instância na execução com o Launch Wizard

É possível especificar dados do usuário quando executar uma instância com o Launch Wizard no console do EC2. Para especificar os dados do usuário na execução, siga o procedimento para executar uma instância. O campo User data (Dados do usuário) está localizado na seção Detalhes avançados do assistente de inicialização de instância. Insira seu script do PowerShell no campo Dados do usuário e conclua o procedimento de execução de instância.

Na seguinte captura de tela do campo Dados do usuário, o script de exemplo cria um arquivo na pasta temporária do Windows usando a data e a hora atuais no nome de arquivo. Ao incluir `<persist>true</persist>`, o script é executado sempre que você reiniciar ou iniciar a instância. Se deixar a caixa de seleção Os dados do usuário já foram codificados em base64 vazia, o console do Amazon EC2 executará a codificação em base64 para você.



Para obter mais informações, consulte Especificar os dados do usuário da instância na execução com o Launch Wizard. Para obter um exemplo do Linux que usa a AWS CLI, consulte the section called “Dados do usuário e AWS CLI”. Para obter um exemplo do Windows que usa o Tools for Windows PowerShell, consulte the section called “Dados do usuário e Tools for Windows PowerShell”.

Visualizar e atualizar os dados do usuário da instância

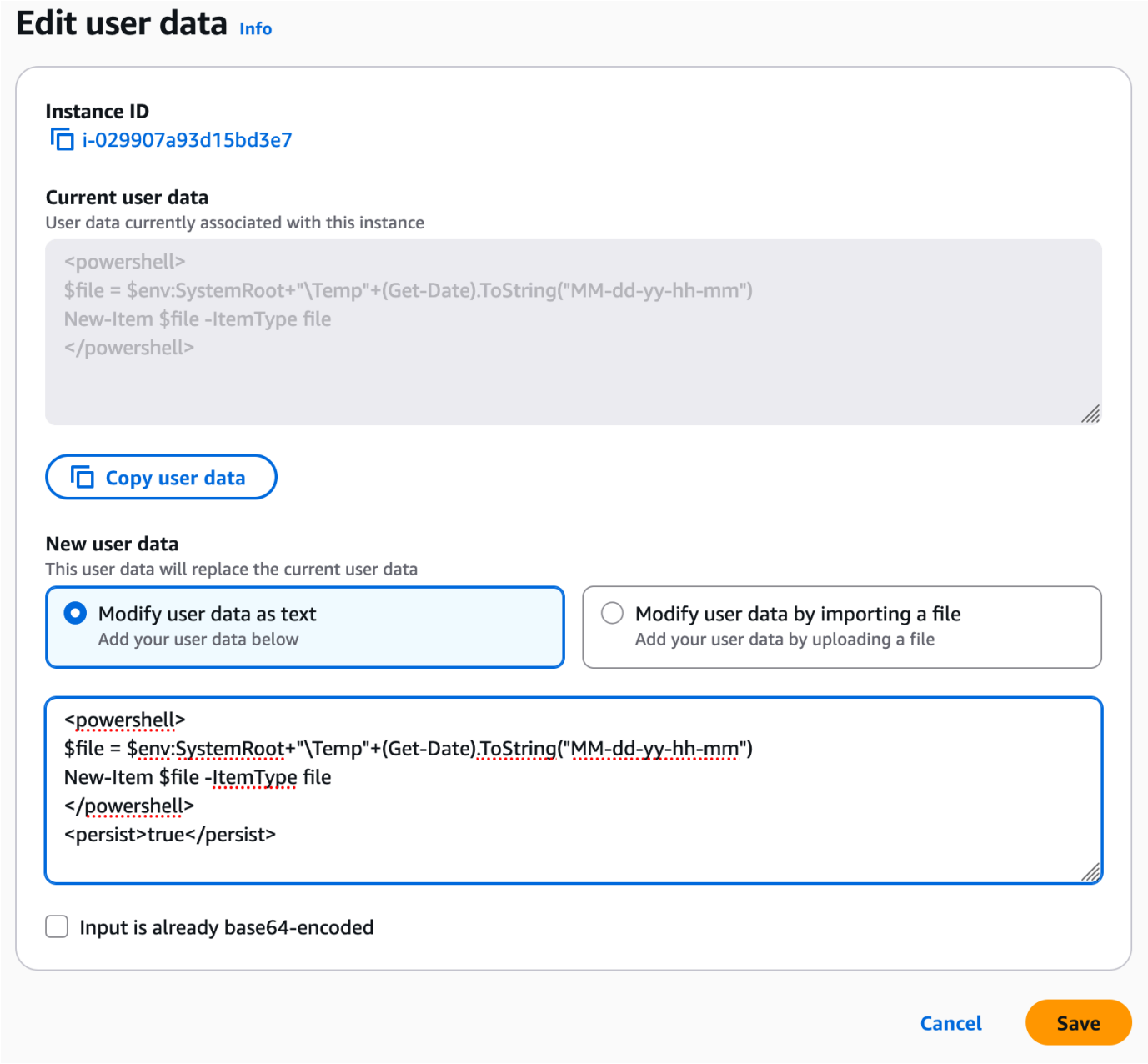
É possível visualizar dados do usuário da instância para qualquer instância e atualizar dados do usuário da instância para uma instância interrompida.

Para atualizar os dados do usuário para uma instância usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância e escolha Actions (Ações), Instance state (Estado da instância) e Stop instance (Interromper instância).

> **Warning**
>
> Quando você interrompe uma instância, os dados em todos os volumes de armazenamento de instâncias são apagados. Para manter dados longe dos volumes de armazenamento de instância, faça backup no armazenamento persistente.

4. Quando a confirmação for solicitada, escolha Parar. Pode demorar alguns minutos para que a instância pare.
5. Com a instância ainda selecionada, escolha Actions (Ações), Instance settings (Configurações de instância), Edit user data (Editar dados de usuário). Não é possível alterar os dados do usuário se a instância estiver em execução, mas é possível visualizá-la.
6. Na caixa de diálogo Edit user data (Editar dados do usuário), atualize os dados do usuário e escolha Save (Salvar). Para executar os scripts de dados do usuário sempre que você reiniciar ou iniciar a instância, adicione `<persist>true</persist>`, como mostrado no exemplo a seguir:



7. Inicie a instância. Se você habilitou a execução de dados do usuário para reinicializações ou inicializações subsequentes, os scripts de dados do usuário atualizados serão executados como parte do processo de inicialização da instância.

Como o Amazon EC2 lida com os dados dos usuários para instâncias do Linux

Os exemplos a seguir usam dados do usuário para executar comandos que configuram um servidor LAMP quando a instância é inicializada. Em cada exemplo, as seguintes tarefas são executadas:

- Os pacotes de distribuição de software são atualizados.

- O servidor Web, o php e os pacotes `mariadb` são instalados.
- O serviço `httpd` é iniciado e ativado.
- O usuário `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.

Conteúdos

- Pré-requisitos
- Dados de usuário e scripts de shell
- Atualizar os dados do usuário da instância
- Diretivas de cloud-init e dados de usuário
- Dados do usuário e AWS CLI
- Combinar scripts de shell e diretivas de cloud-init

Pré-requisitos

Para os exemplos deste tópico, suponha o seguinte:

- Sua instância tem um nome DNS público que é acessível pela Internet.
- O grupo de segurança associado à sua instância é configurado para permitir tráfego SSH (porta 22), de modo que você possa se conectar à instância para visualizar os arquivos de log de saída.
- Sua instância é inicializada usando uma AMI do Amazon Linux. Os comandos e diretivas podem não funcionar para outras distribuições Linux. Para obter mais informações sobre outras distribuições, como suporte para cloud-init, consulte a documentação específica da distribuição.

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. É necessário reservar alguns minutos extras para que as tarefas sejam concluídas antes de testar se o script de usuário foi concluído com êxito.

> **Important**
>
> Por padrão, os scripts de dados do usuário e as diretrizes cloud-init são executados somente durante o ciclo de inicialização quando você inicia uma instância pela primeira vez. É possível atualizar sua configuração para garantir que seus scripts de dados de usuário e diretrizes cloud-init sejam executados sempre que você reiniciar sua instância. Para obter mais informações, consulte How can I utilize user data to automatically run a script with every restart of my Amazon EC2 Linux instance? (Como posso utilizar os dados do usuário para executar automaticamente um script a cada reinicialização da minha instância do Linux do Amazon EC2?) na Central de Conhecimento da AWS.

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 uma introdução sobre scripts de shell, consulte o Manual de referência do Bash no site do Sistema operacional GNU.

Os scripts inseridos como dados de usuário são executados como usuário raiz,, portanto, não use o comando sudo no script. Lembre-se de que todos os arquivos que você criar serão de propriedade do usuário raiz. Caso precise que um usuário não raiz tenha acesso aos arquivos, modifique as permissões em conformidade com o script. Além disso, como o script não é executado interativamente, você não pode incluir os comandos que exigem feedback do usuário (como yum update sem o sinalizador `-y`).

Se você usar uma API da AWS, incluindo a CLI da AWS em um script de dados de usuário, deverá usar um perfil de instância ao inicializar a instância. Um perfil de instância fornece as credenciais apropriadas da AWS exigidas pelo script de dados do usuário para emitir a chamada de API. Para obter mais informações, consulte Usar perfis de instâncias no Guia do usuário do IAM. As permissões que atribui à função do IAM dependem de quais serviços você chama com a API. Para obter mais informações, consulte Funções do IAM para Amazon EC2.

O arquivo de log de saída de cloud-init captura a saída do console para facilitar a depuração de seus scripts após uma execução se a instância não se comportar da maneira desejada. Para exibir o arquivo de log, conecte-se à instância e abra `/var/log/cloud-init-output.log`.

Quando um script de dados do usuário é processado, ele é copiado para e executado a partir deste diretório `/var/lib/cloud/instances/`*`instance-id`*`/`. O script não é excluído depois de ser executado. Certifique-se de excluir os scripts de dados do usuário de `/var/lib/cloud/`

`instances/instance-id/` antes de criar uma AMI a partir da instância. Caso contrário, o script existirá nesse diretório em qualquer instância iniciada na AMI.

Atualizar os dados do usuário da instância

Para atualizar os dados do usuário da instância, primeiro é necessário interromper a instância. Se a instância estiver em execução, será possível visualizar os dados do usuário, mas não modificá-los.

> **Warning**
>
> Quando você interrompe uma instância, os dados em todos os volumes de armazenamento de instâncias são apagados. Para manter dados longe dos volumes de armazenamento de instância, faça backup no armazenamento persistente.

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 Estado da instância e Parar instância. Se a opção estiver desabilitada, significa que a instância já está interrompida ou que o volume raiz é um armazenamento de instância.
4. Quando a confirmação for solicitada, escolha Parar. Pode demorar alguns minutos para que a instância pare.
5. Com a instância ainda selecionada, escolha Actions (Ações), Instance settings (Configurações de instância), Edit user data (Editar dados de usuário).
6. Modifique os dados do usuário conforme necessário e escolha Save (Salvar).
7. Inicie a instância. Os novos dados do usuário ficam visíveis na instância depois que você a inicia. Contudo, os scripts dos dados do usuário não são executados.

Diretivas de cloud-init e dados de usuário

O pacote de cloud-init configura aspectos específicos de uma nova instância do Amazon Linux quando ela é executada. Em particular, ele configura o arquivo `.ssh/authorized_keys` para o usuário ec2 para que você possa se conectar com sua própria chave privada. Para obter mais informações sobre as tarefas de configuração que o pacote cloud-init executa para instâncias do Amazon Linux, consulte a seguinte documentação:

- Amazon Linux 2023 – Customized cloud-init
- Amazon Linux 2 – Using cloud-init on Amazon Linux 2

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 o cloud-init, consulte https://cloudinit.readthedocs.org/en/latest/index.html.

> **Important**
>
> Por padrão, os scripts de dados do usuário e as diretrizes cloud-init são executados somente durante o ciclo de inicialização quando você inicia uma instância pela primeira vez. É possível atualizar sua configuração para garantir que seus scripts de dados de usuário e diretrizes cloud-init sejam executados sempre que você reiniciar sua instância. Para obter mais informações, consulte How can I utilize user data to automatically run a script with every restart of my Amazon EC2 Linux instance? (Como posso utilizar os dados do usuário para executar automaticamente um script a cada reinicialização da minha instância Linux do Amazon EC2?) na Central de Conhecimento da AWS.

Se você adicionar essas tarefas no momento da inicialização, será necessário mais tempo para iniciar uma instância. É necessário 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 do cloud-init para uma instância do Amazon Linux

1. Siga o procedimento para iniciar uma instância. O campo User data (Dados do usuário) está localizado na seção Detalhes avançados do assistente de inicialização de instância. Insira o texto da diretiva cloud-init no campo User data (Dados do usuário) e conclua o procedimento de inicialização de instância.

   No exemplo a seguir, as diretivas criam e configuram um servidor Web no Amazon Linux. A linha `#cloud-config` na parte superior é necessária para identificar os comandos como diretrizes cloud-init.

   AL2023

   ```
   #cloud-config
   package_update: true
   ```

```
package_upgrade: all

packages:
- httpd
- mariadb105-server
- php8.1
- php8.1-mysqlnd

runcmd:
- systemctl start httpd
- 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' ]
```

AL2

```
#cloud-config
package_update: true
package_upgrade: all

packages:
- httpd
- mariadb-server

runcmd:
- [ sh, -c, "amazon-linux-extras install -y lamp-mariadb10.2-php7.2 php7.2" ]
- systemctl start httpd
- 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' ]
```

2. Reserve tempo suficiente para que a instância seja executada e execute as diretivas nos dados de usuário. Depois, verifique se as diretivas concluíram as tarefas previstas.

Para este exemplo, em um navegador da 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
```

É necessário 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 Configurar regras de grupos de segurança.

3. (Opcional) Se as diretivas não tiverem realizado as tarefas que você esperava ou se você quiser simplesmente verificar se as diretivas foram concluídas sem erros, conecte-se à instância, examine o arquivo de log de saída (`/var/log/cloud-init-output.log`) e procure mensagens de erro na saída. Para informações adicionais de depuração, é possível 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

É possível 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 Acessar metadados de instância para uma instância do EC2.

No Windows, é possível usar o AWS Tools for Windows PowerShell em vez de usar a AWS CLI. Para ter mais informações, consulte Dados do usuário e Tools for Windows PowerShell .

Exemplo: especificar dados do usuário na execução

Para especificar dados de usuário ao executar a instância, use o comando run-instances com o parâmetro `--user-data`. Com run-instances, a AWS CLI executa codificação de base64 dos dados de usuário para você.

O exemplo a seguir mostra como especificar um script como uma string na linha de comando:

```
aws ec2 run-instances --image-id ami-abcd1234 --count 1 --instance-type m3.medium \
```

```
    --key-name my-key-pair --subnet-id subnet-abcd1234 --security-group-ids sg-abcd1234
 \
    --user-data echo user data
```

O exemplo a seguir mostra como especificar um script usando um arquivo de texto. Certifique-se de usar o prefixo `file://` para especificar o arquivo.

```
aws ec2 run-instances --image-id ami-abcd1234 --count 1 --instance-type m3.medium \
    --key-name my-key-pair --subnet-id subnet-abcd1234 --security-group-ids sg-abcd1234
 \
    --user-data file://my_script.txt
```

A seguir, temos um exemplo de arquivo de texto com um script de shell.

```
#!/bin/bash
yum update -y
service httpd start
chkconfig httpd on
```

Exemplo: modificar os dados do usuário de uma instância interrompida

É possível modificar os dados de usuário de uma instância interrompida usando o comando modify-instance-attribute. Com modify-instance-attribute, a AWS CLI não executa a codificação de base64 dos dados de usuário para você.

- Em um computador Linux, use o comando base64 para codificar os dados de usuário.

  ```
  base64 my_script.txt >my_script_base64.txt
  ```

- Em um computador Windows, use o comando certutil para codificar os dados de usuário. Para poder usar esse arquivo com a AWS CLI, é necessário remover as primeiras (INICIAR CERTIFICADO) e últimas (ENCERRAR CERTIFICADO) linhas.

  ```
  certutil -encode my_script.txt my_script_base64.txt
  notepad my_script_base64.txt
  ```

Use os parâmetros `--attribute` e `--value` para usar o arquivo de texto codificado para especificar os dados de usuário. Certifique-se de usar o prefixo `file://` para especificar o arquivo.

```
aws ec2 modify-instance-attribute --instance-id i-1234567890abcdef0 --attribute
 userData --value file://my_script_base64.txt
```

Exemplo: limpar os dados do usuário de uma instância interrompida

Para excluir os dados do usuário existentes, use o comando modify-instance-attribute da seguinte maneira:

```
aws ec2 modify-instance-attribute --instance-id i-1234567890abcdef0 --user-data Value=
```

Exemplo: visualizar dados do usuário

Para recuperar os dados de usuário de uma instância, use o comando describe-instance-attribute. Com describe-instance-attribute, a AWS CLI não executa a decodificação de base64 dos dados de usuário para você.

```
aws ec2 describe-instance-attribute --instance-id i-1234567890abcdef0 --attribute
 userData
```

Esta é uma saída de exemplo com dados de usuário com codificação base64.

```
{
    "UserData": {
        "Value":
 "IyEvYmluL2Jhc2gKeXVtIHVwZGF0ZSAteQpzZXJ2aWNlIGh0dHBkIHN0YXJ0CmNoa2NvbmZpZyBodHRwZCBvbg=="
    },
    "InstanceId": "i-1234567890abcdef0"
}
```

- Em um computador Linux, use a opção `--query` para obter os dados de usuário codificados e o comando base64 para descodificá-los.

  ```
  aws ec2 describe-instance-attribute --instance-id i-1234567890abcdef0 --attribute
   userData --output text --query "UserData.Value" | base64 --decode
  ```

- Em um computador Windows, use a opção `--query` para obter os dados de usuário codificados e o comando certutil para descodificá-los. Observe que a saída codificada está armazenada em um arquivo e a saída descodificada 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
```

O seguinte é um exemplo de saída.

```
#!/bin/bash
yum update -y
service httpd start
chkconfig httpd on
```

Combinar scripts de shell e diretivas de cloud-init

Por padrão, você só pode incluir um tipo de conteúdo em dados de usuário de cada vez. Porém, você pode usar os tipos de conteúdo `text/cloud-config` e `text/x-shellscript` em um arquivo mime-multi part para incluir um script de shell e diretivas de cloud-init nos dados de usuário.

O exemplo a seguir mostra o formato mime-multi part.

```
Content-Type: multipart/mixed; boundary="//"
MIME-Version: 1.0

--//
Content-Type: text/cloud-config; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Content-Disposition: attachment; filename="cloud-config.txt"

#cloud-config
cloud-init directives

--//
Content-Type: text/x-shellscript; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Content-Disposition: attachment; filename="userdata.txt"

#!/bin/bash
shell script commands
```

```
--//--
```

Por exemplo, os seguintes dados de usuário incluem diretivas cloud-init e um script de shell bash. As diretivas cloud-init criam um arquivo (`/test-cloudinit/cloud-init.txt`) e gravam `Created by cloud-init` nesse arquivo. O script de shell bash cria um arquivo (`/test-userscript/userscript.txt`) e grava `Created by bash shell script` nesse arquivo.

```
Content-Type: multipart/mixed; boundary="//"
MIME-Version: 1.0

--//
Content-Type: text/cloud-config; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Content-Disposition: attachment; filename="cloud-config.txt"

#cloud-config
runcmd:
- [ mkdir, /test-cloudinit ]
write_files:
- path: /test-cloudinit/cloud-init.txt
content: Created by cloud-init

--//
Content-Type: text/x-shellscript; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Content-Disposition: attachment; filename="userdata.txt"

#!/bin/bash
mkdir test-userscript
touch /test-userscript/userscript.txt
echo "Created by bash shell script" >> /test-userscript/userscript.txt
--//--
```

Como o Amazon EC2 lida com os dados dos usuários para instâncias do Windows

Nas instâncias do Windows, o agente de inicialização executa as tarefas relacionadas aos dados do usuário. Para saber mais, consulte:

- EC2Launch v2
- EC2Launch

- Serviço EC2Config

Para obter exemplos de assembly de uma propriedade `UserData` em um modelo do CloudFormation, consulte Propriedade UserData codificada em Base64 e Propriedade UserData codificada em Base64 com AccessKey e SecretKey.

Para obter um exemplo de comandos de execução em uma instância dentro de um grupo do Auto Scaling que funciona com ganchos do ciclo de vida, consulte Tutorial: Configure user data to retrieve the target lifecycle state through instance metadata no Guia do usuário do Amazon EC2 Auto Scaling.

Conteúdo

- Scripts de dados do usuário
- Dados de usuários compactados
- Execução de dados do usuário
- Dados do usuário e Tools for Windows PowerShell

Scripts de dados do usuário

Para que o `EC2Config` ou o `EC2Launch` execute scripts, é necessário colocar o script em uma etiqueta especial ao adicioná-lo aos dados do usuário. A tag usada depende de os comandos serem executados em uma janela de prompt de comando (comandos de lote) ou usando o Windows PowerShell.

Se você especificar um script em lote e um script do Windows PowerShell, o script em lote é executado primeiro e o script do Windows PowerShell é executado em seguida, independentemente da ordem em que eles aparecem nos dados do usuário da instância.

Se você usar uma API da AWS, incluindo a AWS CLI, em um script de dados de usuário, deverá usar um perfil de instância ao inicializar a instância. Um perfil de instância fornece as credenciais apropriadas da AWS exigidas pelo script de dados do usuário para executar a chamada de API. Para obter mais informações, consulte Perfis de instância. As permissões que atribui à função do IAM dependem de quais serviços você chama com a API. Para obter mais informações, consulte Funções do IAM para Amazon EC2.

Tipo de script

- Sintaxe para scripts em lote

- Sintaxe para scripts do Windows PowerShell
- Sintaxe para scripts de configuração YAML
- Codificação base64

Sintaxe para scripts em lote

Especifique um script em lote usando a tag `script`. Separe os comandos usando quebras de linha, conforme mostrado no exemplo a seguir.

```
<script>
    echo Current date and time >> %SystemRoot%\Temp\test.log
    echo %DATE% %TIME% >> %SystemRoot%\Temp\test.log
</script>
```

Por padrão, os scripts de dados do usuário são executados uma vez ao inicializar a instância. Para executar os scripts de dados do usuário sempre que você reiniciar ou iniciar a instância, adicione `<persist>true</persist>` aos dados do usuário.

```
<script>
    echo Current date and time >> %SystemRoot%\Temp\test.log
    echo %DATE% %TIME% >> %SystemRoot%\Temp\test.log
</script>
<persist>true</persist>
```

Agente do EC2Launch v2

Para executar um script de dados do usuário XML como um processo separado com a tarefa executeScript do EC2Launch v2 no estágio `UserData`, adicione `<detach>true</detach>` aos dados do usuário.

> **Note**
>
> A tag detach não é compatível com agentes de inicialização anteriores.

```
<script>
    echo Current date and time >> %SystemRoot%\Temp\test.log
    echo %DATE% %TIME% >> %SystemRoot%\Temp\test.log
</script>
```

```
<detach>true</detach>
```

Sintaxe para scripts do Windows PowerShell

As AMIs do Windows da AWS incluem o AWS Tools for Windows PowerShell para que você possa especificar esses cmdlets nos dados do usuário. Se você associar uma função do IAM à sua instância, não será necessário especificar as credenciais para os cmdlets, pois os aplicações em execução na instância usam as credenciais da função para acessar os recursos da AWS (por exemplo, buckets do Amazon S3).

Especifique um script do Windows PowerShell usando a tag `<powershell>`. Separe os comandos usando quebras de linha. A tag `<powershell>` não diferencia maiúsculas de minúsculas.

Por exemplo:

```
<powershell>
    $file = $env:SystemRoot + "\Temp\" + (Get-Date).ToString("MM-dd-yy-hh-mm")
    New-Item $file -ItemType file
</powershell>
```

Por padrão, os scripts de dados do usuário são executados uma vez ao inicializar a instância. Para executar os scripts de dados do usuário sempre que você reiniciar ou iniciar a instância, adicione `<persist>true</persist>` aos dados do usuário.

```
<powershell>
    $file = $env:SystemRoot + "\Temp\" + (Get-Date).ToString("MM-dd-yy-hh-mm")
    New-Item $file -ItemType file
</powershell>
<persist>true</persist>
```

É possível especificar um ou mais argumentos do PowerShell com tag `<powershellArguments>`. Se nenhum argumento for passado, o EC2Launch e o EC2Launch v2 adicionarão o seguinte argumento por padrão: `-ExecutionPolicy Unrestricted`.

Exemplo do:

```
<powershell>
    $file = $env:SystemRoot + "\Temp" + (Get-Date).ToString("MM-dd-yy-hh-mm")
    New-Item $file -ItemType file
</powershell>
```

```
<powershellArguments>-ExecutionPolicy Unrestricted -NoProfile -NonInteractive</
powershellArguments>
```

Agente do EC2Launch v2

Para executar um script de dados do usuário XML como um processo separado com a tarefa executeScript do EC2Launch v2 no estágio `UserData`, adicione `<detach>true</detach>` aos dados do usuário.

> **Note**
>
> A tag detach não é compatível com agentes de inicialização anteriores.

```
<powershell>
    $file = $env:SystemRoot + "\Temp\" + (Get-Date).ToString("MM-dd-yy-hh-mm")
    New-Item $file -ItemType file
</powershell>
<detach>true</detach>
```

Sintaxe para scripts de configuração YAML

Se você estiver usando o EC2Launch v2 para executar scripts, poderá usar o formato YAML. Para visualizar tarefas de configuração, detalhes e exemplos do EC2Launch v2, consulte Configuração de tarefas do EC2Launch v2.

Especifique um script YAML com a tarefa `executeScript`.

Exemplo de sintaxe do YAML para executar um script do PowerShell

```
version: 1.0
tasks:
- task: executeScript
  inputs:
  - frequency: always
    type: powershell
    runAs: localSystem
    content: |-
      $file = $env:SystemRoot + "\Temp\" + (Get-Date).ToString("MM-dd-yy-hh-mm")
      New-Item $file -ItemType file
```

Exemplo de sintaxe do YAML para executar um script em lote

```
version: 1.1
tasks:
- task: executeScript
  inputs:
  - frequency: always
    type: batch
    runAs: localSystem
    content: |-
      echo Current date and time >> %SystemRoot%\Temp\test.log
      echo %DATE% %TIME% >> %SystemRoot%\Temp\test.log
```

Codificação base64

Se você estiver usando a API do Amazon EC2 ou uma ferramenta que não execute codificação base64 dos dados do usuário, codifique você mesmo os dados do usuário. Caso contrário, será registrado um erro sobre não ser possível encontrar as tags `script` ou `powershell` para executar. A seguir está um exemplo que codifica usando o Windows PowerShell.

```
$UserData =
 [System.Convert]::ToBase64String([System.Text.Encoding]::ASCII.GetBytes($Script))
```

A seguir está um exemplo que decodifica usando o PowerShell.

```
$Script =
 [System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String($UserData))
```

Para obter mais informações sobre a codificação base64, consulte https://www.ietf.org/rfc/rfc4648.txt.

Dados de usuários compactados

O EC2Launch v2 é compatível com dados de usuário compactados como um método para enviar dados de usuários acima do limite de 16 KB imposto pelo IMDS. Para usar esse atributo, compacte o script de dados de usuário em um arquivo `.zip` e passe-o para a instância do EC2. Quando o EC2Launch v2 detecta dados de usuário compactados, ele automaticamente descompacta e executa o script compactado de dados de usuário.

Como acontece com os dados de usuário padrão, se estiver usando a API do Amazon EC2 ou uma ferramenta que não faça codificação base64 de dados do usuário, você mesmo deverá codificar os

dados de usuário compactados. Para obter mais informações sobre o limite de tamanho dos dados de usuário e a codificação base64, consulte Acessar metadados de instância para uma instância do EC2.

Execução de dados do usuário

Por padrão, todas as AMIs do Windows da AWS têm a execução de dados de usuário habilitada para a execução inicial. É possível especificar que os scripts de dados do usuário sejam executados na próxima vez que a instância for reiniciada. Também é possível especificar que os scripts de dados do usuário sejam executados toda vez que a instância for reiniciada.

> **Note**
>
> Os dados do usuário não são habilitados para execução por padrão após a inicialização inicial. Para permitir que os dados do usuário sejam executados ao reinicializar ou iniciar a instância, consulte Executar scripts durante inícios ou reinicializações subsequentes.

Os scripts de dados do usuário são executados na conta do administrador local quando uma senha aleatória é gerada. Caso contrário, os scripts de dados do usuário são executados na conta do sistema.

Scripts de execução de instância

Os scripts nos dados do usuário da instância são executados durante a execução inicial da instância. Se a tag `persist` for localizada, a execução de dados do usuário será habilitada para reinicializações ou inicializações subsequentes. Os arquivos de log do EC2Launch v2, EC2Launch e EC2Config contêm a saída da saída padrão e dos fluxos de erro padrão.

EC2Launch v2

O arquivo de log para EC2Launch v2 é `C:\ProgramData\Amazon\EC2Launch\log\agent.log`.

> **Note**
>
> A pasta `C:\ProgramData` pode estar oculta. Para visualizar a pasta, é necessário mostrar arquivos e pastas ocultos.

As informações a seguir são registradas quando os dados do usuário são executados.

- `Info: Converting user-data to yaml format` – Se os dados do usuário tiverem sido fornecidos no formato XML
- `Info: Initialize user-data state`: o início da execução de dados do usuário
- `Info: Frequency is: always` – Se a tarefa de dados do usuário estiver sendo executada em cada inicialização
- `Info: Frequency is: once` – Se a tarefa de dados do usuário estiver sendo executada apenas uma vez
- `Stage: postReadyUserData execution completed` – O final da execução de dados do usuário

EC2Launch

O arquivo de log do EC2Launch é `C:\ProgramData\Amazon\EC2-Windows\Launch\Log\UserdataExecution.log`.

A pasta `C:\ProgramData` pode estar oculta. Para visualizar a pasta, é necessário mostrar arquivos e pastas ocultos.

As informações a seguir são registradas quando os dados do usuário são executados.

- `Userdata execution begins`: o início da execução de dados do usuário
- `<persist> tag was provided: true` –se a etiqueta persist for encontrada
- `Running userdata on every boot` –se a etiqueta persist for encontrada
- `<powershell> tag was provided.. running powershell content`: se a tag powershell for encontrada
- `<script> tag was provided.. running script content` – se a etiqueta script for encontrada
- `Message: The output from user scripts` – Se os scripts de dados do usuário forem executados, a saída será registrada

EC2Config

O arquivo de log do EC2Config é `C:\Program Files\Amazon\Ec2ConfigService\Logs\Ec2Config.log`. As informações a seguir são registradas quando os dados do usuário são executados.

- `Ec2HandleUserData: Message: Start running user scripts`: o início da execução de dados do usuário
- `Ec2HandleUserData: Message: Re-enabled userdata execution` –se a etiqueta persist for encontrada
- `Ec2HandleUserData: Message: Could not find <persist> and </persist>`: se a tag persist não for encontrada
- `Ec2HandleUserData: Message: The output from user scripts` – Se os scripts de dados do usuário forem executados, a saída será registrada

Executar scripts durante inícios ou reinicializações subsequentes

Quando você atualiza os dados de usuários da instância, o conteúdo atualizado desses dados é refletido automaticamente nos metadados da instância na próxima vez que você reinicializar ou iniciar a instância. Porém, dependendo do agente de inicialização instalado, pode ser necessária uma configuração adicional para configurar scripts de dados de usuários a serem executados em reinicializações ou inicializações subsequentes.

Se você escolher a opção Desativar com Sysprep, os scripts de dados do usuário serão executados na próxima vez que a instância for reiniciada ou iniciada, mesmo que você não tenha habilitado a execução de dados do usuário para reinicializações ou inicializações subsequentes.

Para obter instruções sobre como habilitar a execução de dados de usuários, selecione a guia que corresponde ao seu agente de lançamento.

EC2Launch v2

Ao contrário de EC2Launch v1, EC2Launch v2 avalia a tarefa de dados de usuários em cada inicialização. Não é necessário programar manualmente a tarefa de dados de usuários. Os dados de usuários são executados com base na frequência incluída ou em opções de persistência.

Para scripts de dados de usuários de XML

Para executar scripts de dados de usuários em cada inicialização, adicione o sinalizador `<persist>true</persist>` a esses dados. Se o sinalizador de persistência não estiver incluído, o script de dados de usuários será executado somente na inicialização inicial.

Para dados de usuários YAML

- Para executar uma tarefa em dados de usuários na inicialização inicial, defina a tarefa `frequency` como `once`.

- Para executar uma tarefa em dados de usuários em cada inicialização, defina `frequency` como `always`.

EC2Launch

1. Conecte-se à sua instância do Windows.
2. Abra uma janela de comando do PowerShell e execute um dos seguintes comandos:

   Executar uma vez

   Para executar dados de usuários uma vez na próxima inicialização, use o sinalizador `-Schedule`.

   ```
   C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeInstance.ps1 -Schedule
   ```

   Executar em todas as inicializações subsequentes

   Para executar dados de usuários em todas as inicializações subsequentes, use o sinalizador `-SchedulePerBoot`.

   ```
   C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeInstance.ps1 -SchedulePerBoot
   ```
3. Desconecte-se da instância do Windows. Para executar scripts atualizados na próxima vez que a instância for iniciada, interrompa a instância e atualize os dados do usuário.

EC2Config

1. Conecte-se à sua instância do Windows.
2. Aberto `C:\Program Files\Amazon\Ec2ConfigService\Ec2ConfigServiceSetting.exe`.
3. Em User Data (Dados do usuário), selecione Enable UserData execution for next service start (Habilitar execução de dados do usuário para o próximo início de serviço).
4. Desconecte-se da instância do Windows. Para executar scripts atualizados na próxima vez que a instância for iniciada, interrompa a instância e atualize os dados do usuário.

Dados do usuário e Tools for Windows PowerShell

É possível usar Tools for Windows PowerShell para especificar, modificar e ver os dados do usuário para sua instância. Para obter informações sobre como visualizar os dados do usuário da sua instância usando metadados de instância, consulte Acessar metadados de instância para uma instância do EC2. Para obter informações sobre os dados do usuário e a AWS CLI, consulte Dados do usuário e AWS CLI.

Exemplo: especifique os dados do usuário da instância no lançamento

Crie um arquivo de texto com dados do usuário da instância. Para executar os scripts de dados do usuário sempre que você reiniciar ou iniciar a instância, adicione `<persist>true</persist>`, como mostrado no exemplo a seguir:

```
<powershell>
    $file = $env:SystemRoot + "\Temp\" + (Get-Date).ToString("MM-dd-yy-hh-mm")
    New-Item $file -ItemType file
</powershell>
<persist>true</persist>
```

Para especificar dados do usuário da instância ao executar a instância, use o comando New-EC2Instance. Esse comando não executa a codificação base64 dos dados do usuário para você. Use os comandos a seguir para codificar os dados do usuário em um arquivo de texto denominado `script.txt`.

```
PS C:\> $Script = Get-Content -Raw script.txt
PS C:\> $UserData =
 [System.Convert]::ToBase64String([System.Text.Encoding]::ASCII.GetBytes($Script))
```

Use o parâmetro `-UserData` para passar os dados do usuário para o comando New-EC2Instance.

```
PS C:\> New-EC2Instance -ImageId ami-abcd1234 -MinCount 1 -MaxCount 1 -
InstanceType m3.medium \
    -KeyName my-key-pair -SubnetId subnet-12345678 -SecurityGroupIds sg-1a2b3c4d \
    -UserData $UserData
```

Exemplo: atualizar dados do usuário da instância para uma instância interrompida

É possível modificar os dados do usuário de uma instância interrompida usando o comando Edit-EC2InstanceAttribute.

Crie um arquivo de texto com o novo script. Use os comandos a seguir para codificar os dados do usuário no arquivo de texto denominado `new-script.txt`.

```
PS C:\> $NewScript = Get-Content -Raw new-script.txt
PS C:\> $NewUserData =
 [System.Convert]::ToBase64String([System.Text.Encoding]::ASCII.GetBytes($NewScript))
```

Use os parâmetros `-UserData` e `-Value` para especificar os dados do usuário.

```
PS C:\> Edit-EC2InstanceAttribute -InstanceId i-1234567890abcdef0 -Attribute userData -
Value $NewUserData
```

Exemplo: visualizar dados do usuário da instância

Para recuperar os dados do usuário para uma instância, use o comando Get-EC2InstanceAttribute.

```
PS C:\> (Get-EC2InstanceAttribute -InstanceId i-1234567890abcdef0 -Attribute
 userData).UserData
```

A seguir está um exemplo de saída. Observe que os dados do usuário são codificados.

```
PHBvd2Vyc2hlbGw
+DQpSZW5hbWUtQ29tcHV0ZXIgLU5ld05hbWUgdXNlci1kYXRhLXRlc3QNCjwvcG93ZXJzaGVsbD4=
```

Use os comandos a seguir para armazenar os dados de usuário codificados em uma variável e decodifique-os.

```
PS C:\> $UserData_encoded = (Get-EC2InstanceAttribute -InstanceId i-1234567890abcdef0 -
Attribute userData).UserData
PS C:
\> [System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String($UserData_encoded)
```

A seguir está um exemplo de saída.

```
<powershell>
    $file = $env:SystemRoot + "\Temp\" + (Get-Date).ToString("MM-dd-yy-hh-mm")
    New-Item $file -ItemType file
</powershell>
```

```
<persist>true</persist>
```

Exemplo: renomear a instância para corresponder ao valor da tag

É possível usar o comando Get-EC2Tag para ler o valor da tag. Renomeie a instância na primeira inicialização para corresponder ao valor da tag e reinicialize. Para executar esse comando com êxito, é necessário ter uma função com permissões `ec2:DescribeTags` vinculadas à instância, pois as informações de tag são recuperadas pela chamada de API. Para obter mais informações sobre as permissões de configuração ao usar perfis do IAM, consulte Anexar uma função do IAM a uma instância.

IMDSv2

```
<powershell>
    [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-
seconds" = "21600"} -Method PUT -Uri 'http://169.254.169.254/latest/api/token' -
UseBasicParsing
    $instanceId = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" =
 $token} -Method GET -Uri 'http://169.254.169.254/latest/meta-data/instance-id' -
UseBasicParsing
 $nameValue = (Get-EC2Tag -Filter @{Name="resource-id";Value=
$instanceid},@{Name="key";Value="Name"}).Value
 $pattern = "^(?![0-9]{1,15}$)[a-zA-Z0-9-]{1,15}$"
 #Verify Name Value satisfies best practices for Windows hostnames
 If ($nameValue -match $pattern)
     {Try
         {Rename-Computer -NewName $nameValue -Restart -ErrorAction Stop}
     Catch
         {$ErrorMessage = $_.Exception.Message
         Write-Output "Rename failed: $ErrorMessage"}}
 Else
     {Throw "Provided name not a valid hostname. Please ensure Name value is between
 1 and 15 characters in length and contains only alphanumeric or hyphen characters"}
</powershell>
```

IMDSv1

```
<powershell>
 $instanceId = (Invoke-WebRequest http://169.254.169.254/latest/meta-data/instance-
id -UseBasicParsing).content
 $nameValue = (Get-EC2Tag -Filter @{Name="resource-id";Value=
$instanceid},@{Name="key";Value="Name"}).Value
```

```
 $pattern = "^(?![0-9]{1,15}$)[a-zA-Z0-9-]{1,15}$"
 #Verify Name Value satisfies best practices for Windows hostnames
 If ($nameValue -match $pattern)
     {Try
         {Rename-Computer -NewName $nameValue -Restart -ErrorAction Stop}
     Catch
         {$ErrorMessage = $_.Exception.Message
         Write-Output "Rename failed: $ErrorMessage"}}
 Else
     {Throw "Provided name not a valid hostname. Please ensure Name value is between
 1 and 15 characters in length and contains only alphanumeric or hyphen characters"}
</powershell>
```

Também é possível renomear a instância usando tags em metadados de instância, se sua instância estiver configurada para acessar tags a partir dos metadados da instância. Para obter mais informações, consulte Visualizar tags para as instâncias do EC2 usando os metadados de instância.

IMDSv2

```
<powershell>
    [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-
seconds" = "21600"} -Method PUT -Uri 'http://169.254.169.254/latest/api/token' -
UseBasicParsing
 $nameValue = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token}
 -Method GET -Uri 'http://169.254.169.254/latest/meta-data/tags/instance/Name' -
UseBasicParsing
 $pattern = "^(?![0-9]{1,15}$)[a-zA-Z0-9-]{1,15}$"
 #Verify Name Value satisfies best practices for Windows hostnames
 If ($nameValue -match $pattern)
     {Try
         {Rename-Computer -NewName $nameValue -Restart -ErrorAction Stop}
     Catch
         {$ErrorMessage = $_.Exception.Message
         Write-Output "Rename failed: $ErrorMessage"}}
 Else
     {Throw "Provided name not a valid hostname. Please ensure Name value is between
 1 and 15 characters in length and contains only alphanumeric or hyphen characters"}
</powershell>
```

IMDSv1

```
<powershell>
```

```
 $nameValue = Get-EC2InstanceMetadata -Path /tags/instance/Name
 $pattern = "^(?![0-9]{1,15}$)[a-zA-Z0-9-]{1,15}$"
 #Verify Name Value satisfies best practices for Windows hostnames
 If ($nameValue -match $pattern)
     {Try
         {Rename-Computer -NewName $nameValue -Restart -ErrorAction Stop}
     Catch
         {$ErrorMessage = $_.Exception.Message
         Write-Output "Rename failed: $ErrorMessage"}}
 Else
     {Throw "Provided name not a valid hostname. Please ensure Name value is between
 1 and 15 characters in length and contains only alphanumeric or hyphen characters"}
</powershell>
```

Identificar cada instância executada em uma única solicitação

Este exemplo demonstra como usar dados do usuário e metadados de instância para configurar as instâncias do Amazon EC2.

> **Note**
>
> Os exemplos nesta seção usam o endereço IPv4 do IMDS: `169.254.169.254`. Se você estiver recuperando metadados de instância para instâncias do EC2 pelo endereço IPv6, certifique-se de habilitar e usar o endereço IPv6: `[fd00:ec2::254]`. O endereço IPv6 do IMDS é compatível com comandos IMDSv2. O endereço IPv6 só é acessível em instâncias baseadas em Nitro em sub-redes compatíveis com IPv6 (pilha dupla ou IPv6 apenas).

Alice deseja executar quatro instâncias de sua AMI de banco de dados favorita, em que a primeira atua como a instância original e as três restantes como réplicas. Ao executá-las, ela deseja adicionar dados do usuário sobre a estratégia de replicação para cada réplica. Ela sabe que esses dados estarão disponíveis para todas as quatro instâncias, então, ela precisa estruturar os dados do usuário de forma que permita a cada instância reconhecer quais partes são aplicáveis a ela. Ela pode fazer isso usando o valor de metadados da instância `ami-launch-index`, que será exclusivo para cada instância. Se você iniciar mais de uma instância ao mesmo tempo, o `ami-launch-index`indicará a ordem em que as instâncias foram executadas. O valor da primeira instância iniciada é `0`.

Veja a seguir os dados de usuário construídos por Alice.

```
replicate-every=1min | replicate-every=5min | replicate-every=10min
```

Os dados `replicate-every=1min` definem a configuração da primeira réplica, `replicate-every=5min` definem a configuração da segunda réplica e assim por diante. Alice decide fornecer esses dados como uma string ASCII com um símbolo de pipe (`|`) que limita os dados para as instâncias separadas.

Alice executa quatro instâncias usando o comando run-instances e especificando os dados do usuário.

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --count 4 \
    --instance-type t2.micro \
    --user-data "replicate-every=1min | replicate-every=5min | replicate-every=10min"
```

Depois de executadas, todas as instâncias têm uma cópia dos dados do usuário e os metadados comuns mostrados aqui:

- ID da AMI: ami-0abcdef1234567890
- ID da reserva: r-1234567890abcabc0
- Chaves públicas: nenhuma
- Nome do security group: padrão
- Tipo de instância: t2.micro

No entanto, cada instância tem metadados exclusivos, conforme mostrado nas tabelas a seguir.

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

Metadados	Valor
local-ipv4	10.251.50.35

Metadados	Valor
instance-id	i-0598c7d356eba48d7
ami-launch-index	1
public-hostname	ec2-67-202-51-224.compute-1.amazonaws.com
public-ipv4	67.202.51.224
local-hostname	ip-10-251-50-36.ec2.internal
local-ipv4	10.251.50.36

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

Metadados	Valor
instance-id	i-1234567890abcdef0

Metadados	Valor
ami-launch-index	3
public-hostname	ec2-67-202-51-226.compute-1.amazonaws.com
public-ipv4	67.202.51.226
local-hostname	ip-10-251-50-38.ec2.internal
local-ipv4	10.251.50.38

Alice pode usar o valor `ami-launch-index` para determinar qual parte dos dados do usuário é aplicável a uma instância específica.

1. Ela se conecta a uma das instâncias e recupera o `ami-launch-index` dessa instância para garantir que ela seja uma das réplicas:

   IMDSv2

   ```
   [ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/meta-data/api/
   token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
   && curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-
   data/ami-launch-index
   2
   ```

   Para as etapas a seguir, as solicitações do IMDSv2 usam o token armazenado do comando anterior do IMDSv2, supondo-se que o token não tenha expirado.

   IMDSv1

   ```
   [ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/ami-launch-index
   2
   ```

2. Ela salva o `ami-launch-index` como uma variável.

   IMDSv2

   ```
   [ec2-user ~]$ ami_launch_index=`curl -H "X-aws-ec2-metadata-token: $TOKEN"
    http://169.254.169.254/latest/meta-data/ami-launch-index`
   ```

IMDSv1

```
[ec2-user ~]$ ami_launch_index=`curl http://169.254.169.254/latest/meta-data/ami-launch-index`
```

3. Ela salva os dados do usuário como uma variável.

   IMDSv2

   ```
   [ec2-user ~]$ user_data=`curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/user-data`
   ```

   IMDSv1

   ```
   [ec2-user ~]$ user_data=`curl http://169.254.169.254/latest/user-data`
   ```

4. Finalmente, Alice usa o comando cut para extrair a parte dos dados do usuário aplicável à instância.

   IMDSv2

   ```
   [ec2-user ~]$ echo $user_data | cut -d"|" -f"$ami_launch_index"
   replicate-every=5min
   ```

   IMDSv1

   ```
   [ec2-user ~]$ echo $user_data | cut -d"|" -f"$ami_launch_index"
   replicate-every=5min
   ```

Detectar se um host é uma instância do EC2

Talvez seja necessário determinar se a aplicação ou o site está sendo executado em uma instância do EC2, especialmente se você tiver um ambiente de computação misto. Você pode usar uma das opções a seguir para determinar se o host da aplicação ou do site é uma instância do EC2.

Opções

- Inspecione o documento de identidade da instância
- Inspecione o UUID do sistema
- Inspecione o identificador de geração da máquina virtual do sistema

Inspecione o documento de identidade da instância

Cada instância tem um documento de identidade de instância assinado que você pode verificar criptograficamente. Você pode encontrar esses documentos usando o serviço de metadados de instância (IMDS).

Para obter mais informações, consulte Documentos de identidade da instância.

Inspecione o UUID do sistema

Você pode obter o UUID do sistema e procurar no octeto inicial do UUID por `EC2` (no Linux, pode ser `ec2` em letras minúsculas). Esse método é rápido, mas potencialmente impreciso, pois há uma pequena possibilidade de que um sistema que não seja uma instância do EC2 possa ter um UUID que comece com esses caracteres. Além disso, algumas versões do SMBIOS usam o formato little-endian, que não inclui `EC2` no início do UUID. Esse pode ser o caso de instâncias do EC2 que usam o SMBIOS 2.4 para Windows ou para distribuições do Linux diferentes do Amazon Linux que têm as próprias implementações de SMBIOS.

Exemplo do Linux: obtenha o UUID da DMI (somente para AMIs de HVM)

Use o seguinte comando para obter o UUID usando a Desktop Management Interface (DMI):

```
[ec2-user ~]$ sudo dmidecode --string system-uuid
```

Na próxima saída de exemplo, o UUID começa com "EC2", que indica que o sistema é provavelmente uma instância do EC2.

```
EC2E1916-9099-7CAF-FD21-012345ABCDEF
```

No exemplo de saída a seguir, o UUID é representado no formato little-endian.

```
45E12AEC-DCD1-B213-94ED-012345ABCDEF
```

Como alternativa, para instâncias criadas no sistema Nitro, é possível usar o seguinte comando:

```
[ec2-user ~]$ cat /sys/devices/virtual/dmi/id/board_asset_tag
```

Se a saída for um ID de instância, como a saída de exemplo a seguir, o sistema será uma instância do EC2:

```
i-0af01c0123456789a
```

Exemplo do Linux: obtenha o UUID do hipervisor (somente para AMIs PV)

Use o seguinte comando para obter o UUID do hipervisor:

```
[ec2-user ~]$ cat /sys/hypervisor/uuid
```

Na próxima saída de exemplo, o UUID começa com "ec2", que indica que o sistema é provavelmente uma instância do EC2.

```
ec2e1916-9099-7caf-fd21-012345abcdef
```

Exemplo do Windows: obtenha o UUID usando o WMI ou o Windows PowerShell

Use a linha de comando de Instrumentação de Gerenciamento do Windows (WMIC) da seguinte forma:

```
wmic path win32_computersystemproduct get uuid
```

Alternativamente, se você estiver usando o Windows PowerShell, use o cmdlet Get-WmiObject da seguinte maneira:

```
PS C:\> Get-WmiObject -query "select uuid from Win32_ComputerSystemProduct" | Select
 UUID
```

Na próxima saída de exemplo, o UUID começa com "EC2", que indica que o sistema é provavelmente uma instância do EC2.

```
EC2AE145-D1DC-13B2-94ED-012345ABCDEF
```

Para instâncias que usam o SMBIOS 2.4, o UUID pode ser representado no formato little-endian; por exemplo:

```
45E12AEC-DCD1-B213-94ED-012345ABCDEF
```

Inspecione o identificador de geração da máquina virtual do sistema

Um identificador de geração de máquina virtual consiste em um buffer exclusivo de 128 bits interpretado como identificador de inteiro aleatório criptográfico. É possível recuperar o identificador de geração de máquina virtual para identificar sua instância do Amazon Elastic Compute Cloud. O identificador de geração é exposto no sistema operacional convidado da instância por meio de uma entrada de tabela ACPI. O valor mudará se sua máquina for clonada, copiada ou importada para AWS, como com VM Import/Export.

Exemplo: como recuperar o identificador de geração de máquina virtual do Linux

É possível usar os seguintes comandos para recuperar o identificador de geração de máquina virtual de suas instâncias que executem o Linux:

Amazon Linux 2

1. Atualize seus pacotes de software existentes, conforme necessário, usando o seguinte comando:

   ```
   sudo yum update
   ```

2. Se necessário, utilize o pacote busybox com o seguinte comando:

   ```
   sudo curl https://www.rpmfind.net/linux/epel/next/8/Everything/x86_64/Packages/
   b/busybox-1.35.0-2.el8.next.x86_64.rpm --output busybox.rpm
   ```

3. Se necessário, instale os pacotes de pré-requisitos usando o seguinte comando:

   ```
   sudo yum install busybox.rpm iasl -y
   ```

4. Execute o seguinte `iasl` para produzir saída da tabela ACPI:

   ```
   sudo iasl -p ./SSDT2 -d /sys/firmware/acpi/tables/SSDT2
   ```

5. Execute o seguinte comando para revisar a saída do comando `iasl`:

   ```
   cat SSDT2.dsl
   ```

   A saída deve gerar o espaço de endereço necessário para recuperar o identificador de geração da máquina virtual:

```
Intel ACPI Component Architecture
ASL+ Optimizing Compiler/Disassembler version 20190509
Copyright (c) 2000 - 2019 Intel Corporation

File appears to be binary: found 32 non-ASCII characters, disassembling
Binary file appears to be a valid ACPI table, disassembling
Input file /sys/firmware/acpi/tables/SSDT2, Length 0x7B (123) bytes
ACPI: SSDT 0x0000000000000000 00007B (v01 AMAZON AMZNSSDT 00000001 AMZN
 00000001)
Pass 1 parse of [SSDT]
Pass 2 parse of [SSDT]
Parsing Deferred Opcodes (Methods/Buffers/Packages/Regions)

Parsing completed
Disassembly completed
ASL Output:    ./SSDT2.dsl - 1065 bytes
$
/*
* Intel ACPI Component Architecture
* AML/ASL+ Disassembler version 20190509 (64-bit version)
* Copyright (c) 2000 - 2019 Intel Corporation
*
* Disassembling to symbolic ASL+ operators
*
* Disassembly of /sys/firmware/acpi/tables/SSDT2, Tue Mar 29 16:15:14 2022
*
* Original Table Header:
*     Signature        "SSDT"
*     Length           0x0000007B (123)
*     Revision         0x01
*     Checksum         0xB8
*     OEM ID           "AMAZON"
*     OEM Table ID     "AMZNSSDT"
*     OEM Revision     0x00000001 (1)
*     Compiler ID      "AMZN"
*     Compiler Version 0x00000001 (1)
*/
DefinitionBlock ("", "SSDT", 1, "AMAZON", "AMZNSSDT", 0x00000001)
{
Scope (\_SB)
{
    Device (VMGN)
    {
```

```
        Name (_CID, "VM_Gen_Counter")  // _CID: Compatible ID
        Name (_DDN, "VM_Gen_Counter")  // _DDN: DOS Device Name
        Name (_HID, "AMZN0000")  // _HID: Hardware ID
        Name (ADDR, Package (0x02)
        {
            0xFED01000,
            Zero
        })
    }
}
}
```

6. (Opcional) Eleve suas permissões de terminal para as etapas restantes com o seguinte comando:

```
sudo -s
```

7. Use o comando a seguir para armazenar o espaço de endereço coletado anteriormente:

```
VMGN_ADDR=0xFED01000
```

8. Use o seguinte comando para iterar pelo espaço de endereço e criar o identificador de geração de máquina virtual:

```
for offset in 0x0 0x4 0x8 0xc; do busybox devmem $(($VMGN_ADDR + $offset)) | sed
 's/0x//' | sed -z '$ s/\n$//' >> vmgenid; done
```

9. Recupere o identificador de geração da máquina virtual do arquivo de saída com o seguinte comando:

```
cat vmgenid ; echo
```

Sua saída deve ser similar à seguinte:

```
EC2F335D979132C4165896753E72BD1C
```

Ubuntu

1. Atualize seus pacotes de software existentes, conforme necessário, usando o seguinte comando:

```
sudo apt update
```

2. Se necessário, instale os pacotes de pré-requisitos usando o seguinte comando:

```
sudo apt install busybox iasl -y
```

3. Execute o seguinte `iasl` para produzir saída da tabela ACPI:

```
sudo iasl -p ./SSDT2 -d /sys/firmware/acpi/tables/SSDT2
```

4. Execute o seguinte comando para revisar a saída do comando `iasl`:

```
cat SSDT2.dsl
```

A saída deve gerar o espaço de endereço necessário para recuperar o identificador de geração da máquina virtual:

```
Intel ACPI Component Architecture
ASL+ Optimizing Compiler/Disassembler version 20190509
Copyright (c) 2000 - 2019 Intel Corporation

File appears to be binary: found 32 non-ASCII characters, disassembling
Binary file appears to be a valid ACPI table, disassembling
Input file /sys/firmware/acpi/tables/SSDT2, Length 0x7B (123) bytes
ACPI: SSDT 0x0000000000000000 00007B (v01 AMAZON AMZNSSDT 00000001 AMZN
 00000001)
Pass 1 parse of [SSDT]
Pass 2 parse of [SSDT]
Parsing Deferred Opcodes (Methods/Buffers/Packages/Regions)

Parsing completed
Disassembly completed
ASL Output:    ./SSDT2.dsl - 1065 bytes
$
/*
* Intel ACPI Component Architecture
* AML/ASL+ Disassembler version 20190509 (64-bit version)
* Copyright (c) 2000 - 2019 Intel Corporation
*
* Disassembling to symbolic ASL+ operators
*
```

```
* Disassembly of /sys/firmware/acpi/tables/SSDT2, Tue Mar 29 16:15:14 2022
*
* Original Table Header:
*     Signature        "SSDT"
*     Length           0x0000007B (123)
*     Revision         0x01
*     Checksum         0xB8
*     OEM ID           "AMAZON"
*     OEM Table ID     "AMZNSSDT"
*     OEM Revision     0x00000001 (1)
*     Compiler ID      "AMZN"
*     Compiler Version 0x00000001 (1)
*/
DefinitionBlock ("", "SSDT", 1, "AMAZON", "AMZNSSDT", 0x00000001)
{
Scope (\_SB)
{
    Device (VMGN)
    {
        Name (_CID, "VM_Gen_Counter")  // _CID: Compatible ID
        Name (_DDN, "VM_Gen_Counter")  // _DDN: DOS Device Name
        Name (_HID, "AMZN0000")  // _HID: Hardware ID
        Name (ADDR, Package (0x02)
        {
            0xFED01000,
            Zero
        })
    }
}
}
```

5. (Opcional) Eleve suas permissões de terminal para as etapas restantes com o seguinte comando:

```
sudo -s
```

6. Use os seguintes comandos para armazenar o espaço de endereço coletado anteriormente:

```
VMGN_ADDR=0xFED01000
```

7. Use o seguinte comando para iterar pelo espaço de endereço e criar o identificador de geração de máquina virtual:

```
for offset in 0x0 0x4 0x8 0xc; do busybox devmem $(($VMGN_ADDR + $offset)) | sed
 's/0x//' | sed -z '$ s/\n$//' >> vmgenid; done
```

8. Recupere o identificador de geração da máquina virtual do arquivo de saída com o seguinte comando:

```
cat vmgenid ; echo
```

Sua saída deve ser similar à seguinte:

```
EC2F335D979132C4165896753E72BD1C
```

Exemplo: como recuperar o identificador de geração de máquina virtual do Windows

É possível criar uma aplicação de exemplo para recuperar o identificador de geração de máquina virtual de suas instâncias que executam o Windows. Para obter mais informações, consulte Obter o identificador de geração de máquina virtual na documentação da Microsoft.

Documentos de identidade da instância para instâncias do Amazon EC2

Cada instância iniciada tem um documento de identidade da instância que fornece informações sobre a própria instância. É possível usar o documento de identidade da instância para validar os atributos da instância.

O documento de identidade da instância é gerado quando a instância é interrompida e iniciada, reiniciada ou lançada. É possível acessar o documento de identidade da instância para uma instância por meio do serviço de metadados de instância (IMDS). Para obter instruções, consulte Recuperar o documento de identidade da instância.

O documento de identidade da instância usa o formato JSON de texto simples. Isso inclui as informações a seguir.

Dados	Descrição
`accountId`	O ID da conta da AWS que iniciou a instância.

Dados	Descrição
`architecture`	A arquitetura da AMI usada para iniciar a instância (i386 | x86_64 | arm64).
`availabilityZone`	O nome da zona de disponibilidade na qual a instância está sendo executada. Por exemplo, `us-east-1` . Lembre-se de que os nomes das zonas de disponibilidade podem ser diferentes entre as contas da AWS.
`billingProducts`	Os produtos de faturamento da instância.
`devpayProductCodes`	Suspenso.
`imageId`	A ID do AMI usado para executar a instância.
`instanceId`	O ID da instância.
`instanceType`	O tipo de instância da instância.
`kernelId`	O ID do kernel associado à instância, se aplicável.
`marketplaceProductCodes`	O código do produto AWS Marketplace da AMI usada para iniciar a instância.
`pendingTime`	A data e a hora em que a instância foi iniciada.
`privateIp`	O endereço IP privado da instância. Para instâncias somente IPv4 e dual-stack, isso contém o endereço IPv4. Para instâncias somente IPv6, isso contém o endereço IPv6.
`ramdiskId`	O ID do disco de RAM associado a essa instância, se aplicável.
`region`	A região em que a instância está em execução.
`version`	A versão do formato do documento de identidade da instância.

Recuperar o documento de identidade da instância de uma instância do EC2

O documento de identidade da instância para uma instância do Amazon EC2 usa um formato JSON de texto simples. Para obter uma descrição do conteúdo de um documento de identidade da instância, consulte the section called “Documentos de identidade da instância”.

O documento de identidade de instância é armazenado nos metadados da instância para a instância, na categoria de dados dinâmicos `instance-identity/document`. Você acessa o documento de identidade da instância conectando-se à instância e recuperando-o dos metadados da instância.

É possível acessar os metadados da instância usando o endereço IPv4 169.254.169.254 ou o endereço IPv6 fd00:ec2::254. Esses são Endereços locais de link, o que significa que é possível acessá-los apenas na instância. Os exemplos nesta página usam o endereço IPv4 do IMDS: 169.254.169.254. Para recuperar os metadados de instância para instâncias do EC2 via IPv6, use fd00:ec2::254.

Para verificar a autenticidade de um documento de identidade da instância após recuperá-lo, consulte Verificar documento de identidade da instância.

IMDSv2

Linux

Para recuperar o documento de identidade da instância, use o seguinte comando em sua instância Linux.

```
TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
    && curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/dynamic/instance-identity/document
```

Windows

Para recuperar o documento de identidade da instância, use o seguinte cmdlet em sua instância Windows.

```
[string]$token = (Invoke-WebRequest -Headers @{'X-aws-ec2-metadata-token-ttl-seconds' = '21600'} `
```

```
    -Method PUT -Uri 'http://169.254.169.254/latest/api/token' -
UseBasicParsing).Content
```

```
(Invoke-WebRequest -Headers @{'X-aws-ec2-metadata-token' = $token} `
    -Uri 'http://169.254.169.254/latest/dynamic/instance-identity/document' -
UseBasicParsing).Content
```

IMDSv1

Linux

Para recuperar o documento de identidade da instância, use o seguinte comando em sua instância Linux.

```
curl http://169.254.169.254/latest/dynamic/instance-identity/document
```

Windows

Para recuperar o documento de identidade da instância, use o seguinte cmdlet em sua instância Windows.

```
(Invoke-WebRequest http://169.254.169.254/latest/dynamic/instance-identity/
document).Content
```

O seguinte é um exemplo de saída.

```
{
    "devpayProductCodes" : null,
    "marketplaceProductCodes" : [ "1abc2defghijklm3nopqrs4tu" ],
    "availabilityZone" : "us-west-2b",
    "privateIp" : "10.158.112.84",
    "version" : "2017-09-30",
    "instanceId" : "i-1234567890abcdef0",
    "billingProducts" : null,
    "instanceType" : "t2.micro",
    "accountId" : "123456789012",
    "imageId" : "ami-5fb8c835",
    "pendingTime" : "2016-11-19T16:32:11Z",
    "architecture" : "x86_64",
    "kernelId" : null,
```

```
    "ramdiskId" : null,
    "region" : "us-west-2"
}
```

Verifique o documento de identidade de uma instância do Amazon EC2

Se você pretende usar o conteúdo do documento de identidade da instância para um propósito importante, deve verificar seu conteúdo e autenticidade antes de usá-lo.

O documento de identidade da instância de texto simples é acompanhado por três assinaturas hash e criptografadas. É possível usar essas assinaturas para verificar a origem e a autenticidade do documento de identidade da instância e as informações incluídas nele. São fornecidas as seguintes assinaturas:

- Assinatura codificada em base64 – trata-se de um hash SHA256 codificado em base64 do documento de identidade da instância que é criptografado usando um par de chaves RSA.
- Assinatura PKCS7 – trata-se de um hash SHA1 do documento de identidade da instância que é criptografado usando um par de chaves DSA.
- Assinatura RSA-2048 – trata-se de um hash SHA256 do documento de identidade da instância que é criptografado usando um par de chaves RSA-2048.

Cada assinatura está disponível em um endpoint diferente nos metadados da instância. É possível usar qualquer uma dessas assinaturas dependendo dos requisitos de hash e criptografia. Para verificar as assinaturas, é necessário usar o certificado público da AWS correspondente.

Opções

- Opção 1: verificar o documento de identidade da instância usando a assinatura PKCS7
- Opção 2: verificar o documento de identidade da instância usando a assinatura codificada em base64
- Opção 3: verificar o documento de identidade da instância usando a assinatura RSA-2048

Opção 1: verificar o documento de identidade da instância usando a assinatura PKCS7

Este tópico explica como verificar o documento de identidade da instância usando a assinatura PKCS7 e o certificado público DSA da AWS.

Instâncias do Linux

Para verificar o documento de identidade da instância usando a assinatura PKCS7 e o certificado público AWS DSA

1. Conecte-se à instância.
2. Recupere a assinatura PKCS7 dos metadados da instância e adicione-a a um arquivo chamado `pkcs7` junto com o cabeçalho e rodapé necessários. Use um dos comandos a seguir dependendo da versão do IMDS usada pela instância.

   IMDSv2

   ```
   $ echo "-----BEGIN PKCS7-----" >> pkcs7 \
    && TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-
   metadata-token-ttl-seconds: 21600"` \
    && curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
   dynamic/instance-identity/pkcs7 >> pkcs7 \
    && echo "" >> pkcs7 \
    && echo "-----END PKCS7-----" >> pkcs7
   ```

   IMDSv1

   ```
   $ echo "-----BEGIN PKCS7-----" >> pkcs7 \
    && curl -s http://169.254.169.254/latest/dynamic/instance-identity/pkcs7
    >> pkcs7 \
    && echo "" >> pkcs7 \
    && echo "-----END PKCS7-----" >> pkcs7
   ```

3. Encontre o certificado público DSA da sua região em Certificados públicos da AWS para assinaturas de documento de identidade da instância e adicione o conteúdo a um novo arquivo chamado `certificate`.
4. Use o comando OpenSSL smime para verificar a assinatura. Inclua a opção `-verify` para indicar que a assinatura precisa ser verificada, e a opção `-noverify` para indicar que o certificado não precisa ser verificado.

   ```
   $ openssl smime -verify -in pkcs7 -inform PEM -certfile certificate -noverify | tee
    document
   ```

   Se a assinatura for válida, a mensagem `Verification successful` será exibida.

O comando também grava o conteúdo do documento de identidade da instância em um novo arquivo denominado `document`. É possível comparar o conteúdo do documento de identidade da instância dos metadados da instância com o conteúdo desse arquivo usando os comandos a seguir.

```
$ openssl dgst -sha256 < document
```

```
$ curl -s -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
dynamic/instance-identity/document | openssl dgst -sha256
```

Se não for possível verificar a assinatura, entre em contato com o Suporte.

Instâncias do Windows

Pré-requisitos

Este procedimento exige a classe `System.Security` Microsoft .NET Core. Para adicionar a classe à sessão do PowerShell, execute o comando a seguir.

```
PS C:\> Add-Type -AssemblyName System.Security
```

> **Note**
>
> O comando adiciona a classe somente à sessão atual do PowerShell. Se você iniciar uma nova sessão, deverá executar o comando novamente.

Para verificar o documento de identidade da instância usando a assinatura PKCS7 e o certificado público AWS DSA

1. Conecte-se à instância.
2. Recupere a assinatura PKCS7 dos metadados da instância, converta-a em uma matriz de bytes e adicione-a a uma variável chamada `$Signature`. Use um dos comandos a seguir dependendo da versão do IMDS usada pela instância.

IMDSv2

```
PS C:\> [string]$token = (Invoke-WebRequest -Method Put -Headers @{'X-aws-ec2-
metadata-token-ttl-seconds' = '21600'} -Uri http://169.254.169.254/latest/api/
token).Content
```

```
PS C:\> $Signature = [Convert]::FromBase64String((Invoke-WebRequest -Headers
 @{'X-aws-ec2-metadata-token' = $Token} -Uri http://169.254.169.254/latest/
dynamic/instance-identity/pkcs7).Content)
```

IMDSv1

```
PS C:\> $Signature = [Convert]::FromBase64String((Invoke-WebRequest -Uri
 http://169.254.169.254/latest/dynamic/instance-identity/pkcs7).Content)
```

3. Recupere o documento de identidade da instância de texto simples dos metadados da instância, converta-o em uma matriz de bytes e adicione-o a uma variável chamada `$Document`. Use um dos comandos a seguir dependendo da versão do IMDS usada pela instância.

   IMDSv2

   ```
   PS C:\> $Document = [Text.Encoding]::UTF8.GetBytes((Invoke-WebRequest -Headers
    @{'X-aws-ec2-metadata-token' = $Token} -Uri http://169.254.169.254/latest/
   dynamic/instance-identity/document).Content)
   ```

   IMDSv1

   ```
   PS C:\> $Document =  [Text.Encoding]::UTF8.GetBytes((Invoke-WebRequest
    http://169.254.169.254/latest/dynamic/instance-identity/document).Content)
   ```

4. Encontre o certificado público DSA da sua região em Certificados públicos da AWS para assinaturas de documento de identidade da instância e adicione o conteúdo a um novo arquivo chamado `certificate.pem`.

5. Extraia o certificado do arquivo de certificado e armazene-o em uma variável chamada `$Store`.

   ```
   PS C:\> $Store =
    [Security.Cryptography.X509Certificates.X509Certificate2Collection]::new([Security.Cryptog
   Path certificate.pem)))
   ```

6. Verifique a assinatura.

```
PS C:\> $SignatureDocument = [Security.Cryptography.Pkcs.SignedCms]::new()
```

```
PS C:\> $SignatureDocument.Decode($Signature)
```

```
PS C:\> $SignatureDocument.CheckSignature($Store, $true)
```

   Se a assinatura for válida, o comando não retornará nenhuma saída. Se não for possível verificar a assinatura, o comando retornará `Exception calling "CheckSignature" with "2" argument(s): "Cannot find the original signer`. Se não for possível verificar a assinatura, entre em contato com o AWS Support.

7. Valide o conteúdo do documento de identidade da instância.

```
PS C:
\> [Linq.Enumerable]::SequenceEqual($SignatureDocument.ContentInfo.Content, $Document)
```

   Se o conteúdo do documento de identidade da instância for válido, o comando retornará `True`. Se o documento de identidade da instância não puder ser validado, entre em contato com o AWS Support.

Opção 2: verificar o documento de identidade da instância usando a assinatura codificada em base64

Este tópico explica como verificar o documento de identidade da instância usando a assinatura codificada em base64 e o certificado público RSA da AWS.

Instâncias do Linux

Para validar o documento de identidade da instância usando a assinatura codificada em base64 e do certificado público RSA da AWS

1. Conecte-se à instância.
2. Recupere a assinatura codificada em base64 dos metadados da instância, converta-a em binário e adicione-o a um arquivo chamado `signature`. Use um dos comandos a seguir dependendo da versão do IMDS usada pela instância.

IMDSv2

```
$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-
metadata-token-ttl-seconds: 21600"` \
 && curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
dynamic/instance-identity/signature | base64 -d >> signature
```

IMDSv1

```
$ curl -s http://169.254.169.254/latest/dynamic/instance-identity/signature |
 base64 -d >> signature
```

3. Recupere o documento de identidade da instância de texto simples dos metadados da instância e adicione-o a um arquivo chamado `document`. Use um dos comandos a seguir dependendo da versão do IMDS usada pela instância.

   IMDSv2

   ```
   $ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-
   metadata-token-ttl-seconds: 21600"` \
    && curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
   dynamic/instance-identity/document >> document
   ```

   IMDSv1

   ```
   $ curl -s http://169.254.169.254/latest/dynamic/instance-identity/document
    >> document
   ```

4. Encontre o certificado público RSA para a sua região em Certificados públicos da AWS para assinaturas de documento de identidade da instância e adicione o conteúdo a um novo arquivo denominado `certificate`.
5. Extraia a chave pública do certificado público RSS da AWS e salve-a em um arquivo denominado `key`.

   ```
   $ openssl x509 -pubkey -noout -in certificate >> key
   ```

6. Use o comando OpenSSL dgst para verificar o documento de identidade da instância.

   ```
   $ openssl dgst -sha256 -verify key -signature signature document
   ```

Se a assinatura for válida, a mensagem `Verification successful` será exibida.

O comando também grava o conteúdo do documento de identidade da instância em um novo arquivo denominado `document`. É possível comparar o conteúdo do documento de identidade da instância dos metadados da instância com o conteúdo desse arquivo usando os comandos a seguir.

```
$ openssl dgst -sha256 < document
```

```
$ curl -s -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
dynamic/instance-identity/document | openssl dgst -sha256
```

Se não for possível verificar a assinatura, entre em contato com o Suporte.

Instâncias do Windows

Para validar o documento de identidade da instância usando a assinatura codificada em base64 e do certificado público RSA da AWS

1. Conecte-se à instância.
2. Recupere a assinatura codificada em base64 dos metadados da instância, converta-a em uma matriz de bytes e adicione-a à variável chamada `$Signature`. Use um dos comandos a seguir dependendo da versão do IMDS usada pela instância.

   IMDSv2

   ```
   PS C:\> [string]$token = (Invoke-WebRequest -Method Put -Headers @{'X-aws-
   ec2-metadata-token-ttl-seconds' = '21600'} http://169.254.169.254/latest/api/
   token).Content
   ```

   ```
   PS C:\> $Signature = [Convert]::FromBase64String((Invoke-WebRequest -Headers
    @{'X-aws-ec2-metadata-token' = $Token} http://169.254.169.254/latest/dynamic/
   instance-identity/signature).Content)
   ```

IMDSv1

```
PS C:\> $Signature = [Convert]::FromBase64String((Invoke-WebRequest
 http://169.254.169.254/latest/dynamic/instance-identity/signature).Content)
```

3. Recupere o documento de identidade da instância de texto simples dos metadados da instância, converta-o em uma matriz de bytes e adicione-o a uma variável chamada `$Document`. Use um dos comandos a seguir dependendo da versão do IMDS usada pela instância.

   IMDSv2

   ```
   PS C:\> $Document = [Text.Encoding]::UTF8.GetBytes((Invoke-WebRequest -Headers
    @{'X-aws-ec2-metadata-token' = $Token} http://169.254.169.254/latest/dynamic/
   instance-identity/document).Content)
   ```

   IMDSv1

   ```
   PS C:\> $Document =  [Text.Encoding]::UTF8.GetBytes((Invoke-WebRequest
    http://169.254.169.254/latest/dynamic/instance-identity/document).Content)
   ```

4. Encontre o certificado público RSA para a sua região em Certificados públicos da AWS para assinaturas de documento de identidade da instância e adicione o conteúdo a um novo arquivo denominado `certificate.pem`.
5. Verifique o documento de identidade da instância.

   ```
   PS C:\> [Security.Cryptography.X509Certificates.X509Certificate2]::new((Resolve-
   Path certificate.pem)).PublicKey.Key.VerifyData($Document, 'SHA256', $Signature)
   ```

   Se a assinatura for válida, o comando retornará `True`. Se não for possível verificar a assinatura, entre em contato com o Suporte.

Opção 3: verificar o documento de identidade da instância usando a assinatura RSA-2048

Este tópico explica como verificar o documento de identidade da instância usando a assinatura RSA-2048 e o certificado público RSA-2048 da AWS.

Instâncias do Linux

Para verificar o documento de identidade da instância usando a assinatura RSA-2048 e o certificado público RSA-2048 da AWS

1. Conecte-se à instância.
2. Recupere a assinatura RSA-2048 dos metadados da instância e adicione-a a um novo arquivo chamado `rsa2048` junto com o cabeçalho e rodapé necessários. Use um dos comandos a seguir dependendo da versão do IMDS usada pela instância.

   IMDSv2

   ```
   $ echo "-----BEGIN PKCS7-----" >> rsa2048 \
    && TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
    && curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/dynamic/instance-identity/rsa2048 >> rsa2048 \
    && echo "" >> rsa2048 \
    && echo "-----END PKCS7-----" >> rsa2048
   ```

   IMDSv1

   ```
   $ echo "-----BEGIN PKCS7-----" >> rsa2048 \
    && curl -s http://169.254.169.254/latest/dynamic/instance-identity/rsa2048 >> rsa2048 \
    && echo "" >> rsa2048 \
    && echo "-----END PKCS7-----" >> rsa2048
   ```

3. Encontre o certificado público RSA-2048 para a sua região em Certificados públicos da AWS para assinaturas de documento de identidade da instância e adicione o conteúdo a um novo arquivo denominado `certificate`.
4. Use o comando OpenSSL smime para verificar a assinatura. Inclua a opção `-verify` para indicar que a assinatura precisa ser verificada, e a opção `-noverify` para indicar que o certificado não precisa ser verificado.

   ```
   $ openssl smime -verify -in rsa2048 -inform PEM -certfile certificate -noverify |
    tee document
   ```

   Se a assinatura for válida, a mensagem `Verification successful` será exibida. Se não for possível verificar a assinatura, entre em contato com o Suporte.

Instâncias do Windows

Pré-requisitos

Este procedimento exige a classe `System.Security` Microsoft .NET Core. Para adicionar a classe à sessão do PowerShell, execute o comando a seguir.

```
PS C:\> Add-Type -AssemblyName System.Security
```

> **Note**
>
> O comando adiciona a classe somente à sessão atual do PowerShell. Se você iniciar uma nova sessão, deverá executar o comando novamente.

Para verificar o documento de identidade da instância usando a assinatura RSA-2048 e o certificado público RSA-2048 da AWS

1. Conecte-se à instância.
2. Recupere a assinatura RSA-2048 dos metadados da instância, converta-a em uma matriz de bytes e adicione-a a uma variável chamada `$Signature`. Use um dos comandos a seguir dependendo da versão do IMDS usada pela instância.

   IMDSv2

   ```
   PS C:\> [string]$token = (Invoke-WebRequest -Method Put -Headers @{'X-aws-
   ec2-metadata-token-ttl-seconds' = '21600'} http://169.254.169.254/latest/api/
   token).Content
   ```

   ```
   PS C:\> $Signature = [Convert]::FromBase64String((Invoke-WebRequest -Headers
    @{'X-aws-ec2-metadata-token' = $Token} http://169.254.169.254/latest/dynamic/
   instance-identity/rsa2048).Content)
   ```

   IMDSv1

   ```
   PS C:\> $Signature = [Convert]::FromBase64String((Invoke-WebRequest
    http://169.254.169.254/latest/dynamic/instance-identity/rsa2048).Content)
   ```

3. Recupere o documento de identidade da instância de texto simples dos metadados da instância, converta-o em uma matriz de bytes e adicione-o a uma variável chamada `$Document`. Use um dos comandos a seguir dependendo da versão do IMDS usada pela instância.

   IMDSv2

   ```
   PS C:\> $Document = [Text.Encoding]::UTF8.GetBytes((Invoke-WebRequest -Headers
    @{'X-aws-ec2-metadata-token' = $Token} http://169.254.169.254/latest/dynamic/
   instance-identity/document).Content)
   ```

   IMDSv1

   ```
   PS C:\> $Document =  [Text.Encoding]::UTF8.GetBytes((Invoke-WebRequest
    http://169.254.169.254/latest/dynamic/instance-identity/document).Content)
   ```

4. Encontre o certificado público RSA-2048 para a sua região em Certificados públicos da AWS para assinaturas de documento de identidade da instância e adicione o conteúdo a um novo arquivo denominado `certificate.pem`.

5. Extraia o certificado do arquivo de certificado e armazene-o em uma variável chamada `$Store`.

   ```
   PS C:\> $Store =
    [Security.Cryptography.X509Certificates.X509Certificate2Collection]::new([Security.Cryptog
   Path certificate.pem)))
   ```

6. Verifique a assinatura.

   ```
   PS C:\> $SignatureDocument = [Security.Cryptography.Pkcs.SignedCms]::new()
   ```

   ```
   PS C:\> $SignatureDocument.Decode($Signature)
   ```

   ```
   PS C:\> $SignatureDocument.CheckSignature($Store, $true)
   ```

   Se a assinatura for válida, o comando não retornará nenhuma saída. Se não for possível verificar a assinatura, o comando retornará `Exception calling "CheckSignature" with "2" argument(s): "Cannot find the original signer`. Se não for possível verificar a assinatura, entre em contato com o AWS Support.

7. Valide o conteúdo do documento de identidade da instância.

```
PS C:
\> [Linq.Enumerable]::SequenceEqual($SignatureDocument.ContentInfo.Content, $Document)
```

Se o conteúdo do documento de identidade da instância for válido, o comando retornará `True`. Se o documento de identidade da instância não puder ser validado, entre em contato com o AWS Support.

Certificados públicos da AWS para assinaturas de documento de identidade da instância

Os seguintes certificados públicos da AWS podem ser usados para verificar o conteúdo do documento de identidade de uma instância, conforme descrito em Verificar documento de identidade da instância.

Certifique-se de usar o certificado correto para a sua região e para o procedimento de verificação que está sendo usado. Se você estiver verificando a assinatura PKCS7, use o certificado DSA. Se você estiver verificando a assinatura codificada em base64, use o certificado RSA. Se você estiver verificando a assinatura RSA-2048, use o certificado RSA-2048.

Expanda cada região abaixo para visualizar os certificados específicos da região.

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

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
```

```
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUE1y2NIKCU+Rg4uu4u32koG9QEYIwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE3MzQwMVoXDTI5MDQyODE3MzQwMVowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUE1y2NIKC
U+Rg4uu4u32koG9QEYIwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQAlxSmwcWnhT4uAeSinJuz+1BTcKhVSWb5jT8pYjQb8ZoZkXXRGb09mvYeU
NeqOBr27rvRAnaQ/9LUQf72+SahDFuS4CMI8nwowytqbmwquqFr4dxA/SDADyRiF
ea1UoMuNHTY49J/1vPomqsVn7mugTp+TbjqCfOJTpu0temHcFA==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJALFpzEAVWaQZMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTA4MTQw
ODU5MTJaGA8yMTk1MDExNzA4NTkxMlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAjS2vqZu9mEOhOq+0bRpAbCUiapbZMFNQqRg7kTlr7Cf+gDqXKpHPjsng
SfNz+JHQd8WPI+pmNs+q0Z2aTe23klmf2U52KH9/j1k8RlIbap/yFibFTSedmegX
E5r447GbJRsHUmuIIfZTZ/oRlpuIIO5/Vz7SOj22tdkdY2ADp7caZkNxhSP915fk
2jJMTBUOzyXUS2rBU/ulNHbTTeePjcEkvzVYPahD30TeQ+/A+uWUu89bHSQOJR8h
Um4cFApzZgN3aD5j2LrSMu2pctkQwf9CaWyVznqrsGYjYOY66LuFzSCXwqSnFBfv
fFBAFsjCgY24G2DoMyYkF3MyZlu+rwIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQUrynSPp4uqSECwy+PiO4qyJ8TWSkwgY4GA1UdIwSBhjCBg4AUrynS
```

```
Pp4uqSECwy+PiO4qyJ8TWSmhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJALFpzEAVWaQZMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBADW/s8lXijwdP6NkEoH1m9XLrvK4YTqkNfR6
er/uRRgTx2QjFcMNrx+g87gAml11z+D0crAZ5LbEhDMs+JtZYR3ty0HkDk6SJM85
haoJNAFF7EQ/zCp1EJRIkLLsC7bcDL/Eriv1swt78/BB4RnC9W9kSp/sxd5svJMg
N9a6FAplpNRsWAnbP8JBlAP93oJzblX2LQXgykTghMkQO7NaY5hg/H5o4dMPclTK
lYGqlFUCH6A2vdrxmpKDLmTn5//5pujdD2MN0df6sZWtxwZ0osljV4rDjm9Q3VpA
NWIsDEcp3GUB4proOR+C7PNkY+VGODitBOw09qBGosCBstwyEqY=
-----END CERTIFICATE-----
```

Leste dos EUA (Ohio): us-east-2

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUVJTc+hOU+8Gk3JlqsX438Dk5c58wDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE3MTE0OVoXDTI5MDQyODE3MTE0OVowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
```

```
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUVJTc+hOU
+8Gk3JlqsX438Dk5c58wEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQAywJQaVNWJqW0R0T0xVOSoN1GLk9x9kKEuN67RN9CLin4dA97qa7Mr5W4P
FZ6vnh5CjOhQBRXV9xJUeYSdqVItNAUFK/fEzDdjf1nUfPlQ3OJ49u6CV01NoJ9m
usvY9kWcV46dqn2bk2MyfTTgvmeqP8fiMRPxxnVRkSzlldP5Fg==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAM07oeX4xevdMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNjA2MTAx
MjU4MThaGA8yMTk1MTExNDEyNTgxOFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA6v6kGMnRmFDLxBEqXzP4npnL65OO0kmQ7w8YXQygSdmNIoScGSU5wfh9
mZdcvCxCdxgALFsFqPvH8fqiE9ttI0fEfuZvHOs8wUsIdKr0Zz0MjSx3cik4tKET
ch0EKfMnzKOgDBavraCDeX1rUDU0Rg7HFqNAOry3uqDmnqtk00XC9GenS3z/7ebJ
fIBEPAam5oYMVFpX6M6St77WdNE8wEU8SuerQughiMVx9kMB07imeVHBiELbMQ0N
lwSWRL/61fA02keGSTfSp/0m3u+lesf2VwVFhqIJs+JbsEscPxOkIRlzy8mGd/JV
ONb/DQpTedzUKLgXbw7KtO3HTG9iXQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQU2CTGYE5fTjx7gQXzdZSGPEWAJY4wgY4GA1UdIwSBhjCBg4AU2CTG
YE5fTjx7gQXzdZSGPEWAJY6hYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAM07oeX4xevdMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBANdqkIpVypr2PveqUsAKke1wKCOSuw1UmH9k
xX1/VRoHbrI/UznrXtPQOPMmHA2LKSTedwsJuorUn3cFH6qNs8ixBDrl8pZwfKOY
IBJcTFBbI1xBEFkZoO3wczzo5+8vPQ60RVqAaYb+iCa1HFJpccC3Ovajfa4GRdNb
n6FYnluIcDbmpcQePoVQwX7W3oOYLB1QLN7fE6H1j4TBIsFdO3OuKzmaifQlwLYt
DVxVCNDabpOr6Uozd5ASm4ihPPoEoKo7Ilp0fOT6fZ41U2xWA4+HF/89UoygZSo7
K+cQ90xGxJ+gmlYbLFR5rbJOLfjrgDAb2ogbFy8LzHo2ZtSe60M=
-----END CERTIFICATE-----
```

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

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUK2zmY9PUSTR7rc1k2OwPYu4+g7wwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE3MDI0M1oXDTI5MDQyODE3MDI0M1owXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUK2zmY9PU
STR7rc1k2OwPYu4+g7wwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQA1Ng4QmN4n7iPh5CnadSOc0ZfM7by0dBePwZJyGvOHdaw6P6E/vEk76KsC
Q8p+akuzVzVPkU4kBK/TRqLp19wEWoVwhhTaxHjQ1tTRHqXIVlrkw4JrtFbeNM21
GlkSLonuzmNZdivn9WuQYeGe7nUD4w3q9GgiF3CPorJe+UxtbA==
```

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

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJANNPkIpcyEtIMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTEwMjkw
OTAzMDdaGA8yMTk1MDQwMzA5MDMwN1owXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEApHQGvHvq3SVCzDrC7575BW7GWLzcj8CLqYcL3YY7Jffupz7OjcftO57Z
4fo5Pj0CaS8DtPzh8+8vdwUSMbiJ6cDd3ooio3MnCq6DwzmsY+pY7CiI3UVG7KcH
4TriDqr1Iii7nB5MiPJ8wTeAqX89T3SYaf6Vo+4GCb3LCDGvnkZ9TrGcz2CHkJsj
AIGwgopFpwhIjVYm7obmuIxSIUv+oNH0wXgDL029Zd98SnIYQd/njiqkzE+lvXgk
4h4Tu17xZIKBgFcTtWPky+POGu81DYFqiWVEyR2JKKm2/iR1dL1YsT39kbNg47xY
aR129sS4nB5Vw3TRQA2jL0ToTIxzhQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQUgepyiONs8j+q67dmcWu+mKKDa+gwgY4GA1UdIwSBhjCBg4AUgepy
iONs8j+q67dmcWu+mKKDa+ihYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJANNPkIpcyEtIMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAGLFWyutf1u0xcAc+kmnMPqtc/Q6b79VIX0E
tNoKMI2KR8lcV8ZElXDb0NC6v8UeLpe1WBKjaWQtEjL1ifKg9hdY9RJj4RXIDSK7
33qCQ8juF4vep2U5TTBd6hfWxt1Izi88xudjixmbpUU4YKr8UPbmixldYR+BEx0u
B1KJi9l1lxvuc/Igy/xeHOAZEjAXzVvHp8Bne33VVwMiMxWECZCiJxE4I7+Y6fqJ
pLLSFFJKbNaFyXlDiJ3kXyePEZSc1xiWeyRB2ZbTi5eu7vMG4i3AYWuFVLthaBgu
lPfHafJpj/JDcqt2vKUKfur5edQ6j1CGdxqqjawhOTEqcN8m7us=
-----END CERTIFICATE-----
```

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

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
```

```
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUFx8PxCkbHwpD31bOyCtyz3GclbgwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE3MjM1OVoXDTI5MDQyODE3MjM1OVowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUFx8PxCkb
HwpD31bOyCtyz3GclbgwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQBzOl+9Xy1+UsbUBI95HO9mbbdnuX+aMJXgG9uFZNjgNEbMcvx+h8P9IMko
z7PzFdheQQ1NLjsHH9mSR1SyC4m9ja6BsejH5nLBWyCdjfdP3muZM4O5+r7vUa1O
dWU+hP/T7DUrPAIVMOE7mpYa+WPWJrN6BlRwQkKQ7twm9kDalA==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJALZL3lrQCSTMMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTA4MTQw
OTAxMzJaGA8yMTk1MDExNzA5MDEzMlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA02Y59qtAA0a6uzo7nEQcnJ26OKF+LRPwZfixBH+EbEN/Fx0gYy1jpjCP
s5+VRNg6/WbfqAsV6X2VSjUKN59ZMnMY9ALA/Ipz0n00Huxj38EBZmX/NdNqKm7C
```

```
qWu1q5kmIvYjKGiadfboU8wLwLcHo8ywvfgI6FiGGsEO9VMC56E/hL6Cohko11LW
dizyvRcvg/IidazVkJQCN/4zC9PUOVyKdhW33jXy8BTg/QH927QuNk+ZzD7HH//y
tIYxDhR6TIZsSnRjz3bOcEHxt1nsidc65mY0ejQty4hy7ioSiapw316mdbtE+RTN
fcH9FPIFKQNBpiqfAW5Ebp3Lal3/+wIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQU7coQx8Qnd75qA9XotSWT3IhvJmowgY4GA1UdIwSBhjCBg4AU7coQ
x8Qnd75qA9XotSWT3IhvJmqhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJALZL3lrQCSTMMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAFZ1e2MnzRaXCaLwEC1pW/f0oRG8nHrlPZ9W
OYZEWbh+QanRgaikBNDtVTwARQcZm3z+HWSkaIx3cyb6vM0DSkZuiwzm1LJ9rDPc
aBm03SEt5v8mcc7sXWvgFjCnUpzosmky6JheCD4O1Cf8k0olZ93FQnTrbg62OK0h
83mGCDeVKU3hLH97FYoUq+3N/IliWFDhvibAYYKFJydZLhIdlCiiB99AM6Sg53rm
oukS3csyUxZyTU2hQfdjyo1nqW9yhvFAKjnnggiwxNKTTPZzstKW8+cnYwiiTwJN
QpVoZdt0SfbuNnmwRUMi+QbuccXweav29QeQ3ADqjgB0CZdSRKk=
-----END CERTIFICATE-----
```

África (Cidade do Cabo): af-south-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7DCCAqwCCQCncbCtQbjuyzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xOTA2MDQxMjQ4MDVaFw00
NTA2MDQxMjQ4MDVaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbYwggErBgcqhkjOOAQBMIIBHgKBgQC12Nr1gMrHcFSZ7S/A
pQBSCMHWmn2qeoQTMVWqe50fnTd0zGFxDdIjKxUK58/8zjWG5uR4TXRzmZpGpmXB
bSufAR6BGqud2LnT/HIWGJAsnX2uOtSyNfCoJigqwhea5w+CqZ6I7iBDdnB4TtTw
qO6TlnExHFVj8LMkylZgiaE1CQIVAIhdobse4K0QnbAhCL6R2euQzloXAoGAV/21
WUuMz/79Ga0JvQcz1FNy1sT0pU9rU4TenqLQIt5iccn/7EIfNtvVO5TZKulIKq7J
gXZr0x/KIT8zsNweetLOaGehPIYRMPX0vunMMR7hN7qA7W17WZv/76adywIsnDKq
ekfe15jinaX8MsKUdyDK7Y+ifCG4PVhoM4+W2XwDgYQAAoGAIxOKbVgwLxbn6Pi2
6hBOihFv16jKxAQI0hHzXJLV0Vyv9QwnqjJJRfOCy3dB0zicLXiIxeIdYfvqJr+u
hlN8rGxEZYYJjEUKMGvsc0DW85jonXz0bNfcP0aaKH0lKKVjL+OZi5n2kn9wgdo5
F3CVnMl8BUra8A1Tr2yrrE6TVZ4wCQYHKoZIzjgEAwMvADAsAhQfa7MCJZ+/TEY5
AUr0J4wm8VzjoAIUSYZVu2NdRJ/ERPmDfhW5EsjHlCA=
-----END CERTIFICATE-----
```

RSA

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

```
MIICNjCCAZ+gAwIBAgIJAKumfZiRrNvHMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xOTExMjcw
NzE0MDVaGA8yMTk5MDUwMjA3MTQwNVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKB
gQDFd571nUzVtke3rPyRkYfvs3jh0C0EMzzG72boyUNjnfw1+m0TeFraTLKb9T6F
7TuB/ZEN+vmlYqr2+5Va8U8qLbPF0bRH+FdaKjhgWZdYXxGzQzU3ioy5W5ZM1VyB
7iUsxEAlxsybC3ziPYaHI42UiTkQNahmoroNeqVyHNnBpQIDAQABMA0GCSqGSIb3
DQEBCwUAA4GBAAJLylWyElEgOpW4B1XPyRVD4pAds8Guw2+krgqkY0HxLCdjosuH
RytGDGN+q75aAoXzW5a7SGpxLxk6Hfv0xp3RjDHsoeP0i1d8MD3hAC5ezxS4oukK
s5gbPOnokhKTMPXbTdRn5ZifCbWlx+bYN/mTYKvxho7b5SVg2o1La9aK
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJAIFI+O5A6/ZIMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xOTA2MDQx
MjQ4MDRaGA8yMTk4MTEwNzEyNDgwNFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAy7/WHBBHOrk+20aumT07g8rxrSM0UXgki3eYgKauPCG4Xx//vwQbuZwI
oeVmR9nqnhfij2wOcQdbLandh0EGtbxerete3IoXzd1KXJb11PVmzrzyu5SPBPuP
iCeV4qdjjkXo2YWM6t9YQ911hcG96YSp89TBXFYUh3KLxfqAdTVhuC0NRGhXpyii
j/czo9njofHhqhTr7UEyPun8NVS2QWctLQ86N5zWR3Q0GRoVqqMrJs0cowHTrVw2
9Qr7QBjjBOVbyYmtYxm/DtiKprYV/e6bCAVok015X1sZDd3oCOQNoGlv5XbHJe2o
JFD8GRRy2rkWO/lNwVFDcwec6zC3QwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQCE
goqzjpCpmMgCpszFHwvRaSMbspKtK7wNImUjrSBOfBJsfFulyg1Zgn2nDCK7kQhx
jMJmNIvXbps3yMqQ2cHUkKcKf5t+WldfeT4Vk1Rz6HSA8sd0kgVcIesIaoy2aaXU
VEB/oQziRGyKdN1d4TGYVZXG44CkrzSDvlbmfiTq5tL+kAieznVF3bzHgPZW6hKP
EXC3G/IXrXicFEe6YyE1Rakl62VncYSXiGe/i2XvsiNH3Qlmnx5XS7W0SCN0oAxW
EH9twibauv82DVg1WOkQu8EwFw8hFde9X0Rkiu0qVcuU8lJgFEvPWMDFU5sGB6ZM
gkEKTzMvlZpPbBhg99Jl
-----END CERTIFICATE-----
```

Ásia-Pacífico (Hong Kong): ap-east-1

DSA

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

```
MIIC7zCCAq4CCQCO7MJe5Y3VLjAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xOTAyMDMwMjIxMjFaFw00
NTAyMDMwMjIxMjFaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbgwggEsBgcqhkjOOAQBMIIBHwKBgQDvQ9RzVvf4MAwGbqfX
blCvCoVb9957OkLGn/04CowHXJ+vTBR7eyIa6AoXltsQXBOmrJswToFKKxT4gbuw
jK7s9QQX4CmTRWcEgO2RXtZSVjOhsUQMh+yf7Ht4OVL97LWnNfGsX2cwjcRWHYgI
7lvnuBNBzLQHdSEwMNq0Bk76PwIVAMan6XIEEPnwr4e6u/RNnWBGKd9FAoGBAOCG
eSNmxpW4QFu4pIlAykm6EnTZKKHT87gdXkAkfoC5fAfOxxhnE2HezZHp9Ap2tMV5
8bWNvoPHvoKCQqwfm+OUBlAxC/3vqoVkKL2mG1KgUH9+hrtpMTkwO3RREnKe7I5O
x9qDimJpOihrL4I0dYvy9xUOoz+DzFAW8+ylWVYpA4GFAAKBgQDbnBAKSxWr9QHY
6Dt+EFdGz6lAZLedeBKpaP53Z1DTO34J0C55YbJTwBTFGqPtOLxnUVDlGiD6GbmC
80f3jvogPR1mSmGsydbNbZnbUEVWrRhe+y5zJ3g9qs/DWmDW0deEFvkhWVnLJkFJ
9pdOu/ibRPH1lE2nz6pK7GbOQtLyHTAJBgcqhkjOOAQDAzAAMC0CFQCoJlwGtJQC
cLoM4p/jtVFOj26xbgIUUS4pDKyHaG/eaygLTtFpFJqzWHc=
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICSzCCAbQCCQDtQvkVxRvK9TANBgkqhkiG9w0BAQsFADBqMQswCQYDVQQGEwJV
UzETMBEGA1UECBMKV2FzaGluZ3RvbjEQMA4GA1UEBxMHU2VhdHRsZTEYMBYGA1UE
ChMPQW1hem9uLmNvbSBJbmMuMRowGAYDVQQDExFlYzIuYW1hem9uYXdzLmNvbTAe
Fw0xOTAyMDMwMzAwMDZaFw0yOTAyMDIwMzAwMDZaMGoxCzAJBgNVBAYTAlVTMRMw
EQYDVQQIEwpXYXNoaW5ndG9uMRAwDgYDVQQHEwdTZWF0dGxlMRgwFgYDVQQKEw9B
bWF6b24uY29tIEluYy4xGjAYBgNVBAMTEWVjMi5hbWF6b25hd3MuY29tMIGfMA0G
CSqGSIb3DQEBAQUAA4GNADCBiQKBgQC1kkHXYTfc7gY5Q55JJhjTieHAgacaQkiR
Pity9QPDE3b+NXDh4UdP1xdIw73JcIIG3sG9RhWiXVCHh6KkuCTqJfPUknIKk8vs
M3RXflUpBe8Pf+P92pxqPMCz1Fr2NehS3JhhpkCZVGxxwLC5gaG0Lr4rFORubjYY
Rh84dK98VwIDAQABMA0GCSqGSIb3DQEBCwUAA4GBAA6xV9f0HMqXjPHuGILDyaNN
dKcvplNFwDTydVg32MNubAGnecoEBtUPtxBsLoVYXCOb+b5/ZMDubPF9tU/vSXuo
TpYM5Bq57gJzDRaBOntQbX9bgHiUxw6XZWaTS/6xjRJDT5p3S1E0mPI3lP/eJv4o
Ezk5zb3eIf10/sqt4756
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJAMoxixvs3YssMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xODA3MjAw
ODQ0NDRaGA8yMTk3MTIyMzA4NDQ0NFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
```

```
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA4T1PNsOg0FDrGlWePoHeOSmOJTA3HCRy5LSbYD33GFU2eBrOIxoU/+SM
rInKu3GghAMfH7WxPW3etIAZiyTDDU5RLcUq2Qwdr/ZpXAWpYocNc/CEmBFtfbxF
z4uwBIN3/drM0RSbe/wP9EcgmNUGQMMZWeAji8sMtwpOblNWAP9BniUG0Flcz6Dp
uPovwDTLdAYT3TyhzlohKL3f6O48TR5yTaV+3Ran2SGRhyJjfh3FRpP4VC+z5LnT
WPQHN74Kdq35UgrUxNhJraMGCzznolUuoR/tFMwR93401GsM9fVA7SW3jjCGF81z
PSzjy+ArKyQqIpLW1YGWDFk3sf08FQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQDK
2/+C3nPMgtyOFX/I3Cyk+Pui44IgOwCsIdNGwuJysdqp5VIfnjegEu2zIMWJSKGO
lMZoQXjffkVZZ97J7RNDW06oB7kj3WVE8a7U4WEOfnO/CbMUf/x99CckNDwpjgW+
K8V8SzAsQDvYZs2KaE+18GFfLVF1TGUYK2rPSZMHyX+v/TIlc/qUceBycrIQ/kke
jDFsihUMLqgmOV2hXKUpIsmiWMGrFQV4AeV0iXP8L/ZhcepLf1t5SbsGdUA3AUY1
3If8s81uTheiQjwY5t9nM0SY/1Th/tL3+RaEI79VNEVfG1FQ8mgqCK0ar4m0oZJl
tmmEJM7xeURdpBBx36Di
-----END CERTIFICATE-----
```

Ásia-Pacífico (Hyderabad): ap-south-2

DSA

```
-----BEGIN CERTIFICATE-----
MIIC8DCCArCgAwIBAgIGAXjrQ4+XMAkGByqGSM44BAMwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgMEFdhc2hpbmd0b24g
U4EddRIpUt9KnC7s5Of2EbdSPO9EAMMeP4C2USZpRV1AIlH7WT2NWPq/
xfW6MPbLm1Vs14E7gB00b/JmYLdrmVClpJ+f6AR7ECLCT7up1/63xhv4O1fnxqimFQ8E
+4P208UewwI1VBNaFpEy9nXzrith1yrv8iIDGZ3RSAHHAhUAl2BQjxUjC8yykrmCouuEC/
BYHPUCgYEA9+GghdabPd7LvKtcNrhXuXmUr7v6OuqC+VdMCz0HgmdRWVeOutRZT
+ZxBxCBgLRJFnEj6EwoFhO3zwkyjMim4TwWeotUfI0o4KOuHiuzpnWRbqN/C/ohNWLx
+2J6ASQ7zKTxvqhRkImog9/
hWuWfBpKLZl6Ae1UlZAFMO/7PSSoDgYUAAoGBAJCKGBBoxIUxqBk94JHhwZZbgvbP0DAOoHENQWxp/98lI7/
YOfYJOVMJS22aCnHDurofmo5rvNIkgXi7Rztbhu
+lko9rK6DgpmpUwBU0WZtf34aZ2IWNBwHaVhHvWAQf9/46u18dMa2YucK1Wi+Vc+M
+KldrvgXmhym6ErNlzhJyMAkGByqGSM44BAMDLwAwLAIUaaPKxaOHoYvwz709xXpsQueIq+UCFFa/
GpzoDOSokl1057NU/2hnsiW4
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICMzCCAZygAwIBAgIGAXjwLj9CMA0GCSqGSIb3DQEBBQUAMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIDBBXYXNoaW5n
+sFcobrjvcAYm0PNRD8f4R1jAzvoLt2+qGeOTAyO1Httj6cmsYN3AP1hN5iYuppFiYsl2eNPa/
CD0Vg0BAfDFlV5rzjpA0j7TJabVh4kj7JvtD+xYMi6wEQA4x6SPONY4OeZ2+8o/
```

```
HS8nucpWDVdPRO6ciWUlMhjmDmwIDAQABMA0GCSqGSIb3DQEBBQUAA4GBAAy6sgTdRkTqELHBeWj69q60xHyUmsWqHAQ
TGGbYP0yP2qfMl0cCImzRI5W0gn8gogdervfeT7nH5ih0TWEy/QDWfkQ601L4erm4yh4YQq8vcqAPSkf04N
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAIVWfPw/X82fMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yMjA3MDQx
NDMwMjhaGA8yMjAxMTIwODE0MzAyOFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAg29QEFriG+qFEjYW/v62nN70lMJY/Hevx5TtmU/VIYBPQa3HUGTBAbbI
2Tmy8UMpa8kZeaYeI3RAfiQWt0Ws7wUrBuO2Pdp518WDPaJUH7RWEuu1BDDkyZRW
NAMNPCn3ph7Od243IFcLGku7HVekel5poqRpSfojrMasjlf+CvixUeAJbmFoxUHK
kh5unzG2sZyO4wHXcJPQkRf5a8zSTPe9YZP1kXPPEv4p/jTSggaYPxXyS6QVaTlV
zLeLFZ0fesLPMeil3KYQtV7IKLQiEA2F6dxWnxNWQlyMHtdq6PucfEmVx17i/Xza
yNBRo0azY8WUNVkEXrRhp/pU8Nh3GQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQU9AO1aZk9RLXk2ZvRVoUxYvQy9uwwgY4GA1UdIwSBhjCBg4AU9AO1
aZk9RLXk2ZvRVoUxYvQy9uyhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAIVWfPw/X82fMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBADexluMRQRftqViahCnauEWGdMvLCBr8A+Yr
6hJq0guoxEk/lahxR137DnfMPuSbi1Rx5QKo7oBrWfG/zsgQUnF2IwHTzwD+i/2m
XCane6FiS5RpK3lGdILq8ZmlhQk+6iI8yoZLr0LCfTh+CLgIKHOknfR5lFzgzAiF
SI8/Q9mm+uvYtSTZECI6Zh57QZPoETAG/yl+9jiOy2lAelqa/k1i+Qo8gMfOc+Pm
dwY7o6fV+oucgRlsdey6VM45LeyILQqv0RXtVzjuowanzmCCFMjgqiO9oZAWu4Oh
+F3unijELo01vZJs8s2N3KGlo3/jtUFTX6RTKShZlAPLwBi5GMI=
-----END CERTIFICATE-----
```

Ásia-Pacífico (Jacarta): ap-southeast-3

DSA

```
-----BEGIN CERTIFICATE-----
MIIC8DCCArCgAwIBAgIGAXbVDEikMAkGByqGSM44BAMwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgMEFdhc2hpbmd0b24g
U4EddRIpUt9KnC7s5Of2EbdSPO9EAMMeP4C2USZpRV1AIlH7WT2NWPq/
xfW6MPbLm1Vs14E7gB00b/JmYLdrmVClpJ+f6AR7ECLCT7up1/63xhv4O1fnxqimFQ8E
+4P208UewwI1VBNaFpEy9nXzrith1yrv8iIDGZ3RSAHHAhUAl2BQjxUjC8yykrmCouuEC/
BYHPUCgYEA9+GghdabPd7LvKtcNrhXuXmUr7v6OuqC+VdMCz0HgmdRWVeOutRZT
+ZxBxCBgLRJFnEj6EwoFhO3zwkyjMim4TwWeotUfI0o4KOuHiuzpnWRbqN/C/ohNWLx
```

```
+2J6ASQ7zKTxvqhRkImog9/
hWuWfBpKLZl6Ae1UlZAFMO/7PSSoDgYUAAoGBAPjuiEx05N3JQ6cVwntJie67D8OuNo4jGRn
+crEtL7YO0jSVB9zGE1ga
+UgRPIaYETL293S8rTJTVgXAqdpBwfaHC6NUzre8U8iJ8FMNnlP9Gw1oUIlgQBjORyynVJexoB31TDZM
+/52g9O/bpq1QqNyKbeIgyBBlc1dAtr1QLnsMAkGByqGSM44BAMDLwAwLAIUK8E6RDIRtwK+9qnaTOBhvO/
njuQCFFocyT1OxK+UDR888oNsdgtif2Sf
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICMzCCAZygAwIBAgIGAXbVDG2yMA0GCSqGSIb3DQEBBQUAMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIDBBXYXNoaW5n
Vbt0gQ1ebWcur2hSO7PnJifE4OPxQ7RgSAlc4/spJp1sDP+ZrS0LO1ZJfKhXf1R9S3AUwLnsc7b
+IuVXdY5LK9RKqu64nyXP5dx170zoL8loEyCSuRR2fs+04i2QsWBVP+KFNAn7P5L1EHRjkgTO8kjNKviwRV
+OkP9ab5wIDAQABMA0GCSqGSIb3DQEBBQUAA4GBAI4WUy6+DKh0JDSzQEZNyBgNlSoSuC2owtMxCwGB6nBfzzfcekWvs
+87w/g9lNwUnUt0ZHYyh2tuBG6hVJuUEwDJ/z3wDd6wQviLOTF3MITawt9P8siR1hXqLJNxpjRQFZrgHqi
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAMtdyRcH51j9MA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yMjA0MDgx
MjM5MTZaGA8yMjAxMDkxMjEyMzkxNlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAvUsKCxoH6KXRYJLeYTWAQfaBQeCwhJaR56mfUeFHJE4g8aFjWkiN4uc1
TvOyYNnIZKTHWmzmulmdinWNbwP0GiROHb/i7ro0Hhvnptyyc Gt8ag8affiIbx5X
7ohdwSN2KJ6G0IKflIx7f2NEI0oAMM/9k+T1eVF+MVWzpZoiDp8frLNkqp8+RAgz
ScZsbRfwv3u/if5xJAvdg2nCkIWDMSHEVPoz0lJo7v0ZuDtWWsL1LHnL5ozvsKEk
+ZJyEi23r+U1hIT1NTBdp4yoigNQexedtwCSr7q36oOdDwvZpqYlkLi3uxZ4ta+a
01pzOSTwMLgQZSbKWQrpMvsIAPrxoQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQU1GgnGdNpbnL3lLF30Jomg7Ji9hYwgY4GA1UdIwSBhjCBg4AU1Ggn
GdNpbnL3lLF30Jomg7Ji9hahYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAMtdyRcH51j9MBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBACVl00qQlatBKVeiWMrhpczsJroxDxlZTOba
6wTMZk7c3akb6XMOSZFbGaifkebPZqTHEhDlrClM2j9AIlYcCx6YCrTf4cuhn2mD
gcJN33143eOWSaeRY3ee4j+V9ne98y3kO2wLz95VrRgclPFR8po2iWGzGhwUi+FG
q8dXeCH3N0DZgQsSgQWwmdNQXZZej6RHLU/8In5trHKLY0ppnLBjn/UZQbeTyW5q
RJB3GaveXjfgFUWj2qOcDuRGaikdS+dYaLsi5z9cA3FolHzWxx9MOs8io8vKqQzV
XUrLTNWwuhZy88cOlqGPxnoRbw7TmifwPw/cunNrsjUUOgs6ZTk=
```

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

Ásia-Pacífico (Malásia): ap-southeast-5

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7zCCAq4CCQC5X6U+vgoLEDAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yNDAxMDMxMjU3NTRaGA8y
MDUwMDEwMzEyNTc1NFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0
b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIg
U2VydmljZXMgTExDMIIBtjCCASsGByqGSM44BAEwggEeAoGBAIzEMPCIPFfOYCg4
BCjKGyl60wOfmwHPzSOXZ3Z2wS/LYNHUtHGwtVNePSTyCu/CuZF6gC9n/wBORtQp
+SSkn+weGc/BmUA1mp/vrN7v+aSCgKJoO+sgpa1PPOgNvUaMw6O5odsZWQCMSjkU
6RTo/PL2v/tMfiCocF4ghvyRC6hvAhUA0VoObKC2IXzXgVvRRupo4qHbcm8CgYAe
bbNuawh3rAxkFvUs9FPzW5E+xllG16Z//61PENKqonmk+zBiBdiIlS1F6ZqmTqkI
z5+qfSt1m3pb3j2W0NT7lEDFvy8Gr6Y2vohCHmL+T1u1Yy4PeqbgrFwcen7y7WoO
/KCV7Y9/ODQMMyuAzT3h5wJNweT7L5MUN8JYpZSi3QOBhAACgYBqaDuG2u6V91Qj
K2wEAElxaaRaNo/ewg/wWDmHYqoeHOR0HfuFCYgASE9f7ULqYtX1VURcgcjw9XN4
BDmPilXvfi04INPTnw4IxFJKDzzC0kVH7esVas982Po8v3megH32H9Rl87r7UG1c
ZEbkSkKVX6YKYg1PR3rfjXgdwVZv/zAJBgcqhkjOOAQDAzAAMC0CFFWeRe2fYW2i
6mMd26Wzbx87Y0DXAhUAoPCnF+5hGJw0jT9aL7QsgcfLi9Y=
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICNjCCAZ+gAwIBAgIJAMuBl6rhZCJKMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yNDAxMDMx
MjU3NTRaGA8yMjAzMDYwOTEyNTc1NFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKB
gQDFuKydxZsordNH7bLwIluEGOkX7/CdLdpeqkDKEhQkFwzpRxaX4EAlkGh2/o7D
8qneC9cGQhqSG5WVVBrmZG7sfkFOM4m1AtY++kfv+MYto1VFgLk1xJbkpq1r4YeQ
Ul+ZsJYsZpyX/t+g8s7rW0OVcBsYx4L75bf34z38mwK8PQIDAQABMA0GCSqGSIb3
DQEBCwUAA4GBADD9C4pWL8RUvF1CJW8kExj35xmozlFlmrKs8Zpi8+Eg6q+W9dgd
xMdH95tgZtmVMDqlvVR+DK0iO1BNpqPjrqWkk2tTLivpS+sGzCE/jCl18Q28Rk71
/A3gLD7Rtbq5TKNvuFCHwYMjrTDHI6aBjIaAlDm4e2/j/OxVtHyZGTre
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJANC3xtbPhQ2GMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yNDAxMDMx
MjU3NTRaGA8yMjAzMDYwOTEyNTc1NFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAt3aMy7Hsp4ySG3mlfi+pdTcZw6H6XNU1Y36fNdi4c+MzinQQbnqMPyt7
QLgU+XCWmcWsVo7GQF6n9N01Rh+UXXUZU4jcXlFocQPCWf9O+IIIPXkd67kFMUV
HAxCELjfxHbC+I8e7dwOJhmdF4Bfi52Ty8zz0HdE8JDypPkTDlXuGvTgDyW7NP56
I/vlQaXLoYSbcQe5pv2a9gyBaaCM1QoeqwAHAeCNXb9Nuj9ZX3GHGJb3TuqAeKCD
5i9TscCB9XjY6Fx+zfSAobjBZwgLEtLOwJhbZnKmx4gJMaaNFipAjVT2FSS3+yev
eTYBoa1dvhk0ivQyQIPpHmihrmkWuwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQBC
fdgyI8GjmCqiHAlh+L1bj0LdNql9zl7RXmOEzsuRdtdMumkxYXX88UtROy3fdi1i
VaEwHdAK8ThzRkesgHza/cXzqCMewaYxujSI6p6G7x99FFeGif1x0FJdj8AoeTL7
4h9bmS/6l4/NL7DJI9G7ovES/hoUA9v9TDhv+vauxXlgfrp0MPecprxBYlrc+DH2
adGCdKCp2lQ2YDKOD9TCEjYIli8XSoyevoWHUjfDYrCrCp8l4s/p7HOgYr8fJBAs
EuVy8211LVz1/X4EMBRNtNjXK9sklsxAOX14NDfBFSS0toxl3K6Tf9t/PviBl95d
hncyDAcFgDCK4w8LLlVW
-----END CERTIFICATE-----
```

Ásia-Pacífico (Melbourne): ap-southeast-4

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7zCCAq
+gAwIBAgIGAXjWF7P2MAkGByqGSM44BAMwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgMEFdhc2hpbmd0b24gU3RhdGUxED
U4EddRIpUt9KnC7s5Of2EbdSPO9EAMMeP4C2USZpRV1AIlH7WT2NWPq/
xfW6MPbLm1Vs14E7gB00b/JmYLdrmVClpJ+f6AR7ECLCT7up1/63xhv4O1fnxqimFQ8E
+4P208UewwI1VBNaFpEy9nXzrith1yrv8iIDGZ3RSAHHAhUAl2BQjxUjC8yykrmCouuEC/
BYHPUCgYEA9+GghdabPd7LvKtcNrhXuXmUr7v6OuqC+VdMCz0HgmdRWVeOutRZT
+ZxBxCBgLRJFnEj6EwoFhO3zwkyjMim4TwWeotUfI0o4KOuHiuzpnWRbqN/C/ohNWLx
+2J6ASQ7zKTxvqhRkImog9/
hWuWfBpKLZl6Ae1UlZAFMO/7PSSoDgYQAAoGAPRXSsQP9E3dw8QXKlrgBgEVCprLHdK/bbrMas0XMu1EhOD
+q
+0PcTr8+iwbtoXlY5MCeatWIp1GrXQjVqsF8vQqxlEuRuYKbR3nq4mWwaeGlx9AG5EjQHRa3GQ44wWHOdof0M3NRI1MP
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICMzCCAZygAwIBAgIGAXjSh40SMA0GCSqGSIb3DQEBBQUAMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIDBBXYXNoaW5n
+qWTGAbGsPeMX4hBMjAJUKys2NIRcRZaLM/BCew2FIPVjNtlaj6Gwn9ipU4Mlz3zIwAMWi1AvGMSreppt
+wV6MRtfOjh0Dvj/veJe88aEZJMozNgkJFRS
+WFWsckQeL56tf6kY6QTlNo8V/0CsQIDAQABMA0GCSqGSIb3DQEBBQUAA4GBAF7vpPghH0FRo5gu49EArRNPrIvW1egM
wcgkqIwwuXYj+1rhlL+/
iMpQWjdVGEqIZSeXn5fLmdx50eegFCwND837r9e8XYTiQS143Sxt9+Yi6BZ7U7YD8kK9NBWoJxFqUeHdpRCs0O7COjT3
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAN4GTQ64zVs8MA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yMjA3MTMx
MzMzMDBaGA8yMjAxMTIxNzEzMzMwMFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA2BYgeCr+Rk/jIAEDOHS7wJql62vc83QEwjuzk0qOFEReIZzlN1fBRNXK
g0T178Kd3gLYcE59wEFbTe/X5yOA1Lo95x1anSAo7R+Cisf9C2HQuJp+gVb+zx71
lniPF7gHziGpm0M8DdAU/IW+wkZwGbP4z7Hq9+bJ0P2ltvPJ5yxSgkFuDsI9VBHa
CLoprHsCHh2VdP8KcMgQQMmHe1NmBpyTk0ul/aLmQkCQEX6ZIRGOeq228fwlh/t+
Ho+jv87duihVKic6MrL32SlD+maX0LSDUydWdaOLLTGkh7oV7+bFuH6msrXUu+Ur
ZEP1r/MidCWMhfgrFzeTBzOHA97qxQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQUcHMd1cHqzmsQ5hpUK3EMLhHdsi4wgY4GA1UdIwSBhjCBg4AUcHMd
1cHqzmsQ5hpUK3EMLhHdsi6hYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAN4GTQ64zVs8MBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAI4PFyVN+7EGSObioiPnv0LL0f70SSzUZJ8p
XO90d4rWea7jIbgZ2AKb+ErynkU9xVg7XQQ5k6KDWgp/4jYFL2dqnt/YAY4PS0un
RSrYElawxLT0BcLn4rcSDC79vQe1xGC5//wDdV6b399COAHRAK6axWYy5w32u9PL
uw0cIp3Ch8JoNwcgTHKRRGzePmBeR4PNqhHTArG4/dJk6/aUO4OpX0WzI6L67CGY
6Nex3dau+gkLCK93dTEkrXtyXHu4wB0J9zd1w+iQ0SEa9eKc78/NjEsF/FZdGrWC
t57lIMOOXJhQ1kRgSwNeZdQWV1dRakvO6sfcvVYkfj1wAvZvvAw=
-----END CERTIFICATE-----
```

Ásia-Pacífico (Mumbai): ap-south-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUDLA+x6tTAP3LRTr0z6nOxfsozdMwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE0MTMwMVoXDTI5MDQyODE0MTMwMVowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIEExMQ4IUDLA+x6tT
AP3LRTr0z6nOxfsozdMwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQAZ7rYKoAwwiiH1M5GJbrT/BEk3OO2VrEPw8ZxgpqQ/EKlzMlOs/0Cyrmp7
UYyUgYFQe5nq37Z94rOUSeMgv/WRxaMwrLlLqD78cuF9DSkXaZIX/kECtVaUnjk8
BZx0QhoIHOpQocJUSlm/dLeMuE0+0A3HNR6JVktGsUdv9ulmKw==
```

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

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJAPRYyD8TtmC0MA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNjAzMDcx
MDQ1MDFaGA8yMTk1MDgxMTEwNDUwMVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA0LSS5I/eCT2PM0+qusorBx67QL26BIWQHd/yF6ARtHBb/1DdFLRqE5Dj
07Xw7eENC+T79mOxOAbeWg91KaODOzw6i9I/2/HpK0+NDEdD6sPKDA1d45jRra+v
CqAjI+nV9Vw91wv7HjMk3RcjWGziM8/hw+3YNIutt7aQzZRwIWlBpcqx3/AFd8Eu
2UsRMSHgkGUW6UzUF+h/U8218XfrauKNGmNKDYUhtmyBrHT+k6J0hQ4pN7fe6h+Z
w9RVHm24BGhlLxLHLmsOIxvbrF277uX9Dxu1HfKfu5D2kimTY7xSZDNLR2dt+kNY
/+iWdIeEFpPT0PLSILt52wP6stF+3QIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQBI
E6w+WWC2gCfoJO6c9HMyGLMFEpqZmz1n5IcQt1h9iyO7Vkm1wkJiZsMhXpk73zXf
TPxuXEacTX3SOEa07OIMCFwkusO5f6leOyFTynHCzBgZ3U0UkRVZA3WcpbNB6Dwy
h7ysVlqyT9WZd7EOYm5j5oue2G2xdei+6etgn5UjyWm6liZGrcOF6WPTdmzqa6WG
ApEqanpkQd/HM+hUYex/ZS6zEhd4CCDLgYkIjlrFbFb3pJ1OVLztIfSN5J4Oolpu
JVCfIq5u1NkpzL7ys/Ub8eYipbzI6P+yxXiUSuF0v9b98ymczMYjrSQXIf1e8In3
OP2CclCHoZ8XDQcvvKAh
-----END CERTIFICATE-----
```

Ásia-Pacífico (Nova Zelândia): ap-southeast-6

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7zCCAq4CCQCcP+D4eLFOajAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yNDEyMDMxMjEzMDZaGA8y
MDUwMTIwNDEyMTMwNlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0
b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIg
U2VydmljZXMgTExDMIIBtjCCASsGByqGSM44BAEwggEeAoGBANBMmM/LbAX13IeB
3yr2pMMpiTW1b1go/axNLfcxEmj0fThKk8y0FAT1frN/UPdI9qRInsyBdEZQLiIH
4WHCXk8IidQLh4DED3G9DvSFFC4Gb8ax+UIQY11wfHPWO4+wA9q8liYTg/FxdJMM
tZS9tZAZxjH6+8yfV8Bt0wUd2Y+lAhUAwg0CxCmZPinHtKbFnpMQfKnzjCMCgYAf
i+D7nGVFOWJ8EYOpRYbG0pHkrpwNy+h01csn6IAwQbIfeOG+SF4N3LeuOAC9vXGY
VGh9XNxuasvqkRAzgRmJ/EYM5Xa/YN62EhddRuN8wCOg66MeczUDh3RTb+Tu6HK0
UR6oTSOQ6rxA5aA1qTc7TqI0+pRZv+QYIZK/ozsZzgOBhAACgYAbVm+rOX8J38cG
```

```
LxKjUXVM0KB69SksGLEqjO4ps80EcZ/0W3g1hGLnSX/RjYfAS60hbKK1GX9PpcaO
4mDzCTm3dZ6shbae5t8bBU+mUi8BmaK+Pdu3z5J77y4zv22/yXte8ulZ5J0zKP9K
QP3p3pa7XI9NaXpKGT3yZsJ0BWY2xTAJBgcqhkjOOAQDAzAAMC0CFBs4KQmrxHjQ
OHh0r8JqB8UiwlutAhUAwgxid7wT6FNm8Zwq9hioQ2v2K0A=
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICNjCCAZ+gAwIBAgIJAMwLuv2/tk9eMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yNDEyMDMx
MjEzMDZaGA8yMjA0MDUwOTEyMTMwNlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKB
gQC9AsBNOUfT8QpguHqMa9KIXP/YgZOmfRAgEmnLawXTC+40bXUq/fwkx+cebv3x
CvUx6d07/iDlD0dm2Hf2HhPFi3OaCI7vc8c3lqVBvcn6yzmwv35aSEvtVm2NHC3j
4/q6vN2tR2d4a1Mf1QhmOVOJ7XiTEbCy2Yv+pmDbk29V6QIDAQABMA0GCSqGSIb3
DQEBCwUAA4GBAHatyQIy612kio8neI4r5VBg8pgKwW+mFGpAzOQ2NOyLCNoOeD1D
lPRaSipBN7WW6jpIozbz7JG7Kqc3N+piPGGzfjH9gZjqUqfOGrNHB5nsxvMHI2iL
e+DwsOcV7qnEVRgYbmLYOVKJv25wCsM/Tcn/6f6scEX2x+H0hAh7rwiP
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJAI/xUfWwSQOtMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yNDEyMDMx
MjEzMDZaGA8yMjA0MDUwOTEyMTMwNlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEArbid9Tnunu0pWCQUqZCkGeiF8hWixi+LBS1AOew2UsT9keAt2rXXGlU/
wSMriKHsvcrfKtuVKj5chArsOyFvagszH5lIKhI+GfWVQEd2aZiOvAJ+iRUQq1+R
gOr2gyjWlf3znZXTcyhHcJoXDhbn5e+kEa3pwS4yKNRpM3P61V4M2702xis08hjP
qMDxwXMa1Fiy4b7nAyNQifgrwb3bCA5k5prmkl/iajaWa1zMMFgLI9vA6UwUSbTK
H9iOuL/xNfMX+Xzq4CCaQYiJ8zdi56kqnB/lrA05NSjOPLskg6sUGkyiDxGK4gzC
DFrO6oygcdlBaxnyAECGdJcOM6TOmwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQBg
8yVPNpctrvSvTazf/Ij8qC6+q6df1SptdYKQkOYWeUVZR7+3uTZ9Yiyq+Bh8Hbyf
NcR0eR6UqhgiB3p5slYNhTvLkpuMuqTpVJFvQtzZycnmKXAQ35G5zCYV0+pkF59L
ch26SukWk0+VP3kIM9VmaIZQKJEBlBLcnbDZyXlHUDnZAYPcxxKQ8uFPkW0GOFMr
ekFCGOUmFSItFXOHy5hD2xmctKNk3l12m6cKydYvONtk/3DovKNnw3c5k40WHQW/
Zdh/LWd4/Jrkan+kQnqm4rkrXF+x3aF0qrKTtHMICvpkZ8g7/588hBs4mZnCmFLa
```

```
q/g9WqIcd9SMmBkT6KZ8
-----END CERTIFICATE-----
```

Asia Pacific (Osaka): ap-northeast-3

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUHTRhxHhBZFOGvTFKxHoy9+f5Hl8wDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE2NTQwN1oXDTI5MDQyODE2NTQwN1owXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUHTRhxHhB
```

```
ZFOGvTFKxHoy9+f5Hl8wEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQAUZx7DcYbhWNTD4BNGhr5beruT2OUoGHH9J73UKxwdqeb9bH1LIWhIZO0X
/1mjn3bWBgCwfoS8gjZwsVB6fZbNBRy8urdBZJ87xF/4JPBjt7S9oGx/zthDUYrC
yK0Y0v4G0PgiS81CvYLg09LpmYhLSJbXENlkC04v5yxdKxZxyg==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJAMn1yPk22ditMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNzA3MTkx
MTEyNThaGA8yMTk2MTIyMjExMTI1OFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEArznEYef8IjhrJoazI0QGZkmlmHm/4rEbyQbMNifxjsDE8YWtHNwaM91z
zmyK6Sk/tKlWxcnl3g31iq305ziyFPEewe5Qbwf1iz2cMsvfNBcTh/E6u+mBPH3J
gvGanqUJt6c4IbipdEouIjjnynyVWd4D6erLl/ENijeR1OxVpaqSW5SBK7jms49E
pw3wtbchEl3qsE42Ip4IYmWxqjgaxB7vps91n4kfyzAjUmklcqTfMfPCkzmJCRgp
Vh1C79vRQhmriVKD6BXwfZ8tG3a7mijeDn7kTsQzgO07Z2SAE63PIO48JK8HcObH
tXORUQ/XF1jzi/SIaUJZT7kq3kWl8wIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQBj
ThtO9dLvU2QmKuXAhxXjsIdlQgGG3ZGh/Vke4If1ymgLx95v2Vj9Moxk+gJuUSRL
BzFte3TT6b3jPolbECgmAorjj8NxjC17N8QAAI1d0S0gI8kqkG7V8iRyPIFekv+M
pcai1+cIv5IV5qAz8QOMGYfGdYkcoBjsgiyvMJu/2N2UbZJNGWvcEGkdjGJUYYOO
NaspCAFm+6HA/K7BD9zXB1IKsprLgqhiIUgEaW3UFEbThJT+z8UfHG9fQjzzfN/J
nT6vuY/0RRu1xAZPyh2gr5okN/s6rnmh2zmBHU1n8cbCc64MVfXe2g3EZ9Glq/9n
izPrI09hMypJDP04ugQc
-----END CERTIFICATE-----
```

Ásia-Pacífico (Seul): ap-northeast-2

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
```

```
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUbBSn2UIO6vYk4iNWV0RPxJJtHlgwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTEzMzg0NloXDTI5MDQyODEzMzg0NlowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUbBSn2UIO
6vYk4iNWV0RPxJJtHlgwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQAmjTjalG8MGLqWTC2uYqEM8nzI3px1eo0ArvFRsyqQ3fgmWcQpxExqUqRy
l3+2134Kv8dFab04Gut5wlfRtc2OwPKKicmv/IXGN+9bKFnQFjTqif08NIzrDZch
aFT/uvxrIiM+oN2YsHq66GUhO2+xVRXDXVxM/VObFgPERbJpyA==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJANuCgCcHtOJhMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTA5MTQx
NTU3NDRaGA8yMTk1MDIxNzE1NTc0NFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA66iNv6pJPmGM20W8HbVYJSlKcAg2vUGx8xeAbzZIQdpGfkabVcUHGB6m
Gy59VXDMDlrJckDDk6dxUOhmcX9z785TtVZURq1fua9QosdbTzX4kAgHGdp4xQEs
```

```
mO6QZqg5qKjBP6xr3+PshfQ1rB8Bmwg0gXEm22CC7o77+7N7Mu2sWzWbiUR7vil4
9FjWS8XmMNwFTlShp4l1TDTevDWW/uYmC30RThM9S4QPvTZ0rAS18hHVam8BCTxa
LHaVCH/Yy52rsz0hM/FlghnSnK105ZKj+b+KIp3adBL8OMCjgc/Pxi0+j3HQLdYE
32+FaXWU84D2iP2gDT28evnstzuYTQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQC1
mA4q+12pxy7By6g3nBk1s34PmWikNRJBwOqhF8ucGRv8aiNhRRye9lokcXomwo8r
KHbbqvtK85l0xUZp/Cx4sm4aTgcMvfJP29jGLclDzeqADIvkWEJ4+xncxSYVlS9x
+78TvF/+8h9U2LnSl64PXaKdxHy2IsHIVRN4GtoaP2Xhpa1S0M328Jykq/571nfN
1WRD1c/fQf1edgzRjhQ4whcAhv7WRRF+qTbfQJ/vDxy8lkiOsvU9XzUaZ0fZSfXX
wXxZamQbONvFcxVHY/0PSiM8nQoUmkkBQuKleDwRWvkoJKYKyr3jvXK7HIWtMrO4
jmXe0aMy3thyK6g5sJVg
-----END CERTIFICATE-----
```

Ásia-Pacífico (Singapura): ap-southeast-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUSqP6ih+++5KF07NXngrWf26mhSUwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE0MzAxNFoXDTI5MDQyODE0MzAxNFowXDELMAkGA1UEBhMCVVMx
```

```
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUSqP6ih++
+5KF07NXngrWf26mhSUwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQAw13BxW11U/JL58j//Fmk7qqtrZTqXmaz1qm2WlIpJpW750MOcP4ux1uPy
eM0RdVZ4jHSMv5gtLAv/PjExBfw9n6vNCk+5GZG4Xec5DoapBZHXmfMo93sjxBFP
4x9rWn0GuwAVO9ukjYPevq2Rerilrq5VvppHtbATVNY2qecXDA==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAJVMGw5SHkcvMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTEwMjkw
ODU3MTlaGA8yMTk1MDQwMzA4NTcxOVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAlaSSLfBl7OgmikjLReHuNhVuvM20dCsVzptUyRbut+KmIEEc24wd/xVy
2RMIrydGedkW4tUjkUyOyfET5OAyT43jTzDPHZTkRSVkYjBdcYbe9o/0Q4P7IVS3
XlvwrUu0qo9nSID0mxMnOoF1l8KAqnn10tQ0W+lNSTkasW7QVzcb+3okPEVhPAOq
MnlY3vkMQGI8zX4iOKbEcSVIzf6wuIffXMGHVC/JjwihJ2USQ8fq6oy686g54P4w
ROg415kLYcodjqThmGJPNUpAZ7MOc5Z4pymFuCHgNAZNvjhZDA842Ojecqm62zcm
Tzh/pNMNeGCRYq2EQX0aQtYOIj7bOQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQU6SSB+3qALorPMVNjToM1Bj3oJMswgY4GA1UdIwSBhjCBg4AU6SSB
+3qALorPMVNjToM1Bj3oJMuhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAJVMGw5SHkcvMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAF/0dWqkIEZKg5rca8o0P0VS+tolJJE/FRZO
atHOeaQbWzyac6NEwjYeeV2kY63skJ+QPuYbSuIBLM8p/uTRIvYM4LZYImLGUvoO
IdtJ8mAzq8CZ3ipdMs1hRqF5GRp8lg4w2QpX+PfhnW47iIOBiqSAUkIr3Y3BDaDn
EjeXF6qS4iPIvBaQQ0cvdddNh/pE33/ceghbkZNTYkrwMyBkQlRTTVKXFN7pCRUV
+L9FuQ9y8mP0BYZa5e1sdkwebydU+eqVzsil98ntkhpjvRkaJ5+Drs8TjGaJWlRw
5WuOr8unKj7YxdL1bv7//RtVYVVi296ldoRUYv4SCvJF11z0OdQ=
-----END CERTIFICATE-----
```

Ásia-Pacífico (Sydney): ap-southeast-2

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUFxWyAdk4oiXIOC9PxcgjYYh71mwwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE1MjE0M1oXDTI5MDQyODE1MjE0M1owXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUFxWyAdk4
oiXIOC9PxcgjYYh71mwwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQByjeQe6lr7fiIhoGdjBXYzDfkX0lGGvMIhRh57G1bbceQfaYdZd7Ptc0jl
bpycKGaTvhUdkpMOiV2Hi9dOOYawkdhyJDstmDNKu6P9+b6Kak8He5z3NU1tUR2Y
uTwcz7Ye8Nldx//ws3raErfTI7D6s9m63OX8cAJ/f8bNgikwpw==
```

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

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAL2bOgb+dq9rMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTEwMjkw
OTAwNTdaGA8yMTk1MDQwMzA5MDA1N1owXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAmRcyLWraysQS8yDC1b5Abs3TUaJabjqWu7d5gHik5Icd6dKl8EYpQSeS
vz6pLhkgO4xBbCRGlgE8LS/OijcZ5HwdrxBiKbicR1YvIPaIyEQQvF5sX6UWkGYw
Ma5IRGj4YbRmJkBybw+AAV9Icb5LJNOMWPi34OWM+2tMh+8L234v/JA6ogpdPuDr
sM6YFHMZ0NWo58MQ0FnEj2D7H58Ti//vFPl0TaaPWaAIRF85zBiJtKcFJ6vPidqK
f2/SDuAvZmyHC8ZBHg1moX9bR5FsU3QazfbW+c+JzAQWHj2AaQrGSCITxCMlS9sJ
l51DeoZBjnx8cnRe+HCaC4YoRBiqIQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQU/wHIo+r5U31VIsPoWoRVsNXGxowwgY4GA1UdIwSBhjCBg4AU/wHI
o+r5U31VIsPoWoRVsNXGxoyhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAL2bOgb+dq9rMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBACobLvj8IxlQyORTz/9q7/VJL509/p4HAeve
92riHp6+Moi0/dSEYPeFTgdWB9W3YCNc34Ss9TJq2D7t/zLGGlbI4wYXU6VJjL0S
hCjWeIyBXUZOZKFCb0DSJeUElsTRSXSFuVrZ9EAwjLvHni3BaC9Ve34iP71ifr75
8Tpk6PEj0+JwiijFH8E4GhcV5chB0/iooU6ioQqJrMwFYnwo1cVZJD5v6D0mu9bS
TMIJLJKv4QQQqPsNdjiB7G9bfkB6trP8fUVYLHLsVlIy5lGx+tgwFEYkG1N8IOO/
2LCawwaWm8FYAFd3IZl04RImNs/IMG7VmH1bf4swHOBHgCN1uYo=
-----END CERTIFICATE-----
```

Ásia-Pacífico (Taipei): ap-east-2

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7jCCAq4CCQDrb+HArMxssTAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yNDA1MjQxNDU2MDZaGA8y
MDUwMDUyNTE0NTYwNlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0
b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIg
U2VydmljZXMgTExDMIIBtjCCASsGByqGSM44BAEwggEeAoGBAPFb5R5TBUs2N0YW
aJcOjxr4UCDrpVT3x6EeqoGFNAc1yiZw9iv++ff6wsXm0VG5XV1QkWMQcjPfK/2I
TvXh9XEOhsG7vaBHoWkb2gmIxE6C2u8TfoZu0ZmiMceFK7aYz5w/q2J9CmRs38dT
```

```
I9qgTq0LYX+VkiNYOQnn7sQXQ8CjAhUAp2Lue9SfYTmubbpH+3j91Sivc+cCgYAi
DiyGU5R5VgiNV3mhuAyiHCft3LEmTIxos/hx/rHzgm+vCMH55tYejIrv9n7YGrIZ
MejOt8bGYxqSf0Ir/aoj3ZfHihxUzwyfyzwH7D8kAodXJNsPUTKi0O0pGl/e+nVD
JhTIFV3AwC8Tt0r2hljbjhOiyhdYy5hxWHa/WokLAQOBhAACgYAkGGHXbFr/JXol
itpS1qfiETWSRkXGHrdSmUkRumgti2y7c57TgXPwCyNlP1sTr1duy/kYDpwSwyqi
qEYfko0b/xWpDEQQPsWBgolpEYP7RIT85IxrTCrC9ohz85n7v6m9oF6BiBQGtZdk
GBN7iqemg85UaF6mXfHvl3tUYjsB2jAJBgcqhkjOOAQDAy8AMCwCFED9Ybn6fEVF
wLNjDvULmki5bPBWAhR64pxsHFRHz0ZQi+SYMWdIpEs5RQ==
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICNjCCAZ+gAwIBAgIJAJp99iy2CTXhMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yNDA1MjQx
NDU2MDZaGA8yMjAzMTAyOTE0NTYwNlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKB
gQDVdclgpcIIsyGG51ag8srK1UMfZ+Ioh9E4PLP+cIWQcdh31fv2kV/whKaqfmif
NefBIuHrTPl6L+mJQbsfeA+TiEx1Jamg4lwQfhgQKQCmjZVMaHtK+AY57TVN6FBf
HXxT2MXzktsKxAQRGeSTFQYrHRzSYvu+GkA+37lqyWRfcwIDAQABMA0GCSqGSIb3
DQEBCwUAA4GBABM+WL9MSb7z3bNOTMkM7ufPucvj+LQ+zEAJiuG0rcB8GI2DhGB5
8ohDPUGlq1cP7vYmDkWG/FrLqx7qgIzkbE3zfb62JpdOuX73oHgCmikMfq8ifoS1
CUxMQ36PDZBFNPzGZxv5kEORqhmGBkYCoIUCQ43jh3aALR/A/rfzfij8
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJAJt5hgMuWbpMMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yNDA1MjQx
NDU2MDZaGA8yMjAzMTAyOTE0NTYwNlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA91FXs9Wk9kMI3lkNhjC69C6RTBpSvdLWSohPDlJKXFoaGYIDtyW1ViwO
FORAKz0koarVBx1D4fNKCxf+mhYAf//4Pxt31GzjehHNs2YVGimwhq/SNr+3AuIO
PibA+qScXamaiknE1Pxb4jisbBu2PMAG9OxU2dESNwiqBMvdJvg30YNTUITZ6r0e
MPjR1Y/EFVx/SLHW6wdvwqhNi9hz8HHdThzjCbCQPvmoLBJIKXIfosKqvauSezt1
KJSoS2jMx1OjJB2bBlQTZC8vF0WFNPoiH4jXyJ6+wMUMNSSd5b3uL5stVTMzuIz4
39Hd5YW41rmAy+6jmpGp2eXn6Td0rQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQAs
gcgv+Xr67Cj08jKdAUT4GuCoGxveOFAjSDjs5y0cD+kXIT/Yj/+HKFOx5cwThT8F
```

```
TxNQ/oVuo3bGeuFEX799H0rT9Jupy0WiE1Vx81mk2M/1EDtns437edM4ofiWR8tR
Q1VNiRgz6Crr0nFgNoQa9HmR6/M+bImxevHJkWB3skvnxtA+lpKGwJs8jo6fA7AW
jr00opK0r731iBd1z/5hjIjkHn5NizAdiJEh3lVY/A3WS82aygW8LvYnKZeaBfZJ
J4NgxeflxocLFKBJD+hyf5u1hhvl7Mn/aGr5VI8/0F2oUqYo+xsHLT3keNghywO4
NNcyLcD9u16HVXhRhGvo
-----END CERTIFICATE-----
```

Ásia-Pacífico (Tailândia): ap-southeast-7

DSA

```
-----BEGIN CERTIFICATE-----
MIIC8TCCAq8CCQCOEEMWiJIJpTAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yNDA0MTIxNTI4NTZaGA8y
MDUwMDQxMzE1Mjg1NlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0
b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIg
U2VydmljZXMgTExDMIIBtzCCASsGByqGSM44BAEwggEeAoGBAJWKfrIlz9+/U4wm
NDJPX00avUTdksBKX5RwHkY4o0///2G2HWwiBbxw8F1U+RzCXr80gSoe4+/SCSg3
uDuhJyzN5r4jr7c590CAgsiGdWERs7l4gLQCP504feU4TEjJoq9A8MfRZeqMj7Ug
fT5InTUW7S1/r98ddG/rBHMsJwEbAhUAneIckZ1YeyGcCeL32lujMhj+g68CgYA+
RsyTXCy3Tug5aHun51IfcG2d+pn5K/tv/N3WUR18RplVctrLhwIOUoAsDWPWtxNV
sODetezAyo759CK43JAmYGzXKbRFUHm3n46jP88tSdhuSeJhc/D4l5/0+2L7ndXp
L3+W4N05NdiKSGI8e8t452wTZv/RODivPZ3RtuCDywOBhQACgYEAjVS1Huwzdn1J
+kpd2Rcbe1BAGkmvk5sUu0KhyttqIB1kxTxeWZgsdO8REZSC5gJOwkcGFvXnb3DY
+Ms45r0e0s0rx2FFYjqMLwyRpK9wUjJfSXeJMa9iLQEXuyzBz6zPgfemXbS3zNq/
eoJ9ztIwjB9DMoKL+E1vSLsTGhehqRowCQYHKoZIzjgEAwMxADAuAhUAmljDM3c9
hf0j4XbMjjpnzrx1xhkCFQCASR9pgFNgLK8y6Kojj+P1KJkrSQ==
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICNjCCAZ+gAwIBAgIJAIuIHAhL0xWcMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yNDA0MTIx
NTI4NTZaGA8yMjAzMDkxNzE1Mjg1NlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKB
gQCajgAeOauwvqGDLrHvxujnZ1BnkMzwjrycMUTkj8jqNtWoDQWUJVNPZJILosEU
VwK2I3oNkEsx/ryl9XfXcNNceoYfVEPzkTzozrZyuOG66FWtUU1LKeJ7h9/rX0Zd
9lZEokrdr6dLPt9FsHWaK5ExlUnWBjNltcQLkkKqoeYaFwIDAQABMA0GCSqGSIb3
```

```
DQEBCwUAA4GBAE4G5G+FvKTsX3T7BEcId7f5LSCc2J9gZRDiWn2oTr40CrBMOzJT
KsWr9W89YXW3gaGWltzc0WCwYQbJZgAkuEAZItJjbhdnns87ZbsFO+NZhc6gDtjA
WC3dPlSB9b6rfVoVW9O6Xwa7iNXZo8ddYVJ/ZOIv/totUz9qJt4DmmKk
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJANaQIrYcijxaMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yNDA0MTIx
NTI4NTZaGA8yMjAzMDkxNzE1Mjg1NlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAxtMGK4r6WerVtMfpRRCY3DMP9Q/s4jnRIqolPaxeT99BAFp03HXyOrTz
WjggEHArRGGeDowFkL7Vj+QNY7ran2lnYVlAQ7Ow6OLl6WttT6lMsgsLUIcsED6G
eJ1Ko+ovT1qvmuush1U5R2pHkcCJ1IT2s6uQff85l066K7dCFpaoA1QHUk9zACHj
i0DtWuTAWBXirAZSGlmtP6uj1Aw6y5kACDTjIvZJeW/kmswfApTKaJ56eNkJsUBU
NpKwt3um1BMZduy0cjUv0Sc3dIbLNyfOdyPn8tX5u5ck0EPdtBB5WjEh71IXdZJD
oaBREV7AHg5ERPQsm0BqSvMQt09KiwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQDG
qJyZbv/GUQnm8dEyVYgilQr3Yu35n8sfTwwZ1OJzIVce7NBPWePMfYii/tvGoKNp
KwFa/Vugbn1EwqpTEKqkPE1dOZvnUa97XxhYkoW5U7sgdKCANi1KWjywn7MiJ3Eg
j4gdqYK8wxvHi21ppqr572UO77uA8YMBoBT/CyQzWYUSmbqwKnnzaQBAZeO2iAk
VHuNU+9UsntNB676gRl9ag3Wfxq3yx5Ee1CeQf+US3HJn/pKk1H8dExXmBHvHwO6
GKUVNPN1rxfjTiaSt8wuO80uElAnyHIM3VOR8rJO7PKsobyEeJV0WI1hURO+wxpL
h3IsW7iBrFVvhX5xx7ZU
-----END CERTIFICATE-----
```

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

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
```

```
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIULgwDh7TiDrPPBJwscqDwiBHkEFQwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTEyMjMxMFoXDTI5MDQyODEyMjMxMFowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IULgwDh7Ti
DrPPBJwscqDwiBHkEFQwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQBtjAglBde1t4F9EHCZOj4qnY6Gigy07Ou54i+lR77MhbpzE8V28Li9l+YT
QMIn6SzJqU3/fIycIro1OVY1lHmaKYgPGSEZxBenSBHfzwDLRmC9oRp4QMe0BjOC
gepj1lUoiN7OA6PtA+ycNlsP0oJvdBjhvayLiuM3tUfLTrgHbw==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAL9KIB7Fgvg/MA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTA4MTQw
OTAwMjVaGA8yMTk1MDExNzA5MDAyNVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAz0djWUcmRW85C5CiCKPFiTIvj6y2OuopFxNE5d3Wtab10bm06vnXVKXu
tz3AndG+Dg0zIL0gMlU+QmrSR0PH2PfV9iejfLak9iwdm1WbwRrCEAj5VxPe0Q+I
KeznOtxzqQ5Wo5NLE9bA61sziUAFNVsTFUzphEwRohcekYyd3bBC4v/RuAjCXHVx
```

```
40z6AIksnAOGN2VABMlTeMNvPItKOCIeRLlllSqXX1gbtL1gxSW40JWdF3WPB68E
e+/1U3F7OEr7XqmNODOL6yh92QqZ8fHjG+afOL9Y2Hc4g+P1nk4w4iohQOPABqzb
MPjK7B2Rze0f9OEc51GBQu13kxkWWQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQU5DS5IFdU/QwYbikgtWvkU3fDwRgwgY4GA1UdIwSBhjCBg4AU5DS5
IFdU/QwYbikgtWvkU3fDwRihYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAL9KIB7Fgvg/MBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAG/N7ua8IE9IMyno0n5T57erBvLTOQ79fIJN
Mf+mKRM7qRRsdg/eumFft0rLOKo54pJ+Kim2cngCWNhkzctRHBV567AJNt4+ZDG5
hDgV0IxWO1+eaLE4qzqWP/9VrO+p3reuumgFZLVpvVpwXBBeBFUf2drUR14aWfI2
L/6VGINXYs7uP8v/2VBS7r6XZRnPBUy/R4hv5efYXnjwA9gq8+a3stC2ur8m5ySl
faKSwE4H320yAyaZWH4gpwUdbUlYgPHtm/ohRtiWPrN7KEG5Wq/REzMIjZCnxOfS
6KR6PNjlhxBsImQhmBvz6j5PLQxOxBZIpDoiK278e/1Wqm9LrBc=
-----END CERTIFICATE-----
```

Canadá (Central): ca-central-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUIrLgixJJB5C4G8z6pZ5rB0JU2aQwDQYJKoZIhvcNAQEL
```

```
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE1MzU0M1oXDTI5MDQyODE1MzU0M1owXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUIrLgixJJ
B5C4G8z6pZ5rB0JU2aQwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQBHiQJmzyFAaSYs8SpiRijIDZW2RIo7qBKb/pI3rqK6yOWDlPuMr6yNI81D
IrKGGftg4Z+2KETYU4x76HSf0s//vfH3QA57qFaAwddhKYy4BhteFQl/Wex3xTlX
LiwI07kwJvJy3mS6UfQ4HcvZy219tY+0iyOWrz/jVxwq7TOkCw==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJAJNKhJhaJOuMMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNjA3Mjkx
MTM3MTdaGA8yMTk2MDEwMjExMzcxN1owXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAhDUh6j1ACSt057nSxAcwMaGr8Ez87VA2RW2HyY8l9XoHndnxmP50Cqld
+26AJtltlqHpI1YdtnZ6OrVgVhXcVtbvte0lZ3ldEzC3PMvmISBhHs6A3SWHA9ln
InHbToLX/SWqBHLOX78HkPRaG2k0COHpRy+fG9gvz8HCiQaXCbWNFDHZev9OToNI
xhXBVzIa3AgUnGMalCYZuh5AfVRCEeALG60kxMMC8IoAN7+HG+pMdqAhJxGUcMO0
LBvmTGGeWhi04MUZWfOkwn9JjQZuyLg6B1OD4Y6s0LB2P1MovmSJKGY4JcF8Qu3z
xxUbl7Bh9pvzFR5gJN1pjM2n3gJEPwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQAJ
UNKM+gIIHNk0G0tzv6vZBT+o/vt+tIp8lEoZwaPQh1121iw/I7ZvhMLAigx7eyvf
IxUt9/nf8pxWaeGzi98RbSmbap+uxYRynqe1p5rifTamOsguuPrhVpl12OgRWLcT
rjg/K60UMXRsmg2w/cxV45pUBcyVb5h6Op5uEVAVq+CVns13ExiQL6kk3guG4+Yq
LvP1p4DZfeC33a2Rfre2IHLsJH5D4SdWcYqBsfTpf3FQThH0l0KoacGrXtsedsxs
9aRd7OzuSEJ+mBxmzxSjSwM84Ooh78DjkdpQgv967p3d+8NiSLt3/n7MgnUy6WwB
KtDujDnB+ttEHwRRngX7
-----END CERTIFICATE-----
```

Oeste do Canadá (Calgary): ca-west-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7zCCAq
+gAwIBAgIGAYPouptUMAkGByqGSM44BAMwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgMEFdhc2hpbmd0b24gU3RhdGUxED
U4EddRIpUt9KnC7s5Of2EbdSPO9EAMMeP4C2USZpRV1AIlH7WT2NWPq/
xfW6MPbLm1Vs14E7gB00b/JmYLdrmVClpJ+f6AR7ECLCT7up1/63xhv4O1fnxqimFQ8E
+4P208UewwI1VBNaFpEy9nXzrith1yrv8iIDGZ3RSAHHAhUAl2BQjxUjC8yykrmCouuEC/
BYHPUCgYEA9+GghdabPd7LvKtcNrhXuXmUr7v6OuqC+VdMCz0HgmdRWVeOutRZT
+ZxBxCBgLRJFnEj6EwoFhO3zwkyjMim4TwWeotUfI0o4KOuHiuzpnWRbqN/C/ohNWLx
+2J6ASQ7zKTxvqhRkImog9/hWuWfBpKLZl6Ae1UlZAFMO/7PSSoDgYQAAoGAMITzTJUa6cBsIfdHN69zW/
aHjUB4r1ZfKb1FMhIp9EZtEf5n+06oXjUG2+dKRSlFQeEK333ehNZsPd6uqey6TYKtHpFb5XRLS8BpqB
+7gnbAd0CBZM5o4NWesSQ1GLnTdQcGZkYG/
QESkbadoCXQTifCujJE682hTDLIVt1d4ewwCQYHKoZIzjgEAwMvADAsAhRJc4gRS/HWTkCR2MESaQEe/
jOMNQIUNoTwLvuPrmGPupPlGiHe0veZiO8=
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICMzCCAZygAwIBAgIGAYPou9weMA0GCSqGSIb3DQEBBQUAMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIDBBXYXNoaW5n
v4XBVH13ZCMgqlRHMqV8AWI5iO6gFn2A9sN3AZXTMqwtZeiDdebq3k6Wt7ieYvpXTg0qvgsjQIovRZWaBDBJy9x8C2hW
+w9lMQjFHkJ7Jy/
PHCJ69EzebQIDAQABMA0GCSqGSIb3DQEBBQUAA4GBAGe9Snkz1A6rHBH6/5kDtYvtPYwhx2sXNxztbhkXErFk40Nw5l4
gvDVtWG7qyb6fAqgoisyAbk8K9LzxSim2S1nmT9vD84B/t/VvwQBylc
+ej8kRxMH7fquZLp7IXfmtBzyUqu6Dpbne+chG2
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJALyTn5IHrIZjMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yMzEyMDcx
NTM3MDFaGA8yMjAzMDUxMzE1MzcwMVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA1GP5os424BJmGPCKOSgOclP7lzUiB85du03M4hfjzSOszsBpmBGFDLz1
owYHtIxlq3+Vi1Lt5Qlx3id/ov1QyaBPFWXVeklHVXy9vieCcI3TdjGjTl1W/8MM
m3X26QPcsnHM/Kk2wJ7s186MrqmdSsp3SCPpxv4vEG2Q9yR2bXY41hpc2rWlW8qU
D0JGXluvmmAdFnto20l1XWZ6xFen1h60DRugek/ufCbN+ljKy0xLqPoavH0Ybjsb
```

```
UpsAsBs7phaoN+X/5hIERfbp5LfVnqq54pNG5KNu4KynfW9+kA/WS4cJ6FTTN5t+
y0P1HvcL+BL2RuDy6T2bB21xw5WqtQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQURTvu/Dd4zDnmS5G5CfVLnmUBNOswgY4GA1UdIwSBhjCBg4AURTvu
/Dd4zDnmS5G5CfVLnmUBNOuhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJALyTn5IHrIZjMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAFt523A3Aug6/F8xxyITgA8gkU0btFhlXNSP
U4U2OQ9n0tWI9WqnKNWH3KBxwY5EPitU6b3LM4xc9lDWpz7h2Pto+WhxP9LVKe6f
r8r7teTLCVZ7cfYZHzHg+flZjVpAgzE5BVfrRlj3QKpv0hYT3J1wMtI++Vorq5Nf
aPjzedehJLhmZVALwnfqfLrgv6/gmraP9Vmoa8U4D6AljNiQGYaLwyoPoRm3bUs2
v1Mh9GkEQ1b9+1pFXcqgzJJTGRuiPCyPbECI79FAnx5JM/CkGJV8HlOmjIW1qkK1
Y2qT7wzErrKLJyB53Pw15BdIM1onbDAQreZb0yZQLdoEl/tx7Uk=
-----END CERTIFICATE-----
```

China (Pequim): cn-north-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIDNjCCAh4CCQD3yZ1w1AVkTzANBgkqhkiG9w0BAQsFADBcMQswCQYDVQQGEwJV
UzEZMBcGA1UECBMQV2FzaGluZ3RvbiBTdGF0ZTEQMA4GA1UEBxMHU2VhdHRsZTEg
MB4GA1UEChMXQW1hem9uIFdlYiBTZXJ2aWNlcyBMTEMwIBcNMTUwNTEzMDk1OTE1
WhgPMjE5NDEwMTYwOTU5MTVaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNo
aW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24g
V2ViIFNlcnZpY2VzIExMQzCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
AMWk9vyppSmDU3AxZ2Cy2bvKeK3F1UqNpMuyeriizi+NTsZ8tQqtNloaQcqhto/l
gsw9+QSnEJeYWnmivJWOBdn9CyDpN7cpHVmeGgNJL2fvImWyWe2f2Kq/BL9l7N7C
P2ZT52/sH9orlck1n2zO8xPi7MItgPHQwu3OxsGQsAdWucdxjHGtdchulpo1uJ31
jsTAPKZ3p1/sxPXBBAgBMatPHhRBqhwHO/Twm4J3GmTLWN7oVDds4W3bPKQfnw3r
vtBj/SM4/IgQ3xJslFcl90TZbQbgxIi88R/gWTbs7GsyT2PzstU30yLdJhKfdZKz
/aIzraHvoDTWFaOdy0+OOaECAwEAATANBgkqhkiG9w0BAQsFAAOCAQEAdSzN2+0E
V1BfR3DPWJHWRf1b7zl+1X/ZseW2hYE5r6YxrLv+1VPf/L5I6kB7GEtqhZUqteY7
zAceoLrVu/7OynRyfQetJVGichaaxLNM3lcr6kcxOowb+WQQ84cwrB3keykH4gRX
KHB2rlWSxta+2panSEO1JX2q5jhcFP90rDOtZjlpYv57N/Z9iQ+dvQPJnChdq3BK
5pZlnIDnVVxqRike7BFy8tKyPj7HzoPEF5mh9Kfnn1YoSVu+61lMVv/qRjnyKfS9
c96nE98sYFj0ZVBzXw8Sq4Gh8FiVmFHbQp1peGC19idOUqxPxWsasWxQXO0azYsP
9RyWLHKxH1dMuA==
-----END CERTIFICATE-----
```

RSA

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

```
MIIDCzCCAnSgAwIBAgIJALSOMbOoU2svMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0yMzA3MDQw
ODM1MzlaFw0yODA3MDIwODM1MzlaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQzCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA
uhhUNlqAZdcWWB/OSDVDGk3OA99EFzOn/mJlmciQ/Xwu2dFJWmSCqEAE6gjufCjQ
q3voxAhC2CF+elKtJW/C0Sz/LYo60PUqd6iXF4h+upB9HkOOGuWHXsHBTsvgkgGA
1CGgel4U0Cdq+23eANr8N8m28UzljjSnTlrYCHtzN4sCAwEAAaOB1DCB0TALBgNV
HQ8EBAMCB4AwHQYDVR0OBBYEFBkZu3wT27NnYgrfH+xJz4HJaNJoMIGOBgNVHSME
gYYwgYOAFBkZu3wT27NnYgrfH+xJz4HJaNJooWCkXjBcMQswCQYDVQQGEwJVUzEZ
MBcGA1UECBMQV2FzaGluZ3RvbiBTdGF0ZTEQMA4GA1UEBxMHU2VhdHRsZTEgMB4G
A1UEChMXQW1hem9uIFdlYiBTZXJ2aWNlcyBMTEOCCQC0jjGzqFNrLzASBgNVHRMB
Af8ECDAGAQH/AgEAMA0GCSqGSIb3DQEBCwUAA4GBAECji43p+oPkYqmzll7e8Hgb
oADS0ph+YUz5P/bUCm61wFjlxaTfwKcuTR3ytj7bFLoW5Bm7Sa+TCl3lOGb2taon
2h+9NirRK6JYk87LMNvbS40HGPFumJL2NzEsGUeK+MRiWu+Oh5/lJGii3qw4YByx
SUDlRyNy1jJFstEZjOhs
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJAOtrM5XLDSjCMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTA4MTQx
MDAxNDJaGA8yMTk1MDExNzEwMDE0MlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAvVBz+WQNdPiM9S+aUULOQEriTmNDUrjLWLr7SfaOJScBzis5D5ju0jh1
+qJdkbuGKtFX5OTWTm8pWhInX+hIOoS3exC4BaANoa1A3o6quoG+Rsv72qQf8LLH
sgEi6+LMlCN9TwnRKOToEabmDKorss4zFl7VSsbQJwcBSfOcIwbdRRaW9Ab6uJHu
79L+mBR3Ea+G7vSDrVIA8goAPkae6jY9WGw9KxsOrcvNdQoEkqRVtHo4bs9fMRHU
Etphj2gh4ObXlFN92VtvzD6QBs3CcoFWgyWGvzg+dNG5VCbsiiuRdmii3kcijZ3H
Nv1wCcZoEAqH72etVhsuvNRC/xAP8wIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQA8
ezx5LRjzUU9EYWYhyYIEShFlP1qDHs7F4L46/5lc4pL8FPoQm5CZuAF31DJhYi/b
fcV7i3n++/ymQbCLC6kAg8DUB7NrcROll5ag8d/JXGzcTCnlDXLXx1905fPNa+jI
0q5quTmdmiSi0taeaKZmyUdhrB+a7ohWdSdlokEIOtbH1P+g5yll3bI2leYE6Tm8
LKbyfK/532xJPqO9abx4Ddn89ZEC6vvWVNDgTsxERg992Wi+/xoSw3XxkgAryIv1
zQ4dQ6irFmXwCWJqc6kHg/M5W+z60S/94+wGTXmp+19U6Rkq5jVMLh16XJXrXwHe
4KcgIS/aQGVgjM6wivVA
-----END CERTIFICATE-----
```

China (Ningxia): cn-northwest-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIDNjCCAh4CCQD3yZ1w1AVkTzANBgkqhkiG9w0BAQsFADBcMQswCQYDVQQGEwJV
UzEZMBcGA1UECBMQV2FzaGluZ3RvbiBTdGF0ZTEQMA4GA1UEBxMHU2VhdHRsZTEg
MB4GA1UEChMXQW1hem9uIFdlYiBTZXJ2aWNlcyBMTEMwIBcNMTUwNTEzMDk1OTE1
WhgPMjE5NDEwMTYwOTU5MTVaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNo
aW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24g
V2ViIFNlcnZpY2VzIExMQzCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
AMWk9vyppSmDU3AxZ2Cy2bvKeK3F1UqNpMuyeriizi+NTsZ8tQqtNloaQcqhto/l
gsw9+QSnEJeYWnmivJWOBdn9CyDpN7cpHVmeGgNJL2fvImWyWe2f2Kq/BL9l7N7C
P2ZT52/sH9orlck1n2zO8xPi7MItgPHQwu3OxsGQsAdWucdxjHGtdchulpo1uJ31
jsTAPKZ3p1/sxPXBBAgBMatPHhRBqhwHO/Twm4J3GmTLWN7oVDds4W3bPKQfnw3r
vtBj/SM4/IgQ3xJslFcl90TZbQbgxIi88R/gWTbs7GsyT2PzstU30yLdJhKfdZKz
/aIzraHvoDTWFaOdy0+OOaECAwEAATANBgkqhkiG9w0BAQsFAAOCAQEAdSzN2+0E
V1BfR3DPWJHWRf1b7zl+1X/ZseW2hYE5r6YxrLv+1VPf/L5I6kB7GEtqhZUqteY7
zAceoLrVu/7OynRyfQetJVGichaaxLNM3lcr6kcxOowb+WQQ84cwrB3keykH4gRX
KHB2rlWSxta+2panSEO1JX2q5jhcFP90rDOtZjlpYv57N/Z9iQ+dvQPJnChdq3BK
5pZlnIDnVVxqRike7BFy8tKyPj7HzoPEF5mh9Kfnn1YoSVu+61lMVv/qRjnyKfS9
c96nE98sYFj0ZVBzXw8Sq4Gh8FiVmFHbQp1peGC19idOUqxPxWsasWxQXO0azYsP
9RyWLHKxH1dMuA==
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDCzCCAnSgAwIBAgIJALSOMbOoU2svMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0yMzA3MDQw
ODM1MzlaFw0yODA3MDIwODM1MzlaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQzCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA
uhhUNlqAZdcWWB/OSDVDGk3OA99EFzOn/mJlmciQ/Xwu2dFJWmSCqEAE6gjufCjQ
q3voxAhC2CF+elKtJW/C0Sz/LYo60PUqd6iXF4h+upB9HkOOGuWHXsHBTsvgkgGA
1CGgel4U0Cdq+23eANr8N8m28UzljjSnTlrYCHtzN4sCAwEAAaOB1DCB0TALBgNV
HQ8EBAMCB4AwHQYDVR0OBBYEFBkZu3wT27NnYgrfH+xJz4HJaNJoMIGOBgNVHSME
gYYwgYOAFBkZu3wT27NnYgrfH+xJz4HJaNJooWCkXjBcMQswCQYDVQQGEwJVUzEZ
MBcGA1UECBMQV2FzaGluZ3RvbiBTdGF0ZTEQMA4GA1UEBxMHU2VhdHRsZTEgMB4G
A1UEChMXQW1hem9uIFdlYiBTZXJ2aWNlcyBMTEOCCQC0jjGzqFNrLzASBgNVHRMB
Af8ECDAGAQH/AgEAMA0GCSqGSIb3DQEBCwUAA4GBAECji43p+oPkYqmzll7e8Hgb
oADS0ph+YUz5P/bUCm61wFjlxaTfwKcuTR3ytj7bFLoW5Bm7Sa+TCl3lOGb2taon
```

```
2h+9NirRK6JYk87LMNvbS40HGPFumJL2NzEsGUeK+MRiWu+Oh5/lJGii3qw4YByx
SUDlRyNy1jJFstEZjOhs
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJAPu4ssY3BlzcMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTEyMDMy
MTI5MzJaGA8yMTk1MDUwODIxMjkzMlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAsOiGi4A6+YTLzCdIyP8b8SCT2M/6PGKwzKJ5XbSBoL3gsnSWiFYqPg9c
uJPNbiy9wSA9vlyfWMd90qvTfiNrT6vewP813QdJ3EENZOx4ERcf/Wd22tV72kxD
yw1Q3I1OMH4bOItGQAxU5OtXCjBZEEUZooOkU8RoUQOU2Pql4NTiUpzWacNutAn5
HHS7MDc4lUlsJqbN+5QW6fFrcNG/0Mrib3JbwdFUNhrQ5j+Yq5h78HarnUivnX/3
Ap+oPbentv1qd7wvPJu556LZuhfqI0TohiIT1Ah+yUdN5osoaMxTHKKtf/CsSJ1F
w3qXqFJQA0VWsqjFyHXFI32I/GOupwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQCn
Um00QHvUsJSN6KATbghowLynHn3wZSQsuS8E0COpcFJFxP2SV0NYkERbXu0n/Vhi
yq5F8v4/bRA2/xpedLWmvFs7QWlomuXhSnYFkd33Z5gnXPb9vRkLwiMSw4uXls35
qQraczUJ9EXDhrv7VmngIk9H3YsxYrlDGEqh/oz4Ze4ULOgnfkauanHikk+BUEsg
/jsTD+7e+niEzJPihHdsvKFDlud5pakEzyxovHwNJ1GS2I//yxrJFIL91mehjqEk
RLPdNse7N6UvSnuXcOokwu6l6kfzigGkJBxkcq4gre3szZFdCQcUioj7Z4xtuTL8
YMqfiDtN5cbD8R8ojw9Y
-----END CERTIFICATE-----
```

Europa (Frankfurt): eu-central-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
```

```
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUFD5GsmkxRuecttwsCG763m3u63UwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE1NTUyOVoXDTI5MDQyODE1NTUyOVowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUFD5Gsmkx
RuecttwsCG763m3u63UwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQBBh0WaXlBsW56Hqk588MmJxsOrvcKfDjF57RgEDgnGnQaJcStCVWDO9UYO
JX2tdsPw+E7AjDqjsuxYaotLn3Mr3mK0sNOXq9BljBnWD4pARg89KZnZI8FN35HQ
O/LYOVHCknuPL123VmVRNs51qQA9hkPjvw21UzpDLxaUxt9Z/w==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAKD+v6LeR/WrMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTA4MTQw
OTA4MTlaGA8yMTk1MDExNzA5MDgxOVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAka8FLhxs1cSJGK+Q+q/vTf8zVnDAPZ3U6oqppOW/cupCtpwMAQcky8DY
Yb62GF7+C6usniaq/9W6xPn/3o//wti0cNt6MLsiUeHqNl5H/4U/Q/fR+GA8pJ+L
npqZDG2tFi1WMvvGhGgIbScrjR4VO3TuKy+rZXMYvMRk1RXZ9gPhk6evFnviwHsE
jV5AEjxLz3duD+u/SjPp1vloxe2KuWnyC+EKInnka909sl4ZAUh+qIYfZK85DAjm
```

```
GJP4W036E9wTJQF2hZJrzsiB1MGyC1WI9veRISd30izZZL6VVXLXUtHwVHnVASrS
zZDVpzj+3yD5hRXsvFigGhY0FCVFnwIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQUxC2l6pvJaRflgu3MUdN6zTuP6YcwgY4GA1UdIwSBhjCBg4AUxC2l
6pvJaRflgu3MUdN6zTuP6YehYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAKD+v6LeR/WrMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAIK+DtbUPppJXFqQMv1f2Gky5/82ZwgbbfXa
HBeGSii55b3tsyC3ZW5ZlMJ7Dtnr3vUkiWbV1EUaZGOUlndUFtXUMABCb/coDndw
CAr53XTv7UwGVNe/AFO/6pQDdPxXn3xBhF0mTKPrOGdvYmjZUtQMSVb9lbMWCFfs
w+SwDLnm5NF4yZchIcTs2fdpoyZpOHDXy0xgxO1gWhKTnYbaZOxkJvEvcckxVAwJ
obF8NyJla0/pWdjhlHafEXEN8lyxyTTyOa0BGTuYOBD2cTYYynauVKY4fqHUkr3v
Z6fboaHEd4RFamShM8uvSu6eEFD+qRmvqlcodbpsSOhuGNLzhOQ=
-----END CERTIFICATE-----
```

Europa (Irlanda): eu-west-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUakDaQ1Zqy87Hy9ESXA1pFC116HkwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
```

```
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE2MTgxMFoXDTI5MDQyODE2MTgxMFowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUakDaQ1Zq
y87Hy9ESXA1pFC116HkwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQADIkn/MqaLGPuK5+prZZ5Ox4bBZLPtreO2C7r0pqU2kPM2lVPyYYydkvP0
lgSmmsErGu/oL9JNztDe2oCA+kNy17ehcsf8cw0uP861czNFKCeU8b7FgBbL+sIm
qi33rAq6owWGi/5uEcfCR+JP7W+oSYVir5r/yDmWzx+BVH5S/g==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAOrmqHuaUt0vMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTEwMjkw
OTA2MTlaGA8yMTk1MDQwMzA5MDYxOVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAjE7nVu+aHLtzp9FYV25Qs1mvJ1JXD7J0iQ1Gs/RirW9a5ZECCtc4ssnf
zQHq2JRVr0GRchvDrbm1HaP/avtFQR/Thvfltwu9AROVT22dUOTvERdkNzveoFCy
hf52Rqf0DMrLXG8ZmQPPXPDFAv+sVMWCDftcChxRYZ6mP9O+TpgYNT1krD5PdvJU
7HcXrkNHDYqbsg8A+Mu2hzl0QkvUET83Csg1ibeK54HP9w+FsD6F5W+6ZSHGJ88l
FI+qYKs7xsjJQYgXWfEt6bbckWs1kZIaIOyMzYdPF6ClYzEec/UhIe/uJyUUNfpT
VIsI5OltBbcPF4c7Y20jOIwwI2SgOQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQUF2DgPUZivKQR/Zl8mB/MxIkjZDUwgY4GA1UdIwSBhjCBg4AUF2Dg
PUZivKQR/Zl8mB/MxIkjZDWhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAOrmqHuaUt0vMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAGm6+57W5brzJ3+T8/XsIdLTuiBSe5ALgSqI
qnO5usUKAeQsa+kZIJPyEri5i8LEodh46DAF1RlXTMYgXXxl0YggX88XPmPtok17
l4hib/D9/lu4IaFIyLzYNSzsETYWKWoGVe7ZFz60MTRTwY2u8YgJ5dec7gQgPSGj
avB0vTIgoW41G58sfw5b+wjXCsh0nROon79RcQFFhGnvup0MZ+JbljyhZUYFzCli
31jPZiKzqWa87xh2DbAyvj2KZrZtTe2LQ48Z4G8wWytJzxEeZdREe4NoETf+Mu5G
4CqoaPR05KWkdNUdGNwXewydb3+agdCgfTs+uAjeXKNdSpbhMYg=
-----END CERTIFICATE-----
```

Europa (Londres): eu-west-2

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUCgCV/DPxYNND/swDgEKGiC5I+EwwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE2MjkxNFoXDTI5MDQyODE2MjkxNFowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUCgCV/DPx
YNND/swDgEKGiC5I+EwwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQATPu/sOE2esNa4+XPEGKlEJSgqzyBSQLQc+VWo6FAJhGG9fp7D97jhHeLC
5vwfmtTAfnGBxadfAOT3ASkxnOZhXtnRna460LtnNHm7ArCVgXKJo7uBn6ViXtFh
uEEw4y6p9YaLQna+VC8Xtgw6WKq2JXuKzuhuNKSFaGGw9vRcHg==
```

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

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJANBx0E2bOCEPMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNjA4MTEx
NDU2NDJaGA8yMTk2MDExNTE0NTY0MlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEArYS3mJLGaMrh2DmiPLbqr4Z+xWXTzBWCjOwpsuHE9H6dWUUyl2Bgnu+Z
d8QvW306Yleec45M4F2RA3J4hWHtShzsMlOJVRt+YulGeTf9OCPr26QmIFfs5nD4
fgsJQEry2MBSGA9Fxq3Cw6qkWcrOPsCR+bHOU0XykdKl0MnIbpBf0kTfciAupQEA
dEHnM2J1L2iI0NTLBgKxy5PXLH9weX20BFauNmHH9/J07OpwL20SN5f8TxcM9+pj
Lbk8h1V4KdIwVQpdWkbDL9BCGlYjyadQJxSxz1J343NzrnDM0M4h4HtVaKOS7bQo
Bqt2ruopLRCYgcuFHck/1348iAmbRQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQBG
wujwU1Otpi3iBgmhjMClgZyMMn0aQIxMigoFNqXMUNx1Mq/e/Tx+SNaOEAu0n2FF
aiYjvY0/hXOx75ewzZvM7/zJWIdLdsgewpUqOBH4DXFhbSk2TxggSPb0WRqTBxq5
Ed7F7+7GRIeBbRzdLqmISDnfqey8ufW0ks51XcQNomDIRG5s9XZ5KHviDCar8FgL
HngBCdFI04CMagM+pwTO9XN1Ivt+NzUj208ca3oP1IwEAd5KhIhPLcihBQA5/Lpi
h1s3170z1JQ1HZbDrH1pgp+8hSI0DwwDVb3IIH8kPR/J0Qn+hvOl2HOpaUg2Ly0E
pt1RCZe+W7/dF4zsbqwK
-----END CERTIFICATE-----
```

Europa (Milão): eu-south-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAqwCCQCMElHPdwG37jAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xOTA0MjkyMDM1MjJaFw00
NTA0MjkyMDM1MjJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbYwggErBgcqhkjOOAQBMIIBHgKBgQDAkoL4YfdMI/MrQ0oL
NPfeEk94eiCQA5xNOnU7+2eVQtEqjFbDADFENh1p3sh9Q9OoheLFH8qpSfNDWn/0
ktCS909ApTY6Esx1ExjGSeQq/U+SC2JSuuTT4WFMKJ63a/czMtFkEPPnVIjJJJmT
HJSKSsVUgpdDIRvJXuyB0zdB+wIVALQ3OLaVGdlPMNfS1nD/Yyn+32wnAoGAPBQ3
7XHg5NLOS4326eFRUT+4ornQFjJjP6dp3pOBEzpImNmZTtkCNNUKE4Go9hv5T4lh
R0pODvWv0CBupMAZVBP9ObplXPCyEIZtuDqVa7ukPOUpQNgQhLLAqkigTyXVOSmt
ECBj9tu5WNP/x3iTZTHJ+g0rhIqpgh012UwJpKADgYQAAoGAV1OEQPYQUg5/M3xf
```

```
6vE7jKTxxyFWEyjKfJK7PZCzOIGrE/swgACy4PYQW+AwcUweSlK/Hx2OaZVUKzWo
wDUbeu65DcRdw2rSwCbBTU342sitFo/iGCV/Gjf+BaiAJtxniZze7J1ob8vOBeLv
uaMQmgOYeZ5e0fl04GtqPl+lhcQwCQYHKoZIzjgEAwMwADAtAhQdoeWLrkm0K49+
AeBK+j6m2h9SKQIVAIBNhS2a8cQVABDCQXVXrc0tOmO8
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICNjCCAZ+gAwIBAgIJAOZ3GEIaDcugMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xOTEwMjQx
NTE5MDlaGA8yMTk5MDMyOTE1MTkwOVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKB
gQCjiPgW3vsXRj4JoA16WQDyoPc/eh3QBARaApJEc4nPIGoUolpAXcjFhWplo2O+
ivgfCsc4AU9OpYdAPha3spLey/bhHPRi1JZHRNqScKP0hzsCNmKhfnZTIEQCFvsp
DRp4zr91/WS06/flJFBYJ6JHhp0KwM81XQG59lV6kkoW7QIDAQABMA0GCSqGSIb3
DQEBCwUAA4GBAGLLrY3P+HH6C57dYgtJkuGZGT2+rMkk2n81/abzTJvsqRqGRrWv
XRKRXlKdM/dfiuYGokDGxiC0Mg6TYy6wvsR2qRhtXW1OtZkiHWcQCnOttz+8vpew
wx8JGMvowtuKB1iMsbwyRqZkFYLcvH+Opfb/Aayi20/ChQLdI6M2R5VU
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJAO/+DgYF78KwMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xOTA0Mjky
MDM1MjJaGA8yMTk4MTAwMjIwMzUyMlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAv1ZLV+Z/P6INq+R1qLkzETBg7sFGKPiwHekbpuB6lrRxKHhj8V9vaReM
lnv1Ur5LAPpMPYDsuJ4WoUbPYAqVqyMAo7ikJHCCM1cXgZJefgN6z9bpS+uA3YVh
V/0ipHh/X2hc2S9wvxKWiSHu6Aq9GVpqL035tJQD+NJuqFd+nXrtcw4yGtmvA6wl
5Bjn8WdsP3xOTKjrByYY1BhXpP/f1ohU9jE9dstsRXLa+XTgTPWcWdCS2oRTWPGR
c5Aeh47nnDsyQfP9gLxHeYeQItV/BD9kU/2Hn6mnRg/B9/TYH8qzlRTzLapXp4/5
iNwusrTNexGl8BgvAPrfhjDpdgYuTwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQB7
5ya11K/hKgvaRTvZwVV8GlVZt0CGPtNvOi4AR/UN6TMm51BzUB5nurB4z0R2MoYO
Uts9sLGvSFALJ4otoB77hyNpH3drttU1CVVwal/yK/RQLSon/IoUkaGEbqalu+mH
nYad5IG4tEbmepX456XXcO58MKmnczNbPyw3FRzUZQtI/sf94qBwJ1Xo6XbzPKMy
xjL57LHIZCssD+XPifXay69OFlsCIgLim11HgPkRIHEOXLSf3dsW9r+4CjoZqB/Z
jj/P4TLCxbYCLkvglwaMjgEWF40Img0fhx7yT2X92MiSrs3oncv/IqfdVTiN8OXq
```

```
jgnq1bf+EZEZKvb6UCQV
-----END CERTIFICATE-----
```

Europa (Paris): eu-west-3

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUaC9fX57UDr6u1vBvsCsECKBZQyIwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE2MzczOFoXDTI5MDQyODE2MzczOFowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUaC9fX57U
```

```
Dr6u1vBvsCsECKBZQyIwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQCARv1bQEDaMEzYI0nPlu8GHcMXgmgA94HyrXhMMcaIlQwocGBs6VILGVhM
TXP2r3JFaPEpmXSQNQHvGA13clKwAZbni8wtzv6qXb4L4muF34iQRHF0nYrEDoK7
mMPR8+oXKKuPO/mv/XKo6XAV5DDERdSYHX5kkA2R9wtvyZjPnQ==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJALWSfgHuT/ARMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNzA1MzEx
MTE4MTZaGA8yMTk2MTEwMzExMTgxNlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAy5V7KDqnEvF3DrSProFcgu/oL+QYD62b1U+Naq8aPuljJe127Sm9WnWA
EBdOSASkOaQ9fzjCPoG5SGgWKxYoZjsevHpmzjVv9+Ci+F57bSuMbjgUbvbRIFUB
bxQojVoXQPHgK5v433ODxkQ4sjRyUbf4YV1AFdfU7zabC698YgPVOExGhXPlTvco
8mlc631ubw2g52j0lzaozUkHPSbknTomhQIvO6kUfX0e0TDMH4jLDG2ZIrUB1L4r
OWKG4KetduFrRZyDHF6ILZu+s6ywiMicUd+2UllDFC6oas+a8D11hmO/rpWU/ieV
jj4rWAFrsebpn+Nhgy96iiVUGS2LuQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQDE
iYv6FQ6knXCg+svlcaQG9q59xUC5z8HvJZ1+SxzPKKC4PKQdKvIIfE8GxVXqlZG1
cl5WKTFDMapnzb9RV/DTaVzWx3cMYT77vm1Hl1XGjhx611CGcENH1egI3lOTILsa
+KfopuJEQQ9TDMAIkGjhA+KieU/U5Ctv9fdej6d0GC6OEuwKkTNzPWue6UMq8d4H
2xqJboWsE1t4nybEosvZfQJcZ8jyIYcYBnsG13vCLM+ixjuU5MVVQNMY/gBJzqJB
V+U0QiGiuT5cYgY/QihxdHt99zwGaE0ZBC7213NKrlNuLSrqhDI2NLu8NsExqOFy
OmY0v/xVmQUQl26jJXaM
-----END CERTIFICATE-----
```

Europa (Espanha): eu-south-2

DSA

```
-----BEGIN CERTIFICATE-----
MIIC8DCCAq
+gAwIBAgIGAXjwLk46MAkGByqGSM44BAMwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgMEFdhc2hpbmd0b24gU3RhdGUxED
U4EddRIpUt9KnC7s5Of2EbdSPO9EAMMeP4C2USZpRV1AIlH7WT2NWPq/
xfW6MPbLm1Vs14E7gB00b/JmYLdrmVClpJ+f6AR7ECLCT7up1/63xhv4O1fnxqimFQ8E
+4P208UewwI1VBNaFpEy9nXzrith1yrv8iIDGZ3RSAHHAhUAl2BQjxUjC8yykrmCouuEC/
BYHPUCgYEA9+GghdabPd7LvKtcNrhXuXmUr7v6OuqC+VdMCz0HgmdRWVeOutRZT
+ZxBxCBgLRJFnEj6EwoFhO3zwkyjMim4TwWeotUfI0o4KOuHiuzpnWRbqN/C/ohNWLx
+2J6ASQ7zKTxvqhRkImog9/hWuWfBpKLZl6Ae1UlZAFMO/7PSSoDgYQAAoGAGG2m8EKmaf5qQqj3Z
```

```
+rzSaTaXE3B/R/4A2VuGqRYR7MljPtwdmU6/3CPjCACcZmTIcOAKbFiDHqadQgBZXfzGpzw8Zo
+eYmmk5fXycgnj57PYH1dIWU6I7mCbAah5MZMcmHaTmIsomGrhcnWB8d8qOU7oZ0UWK4lbiAQs1MihoUwCQYHKoZIzjg
WmbaU7YM5GwCFCvIJOesO5hZ8PHC52dAR8WWC6oe
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICMzCCAZygAwIBAgIGAXjwLkiaMA0GCSqGSIb3DQEBBQUAMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIDBBXYXNoaW5n
VvR1+45Aey5zn3vPk6xBm5o9grSDL6D2iAuprQnfVXn8CIbSDbWFhA3fi5ippjKkh3sl8VyCvCOUXKdOaNrYBrPRkrdH
+3m/
rxIUZ2IK1fDlC6sWAjddf6sBrV2w2a78H0H8EwuwiSgttURBjwJ7KPPJCqaqrQIDAQABMA0GCSqGSIb3DQEBBQUAA4GB
+FzqQDzun/
iMMzcFucmLMl5BxEblrFXOz7IIuOeiGkndmrqUeDCykztLku45s7hxdNy4ltTuVAaE5aNBdw5J8U1mRvsKvHLy2ThH6h
+hBgiphYp84DUbWVYeP8YqLEJSqscKscWC
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJALWSmO6DvSpQMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yMjA3MTgx
MzU4NDNaGA8yMjAxMTIyMjEzNTg0M1owXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAuAAhuSpsHC00/fD2zNlBDpNLRndi9qbHsNeuz3WqN7Samj2aSrM2hS+i
hUxx0BspZj0tZCOsbpPZ+i74NOEQtFeqQoEGvKhB1nJiF4y5I81HDhs5qHvoIivm
7rbbik3zgm1PqS/DmDjVQaXPcD31Rd9ILwBmWEwJqHigyNVlxYtCzTQcrlBrvNZM
dnNgCDAdX/HBEFxx9O12xeu0bSt0s+PJWZ1RTbYrNe7LIH6ntUqHxP/ziQ5trXEZ
uqy7aWk1L8uK4jmyNph0lbaqBa3Y6pYmU1nC27UE4i3fnPB0LSiAr+SrwVvX1g4z
ilo8kr+tbIF+JmcgYLBvO8Jwp+EUqQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQUwvGzKJL9A5LReJ4Fxo5K6I20xcowgY4GA1UdIwSBhjCBg4AUwvGz
KJL9A5LReJ4Fxo5K6I20xcqhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJALWSmO6DvSpQMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAJAZd31jyoTGLawAD2+v/vQsaB9vZIx5EImi
G8YGkd61uFWeNhAmtrwyE/i6FDSIphDrMHBkvw/D3BsqK+Ev/JOK/VYuaYDx/8fp
H4cwp9jC57CXzdIDREWNf6M9PsHFg2WA9XNNtClOZL5WJiJwel8eDSg+sqJUxE0l
MW+QChq/20F6niyaRK4bXrZq14as7h+F9u3A9xHEOVP7Zk9C2ehrBXzCMLSDt3GV
fEuMea2RxMhozwz34Hkdb6j18qoCfygubulovRNQjKw/cEmgPR16KfZPP5caILVt
9qkYPvePmbiVswZDee73cDymJYxLqILpOZwyXvUH8StiH42FHZQ=
-----END CERTIFICATE-----
```

Europa (Estocolmo): eu-north-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUN1c9U6U/xiVDFgJcYKZB4NkH1QEwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE2MDYwM1oXDTI5MDQyODE2MDYwM1owXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUN1c9U6U/
xiVDFgJcYKZB4NkH1QEwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQBTIQdoFSDRHkpqNPUbZ9WXR2O5v/9bpmHojMYZb3Hw46wsaRso7STiGGX/
tRqjIkPUIXsdhZ3+7S/RmhFznmZc8e0bjU4n5vi9CJtQSt+1u4E17+V2bF+D3h/7
wcfE0l3414Q8JaTDtfEf/aF3F0uyBvr4MDMd7mFvAMmDmBPSlA==
```

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

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJALc/uRxg++EnMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xODA0MTAx
NDAwMTFaGA8yMTk3MDkxMzE0MDAxMVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAzwCGJEJIxqtr2PD2a1mA6LhRzKhTBa1AZsg3eYfpETXIVlrpojMfvVoN
qHvGshWLgrGTT6os/3gsaADheSaJKavxwX3X6tJA8fvEGqr3a1C1MffH9hBWbQqC
LbfUTAbkwis4GdTUwOwPjT1Cm3u9R/VzilCNwkj7iQ65AFAI8Enmsw3UGldEsop4
yChKB3KW3WI0FTh0+gD0YtjrqqYJxpGOYBpJp5vwdd3fZ4t1vidmDMs7liv4f9Bx
p0oSmUobU4GUlFhBchK1DukICVQdnOVzdMonYm7s+HtpFbVHR8yf6QoixBKGdSal
mBf7+y0ixjCn0pnC0VLVooGo4mi17QIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQDG
4ONZiixgk2sjJctwbyD5WKLTH6+mxYcDw+3y/F0fWz561YORhP2FNnPOmEkf0Sl/
Jqk4svzJbCbQeMzRoyaya/46d7UioXMHRZam5IaGBhOdQbi97R4VsQjwQj0RmQsq
yDueDyuKTwWLK9KnvI+ZA6e6bRkdNGflK4N8GGKQ+fBhPwVELkbT9f16OJkezeeN
S+F/gDADGJgmPXfjogICb4Kvshq0H5Lm/xZlDULF2g/cYhyNY6EOI/eS5m1I7R8p
D/m6WoyZdpInxJfxW616OMkxQMRVsruLTNGtby3u1g6ScjmpFtvAMhYejBSdzKG4
FEyxIdEjoeO1jhTsck3R
-----END CERTIFICATE-----
```

Europa (Zurique): eu-central-2

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7zCCAq
+gAwIBAgIGAXjXiKJnMAkGByqGSM44BAMwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgMEFdhc2hpbmd0b24gU3RhdGUxED
U4EddRIpUt9KnC7s5Of2EbdSPO9EAMMeP4C2USZpRV1AIlH7WT2NWPq/
xfW6MPbLm1Vs14E7gB00b/JmYLdrmVClpJ+f6AR7ECLCT7up1/63xhv4O1fnxqimFQ8E
+4P208UewwI1VBNaFpEy9nXzrith1yrv8iIDGZ3RSAHHAhUAl2BQjxUjC8yykrmCouuEC/
BYHPUCgYEA9+GghdabPd7LvKtcNrhXuXmUr7v6OuqC+VdMCz0HgmdRWVeOutRZT
+ZxBxCBgLRJFnEj6EwoFhO3zwkyjMim4TwWeotUfI0o4KOuHiuzpnWRbqN/C/ohNWLx
+2J6ASQ7zKTxvqhRkImog9/hWuWfBpKLZl6Ae1UlZAFMO/7PSSoDgYQAAoGAYNjaCNg/
cfgQOOl1BUj5ClUulqwZ9Q+SfDzPZh9D2C0VbiRANiZoxrV8RdgmzzC5T7VcriVwjwvta2Ch//
b+sZ86E5h0XWWr+BeEjD9cu3eDj12XB5sWEbNHNx49p5Tmtu5r2LDtlL8X/
Rpfalu2Z2OJgjFJWGf7hRwxe456n
+lowCQYHKoZIzjgEAwMvADAsAhRChsLcj4U5CVb2cp5M0RE1XbXmhAIUeGSnH+aiUQIWmPEFja+itWDufIk=
```

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

RSA

```
-----BEGIN CERTIFICATE-----
MIICMzCCAZygAwIBAgIGAXjSGFGiMA0GCSqGSIb3DQEBBQUAMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIDBBXYXNoaW5n
opKZAUusJx2hpgU3pUHhlp9ATh/VeVD582jTd9IY
+8t5MDa6Z3fGliByEiXz0LEHdi8MBacLREu1TwIDAQABMA0GCSqGSIb3DQEBBQUAA4GBAILlpoE3k9o7KdALAxsFJNit
+g3RMzdbiFM+7MA63Nv5fsf+0xgcjSNBElvPCDKFvTJl4QQhToy056llO5GvdS9RK
+H8xrP2mrqngApoKTApv93vHBixgFSn5KrczRO0YSm3OjkqbydU7DFlmkXXR7GYE+5jbHvQHYiT1J5sMu
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJALvT012pxTxNMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yMjA3MTgx
NTEyMDdaGA8yMjAxMTIyMjE1MTIwN1owXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAyn+Lsnq1ykrfYlZkk6aAAYNReNd9Iw8AUwCBkgOr2eBiBBepYxHwU85N
++moQ+j0EV2VaahBeTLShGZZS1HsyK8+cYT2QzpghIoamcYhrPXyIxlWiRQlaqSg
OFiE9bsqL3rCF5Vz+tOiTe5W/7ojfOFls6++g7ZpobwJlpMbuJepqyeHMPyjvO5A
age81lJewc4bxo2ntaW0HCqNksqfYB78j6X6kn3PFpX7FaYAwZA+Xx6C7UCY7rNi
UdQzfAo8htfJi4chz7frpUdQ9kl3IOQrsLshBB5fFUjl09NiFipCGBwi+8ZMeSn1
5qwBI01BWXPfG7WX6Owyjhmh6JtE1wIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQU8HN4vvJrsZgPQeksMBgJb9xR1yYwgY4GA1UdIwSBhjCBg4AU8HN4
vvJrsZgPQeksMBgJb9xR1yahYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJALvT012pxTxNMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAGlHYDtcHpfBvdHx9HeQE8HgNugJUPdEqxun
t9U33p8VFrs+uLPtrOd9HDJEGvvs5h84EUie/oGJxRt7V1Vlid1PvHf6cRmpjgqY
YdggAVkZtY/PnFVmzf2bMVlSQPrqCl7U0zaw2Kvnj4zgX0rZyCetgrRZSUSxotyp
978Wy9ccXwVSeYG/YAr5rJpS6ZH7eRQvUY0IzwFNeaOPgOTEVpcjWlV6+MQEvsEx
W85q+s6AVr49eppEx8SLJsl0C23yB+L+t32tAveQImRWtJMpzZ5cxh/sYgDVeoC0
85H1NK/7H9fAzT1cPu1oHSnB0xYzzHGOAmXmusMfwUk8fL1RQkE=
-----END CERTIFICATE-----
```

Israel (Tel Aviv): il-central-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7zCCAq+gAwIBAgIGAX0QPi
+9MAkGByqGSM44BAMwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgMEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcMB1NlYX
U4EddRIpUt9KnC7s5Of2EbdSPO9EAMMeP4C2USZpRV1AIlH7WT2NWPq/
xfW6MPbLm1Vs14E7gB00b/JmYLdrmVClpJ+f6AR7ECLCT7up1/63xhv4O1fnxqimFQ8E
+4P208UewwI1VBNaFpEy9nXzrith1yrv8iIDGZ3RSAHHAhUAl2BQjxUjC8yykrmCouuEC/
BYHPUCgYEA9+GghdabPd7LvKtcNrhXuXmUr7v6OuqC+VdMCz0HgmdRWVeOutRZT
+ZxBxCBgLRJFnEj6EwoFhO3zwkyjMim4TwWeotUfI0o4KOuHiuzpnWRbqN/C/ohNWLx
+2J6ASQ7zKTxvqhRkImog9/
hWuWfBpKLZl6Ae1UlZAFMO/7PSSoDgYQAAoGAbazCL5XXyPmcw3+oMYQUF5/9YogW6D0FZbYuyPgjOoUwWdl6fjlzWca
pq+l1ezuK2DFOzNTEyPEwwCQYHKoZIzjgEAwMvADAsAhRt1jkpXsvrS
+xTo2M9h2s2uLAhEQIUOZ2FcnTSrshF2EIdixZZwtNv66Q=
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICMzCCAZygAwIBAgIGAX0QQGVLMA0GCSqGSIb3DQEBBQUAMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIDBBXYXNoaW5n
+S8vOy5hpLoRe4RkOrY0cM3bN07GdEMlin5mU0y1t8y3ct4YewvmkgT42kTyMM
+t1K4S0xsqjXxxS716uGYh7eWtkxrCihj8AbXN/6pa095h
+7TZyl2n83keiNUzM2KoqQVMwIDAQABMA0GCSqGSIb3DQEBBQUAA4GBADwA6VVEIIZD2YL00F12po40xDLzIc9XvqFPS
FmU7H8s62/jD6cOR1A1cClIyZUe1yT1ZbPySCs43J+Thr8i8FSRxzDBSZZi5foW
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAOVp1h2I9wW7MA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yMjA3MTUx
MjQ0MTJaGA8yMjAxMTIxOTEyNDQxMlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA13PkyWvl61iV/SYfO1UFO76UpDfPm2SF/Rz/o33cm699X++EYPxTnoEc
vmWeS0I7eDXc4OCUiToG0sEx0klE0CX1Z1tK6qJ+zgWQLZ9SZEC9H0NsSA6LhrHu
Nq0dzeK3LjhdfcX46/4GqdiptpdTuM4m/hOQ5yx4JMQ/n1sdpv4M5VLRWwWW9Lem
ufb79Id7O9SispxgRsz1KXIjp7N9S4BY7itSXz97uSyzTqEjWZ6mDUhTu3t21GKC
6flALGTTrG2yghEhz53rkvLsvwzjPSSlT6LIf0mrRPzHaf+EdaKoasElE1SHh+ZH
9mI81HywpE+HZ+W+5hBCvjYp90Y1fwIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
```

```
BgNVHQ4EFgQU58tN2JO+yEGq5JbIXxGi4vRVPyIwgY4GA1UdIwSBhjCBg4AU58tN
2JO+yEGq5JbIXxGi4vRVPyKhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAOVp1h2I9wW7MBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBANBN0e1EqNy4+IU2yQzMJ+Wy5ZIOtTP6GSBR
7muVY1bDeAwtNTEOpwgrZVlC7/xq5Q0LC1y0Z70hHXEf8au7qStaAoUtxzvhTAZI
NC0lwoFU56UFw4N0vZII17iqEfoqRC4PpI3OxqEJHFy0VLlvAzJoKB4QLLqDAYVA
LXCiOLoVT+y9tRYsxw5MyO0Bi6fxQIIADl2bE9xkunTN1Jkkwqo3LxNy/ryz4QWR
8K7jHUItifv4h/hxBKpHEquN8CkdvM9oeGl7I8PFrSFEpGr1euDXY0euZzzYiDBV
m6GpTJgzpVsEuIX52dPcPemwQncoIfZyhWDW85MJUnby2WTEcFo=
-----END CERTIFICATE-----
```

México (Centro): mx-central-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7zCCAq8CCQD4QwfTExrgxTAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yNDExMTQwOTQ4MjRaGA8y
MDUwMTExNTA5NDgyNFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0
b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIg
U2VydmljZXMgTExDMIIBtzCCASwGByqGSM44BAEwggEfAoGBAK+pJEOtD2RFlCbf
oAzONffZa42FB8G6OA/30DT81xWvB2Hnmgw7LfiELYqgfuck3YSDffNDcmiFTJuX
AU9u0NtbbxcOytcdUq4HInpHiB85I6WWWKYB66aGbvYowUPpqBZkASb1i/pYAh5W
nNYvx408008tTzqpMfZDchJHzWqBAhUA0ogoJzTw2/4pKhz9aqTsRCzRVPsCgYEA
qklRUcuU0du/bT/M6kWxYvrTGhO9KXQe+7RtbaIq4dWRsCBnO4smDY/GmI9H8ew1
LRJ9AcLGmxDm795CvVZkHNcht7PDAREagWmz2YvhLA+ev6U0RpfdlBXCck2p1CxQ
LMtoFO7DThksHIQBtnlQdHDvguKEZQz/Iobhne6Kb3wDgYQAAoGAQSTlOqFq6RtR
Jvp406XhGl+eO9SQUpevpzG3Dzbdy6EQ8PBJDOHHJvxbebvpnQssh0CnQfTkSw26
jwPy9V5zRC0ZezwnRTyGSJwiErUKDGeVekEAoNJL1USy8jKkgBajlskZrR+0JHDN
Jv3UwYIPplc4ZS2f2E7btrtlaWt/P70wCQYHKoZIzjgEAwMvADAsAhRXljPWKWYf
61DkDVdgPPHsS2/LuwIUejcGV9WuS3uPvJ6lmn4opxUGBZw=
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICPzCCAaigAwIBAgIUCmzpTTMBQYItpMC2VDYsZfIAS7IwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgMEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcMB1NlYXR0bGUxIDAeBgNVBAoMF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQwMjEyNTAzNloXDTI5MDQwMTEyNTAzNlowXDELMAkGA1UEBhMCVVMx
```

```
GTAXBgNVBAgMEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcMB1NlYXR0bGUxIDAe
BgNVBAoMF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQDfvOnCzm1iN58Nm7k6ehoy6v0lnnFI617D6CY3bfuq01RCdEQL
96+pYawJieTH8JAQKj02CAa3AeaqdXTE/pDhI/YKLreeMb4K68WMn24Wjjs6oxjB
bAmsKXtt9ihKHGBFNUhgFrNFYyA2i7ieJviwpHjQ/XgXiG2u1/t/4VydUwIDAQAB
MA0GCSqGSIb3DQEBCwUAA4GBAL5+vvj4lhaE+J5tuCqV3XJzDd97lsD4le2O2uGw
P0sGdUcRAdxzU3Bwq/hhtzNWnfwo0aCEQKmLM7xyd3nUa0VvKXLq+DDuayipWINr
OATnNxFRe99d38qHTR1dgkjZdKbbtnl6O4fgM57tVEuQJd/N4ILl9jaRcJ5Ip+9t
3y5t
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJALxuE00HoJomMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yNDEwMzEx
MTE0MzNaGA8yMjA0MDQwNjExMTQzM1owXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA13xWucALo8M/TXbZJgHrqFqFON91dSLPE/eLbmeIJbP1pb9ICd33qKAx
HlKSrXI9b9YS3U1Pl0bF3ZgfeE/x4Y0KDDZwzpf07H8IgRittULJoNLYVKCJXWPq
Ky1qvDJX3653dUbUu9eAdVCTRgk7eKpPBLAmW27+pgAGzEYrVV3u2AvqNTonvfTU
sPgEVnAL1J490pNM85KtFynxFTWGigHkd3BHidxmLrTH4I4eRxNZ9q/3gsDW+zKt
jQlpM7JzZa2OqxsF5YQDh1fF52Emqsr+ufLeGqDLOgT1QWcqpz57AX8GqZpgZULo
itCRNXbQDzZY9FxIgpiFJv3y/qYYDQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQCt
MTeH4EgqjJEjb1qm5tzXYurLprVrEVQ+PhGXJFJd3xAZyeaDVYy7kio08E2xhmHd
HtkBDty2KnOHsTQmeAJCci7d4tYXZ/1qe341wwm9OoFcO8jhIndx6FXJCgQUY4dL
AAr9HQJFWG5dMZgbi1Zuhxdio3sSoOBjL2p7QIsGNkITvCDIs/H0/szpJnyyyIqu
wmUhSel5hdy5MwOsyUKVGnAdaS5Vd9oL4kLszS9nBZ7ny6BC9odIkFAdGqQ5vM4z
vcbfOq14hjatQmJgJhksN/0Dpl78Gheq0pIhP8LTkAOEG2832nQLzCa3oxSk8otG
GJXkzzyQjse+13r8+yNJ
-----END CERTIFICATE-----
```

Oriente Médio (Bahrein): me-south-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7jCCAq4CCQCVWIgSmP8RhTAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xOTAyMDUxMzA2MjFaFw00
```

```
NTAyMDUxMzA2MjFaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbgwggEsBgcqhkjOOAQBMIIBHwKBgQDcwojQfgWdV1QliO0B
8n6cLZ38VE7ZmrjZ9OQV//Gst6S1h7euhC23YppKXi1zovefSDwFU54zi3/oJ++q
PHlP1WGL8IZ34BUgRTtG4TVolvp0smjkMvyRu5hIdKtzjV93Ccx15gVgyk+o1IEG
fZ2Kbw/Dd8JfoPS7KaSCmJKxXQIVAIZbIaDFRGa2qcMkW2HWASyNDl7bAoGBANtz
IdhfMq+l2I5iofY2oj3HI21Kj3LtZrWEg3W+/4rVhL3lTm0Nne1rl9yGujrjQwy5
Zp9V4A/w9w2O10Lx4K6hj34Eefy/aQnZwNdNhv/FQP7Az0fju+Yl6L13OOHQrL0z
Q+9cF7zEosekEnBQx3v6psNknKgD3Shgx+GO/LpCA4GFAAKBgQCVS7m77nuNAlZ8
wvUqcooxXMPkxJFl54NxAsAul9KP9KN4svm0O3Zrb7t2FOtXRM8zU3TqMpryq1o5
mpMPsZDg6RXo9BF7Hn0DoZ6PJTamkFA6md+NyTJWJKvXC7iJ8fGDBJqTciUHuCKr
12AztQ8bFWsrTgTzPE3p6U5ckcgV1TAJBgcqhkjOOAQDAy8AMCwCFB2NZGWm5EDl
86ayV3c1PEDukgQIAhQow38rQkN/VwHVeSW9DqEshXHjuQ==
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDPDCCAqWgAwIBAgIJAMl6uIV/zqJFMA0GCSqGSIb3DQEBCwUAMHIxCzAJBgNV
BAYTAlVTMRMwEQYDVQQIDApXYXNoaW5ndG9uMRAwDgYDVQQHDAdTZWF0dGxlMSAw
HgYDVQQKDBdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzEaMBgGA1UEAwwRZWMyLmFt
YXpvbmF3cy5jb20wIBcNMTkwNDI2MTQzMjQ3WhgPMjE5ODA5MjkxNDMyNDdaMHIx
CzAJBgNVBAYTAlVTMRMwEQYDVQQIDApXYXNoaW5ndG9uMRAwDgYDVQQHDAdTZWF0
dGxlMSAwHgYDVQQKDBdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzEaMBgGA1UEAwwR
ZWMyLmFtYXpvbmF3cy5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBALVN
CDTZEnIeoX1SEYqq6k1BV0ZlpY5y3KnoOreCAE589TwS4MX5+8Fzd6AmACmugeBP
Qk7Hm6b2+g/d4tWycyxLaQlcq81DB1GmXehRkZRgGeRge1ePWd1TUA0I8P/QBT7S
gUePm/kANSFU+P7s7u1NNl+vynyi0wUUrw7/wIZTAgMBAAGjgdcwgdQwHQYDVR0O
BBYEFILtMd+T4YgH1cgc+hVsVOV+480FMIGkBgNVHSMEgZwwgZmAFILtMd+T4YgH
1cgc+hVsVOV+480FoXakdDByMQswCQYDVQQGEwJVUzETMBEGA1UECAwKV2FzaGlu
Z3RvbjEQMA4GA1UEBwwHU2VhdHRsZTEgMB4GA1UECgwXQW1hem9uIFdlYiBTZXJ2
aWNlcyBMTEMxGjAYBgNVBAMMEWVjMi5hbWF6b25hd3MuY29tggkAyXq4hX/OokUw
DAYDVR0TBAUwAwEB/zANBgkqhkiG9w0BAQsFAAOBgQBhkNTBIFgWFd+ZhC/LhRUY
4OjEiykmbEp6hlzQ79T0Tfbn5A4NYDI2icBP0+hmf6qSnIhwJF6typyd1yPK5Fqt
NTpxxcXmUKquX+pHmIkK1LKDO8rNE84jqxrxRsfDi6by82fjVYf2pgjJW8R1FAw+
mL5WQRFexbfB5aXhcMo0AA==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJANZkFlQR2rKqMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
```

```
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xOTAyMDUx
MzA2MjBaGA8yMTk4MDcxMTEzMDYyMFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAy4Vnit2eBpEjKgOKBmyupJzJAiT4fr74tuGJNwwa+Is2vH12jMZn9Il1
UpvvEUYTIboIgISpf6SJ5LmV5rCv4jT4a1Wm0kjfNbiIlkUi8SxZrPypcw24m6ke
BVuxQZrZDs+xDUYIZifTmdgD50u5YE+TLg+YmXKnVgxBU6WZjbuK2INohi71aPBw
2zWUR7Gr/ggIpf635JLU3KIBLNEmrkXCVSnDFlsK4eeCrB7+UNak+4BwgpuykSGG
Op9+2vsuNqFeU1l9daQeG9roHR+4rIWSPa0opmMxv5nctgypOrE6zKXx2dNXQldd
VULv+WH7s6Vm4+yBeG8ctPYH5GOo+QIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQBs
ZcViiZdFdpcXESZP/KmZNDxB/kktlIEIhsQ+MNn29jayE5oLmtGjHj5dtA3XNKlr
f6PVygVTKbtQLQqunRT83e8+7iCZMKI5ev7pITUQVvTUwI+Fc01JkYZxRFlVBuFA
WGZO+98kxCS4n6tTwVt+nSuJr9BJRVC17apfHBgSS8c5OWna0VU/Cc9ka4eAfQR4
7pYSDU3wSRE01cs30q34lXZ629IyFirSJ5TTOIc0osNL7vwMQYj8HOn4OBYqxKy8
ZJyvfXsIPh0Na76PaBIs6ZlqAOflLrjGzxBPiwRM/XrGmF8ze4KzoUqJEnK13O6A
KHKgfiigQZ1+gv5FlyXH
-----END CERTIFICATE-----
```

Oriente Médio (EAU): me-central-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7zCCAq
+gAwIBAgIGAXjXhqnnMAkGByqGSM44BAMwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgMEFdhc2hpbmd0b24gU3RhdGUxED
U4EddRIpUt9KnC7s5Of2EbdSPO9EAMMeP4C2USZpRV1AIlH7WT2NWPq/
xfW6MPbLm1Vs14E7gB00b/JmYLdrmVClpJ+f6AR7ECLCT7up1/63xhv4O1fnxqimFQ8E
+4P208UewwI1VBNaFpEy9nXzrith1yrv8iIDGZ3RSAHHAhUAl2BQjxUjC8yykrmCouuEC/
BYHPUCgYEA9+GghdabPd7LvKtcNrhXuXmUr7v6OuqC+VdMCz0HgmdRWVeOutRZT
+ZxBxCBgLRJFnEj6EwoFhO3zwkyjMim4TwWeotUfI0o4KOuHiuzpnWRbqN/C/ohNWLx
+2J6ASQ7zKTxvqhRkImog9/hWuWfBpKLZl6Ae1UlZAFMO/7PSSoDgYQAAoGAW+csuHsWp/7/
pv8CTKFwxsYudxuR6rbWaHCykIeAydXL9AWnphK6yp1ODEMBFl68Xq8Hp23sOWyf8moOhqCom9+0+ovuUFdpvCie86bp
TOZU568Ty1ff3dDWbdRzeNQRHodRG+XEQSizMkAreeWt4kBa+PUwCQYHKoZIzjgEAwMvADAsAhQD3Z
+XGmzKmgaLgGcVX/Qf1+Tn4QIUH1cgksBSVKbWj81tovBMJeKgdYo=
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICMzCCAZygAwIBAgIGAXjRrnDjMA0GCSqGSIb3DQEBBQUAMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIDBBXYXNoaW5n
KyA6zyruJQrYy00a6wqLA7eeUzk3bMiTkLsTeDQfrkaZMfBAjGaaOymRo1C3qzE4rIenmahvUplu9ZmLwL1idWXMRX2R
+d2SeoKOKQWoc2UOFZMHYxDue7zkyk1CIRaBukTeY13/
```

```
RIrlc6X61zJ5BBtZXlHwayjQIDAQABMA0GCSqGSIb3DQEBBQUAA4GBABTqTy3R6RXKPW45FA+cgo7YZEj/
Cnz5YaoUivRRdX2A83BHuBTvJE2+WX00FTEj4hRVjameE1nENoO8Z7fUVloAFDlDo69fhkJeSvn51D1WRrPnoWGgEfr1
B+Wqm3kVEz/QNcz6npmA6
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAM4h7b1CVhqqMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yMjA0MTEx
MDE1MDNaGA8yMjAxMDkxNTEwMTUwM1owXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEApybTWfMOhSoMpqPo72eqAmnn1dXGZM+G8EoZXzwHwT/+IHEXNB4q5N6k
tudYLre1bJxuzEw+iProSHjmb9bB9YscRTofjVhBlt35Fc+i8BaMeH94SR/eE8QO
mll8gnLNW3d62lyuhzuyv1e5wVlRqzYw+X2zRH4/wRDOCOpzjKoHIgyPKsMgwsw5
aTZhNMsGxZN9dbkf0iCGeQLDytwU/JTh/HqvSr3VfUOapTJJiyAxoCtZWgp1/7wC
RvOCSMRJobpUqxZgl/VsttwNkikSFz1wGkcYeSQvk+odbnYQckA8tdddoVI56eD4
qtREQvfpMAX5v7fcqLexl5d5vH8uZQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQUOadrbTs+OhzwoAgUJ7RqQNdwufkwgY4GA1UdIwSBhjCBg4AUOadr
bTs+OhzwoAgUJ7RqQNdwufmhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIEExMQ4IJAM4h7b1CVhqqMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAICTdAOGEOnII8HaGCpCB8us/hGFaLptJaAf
D5SJAyVy66/mdfjGzE1BKkKxnbxemEVUIzbRidOnyilB+pKwN3edAjTZtWdpVA0V
R/G/qQPmcVljtycBz4VC6SuOUYflGzLH1GZ6GJWbuDtFzw8r7HGdRN1wrEPe3UF2
sMpuVezqnRUdvVRoVQP4jFgNsE7kNvtn2NiPhb/CtrxpcwIQ7r6YeoHcBSheuV1Z
xZDHynC3KUprQGx1+Z9QqPrDf180MaoqAlTl4+W6Pr2NJYrVUFGS/ivYshMg574l
CPU6r4wWZSKwEUXq4BInYX6z6iclp/p/J5QnJp2mAwyi6M+I13Y=
-----END CERTIFICATE-----
```

América do Sul (São Paulo) — sa-east-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
```

```
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUX4Bh4MQ86Roh37VDRRX1MNOB3TcwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE2NDYwOVoXDTI5MDQyODE2NDYwOVowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUX4Bh4MQ8
6Roh37VDRRX1MNOB3TcwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQBnhocfH6ZIX6F5K9+Y9V4HFk8vSaaKL5ytw/P5td1h9ej94KF3xkZ5fyjN
URvGQv3kNmNJBoNarcP9I7JIMjsNPmVzqWawyCEGCZImoARxSS3Fc5EAs2PyBfcD
9nCtzMTaKO09Xyq0wqXVYn1xJsE5d5yBDsGrzaTHKjxo61+ezQ==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAMcyoxx4U0xxMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTA4MTQw
ODU4MDJaGA8yMTk1MDExNzA4NTgwMlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
```

```
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAw45IhGZVbQcy1fHBqzROhO8CsrDzxj/WP4cRbJo/2DAnimVrCCDs5O86
FA39Zo1xsDuJHDlwMKqeXYXkJXHYbcPWc6EYYAnR+PlLG+aNSOGUzsy202S03hT0
B20hWPCqpPp39itIRhG4id6nbNRJOzLm6evHuepMAHR4/OV7hyGOiGaV/v9zqiNA
pMCLhbh2xk0PO35HCVBuWt3HUjsgeks2eEsu9Ws6H3JXTCfiqp0TjyRWapM29OhA
cRJfJ/d/+wBTz1fkWOZ7TF+EWRIN5ITEadlDTPnF1r8kBRuDcS/lIGFwrOOHLo4C
cKoNgXkhTqDDBDu6oNBb2rS0K+sz3QIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQUqBy7D847Ya/w321Dfr+rBJGsGTwwgY4GA1UdIwSBhjCBg4AUqBy7
D847Ya/w321Dfr+rBJGsGTyhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAMcyoxx4U0xxMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBACOoWSBf7b9AlcNrl4lr3QWWSc7k90/tUZal
PlT0G3Obl2x9T/ZiBsQpbUvs0lfotG0XqGVVHcIxF38EbVwbw9KJGXbGSCJSEJkW
vGCtc/jYMHXfhx67Szmftm/MTYNvnzsyQQ3v8y3Rdah+xe1NPdpFrwmfL6xe3pFF
cY33KdHA/3PNLdn9CaEsHmcmj3ctaaXLFIzZhQyyjtsrgGfTLvXeXRokktvsLDS/
YgKedQ+jFjzVJqgr4NjfY/Wt7/8kbbdhzaqlB5pCPjLLzv0zp/XmO6k+JvOePOGh
JzGk5t1QrSju+MqNPFk3+1O7o910Vrhqw1QRB0gr1ExrviLbyfU=
-----END CERTIFICATE-----
```

AWS GovCloud (Leste dos EUA): us-gov-east-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIULVyrqjjwZ461qelPCiShB1KCCj4wDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDUwNzE1MjIzNloXDTI5MDUwNjE1MjIzNlowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCpohwYUVPH9I7Vbkb3WMe/JB0Y/bmfVj3VpcK445YBRO9K80al
esjgBc2tAX4KYg4Lht4EBKccLHTzaNi51YEGX1aLNrSmxhz1+WtzNLNUsyY3zD9z
vwX/3k1+JB2dRA+m+Cpwx4mjzZyAeQtHtegVaAytkmqtxQrSCexBxvqRqQIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQU1ZXneBYnPvYXkHVlVjg7918V
gE8wgZkGA1UdIwSBkTCBjoAU1ZXneBYnPvYXkHVlVjg7918VgE+hYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IULVyrqjjw
Z461qelPCiShB1KCCj4wEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQBfAL/YZv0y3zmVbXjyxQCsDloeDCJjFKIu3ameEckeIWJbST9LMto0zViZ
puIAf05x6GQiEqfBMk+YMxJfcTmJB4Ebaj4egFlslJPSHyC2xuydHlr3B04INOH5
Z2oCM68u6GGbj0jZjg7GJonkReG9N72kDva/ukwZKgq8zErQVQ==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJALPB6hxFhay8MA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xODA0MTAx
MjMyNDlaGA8yMTk3MDkxMzEyMzI0OVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAva9xsI9237KYb/SPWmeCVzi7giKNron8hoRDwlwwMC9+uHPd53UxzKLb
pTgtJWAPkZVxEdl2Gdhwr3SULoKcKmkqE6ltVFrVuPT33La1UufguT9k8ZDDuO9C
hQNHUdSVEuVrK3bLjaSsMOS7Uxmnn7lYT990IReowvnBNBsBlcabfQTBV04xfUG0
/m0XUiUFjOxDBqbNzkEIblW7vK7ydSJtFMSljga54UAVXibQt9EAIF7B8k9l2iLa
mu9yEjyQy+ZQICTuAvPUEWe6va2CHVY9gYQLA31/zU0VBKZPTNExjaqK4j8bKs1/
7dOV1so39sIGBz21cUBec1o+yCS5SwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQBt
hO2W/Lm+Nk0qsXW6mqQFsAou0cASc/vtGNCyBfoFNX6aKXsVCHxq2aq2TUKWENs+
mKmYu1lZVhBOmLshyllh3RRoL3Ohp3jCwXytkWQ7ElcGjDzNGc0FArzB8xFyQNdK
MNvXDi/ErzgrHGSpcvmGHiOhMf3UzChMWbIr6udoDlMbSIO7+8F+jUJkh4Xl1lKb
YeN5fsLZp7T/6YvbFSPpmbn1YoE2vKtuGKxObRrhU3h4JHdp1Zel1pZ6lh5iM0ec
SD11SximGIYCjfZpRqI3q50mbxCd7ckULz+UUPwLrfOds4VrVVSj+x0ZdY19Plv2
9shw5ez6Cn7E3IfzqNHO
```

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

AWS GovCloud (Oeste dos EUA): us-gov-west-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUe5wGF3jfb7lUHzvDxmM/ktGCLwwwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDUwNzE3MzAzMloXDTI5MDUwNjE3MzAzMlowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCpohwYUVPH9I7Vbkb3WMe/JB0Y/bmfVj3VpcK445YBRO9K80al
esjgBc2tAX4KYg4Lht4EBKccLHTzaNi51YEGX1aLNrSmxhz1+WtzNLNUsyY3zD9z
vwX/3k1+JB2dRA+m+Cpwx4mjzZyAeQtHtegVaAytkmqtxQrSCexBxvqRqQIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQU1ZXneBYnPvYXkHVlVjg7918V
gE8wgZkGA1UdIwSBkTCBjoAU1ZXneBYnPvYXkHVlVjg7918VgE+hYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUe5wGF3jf
b7lUHzvDxmM/ktGCLwwwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
```

```
AAOBgQCbTdpx1Iob9SwUReY4exMnlwQlmkTLyA8tYGWzchCJOJJEPfsW0ryy1A0H
YIuvyUty3rJdp9ib8h3GZR71BkZnNddHhy06kPs4p8ewF8+d8OWtOJQcI+ZnFfG4
KyM4rUsBrljpG2aOCm12iACEyrvgJJrS8VZwUDZS6mZEnn/lhA==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJANCOF0Q6ohnuMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTA5MTAx
OTQyNDdaGA8yMTk1MDIxMzE5NDI0N1owXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAzIcGTzNqie3f1olrrqcfzGfbymSM2QfbTzDIOG6xXXeFrCDAmOq0wUhi
3fRCuoeHlKOWAPu76B9os71+zgF22dIDEVkpqHCjBrGzDQZXXUwOzhm+PmBUI8Z1
qvbVD4ZYhjCujWWzrsX6Z4yEK7PEFjtf4M4W8euw0RmiNwjy+knIFa+VxK6aQv94
lW98URFP2fD84xedHp6ozZlr3+RZSIFZsOiyxYsgiwTbesRMI0Y7LnkKGCIHQ/XJ
OwSISWaCddbu59BZeADnyhl4f+pWaSQpQQ1DpXvZAVBYvCH97J1oAxLfH8xcwgSQ
/se3wtn095VBt5b7qTVjOvy6vKZazwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQA/
S8+a9csfASkdtQUOLsBynAbsBCH9Gykq2m8JS7YE4TGvqlpnWehz78rFTzQwmz4D
fwq8byPkl6DjdF9utqZ0JUo/Fxelxom0h6oievtBlSkmZJNbgc2WYm1zi6ptViup
Y+4S2+vWZyg/X1PXD7wyRWuETmykk73uEyeWFBYKCHWsO9sI+62O4Vf8Jkuj/cie
1NSJX8fkervfLrZSHBYhxLbL+actVEo00tiyZz8GnhgWx5faCY38D/k4Y/j5Vz99
7lUX/+fWHT3+lTL8ZZK7fOQWh6NQpI0wTP9KtWqfOUwMIbgFQPoxkP00TWRmdmPz
WOwTObEf9ouTnjG9OZ20
-----END CERTIFICATE-----
```

Nuvem soberana da AWS na Europa — eusc-de-east-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC8DCCAq8CCQDyckpYH0omIDAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yNDEwMTgwOTM5MzdaGA8y
MDUwMTAxOTA5MzkzN1owXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0
b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIg
U2VydmljZXMgTExDMIIBtzCCASsGByqGSM44BAEwggEeAoGBAJR1zx7FzSGhXd3m
U1PfwH33QEK4CHnFSnp/DUse0SdLwsvLkHw7Tq3M7IX4E+TZ6OzYZZeoVZttqbyq
OZ8ROUS7CzDWcQ0503de/ya51cTs4BiO4nv2awm1WEoV9XtQyA2JLn0Jv7g2uja0
317krS+Dk3kjs9RpWvkmiyTMu1YhAhUA69U+A26BWLVpNIZZ0uWMZJSNlIkCgYBw
```

```
w1cgrHFGEqJNhqN7Sjs2YwTP+jpp1GvhxKyce5aOh5ErVvufb5gVVoKahrrHEBms
TrBXxnfcPaTupwdmEZ9eM8a+9RS2vye//KU1kGIOMgafPEzBEXs9m7okmAQpYXnG
cVOTtx2gd/E/VfKRiMSAmam178qwvcbcijNqRdLjRQOBhQACgYEAiEFVGYVCntmy
va8c2oU5/owdMws+NZ6u9blat0ymPr/8Q+DR77CgUPJW+K0k41GdgWpVlrsjiiPw
iygzw4DW7Vsl018KcIFUTiSwpzv2in+tKNUkO5Ly0q6arbSxrXZffYe7aOZKtCCH
XWDMKOH2iCvZptMpG7fDDSc7Be8v4AgwCQYHKoZIzjgEAwMwADAtAhQyvCF3q437
RvdPXMFcMc6qrD0svAIVAMvsN3NwOY4KRYlFv9Dnok8D/ixI
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICNjCCAZ+gAwIBAgIJAPybReXZqUSNMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yNDEwMTgw
OTM5MzdaGA8yMjA0MDMyNDA5MzkzN1owXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKB
gQDShbskmohorgcjN7gfApw89CEsg7praCDggaUVXF6gy9JdJ5INcv7+DkwKaAxd
NQWDsWZnxIOqPuPfyAYVP3D2/exP3Rfxj31UomLduu7S83zgiJ8VVL/GzlDELv5/
K2rTcd+580NjLSa6FYDcXDip2ir6TXxRYBYHP65dwniE+wIDAQABMA0GCSqGSIb3
DQEBCwUAA4GBAKu9t3CAtZt7c+k4bCZlmxrwgps1668p24x7QRmLxgXnwj5A2MOM
qEtxA9Q3q3WxUc0nWKaCTvRrTfWW917xsLcvVL8rI6xCjg2bb5FJ73xzcfSxHr9I
Q1mThJgLaWVIbllGJK7+EogR7gfqlPhc0Ql5bYuaozdt+r69xNuJlyR
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAODRxRi5VXBbMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yNTAyMjEx
MjQ0MTRaGA8yMjA0MDcyODEyNDQxNFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAr24OkDrpRU1ffx1PAcHZbKu7fZkhfT/e/PDhSkp2FvOzJEqDUT23E2wp
K/44mhJ3d8blYtgBiRXjqRsAFu8ZbzXLc0gaQ9A5woxfx5b7iOMwneCajS9xS5qr
cE0MMEY9XwG8MCp9YBoDJqDJh74oQqcPROBq16L4k2Ys22n1khus4JpwT7VSRE1I
nnt7fGIYsUmNGM+T2E6ubG3FvkY0HbLvNCcGRMCnDYqloo2BthuSG58KbMAku7VD
hMxzzJte5yMuRpHBojQr9N0hZcSJCtSFo6FhlxCzxGzwoSKzqm99ULYL4lf+IORe
DaKoATZJvbnX0LYAKLtPr1Pz9SD9pQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQUHpdxehvJwYL2o25SXyxsSndDW48wgY4GA1UdIwSBhjCBg4AUHpdx
ehvJwYL2o25SXyxsSndDW4+hYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
```

```
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAODRxRi5VXBbMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAFGcArNlGB3oRBaXohpnhrnVblhJJa6U7r1/
M5TAJCKCkziSz3lOZmZZ1YgSnQC1blhUD2rhuS8a0Mw1Ml48nLjIYMMK0tkJRKCD
LPxxEZp4EzogYj6PqfSubzm59MmBenIcJPaJ9y2uY1U4Q3PMfU6M1JqqQ0Lzplq0
n9eWpJK3+7UbtuyAzigO4DRWEBMxJBUU7f2LfY+qFjskoeHopX20cmn1vc1TGyAF
Qf8xdt1SaPKC26zJsrCkiMZJNm4aa8KqvhqBHVjV4NrGeVGCcdlmSDiL71Egk9kh
744eGQxNnhZNvePW2kVcSuh0HpAo4Q4vfpjN+jz2Ves3kjFsrgc=
-----END CERTIFICATE-----
```

Conformidade com STIG para a instância do EC2

Guias de implementação técnica de segurança (STIGs) são os padrões de fortalecimento de configuração criados pela Agência de Sistemas de Informação de Defesa (DISA) para proteger os sistemas e softwares de informação. Para que seus sistemas estejam em conformidade com os padrões STIG, você deve instalar, definir e testar uma variedade de configurações de segurança.

STIGs são aplicados com base nas seguintes classificações de vulnerabilidade. Ao criar uma imagem com hardening STIG ou ao aplicar as configurações STIG a uma instância existente, você pode escolher o nível a ser aplicado para hardening. Os níveis mais altos incluem as configurações STIG de todos os níveis mais baixos. Por exemplo, o nível Alto (categoria I) inclui as configurações das categorias de Médio e Baixo.

Níveis de conformidade

- Alto (categoria I)

  O risco mais grave. Inclui qualquer vulnerabilidade que possa resultar em perda de confidencialidade, disponibilidade ou integridade.
- Médio (categoria II)

  Inclui qualquer vulnerabilidade que possa resultar em perda de confidencialidade, disponibilidade ou integridade, mas os riscos podem ser mitigados.
- Baixo (categoria III)

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

O Amazon EC2 fornece os seguintes métodos de criação de instâncias com hardening STIG:

- Nas AMIs públicas especializadas do Windows da AWS, você pode iniciar instâncias do Windows pré-configuradas para hardening STIG. Para obter mais informações, consulte STIG Hardened AWS Windows Server AMIs na AWS Windows AMI reference.
- Você pode criar uma AMI personalizada para iniciar instâncias pré-configuradas que são montadas com os componentes de hardening STIG do EC2 Image Builder. Para obter mais informações, consulte STIG hardening components no Image Builder User Guide.
- Você pode usar o documento de comando do AWSEC2-ConfigureSTIG Systems Manager para aplicar as configurações STIG a uma instância EC2 existente. O documento de comando STIG do Systems Manager verifica se há configurações incorretas e executa um script de correção para instalar e atualizar os certificados do DoD e remover os certificados desnecessários para manter a conformidade com STIG. Não há cobranças adicionais pelo uso do documento do STIG Systems Manager.

Tópicos

- Configurações de hardening STIG para instâncias do EC2
- Downloads do scripts de hardening STIG
- Usar o AWS Systems Manager para aplicar configurações STIG à instância

Configurações de hardening STIG para instâncias do EC2

As configurações STIG variam de acordo com o sistema operacional da instância e o nível de conformidade que você escolhe. O conteúdo a seguir contém detalhes específicos do sistema para STIGs que são aplicados em cada nível de conformidade.

Conteúdo

- Configurações STIG para instâncias do Linux do EC2
- Configurações de hardening STIG para instâncias do EC2 Windows

Configurações STIG para instâncias do Linux do EC2

Esta seção contém informações sobre as configurações de hardening STIG do Linux compatíveis com o Amazon EC2. O script de hardening aplica à infraestrutura as configurações STIG compatíveis, com base na distribuição do Linux. Se a distribuição do Linux não tiver suas próprias configurações de hardening STIG, o Amazon EC2 usará as configurações do RHEL.

- Configurações do Red Hat Enterprise Linux (RHEL) 7 STIG
  - RHEL 7
  - CentOS 7
  - Amazon Linux 2 (AL2)
- Configurações do RHEL 8 STIG
  - RHEL 8
  - CentOS 8
- Configurações do RHEL 9 STIG
  - RHEL 9
  - CentOS Stream 9

Linux STIG Low (categoria III)

A lista a seguir contém as configurações do STIG que o Amazon EC2 suporta em sua infraestrutura. Se uma configuração compatível não for aplicável à sua infraestrutura, o Amazon EC2 ignora essa configuração e segue em frente. Por exemplo, algumas configurações de fortalecimento do STIG podem não se aplicar a servidores autônomos. Políticas específicas da organização também podem afetar as configurações aplicáveis, como um requisito para que os administradores revisem as configurações do documento.

Para obter uma lista completa, consulte a Biblioteca de documentos STIGs. Para obter informações sobre como visualizar a lista completa, consulte STIG Viewing Tools.

STIG versão 3 lançamento 15 do RHEL 7

- RHEL 7/CentOS 7/AL2

  V-204452, V-204576 e V-204605

STIG versão 2 lançamento 4 do RHEL 8

- RHEL 8/CentOS 8

  V-230241, V-230269, V-230270, V-230281, V-230285, V-230346, V-230381, V-230395, V-230468, V-230469, V-230485, V-230486, V-230491, V-230494, V-230495, V-230496, V-230497, V-230498, V-230499 e V-244527

STIG versão 2 lançamento 5 do RHEL 9

- RHEL 9/CentOS Stream 9

  V-257782, V-257795, V-257796, V-257824, V-257880, V-257946, V-257947, V-258037, V-258067, V-258069, V-258076, V-258138 e V-258173

STIG versão 1 lançamento 1 do Amazon Linux 2023

V-274141

STIG versão 3 lançamento 3 do SLES 12

V-217108, V-217113, V-217140, V-217198, V-217209, V-217211, V-217212, V-217213, V-217214, V-217215, V-217216, V-217236, V-217237, V-217238, V-217239, V-217282 e V-255915

STIG versão 2 lançamento 5 do SLES 15

V-234811, V-234850, V-234868, V-234868, V-234873, V-234873, V-234905, V-234907, V-234908, V-234909, V-234933, V-234934, V-234935, V-234936, V-234955, V-234963, V-234967 e V-255921

STIG versão 2 lançamento 15 do Ubuntu 18.04

V-219163, V-219164, V-219165, V-219172, V-219173, V-219174, V-219175, V-219178, V-219179, V-219180, V-219210, V-219301, V-219327, V-219332 e V-219333

STIG versão 2 lançamento 3 do Ubuntu 20.04

V-238202, V-238203, V-238221, V-238222, V-238223, V-238224, V-238226, V-238234, V-238235, V-238237, V-238308, V-238323, V-238357, V-238362 e V-238373

STIG versão 2 lançamento 5 do Ubuntu 22.04

V-260479, V-260480, V-260481, V-260521, V-260520, V-260476, V-260472, V-260549, V-260550, V-260551, V-260552, V-260581 e V-260596

STIG versão 1 lançamento 2 do Ubuntu 24.04

V-270645, V-270646, V-270664, V-270820, V-270677, V-270690, V-270706, V-270710, V-270695, V-270749, V-270752 e V-270818

Linux STIG Medium (categoria II)

A lista a seguir contém as configurações do STIG que o Amazon EC2 suporta em sua infraestrutura. Se uma configuração compatível não for aplicável à sua infraestrutura, o Amazon EC2 ignora essa configuração e segue em frente. Por exemplo, algumas configurações de fortalecimento do STIG podem não se aplicar a servidores autônomos. Políticas específicas da organização também podem afetar as configurações aplicáveis, como um requisito para que os administradores revisem as configurações do documento.

Para obter uma lista completa, consulte a Biblioteca de documentos STIGs. Para obter informações sobre como visualizar a lista completa, consulte STIG Viewing Tools.

> **Note**
>
> A categoria Linux STIG Medium inclui todas as configurações de fortalecimento do STIG listadas que se aplicam à Linux STIG Low (categoria III), além das configurações de fortalecimento de STIG que o Amazon EC2 suporta para vulnerabilidades de categoria II.

STIG versão 3 lançamento 15 do RHEL 7

Inclui todas as configurações de fortalecimento do STIG que o Amazon EC2 suporta para vulnerabilidades de categoria III (Baixa), além de:

- RHEL 7/CentOS 7/AL2

  V-204405, V-204406, V-204407, V-204408, V-204409, V-204410, V-204411, V-204412, V-204413, V-204414, V-204415, V-204416, V-204417, V-204418, V-204420, V-204422, V-204423, V-204426, V-204427, V-204431, V-204434, V-204435, V-204437, V-204449, V-204450, V-204451, V-204457, V-204466, V-204490, V-204491, V-204503, V-204507, V-204508, V-204510, V-204511, V-204512, V-204514, V-204515, V-204516, V-204517, V-204521, V-204524, V-204531, V-204536, V-204537, V-204538, V-204539, V-204540, V-204541, V-204542, V-204543, V-204544, V-204545, V-204546, V-204547, V-204548, V-204549, V-204550, V-204551, V-204552, V-204553, V-204554, V-204555, V-204556, V-204557, V-204558, V-204559, V-204560, V-204562, V-204563, V-204564, V-204565, V-204566, V-204567, V-204568, V-204572, V-204579, V-204584, V-204585, V-204587, V-204588, V-204589, V-204590, V-204591, V-204592, V-204593, V-204596, V-204597, V-204598, V-204599, V-204600, V-204601, V-204602, V-204609, V-204610, V-204611, V-204612, V-204613, V-204614, V-204615, V-204616, V-204617, V-204619, V-204622, V-204625, V-204630, V-204631, V-204633, V-233307, V-237634, V-237635, V-251703, V-255925, V-255927 e V-256970

STIG versão 2 lançamento 4 do RHEL 8

Inclui todas as configurações de fortalecimento do STIG que o Amazon EC2 suporta para vulnerabilidades de categoria III (Baixa), além de:

- RHEL 8/CentOS 8

  V-230222, V-230228, V-230231, V-230233, V-230236, V-230237, V-230238, V-230239, V-230240, V-230244, V-230245, V-230246, V-230247, V-230248, V-230249, V-230250, V-230255, V-230256, V-230257, V-230258, V-230259, V-230260, V-230261, V-230262, V-230266, V-230267, V-230268, V-230271, V-230273, V-230275, V-230276, V-230277, V-230278, V-230279, V-230280, V-230282, V-230286, V-230287, V-230288, V-230290, V-230291, V-230296, V-230298, V-230310, V-230311, V-230312, V-230313, V-230314, V-230315, V-230316, V-230318, V-230319, V-230320, V-230321, V-230322, V-230324, V-230325, V-230326, V-230327, V-230330, V-230333, V-230335, V-230337, V-230339, V-230341, V-230343, V-230345, V-230347, V-230348, V-230352, V-230353, V-230354, V-230356, V-230357, V-230358, V-230359, V-230360, V-230361, V-230362, V-230363, V-230365, V-230366, V-230368, V-230369, V-230370, V-230372, V-230373, V-230375, V-230376, V-230377, V-230378, V-230380, V-230382, V-230383, V-230385, V-230386, V-230387, V-230389, V-230390, V-230392, V-230393, V-230394, V-230396, V-230397, V-230398, V-230399, V-230400, V-230401, V-230402, V-230403, V-230404, V-230405, V-230406, V-230407, V-230408, V-230409, V-230410, V-230411, V-230412, V-230413, V-230418, V-230419, V-230421, V-230422, V-230423, V-230424, V-230425, V-230426, V-230427, V-230428, V-230429, V-230430, V-230431, V-230432, V-230433, V-230434, V-230435, V-230436, V-230437, V-230438, V-230439, V-230444, V-230446, V-230447, V-230448, V-230449, V-230455, V-230456, V-230462, V-230463, V-230464, V-230465, V-230466, V-230467, V-230470, V-230471, V-230472, V-230473, V-230474, V-230475, V-230478, V-230480, V-230481, V-230482, V-230483, V-230488, V-230489, V-230493, V-230502, V-230503, V-230505, V-230506, V-230507, V-230523, V-230524, V-230525, V-230526, V-230527, V-230532, V-230535, V-230536, V-230537, V-230538, V-230539, V-230540, V-230541, V-230542, V-230543, V-230544, V-230545, V-230546, V-230547, V-230548, V-230549, V-230550, V-230555, V-230556, V-230557, V-230559, V-230560, V-230561, V-237640, V-237642, V-237643, V-244519, V-244523, V-244524, V-244525, V-244526, V-244528, V-244531, V-244533, V-244535, V-244536, V-244538, V-244539, V-244542, V-244543, V-244544, V-244547, V-244550, V-244551, V-244552, V-244553, V-244554, V-250315, V-250316, V-250317, V-251707, V-251708, V-251709, V-251710, V-251711, V-251713, V-251714, V-251715, V-251716, V-251717, V-251718, V-256974, V-257258 e V-274877

STIG versão 2 lançamento 5 do RHEL 9

Inclui todas as configurações de fortalecimento do STIG que o Amazon EC2 suporta para vulnerabilidades de categoria III (Baixa), além de:

- RHEL 9/CentOS Stream 9

  V-257780, V-257781, V-257783, V-257786, V-257788, V-257790, V-257791, V-257792, V-257793, V-257794, V-257797, V-257798, V-257799, V-257800, V-257801, V-257802, V-257803, V-257804, V-257805, V-257806, V-257807, V-257808, V-257809, V-257810, V-257811, V-257812, V-257813, V-257814, V-257815, V-257816, V-257817, V-257818, V-257825, V-257827, V-257828, V-257829, V-257830, V-257831, V-257832, V-257833, V-257834, V-257836, V-257838, V-257839, V-257840, V-257841, V-257842, V-257849, V-257882, V-257883, V-257884, V-257885, V-257886, V-257887, V-257888, V-257889, V-257890, V-257891, V-257892, V-257893, V-257894, V-257895, V-257896, V-257897, V-257898, V-257899, V-257900, V-257901, V-257902, V-257903, V-257904, V-257905, V-257906, V-257907, V-257908, V-257909, V-257910, V-257911, V-257912, V-257913, V-257914, V-257915, V-257916, V-257917, V-257918, V-257919, V-257920, V-257921, V-257922, V-257923, V-257924, V-257925, V-257926, V-257927, V-257928, V-257929, V-257930, V-257933, V-257934, V-257935, V-257936, V-257939, V-257940, V-257942, V-257943, V-257944, V-257948, V-257951, V-257952, V-257953, V-257954, V-257957, V-257958, V-257959, V-257960, V-257961, V-257962, V-257963, V-257964, V-257965, V-257966, V-257967, V-257968, V-257969, V-257970, V-257971, V-257972, V-257973, V-257974, V-257975, V-257976, V-257977, V-257978, V-257979, V-257980, V-257982, V-257983, V-257985, V-257987, V-257988, V-257992, V-257993, V-257994, V-257995, V-257996, V-257997, V-257998, V-257999, V-258000, V-258001, V-258002, V-258003, V-258004, V-258005, V-258006, V-258007, V-258008, V-258009, V-258010, V-258011, V-258028, V-258034, V-258035, V-258038, V-258039, V-258040, V-258041, V-258043, V-258046, V-258049, V-258052, V-258054, V-258055, V-258056, V-258057, V-258060, V-258063, V-258064, V-258065, V-258066, V-258068, V-258070, V-258071, V-258072, V-258073, V-258074, V-258075, V-258077, V-258079, V-258080, V-258081, V-258082, V-258083, V-258084, V-258085, V-258088, V-258089, V-258090, V-258091, V-258092, V-258093, V-258095, V-258097, V-258098, V-258099, V-258100, V-258101, V-258102, V-258103, V-258104, V-258105, V-258107, V-258108, V-258109, V-258110, V-258111, V-258112, V-258113, V-258114, V-258115, V-258116, V-258117, V-258118, V-258119, V-258120, V-258122, V-258123, V-258124, V-258125, V-258126, V-258128, V-258129, V-258130, V-258133, V-258137, V-258140, V-258141, V-258142, V-258144, V-258145, V-258146, V-258147, V-258148, V-258150, V-258151, V-258152, V-258153, V-258154, V-258156, V-258157, V-258158, V-258159, V-258160, V-258161, V-258162, V-258163, V-258164, V-258165, V-258166, V-258167, V-258168, V-258169, V-258170, V-258171, V-258172, V-258175, V-258176, V-258177, V-258178, V-258179, V-258180, V-258181, V-258182, V-258183, V-258184, V-258185, V-258186, V-258187, V-258188, V-258189, V-258190, V-258191, V-258192, V-258193, V-258194, V-258195, V-258196, V-258197,

V-258198, V-258199, V-258200, V-258201, V-258202, V-258203, V-258204, V-258205, V-258206, V-258207, V-258208, V-258209, V-258210, V-258211, V-258212, V-258213, V-258214, V-258215, V-258216, V-258217, V-258218, V-258219, V-258220, V-258221, V-258222, V-258223, V-258224, V-258225, V-258226, V-258227, V-258228, V-258229, V-258232, V-258233, V-258234, V-258237, V-258239, V-258240, V-270174, V-270175, V-270176, V-270177, V-272488 e V-274878

STIG versão 1 lançamento 1 do Amazon Linux 2023

Inclui todas as configurações de fortalecimento do STIG que o Amazon EC2 suporta para vulnerabilidades de categoria III (Baixa), além de:

V-273995, V-274000, V-274001, V-274002, V-274003, V-274004, V-274005, V-274006, V-274008, V-274009, V-274010, V-274011, V-274012, V-274013, V-274014, V-274017, V-274018, V-274019, V-274020, V-274021, V-274022, V-274023, V-274024, V-274026, V-274027, V-274028, V-274030, V-274031, V-274032, V-274033, V-274034, V-274035, V-274036, V-274037, V-274040, V-274041, V-274042, V-274044, V-274045, V-274047, V-274048, V-274049, V-274050, V-274051, V-274053, V-274054, V-274059, V-274061, V-274062, V-274065, V-274069, V-274070, V-274071, V-274072, V-274073, V-274074, V-274075, V-274076, V-274077, V-274078, V-274079, V-274081, V-274082, V-274083, V-274084, V-274085, V-274086, V-274087, V-274088, V-274089, V-274090, V-274091, V-274092, V-274093, V-274094, V-274095, V-274096, V-274097, V-274098, V-274099, V-274100, V-274101, V-274102, V-274103, V-274104, V-274105, V-274106, V-274107, V-274108, V-274109, V-274110, V-274111, V-274112, V-274113, V-274114, V-274115, V-274116, V-274117, V-274119, V-274120, V-274121, V-274122, V-274123, V-274124, V-274125, V-274126, V-274127, V-274128, V-274129, V-274130, V-274131, V-274132, V-274133, V-274134, V-274135, V-274136, V-274137, V-274138, V-274139, V-274140, V-274142, V-274143, V-274144, V-274145, V-274147, V-274149, V-274151, V-274152, V-274154, V-274155, V-274156, V-274157, V-274160, V-274161, V-274162, V-274164, V-274165, V-274166, V-274167, V-274168, V-274169, V-274170, V-274173, V-274174, V-274177, V-274181, V-274182, V-274185 e V-274187

STIG versão 3 lançamento 3 do SLES 12

Inclui todas as configurações de fortalecimento do STIG que o Amazon EC2 suporta para vulnerabilidades de categoria III (Baixa), além de:

V-217102, V-217105, V-217110, V-217116, V-217117, V-217118, V-217119, V-217120, V-217121, V-217122, V-217124, V-217125, V-217126, V-217127, V-217128, V-217130, V-217134, V-217138, V-217143, V-217147, V-217152, V-217153, V-217154, V-217155, V-217156, V-217158, V-217161, V-217163, V-217166, V-217167, V-217168, V-217169, V-217170, V-217171, V-217182, V-217183,

V-217188, V-217190, V-217191, V-217194, V-217195, V-217196, V-217197, V-217200, V-217201, V-217202, V-217203, V-217204, V-217205, V-217206, V-217207, V-217208, V-217210, V-217217, V-217218, V-217223, V-217227, V-217230, V-217240, V-217241, V-217242, V-217243, V-217244, V-217245, V-217246, V-217247, V-217248, V-217249, V-217250, V-217251, V-217252, V-217253, V-217254, V-217255, V-217257, V-217258, V-217260, V-217265, V-217266, V-217267, V-217269, V-217272, V-217273, V-217274, V-217275, V-217276, V-217277, V-217278, V-217279, V-217280, V-217283, V-217284, V-217286, V-217287, V-217288, V-217289, V-217290, V-217291, V-217292, V-217293, V-217294, V-217295, V-217296, V-217299, V-217300, V-217301, V-217302, V-233308, V-237606, V-237607, V-237608, V-237609, V-237610, V-237611, V-237612, V-237613, V-237614, V-237615, V-237616, V-237617, V-237618, V-237619, V-237620, V-237621, V-237622, V-237623, V-251720, V-251722, V-255914e V-256981

STIG versão 2 lançamento 5 do SLES 15

Inclui todas as configurações de fortalecimento do STIG que o Amazon EC2 suporta para vulnerabilidades de categoria III (Baixa), além de:

V-234802, V-234807, V-234808, V-234809, V-234813, V-234815, V-234817, V-234821, V-234822, V-234823, V-234825, V-234827, V-234828, V-234829, V-234830, V-234832, V-234833, V-234834, V-234835, V-234836, V-234837, V-234838, V-234839, V-234840, V-234841, V-234842, V-234843, V-234844, V-234845, V-234848, V-234854, V-234855, V-234856, V-234857, V-234858, V-234861, V-234862, V-234863, V-234869, V-234870, V-234875, V-234880, V-234881, V-234882, V-234883, V-234884, V-234885, V-234886, V-234887, V-234888, V-234889, V-234891, V-234895, V-234896, V-234897, V-234899, V-234900, V-234901, V-234902, V-234903, V-234904, V-234906, V-234910, V-234911, V-234912, V-234913, V-234914, V-234918, V-234924, V-234928, V-234932, V-234937, V-234938, V-234939, V-234940, V-234941, V-234942, V-234943, V-234944, V-234945, V-234946, V-234947, V-234948, V-234949, V-234950, V-234951, V-234952, V-234954, V-234956, V-234957, V-234958, V-234959, V-234961, V-234962, V-234964, V-234966, V-234969, V-234973, V-234975, V-234976, V-234977, V-234978, V-234979, V-234981, V-234982, V-234983, V-234991, V-235002, V-235003, V-235007, V-235008, V-235009, V-235010, V-235013, V-235014, V-235015, V-235016, V-235017, V-235018, V-235019, V-235020, V-235021, V-235022, V-235023, V-235024, V-235025, V-235026, V-235028, V-235029, V-235030, V-251724, V-255920, V-256983e V-274879

STIG versão 2 lançamento 15 do Ubuntu 18.04

Inclui todas as configurações de fortalecimento do STIG que o Amazon EC2 suporta para vulnerabilidades de categoria III (Baixa), além de:

V-219149, V-219155, V-219156, V-219160, V-219166, V-219168, V-219176, V-219181, V-219184, V-219186, V-219188, V-219189, V-219190, V-219191, V-219192, V-219193, V-219194, V-219195, V-219196, V-219197, V-219198, V-219199, V-219200, V-219201, V-219202, V-219203, V-219204, V-219205, V-219206, V-219207, V-219208, V-219209, V-219213, V-219214, V-219215, V-219216, V-219217, V-219218, V-219219, V-219220, V-219221, V-219222, V-219223, V-219224, V-219225, V-219226, V-219227, V-219228, V-219229, V-219230, V-219231, V-219232, V-219233, V-219234, V-219235, V-219236, V-219238, V-219239, V-219240, V-219241, V-219242, V-219243, V-219244, V-219250, V-219254, V-219257, V-219263, V-219264, V-219265, V-219266, V-219267, V-219268, V-219269, V-219270, V-219271, V-219272, V-219273, V-219274, V-219275, V-219276, V-219277, V-219279, V-219281, V-219287, V-219291, V-219296, V-219297, V-219298, V-219299, V-219300, V-219303, V-219304, V-219306, V-219309, V-219310, V-219311, V-219315, V-219318, V-219319, V-219323, V-219326, V-219328, V-219330, V-219331, V-219335, V-219336, V-219337, V-219338, V-219339, V-219342, V-219344, V-233779, V-233780e V-255906

STIG versão 2 lançamento 3 do Ubuntu 20.04

Inclui todas as configurações de fortalecimento do STIG que o Amazon EC2 suporta para vulnerabilidades de categoria III (Baixa), além de:

V-238200, V-238205, V-238207, V-238209, V-238210, V-238211, V-238212, V-238213, V-238220, V-238225, V-238227, V-238228, V-238229, V-238230, V-238231, V-238232, V-238236, V-238238, V-238239, V-238240, V-238241, V-238242, V-238244, V-238245, V-238246, V-238247, V-238248, V-238249, V-238250, V-238251, V-238252, V-238253, V-238254, V-238255, V-238256, V-238257, V-238258, V-238264, V-238268, V-238271, V-238277, V-238278, V-238279, V-238280, V-238281, V-238282, V-238283, V-238284, V-238285, V-238286, V-238287, V-238288, V-238289, V-238290, V-238291, V-238292, V-238293, V-238294, V-238295, V-238297, V-238298, V-238299, V-238300, V-238301, V-238302, V-238303, V-238304, V-238309, V-238310, V-238315, V-238316, V-238317, V-238318, V-238319, V-238320, V-238324, V-238325, V-238329, V-238330, V-238333, V-238334, V-238337, V-238338, V-238339, V-238340, V-238341, V-238342, V-238343, V-238344, V-238345, V-238346, V-238347, V-238348, V-238349, V-238350, V-238351, V-238352, V-238353, V-238355, V-238356, V-238359, V-238360, V-238369, V-238370, V-238371, V-238376, V-238377, V-238378, V-251505, V-255912, V-274852e V-274853

STIG versão 2 lançamento 5 do Ubuntu 22.04

Inclui todas as configurações de fortalecimento do STIG que o Amazon EC2 suporta para vulnerabilidades de categoria III (Baixa), além de:

V-260471, V-260473, V-260474, V-260475, V-260477, V-260478, V-260485, V-260486, V-260487, V-260488, V-260489, V-260490, V-260491, V-260492, V-260493, V-260494, V-260495, V-260496, V-260497, V-260498, V-260499, V-260500, V-260505, V-260506, V-260507, V-260508, V-260509, V-260510, V-260511, V-260512, V-260513, V-260514, V-260522, V-260527, V-260528, V-260530, V-260533, V-260534, V-260535, V-260537, V-260538, V-260540, V-260542, V-260543, V-260545, V-260546, V-260547, V-260553, V-260554, V-260555, V-260556, V-260557, V-260560, V-260561, V-260562, V-260563, V-260564, V-260565, V-260566, V-260567, V-260569, V-260572, V-260573, V-260574, V-260575, V-260576, V-260582, V-260584, V-260585, V-260586, V-260588, V-260589, V-260590, V-260591, V-260594, V-260597, V-260598, V-260599, V-260600, V-260601, V-260602, V-260603, V-260604, V-260605, V-260606, V-260607, V-260608, V-260609, V-260610, V-260611, V-260612, V-260613, V-260614, V-260615, V-260616, V-260617, V-260618, V-260619, V-260620, V-260621, V-260622, V-260623, V-260624, V-260625, V-260626, V-260627, V-260628, V-260629, V-260630, V-260631, V-260632, V-260633, V-260634, V-260635, V-260636, V-260637, V-260638, V-260639, V-260640, V-260641, V-260642, V-260643, V-260644, V-260645, V-260646, V-260647, V-260648, V-260649, V-274862, V-274864e V-274866

STIG versão 1 lançamento 2 do Ubuntu 24.04

Inclui todas as configurações de fortalecimento do STIG que o Amazon EC2 suporta para vulnerabilidades de categoria III (Baixa), além de:

V-270649, V-270651, V-270652, V-270653, V-270654, V-270656, V-270657, V-270659, V-270660, V-270661, V-270662, V-270663, V-270669, V-270672, V-270673, V-270674, V-270676, V-270678, V-270679, V-270680, V-270681, V-270683, V-270684, V-270685, V-270686, V-270687, V-270688, V-270689, V-270692, V-270693, V-270696, V-270697, V-270698, V-270699, V-270700, V-270701, V-270702, V-270703, V-270704, V-270705, V-270709, V-270715, V-270716, V-270718, V-270720, V-270721, V-270722, V-270723, V-270724, V-270725, V-270726, V-270727, V-270728, V-270729, V-270730, V-270731, V-270732, V-270733, V-270737, V-270739, V-270740, V-270741, V-270742, V-270743, V-270746, V-270750, V-270753, V-270755, V-270756, V-270757, V-270758, V-270759, V-270760, V-270765, V-270766, V-270767, V-270768, V-270769, V-270770, V-270771, V-270772, V-270773, V-270775, V-270776, V-270777, V-270778, V-270779, V-270780, V-270781, V-270782, V-270783, V-270784, V-270785, V-270786, V-270787, V-270788, V-270789, V-270790, V-270791, V-270792, V-270793, V-270794, V-270795, V-270796, V-270797, V-270798, V-270799, V-270800, V-270801, V-270802, V-270803, V-270804, V-270805, V-270806, V-270807, V-270808, V-270809, V-270810, V-270811, V-270812, V-270813, V-270814, V-270815, V-270821, V-270822, V-270823, V-270824, V-270825, V-270826, V-270827, V-270828, V-270829, V-270830, V-270831, V-270832, V-274870, V-274871, V-274872e V-274873

Linux STIG High (categoria I)

A lista a seguir contém as configurações do STIG que o Amazon EC2 suporta em sua infraestrutura. Se uma configuração compatível não for aplicável à sua infraestrutura, o Amazon EC2 ignora essa configuração e segue em frente. Por exemplo, algumas configurações de fortalecimento do STIG podem não se aplicar a servidores autônomos. Políticas específicas da organização também podem afetar as configurações aplicáveis, como um requisito para que os administradores revisem as configurações do documento.

Para obter uma lista completa, consulte a Biblioteca de documentos STIGs. Para obter informações sobre como visualizar a lista completa, consulte STIG Viewing Tools.

> **Note**
>
> A categoria de STIG do Linux média inclui todas as configurações de fortalecimento do STIG listadas que se aplicam às categorias Linux STIG Medium and Low, além das configurações de fortalecimento de STIG que o Amazon EC2 suporta para vulnerabilidades de categoria II.

STIG versão 3 lançamento 15 do RHEL 7

Inclui todas as configurações de fortalecimento do STIG que o Amazon EC2 suporta para vulnerabilidades das categorias II e III (média e baixa), além de:

- RHEL 7/CentOS 7/AL2

  V-204424, V-204425, V-204442, V-204443, V-204447, V-204448, V-204455, V-204497, V-204502, V-204594, V-204620e V-204621

STIG versão 2 lançamento 4 do RHEL 8

Inclui todas as configurações de fortalecimento do STIG que o Amazon EC2 suporta para vulnerabilidades das categorias II e III (média e baixa), além de:

- RHEL 8/CentOS 8

  V-230221, V-230223, V-230226, V-230264, V-230265, V-230283, V-230284, V-230487, V-230492, V-230529, V-230530, V-230531, V-230533, V-230558, V-244540e V-268322

STIG versão 2 lançamento 5 do RHEL 9

Inclui todas as configurações de fortalecimento do STIG que o Amazon EC2 suporta para vulnerabilidades das categorias II e III (média e baixa), além de:

- RHEL 9/CentOS Stream 9

  V-257784, V-257785, V-257820, V-257821, V-257826, V-257835, V-257955, V-257956, V-257984, V-257986, V-258059, V-258078, V-258094, V-258230, V-258235e V-258238

STIG versão 1 lançamento 1 do Amazon Linux 2023

Inclui todas as configurações de fortalecimento do STIG que o Amazon EC2 suporta para vulnerabilidades das categorias II e III (média e baixa), além de:

V-273996, V-273997, V-273999, V-274007, V-274038, V-274039, V-274046, V-274052, V-274057e V-274153

STIG versão 3 lançamento 3 do SLES 12

Inclui todas as configurações de fortalecimento do STIG que o Amazon EC2 suporta para vulnerabilidades das categorias II e III (média e baixa), além de:

V-217101, V-217139, V-217141, V-217142, V-217159, V-217160, V-217264, V-217268, V-222386e V-251721

STIG versão 2 lançamento 5 do SLES 15

Inclui todas as configurações de fortalecimento do STIG que o Amazon EC2 suporta para vulnerabilidades das categorias II e III (média e baixa), além de:

V-234800, V-234804, V-234818, V-234852, V-234859, V-234860, V-234898, V-234984, V-234985, V-234988, V-234989, V-234990, V-235031, V-235032e V-251725

STIG versão 2 lançamento 15 do Ubuntu 18.04

Inclui todas as configurações de fortalecimento do STIG que o Amazon EC2 suporta para vulnerabilidades das categorias II e III (média e baixa), além de:

V-219157, V-219158, V-219177, V-219212, V-219308, V-219314, V-219316, V-251507e V-264388

STIG versão 2 lançamento 3 do Ubuntu 20.04

Inclui todas as configurações de fortalecimento do STIG que o Amazon EC2 suporta para vulnerabilidades das categorias II e III (média e baixa), além de:

V-238201, V-238218, V-238219, V-238326, V-238327, V-238380e V-251504

STIG versão 2 lançamento 5 do Ubuntu 22.04

Inclui todas as configurações de fortalecimento do STIG que o Amazon EC2 suporta para vulnerabilidades das categorias II e III (média e baixa), além de:

V-260469, V-260482, V-260483, V-260523, V-260524, V-260526, V-260529, V-260539, V-260570, V-260571e V-260579

STIG versão 1 lançamento 2 do Ubuntu 24.04

Inclui todas as configurações de fortalecimento do STIG que o Amazon EC2 suporta para vulnerabilidades das categorias II e III (média e baixa), além de:

V-270647, V-270648, V-270665, V-270666, V-270708, V-270711, V-270712, V-270713, V-270714, V-270717e V-270736

Configurações de hardening STIG para instâncias do EC2 Windows

O Amazon EC2 é compatível com linhas de base STIG para as seguintes versões do sistema operacional Windows:

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2

Esta seção lista as configurações atuais do STIG que o Amazon EC2 suporta para sua infraestrutura Windows, seguidas por um log do histórico de versões.

Você pode aplicar configurações de STIG baixas, médias ou altas.

STIG do Windows baixa (categoria III)

A lista a seguir contém as configurações do STIG que o Amazon EC2 suporta em sua infraestrutura. Se uma configuração compatível não for aplicável à sua infraestrutura, o Amazon EC2 ignora essa

configuração e segue em frente. Por exemplo, algumas configurações de fortalecimento do STIG podem não se aplicar a servidores autônomos. Políticas específicas da organização também podem afetar as configurações aplicáveis, como um requisito para que os administradores revisem as configurações do documento.

Para obter uma lista completa dos STIGs do Windows, consulte a STIGs Document Library. Para obter informações sobre como visualizar a lista completa, consulte STIG Viewing Tools.

- STIG versão 2 lançamento 4 do Windows Server 2022

  V-254335, V-254336, V-254337, V-254338, V-254351, V-254357, V-254363 e V-254481
- STIG versão 3 lançamento 4 do Windows Server 2019

  V-205691, V-205819, V-205858, V-205859, V-205860, V-205870, V-205871 e V-205923
- STIG versão 2 lançamento 10 do Windows Server 2016

  V-224916, V-224917, V-224918, V-224919, V-224931, V-224942 e V-225060
- Windows Server 2012 R2 MS STIG Versão 3 Release 5

  V-225250, V-225318, V-225319, V-225324, V-225327, V-225328, V-225330, V-225331, V-225332, V-225333, V-225334, V-225335, V-225336, V-225342, V-225343, V-225355, V-225357, V-225358, V-225359, V-225360, V-225362, V-225363, V-225376, V-225392, V-225394, V-225412, V-225459, V-225460, V-225462, V-225468, V-225473, V-225476, V-225479, V-225480, V-225481, V-225482, V-225483, V-225484, V-225485, V-225487, V-225488, V-225489, V-225490, V-225511, V-225514, V-225525, V-225526, V-225536e V-225537
- STIG versão 2 lançamento 6 do Microsoft .NET Framework 4.0

  Nenhuma configuração STIG é aplicada ao Microsoft .NET Framework para vulnerabilidades de Categoria III.
- STIG versão 2 lançamento 2 do Firewall do Windows

  V-241994, V-241995, V-241996, V-241999, V-242000, V-242001, V-242006, V-242007 e V-242008
- STIG versão 2 lançamento 5 do Internet Explorer 11

  V-223016, V-223056e V-223078
- STIG versão 2 lançamento 2 do Microsoft Edge (somente Windows Server 2022)

  V-235727, V-235731, V-235751, V-235752 e V-235765

Windows STIG Medium (categoria III)

A lista a seguir contém as configurações do STIG que o Amazon EC2 suporta em sua infraestrutura. Se uma configuração compatível não for aplicável à sua infraestrutura, o Amazon EC2 ignora essa configuração e segue em frente. Por exemplo, algumas configurações de fortalecimento do STIG podem não se aplicar a servidores autônomos. Políticas específicas da organização também podem afetar as configurações aplicáveis, como um requisito para que os administradores revisem as configurações do documento.

Para obter uma lista completa dos STIGs do Windows, consulte a STIGs Document Library. Para obter informações sobre como visualizar a lista completa, consulte STIG Viewing Tools.

> **Note**
>
> A categoria Windows STIG Medium inclui todas as configurações de fortalecimento do STIG listadas que se aplicam à STIG do Windows low (categoria III), além das configurações de fortalecimento de STIG que o Amazon EC2 suporta para vulnerabilidades de categoria II.

- STIG versão 2 lançamento 4 do Windows Server 2022

  Inclui todas as configurações de fortalecimento do STIG que o Amazon EC2 suporta para vulnerabilidades de categoria III (Baixa), além de:

  V-254247, V-254265, V-254269, V-254270, V-254271, V-254272, V-254273, V-254274, V-254276, V-254277, V-254278, V-254285, V-254286, V-254287, V-254288, V-254289, V-254290, V-254291, V-254292, V-254300, V-254301, V-254302, V-254303, V-254304, V-254305, V-254306, V-254307, V-254308, V-254309, V-254310, V-254311, V-254312, V-254313, V-254314, V-254315, V-254316, V-254317, V-254318, V-254319, V-254320, V-254321, V-254322, V-254323, V-254324, V-254325, V-254326, V-254327, V-254328, V-254329, V-254330, V-254331, V-254332, V-254333, V-254334, V-254339, V-254341, V-254342, V-254344, V-254345, V-254346, V-254347, V-254348, V-254349, V-254350, V-254355, V-254356, V-254356, V-254358, V-254359, V-254360, V-254361, V-254362, V-254364, V-254365, V-254366, V-254367, V-254368, V-254369, V-254370, V-254371, V-254372, V-254373, V-254375, V-254376, V-254377, V-254379, V-254380, V-254382, V-254383, V-254384, V-254431, V-254432, V-254433, V-254434, V-254435, V-254436, V-254438, V-254439, V-254442, V-254443, V-254444, V-254445, V-254449, V-254450, V-254451, V-254452, V-254453, V-254454, V-254455, V-254456, V-254459, V-254460, V-254461, V-254462, V-254463, V-254464, V-254468, V-254470, V-254471, V-254472, V-254473, V-254476, V-254477, V-254478, V-254479, V-254480, V-254482, V-254483, V-254484, V-254485, V-254486, V-254487, V-254488, V-254489, V-254490,

V-254493, V-254494, V-254495, V-254497, V-254499, V-254501, V-254502, V-254503, V-254504, V-254505, V-254507, V-254508, V-254509, V-254510, V-254511e V-254512

- STIG versão 3 lançamento 4 do Windows Server 2019

  Inclui todas as configurações de fortalecimento do STIG que o Amazon EC2 suporta para vulnerabilidades de categoria III (Baixa), além de:

  V-205625, V-205626, V-205627, V-205629, V-205630, V-205633, V-205634, V-205635, V-205636, V-205637, V-205638, V-205639, V-205643, V-205644, V-205648, V-205649, V-205650, V-205651, V-205652, V-205655, V-205656, V-205659, V-205660, V-205662, V-205671, V-205672, V-205673, V-205675, V-205676, V-205678, V-205679, V-205680, V-205681, V-205682, V-205683, V-205684, V-205685, V-205686, V-205687, V-205688, V-205689, V-205690, V-205692, V-205693, V-205694, V-205697, V-205698, V-205708, V-205709, V-205712, V-205714, V-205716, V-205717, V-205718, V-205719, V-205720, V-205722, V-205729, V-205730, V-205733, V-205747, V-205751, V-205752, V-205754, V-205756, V-205758, V-205759, V-205760, V-205761, V-205762, V-205764, V-205765, V-205766, V-205767, V-205768, V-205769, V-205770, V-205771, V-205772, V-205773, V-205774, V-205775, V-205776, V-205777, V-205778, V-205779, V-205780, V-205781, V-205782, V-205783, V-205784, V-205795, V-205796, V-205797, V-205798, V-205801, V-205808, V-205809, V-205810, V-205811, V-205812, V-205813, V-205814, V-205815, V-205816, V-205817, V-205821, V-205822, V-205823, V-205824, V-205825, V-205826, V-205827, V-205828, V-205830, V-205832, V-205833, V-205834, V-205835, V-205836, V-205837, V-205838, V-205839, V-205840, V-205841, V-205842, V-205861, V-205863, V-205865, V-205866, V-205867, V-205868, V-205869, V-205872, V-205873, V-205874, V-205911, V-205912, V-205915, V-205916, V-205917, V-205918, V-205920, V-205921, V-205922, V-205924, V-205925, V-236001e V-257503

- STIG versão 2 lançamento 10 do Windows Server 2016

  Inclui todas as configurações de fortalecimento do STIG que o Amazon EC2 suporta para vulnerabilidades de categoria III (Baixa), além de:

  V-224850, V-224852, V-224853, V-224854, V-224855, V-224856, V-224857, V-224858, V-224859, V-224866, V-224867, V-224868, V-224869, V-224870, V-224871, V-224872, V-224873, V-224881, V-224882, V-224883, V-224884, V-224885, V-224886, V-224887, V-224888, V-224889, V-224890, V-224891, V-224892, V-224893, V-224894, V-224895, V-224896, V-224897, V-224898, V-224899, V-224900, V-224901, V-224902, V-224903, V-224904, V-224905, V-224906, V-224907, V-224908, V-224909, V-224910, V-224911, V-224912, V-224913, V-224914, V-224915, V-224920, V-224922, V-224924, V-224925, V-224926, V-224927, V-224928, V-224929, V-224930, V-224935, V-224936, V-224937, V-224938, V-224939, V-224940, V-224941, V-224943, V-224944, V-224945, V-224946,

V-224947, V-224948, V-224949, V-224951, V-224952, V-224953, V-224955, V-224956, V-224957, V-224959, V-224960, V-224962, V-224963, V-225010, V-225013, V-225014, V-225015, V-225016, V-225017, V-225018, V-225019, V-225021, V-225022, V-225023, V-225024, V-225028, V-225029, V-225030, V-225031, V-225032, V-225033, V-225034, V-225035, V-225038, V-225039, V-225040, V-225041, V-225042, V-225043, V-225047, V-225049, V-225050, V-225051, V-225052, V-225055, V-225056, V-225057, V-225058, V-225059, V-225061, V-225062, V-225063, V-225064, V-225065, V-225066, V-225067, V-225068, V-225069, V-225072, V-225073, V-225074, V-225076, V-225078, V-225080, V-225081, V-225082, V-225083, V-225084, V-225086, V-225087, V-225088, V-225089, V-225092, V-225093, V-236000e V-257502

- Windows Server 2012 R2 MS STIG Versão 3 Release 5

  Inclui todas as configurações de fortalecimento do STIG que o Amazon EC2 suporta para vulnerabilidades de categoria III (Baixa), além de:

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

- STIG versão 2 lançamento 6 do Microsoft .NET Framework 4.0

Inclui todas as configurações de fortalecimento do STIG que o Amazon EC2 suporta para vulnerabilidades de categoria III (Baixa), além de:

V-225238

- STIG versão 2 lançamento 2 do Firewall do Windows

  Inclui todas as configurações de fortalecimento do STIG que o Amazon EC2 suporta para vulnerabilidades de categoria III (Baixa), além de:

  V-241989, V-241990, V-241991, V-241993, V-241993, V-241998e V-242003

- STIG versão 2 lançamento 5 do Internet Explorer 11

  Inclui todas as configurações de fortalecimento do STIG que o Amazon EC2 suporta para vulnerabilidades de categoria III (Baixa), além de:

  V-223015, V-223017, V-223018, V-223019, V-223020, V-223021, V-223022, V-223023, V-223024, V-223025, V-223026, V-223027, V-223028, V-223029, V-223030, V-223031, V-223032, V-223033, V-223034, V-223035, V-223036, V-223037, V-223038, V-223039, V-223040, V-223041, V-223042, V-223043, V-223044, V-223045, V-223046, V-223048, V-223049, V-223050, V-223051, V-223052, V-223053, V-223054, V-223055, V-223057, V-223058, V-223059, V-223060, V-223061, V-223062, V-223063, V-223064, V-223065, V-223066, V-223067, V-223068, V-223069, V-223070, V-223071, V-223072, V-223073, V-223074, V-223075, V-223076, V-223077, V-223079, V-223080, V-223081, V-223082, V-223083, V-223084, V-223085, V-223086, V-223087, V-223088, V-223089, V-223090, V-223091, V-223092, V-223093, V-223094, V-223095, V-223096, V-223097, V-223098, V-223099, V-223100, V-223101, V-223102, V-223103, V-223104, V-223105, V-223106, V-223107, V-223108, V-223109, V-223110, V-223111, V-223112, V-223113, V-223114, V-223115, V-223116, V-223117, V-223118, V-223119, V-223120, V-223121, V-223122, V-223123, V-223124, V-223125, V-223126, V-223127, V-223128, V-223129, V-223130, V-223131, V-223132, V-223133, V-223134, V-223135, V-223136, V-223137, V-223138, V-223139, V-223140, V-223141, V-223142, V-223143, V-223144, V-223145, V-223146, V-223147, V-223148, V-223149, V-250540e V-250541

- STIG versão 2 lançamento 2 do Microsoft Edge (somente Windows Server 2022)

  V-235720, V-235721, V-235723, V-235724, V-235725, V-235726, V-235728, V-235729, V-235730, V-235732, V-235733, V-235734, V-235735, V-235736, V-235737, V-235738, V-235739, V-235740, V-235741, V-235742, V-235743, V-235744, V-235745, V-235746, V-235747, V-235748, V-235749, V-235750, V-235754, V-235756, V-235760, V-235761, V-235763, V-235764, V-235766, V-235767, V-235768, V-235769, V-235770, V-235771, V-235772, V-235773, V-235774 e V-246736

- STIG versão 2 lançamento 4 do Microsoft Defender

  V-213427, V-213429, V-213430, V-213431, V-213432, V-213433, V-213434, V-213435, V-213436, V-213437, V-213438, V-213439, V-213440, V-213441, V-213442, V-213443, V-213444, V-213445, V-213446, V-213447, V-213448, V-213449, V-213450, V-213451, V-213455, V-213464, V-213465 e V-213466

STIG do Windows High (categoria I)

A lista a seguir contém as configurações do STIG que o Amazon EC2 suporta em sua infraestrutura. Se uma configuração compatível não for aplicável à sua infraestrutura, o Amazon EC2 ignora essa configuração e segue em frente. Por exemplo, algumas configurações de fortalecimento do STIG podem não se aplicar a servidores autônomos. Políticas específicas da organização também podem afetar as configurações aplicáveis, como um requisito para que os administradores revisem as configurações do documento.

Para obter uma lista completa dos STIGs do Windows, consulte a STIGs Document Library. Para obter informações sobre como visualizar a lista completa, consulte STIG Viewing Tools.

> **Note**
>
> A categoria Windows STIG High inclui todas as configurações de fortalecimento do STIG listadas que se aplicam às categorias Windows STIG Medium and Low, além das configurações de fortalecimento de STIG que o Amazon EC2 suporta para vulnerabilidades de categoria II.

- STIG versão 2 lançamento 4 do Windows Server 2022

  V-254293, V-254352, V-254353, V-254354, V-254374, V-254378, V-254381, V-254446, V-254465, V-254466, V-254467, V-254469, V-254474, V-254475 e V-254500
- STIG versão 3 lançamento 4 do Windows Server 2019

  Inclui todas as configurações de fortalecimento do STIG que o Amazon EC2 suporta para vulnerabilidades das categorias II e III (média e baixa), além de:

  V-205653, V-205654, V-205711, V-205713, V-205724, V-205725, V-205757, V-205802, V-205804, V-205805, V-205806, V-205849, V-205908, V-205913, V-205914 e V-205919
- STIG versão 2 lançamento 10 do Windows Server 2016

Inclui todas as configurações de fortalecimento do STIG que o Amazon EC2 suporta para vulnerabilidades das categorias II e III (média e baixa), além de:

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

- Windows Server 2012 R2 MS STIG Versão 3 Release 5

  Inclui todas as configurações de fortalecimento do STIG que o Amazon EC2 suporta para vulnerabilidades das categorias II e III (média e baixa), além de:

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

- STIG versão 2 lançamento 6 do Microsoft .NET Framework 4.0

  Inclui todas as configurações de fortalecimento do STIG que o Amazon EC2 suporta para vulnerabilidades das categorias II e III (média e baixa) do Microsoft.NET Framework. Nenhuma configuração adicional do STIG se aplica a vulnerabilidades da Categoria I.

- STIG versão 2 lançamento 2 do Firewall do Windows

  Inclui todas as configurações de fortalecimento do STIG que o Amazon EC2 suporta para vulnerabilidades das categorias II e III (média e baixa), além de:

  V-241992, V-241997 e V-242002

- STIG versão 2 lançamento 5 do Internet Explorer 11

  Inclui todas as configurações de fortalecimento do STIG que o Amazon EC2 suporta para vulnerabilidades das categorias II e III (média e baixa), além de:

  V-252910

- STIG versão 2 lançamento 2 do Microsoft Edge (somente Windows Server 2022)

  Inclui todas as configurações de fortalecimento do STIG que o Amazon EC2 suporta para vulnerabilidades das categorias II e III (média e baixa), além de:

  V-235758 e V-235759

- STIG versão 2 lançamento 4 do Microsoft Defender

Inclui todas as configurações de fortalecimento do STIG que o Amazon EC2 suporta para vulnerabilidades das categorias II e III (média e baixa), além de:

V-213426, V-213452 e V-213453

Downloads do scripts de hardening STIG

A Amazon agrupa os scripts de hardening STIG em pacotes relativos ao sistema operacional de cada lançamento. Os pacotes são arquivos de arquivamento apropriados para o sistema operacional de destino em que são baixados e executados. Os pacotes de scripts do Linux são armazenados como arquivos TAR (extensão de arquivo .tgz). Os pacotes de scripts para o Windows são armazenados como arquivos ZIP (extensão de arquivo .zip).

A Amazon armazena os pacotes de scripts no bucket `STIG` do Windows S3 do EC2 de cada Região da AWS. Os pacotes do Linux não têm um bucket separado. Use SSL/TLS para se comunicar com os recursos da AWS. Exigimos TLS 1.2 e recomendamos TLS 1.3.

Tópicos

- Pré-requisitos do IAM para downloads STIG
- Detalhes de pacote de download do STIG
- Histórico de versões do STIG do Linux
- Histórico de versões do Windows STIG

Pré-requisitos do IAM para downloads STIG

O perfil do IAM que você associa ao seu perfil de instância deve ter permissões de `s3:GetObject` para baixar os pacotes de scripts do Amazon S3. Você pode anexar o exemplo de política a seguir ao seu perfil de instância.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DownloadSTIGScriptBundles",
            "Effect": "Allow",
            "Action": [
                "s3:GetObject"
```

```
            ],
            "Resource": [
                "arn:aws:s3:::aws-windows-downloads*/STIG/*.zip",
                "arn:aws:s3:::aws-windows-downloads*/STIG/*.tgz"
            ]
        }
    ]
}
```

Para adicionar o exemplo de política de download STIG ao seu perfil de instância como uma política integrada, siga o processo para Atualizar a política de permissões para um perfil no Guia do usuário do AWS Identity and Access Management. Para obter mais informações sobre perfis de instância, consulte Usar perfis de instância.

Detalhes de pacote de download do STIG

> **Important**
>
> Com poucas exceções, os scripts de hardening STIG que o documento do Systems Manager baixa não instalam pacotes de terceiros. Se pacotes de terceiros já estiverem instalados na instância e se o parâmetro `InstallPackage` estiver definido como `yes`, os STIGs com os quais o Amazon EC2 é compatível relacionados àquele pacote serão aplicados.

Quando você executa o comando a seguir na AWS CLI, o Amazon S3 baixa do bucket o arquivo de pacote de hardening STIG mais recente.

```
aws s3 cp s3://aws-windows-downloads-region/STIG/operating system/Latest/bundle-
name destination-directory
```

Exemplo: baixar para um diretório temporário

Esse exemplo mostra um pacote do Linux que é baixado para o diretório `/tmp`

```
aws s3 cp s3://aws-windows-downloads-us-east-1/STIG/Linux/
Latest/LinuxAWSConfigureSTIG.tgz /tmp
```

Os padrões e exemplos de caminhos de armazenamento de arquivo de download e os nomes de arquivo dos pacotes são os seguintes:

Caminho de armazenamento de arquivos de dowanload

`s3://aws-windows-downloads-<region>/STIG/<operating system>/Latest/<bundle file name>`

Variáveis do caminho de download

region

Região da AWS (cada região tem seu próprio bucket de download.)

operating system

A plataforma do sistema operacional da instância em que os STIGs são aplicados, `Linux` ou `Windows`.

bundle file name

O formato é <nome do pacote do sistema operacional>.<extensão do arquivo>.

os bundle name

O prefixo do nome padrão para o pacote do sistema operacional é `LinuxAWSConfigureSTIG` ou `AWSConfigureSTIG`. Para manter a compatibilidade com as versões anteriores, o download para Windows não inclui um prefixo da plataforma.

file extension

Formato de arquivo compactado `tgz` (Linux) ou `zip` (Windows).

Exemplos de nomes de arquivos de pacotes

- `LinuxAWSConfigureSTIG.tgz`
- `AWSConfigureSTIG.zip`

Histórico de versões do STIG do Linux

Esta seção registra em log o histórico das versões dos pacotes de scripts do Linux que são atualizados trimestralmente. Para ver as alterações e as versões publicadas de um trimestre, escolha o título para expandir as informações. Se não houver alterações no trimestre, isso será refletido no título.

Alterações no terceiro trimestre de 2025 (4/09/2025):

Adicionada compatibilidade com o sistema operacional SUSE Linux Enterprise Server (SLES) e o Amazon Linux 2023. Atualizadas as seguintes versões de STIG e aplicados STIGS para o lançamento do terceiro trimestre de 2025 para todos os níveis de conformidade (baixo/médio/alto):

STIG-Build-Linux versão 1.0.x

- STIG versão 3 lançamento 15 do RHEL 7
- STIG versão 2 lançamento 4 do RHEL 8
- STIG versão 2 lançamento 5 do RHEL 9
- STIG versão 1 lançamento 1 do Amazon Linux 2023
- STIG versão 3 lançamento 3 do SLES 12
- STIG versão 2 lançamento 5 do SLES 15
- STIG versão 2 lançamento 15 do Ubuntu 18.04
- STIG versão 2 lançamento 3 do Ubuntu 20.04
- STIG versão 2 lançamento 5 do Ubuntu 22.04
- STIG versão 1 lançamento 2 do Ubuntu 24.04

Alterações no segundo trimestre de 2025 (26/06/2025):

Atualizadas as versões de STIG atualizadas a seguir, aplicados STIGS para o lançamento do segundo trimestre de 2025:

Linux STIG Low (categoria III)

- STIG versão 3 lançamento 15 do RHEL 7
- STIG versão 2 lançamento 3 do RHEL 8
- STIG versão 2 lançamento 4 do RHEL 9
- STIG versão 2 lançamento 15 do Ubuntu 18.04
- STIG versão 2 lançamento 2 do Ubuntu 20.04
- STIG versão 2 lançamento 4 do Ubuntu 22.04
- STIG versão 1 lançamento 1 do Ubuntu 24.04

Linux STIG Medium (categoria II)

- STIG versão 3 lançamento 15 do RHEL 7
- STIG versão 2 lançamento 3 do RHEL 8
- STIG versão 2 lançamento 4 do RHEL 9
- STIG versão 2 lançamento 15 do Ubuntu 18.04

- STIG versão 2 lançamento 2 do Ubuntu 20.04
- STIG versão 2 lançamento 4 do Ubuntu 22.04
- STIG versão 1 lançamento 1 do Ubuntu 24.04

Linux STIG High (categoria I)

- STIG versão 3 lançamento 15 do RHEL 7
- STIG versão 2 lançamento 3 do RHEL 8
- STIG versão 2 lançamento 4 do RHEL 9
- STIG versão 2 lançamento 15 do Ubuntu 18.04
- STIG versão 2 lançamento 2 do Ubuntu 20.04
- STIG versão 2 lançamento 4 do Ubuntu 22.04
- STIG versão 1 lançamento 1 do Ubuntu 24.04

Alterações no primeiro trimestre de 2025 (11/04/2025):

Atualizadas versões de STIG a seguir, aplicados STIGS para o lançamento do primeiro trimestre de 2025 e adicionada compatibilidade com o Ubuntu 24.04:

Linux STIG Low (categoria III)

- STIG versão 3 lançamento 15 do RHEL 7
- STIG versão 2 lançamento 2 do RHEL 8
- STIG versão 2 lançamento 3 do RHEL 9
- STIG versão 2 lançamento 15 do Ubuntu 18.04
- STIG versão 2 lançamento 2 do Ubuntu 20.04
- STIG versão 2 lançamento 3 do Ubuntu 22.04
- STIG versão 1 lançamento 1 do Ubuntu 24.04

Linux STIG Medium (categoria II)

- STIG versão 3 lançamento 15 do RHEL 7
- STIG versão 2 lançamento 2 do RHEL 8
- STIG versão 2 lançamento 3 do RHEL 9

- STIG versão 2 lançamento 15 do Ubuntu 18.04
- STIG versão 2 lançamento 2 do Ubuntu 20.04
- STIG versão 2 lançamento 3 do Ubuntu 22.04
- STIG versão 1 lançamento 1 do Ubuntu 24.04

Linux STIG High (categoria I)

- STIG versão 3 lançamento 15 do RHEL 7
- STIG versão 2 lançamento 2 do RHEL 8
- STIG versão 2 lançamento 3 do RHEL 9
- STIG versão 2 lançamento 15 do Ubuntu 18.04
- STIG versão 2 lançamento 2 do Ubuntu 20.04
- STIG versão 2 lançamento 3 do Ubuntu 22.04
- STIG versão 1 lançamento 1 do Ubuntu 24.04

Alterações no quarto trimestre de 2024 (10/12/2024):

Atualizadas as versões de STIG a seguir, aplicados STIGS para o lançamento do quarto trimestre de 2024 e adicionadas informações sobre dois novos parâmetros de entrada para os componentes Linux:

Linux STIG Low (categoria III)

- STIG versão 3 lançamento 15 do RHEL 7
- STIG versão 2 lançamento 1 do RHEL 8
- STIG versão 2 lançamento 2 do RHEL 9
- STIG versão 2 lançamento 15 do Ubuntu 18.04
- STIG versão 2 lançamento 1 do Ubuntu 20.04
- STIG versão 2 lançamento 2 do Ubuntu 22.04

Linux STIG Medium (categoria II)

- STIG versão 3 lançamento 15 do RHEL 7
- STIG versão 2 lançamento 1 do RHEL 8

- STIG versão 2 lançamento 2 do RHEL 9
- STIG versão 2 lançamento 15 do Ubuntu 18.04
- STIG versão 2 lançamento 1 do Ubuntu 20.04
- STIG versão 2 lançamento 2 do Ubuntu 22.04

Linux STIG High (categoria I)

- STIG versão 3 lançamento 15 do RHEL 7
- STIG versão 2 lançamento 1 do RHEL 8
- STIG versão 2 lançamento 2 do RHEL 9
- STIG versão 2 lançamento 15 do Ubuntu 18.04
- STIG versão 2 lançamento 1 do Ubuntu 20.04
- STIG versão 2 lançamento 2 do Ubuntu 22.04

Alterações no terceiro trimestre de 2024 (04/10/2024) (nenhuma alteração):

Não houve alterações de STIGS para componente Linux para o lançamento do terceiro trimestre de 2024.

Alterações no segundo trimestre de 2024 (10/5/2024):

Versões do STIG atualizadas e STIGS aplicados para o release do segundo trimestre de 2024. Compatibilidade com RHEL 9, CentOS Stream 9 e Ubuntu 22.04 adicionada, conforme a seguir:

Linux STIG Low (categoria III)

- RHEL 7 STIG Versão 3 Release 14
- RHEL 8 STIG Versão 1 Release 14
- RHEL 9 STIG Versão 1 Release 3
- Ubuntu 18.04 STIG Versão 2 Release 14
- Ubuntu 20.04 STIG Versão 1 Release 12
- Ubuntu 22.04 STIG Versão 1 Release 1

Linux STIG Medium (categoria II)

- RHEL 7 STIG Versão 3 Release 14

- RHEL 8 STIG Versão 1 Release 14
- RHEL 9 STIG Versão 1 Release 3
- Ubuntu 18.04 STIG Versão 2 Release 14
- Ubuntu 20.04 STIG Versão 1 Release 12
- Ubuntu 22.04 STIG Versão 1 Release 1

Linux STIG High (categoria I)

- RHEL 7 STIG Versão 3 Release 14
- RHEL 8 STIG Versão 1 Release 14
- RHEL 9 STIG Versão 1 Release 3
- Ubuntu 18.04 STIG Versão 2 Release 14
- Ubuntu 20.04 STIG Versão 1 Release 12
- Ubuntu 22.04 STIG Versão 1 Release 1

Alterações no primeiro trimestre de 2024 (6/2/2024):

Versões do STIG atualizadas e STIGS aplicados para o lançamento do primeiro trimestre de 2024 da seguinte forma:

Linux STIG Low (categoria III)

- RHEL 7 STIG Versão 3 Release 14
- RHEL 8 STIG Versão 1 Release 13
- Ubuntu 18.04 STIG Versão 2 Release 13
- Ubuntu 20.04 STIG Versão 1 Release 11

Linux STIG Medium (categoria II)

- RHEL 7 STIG Versão 3 Release 14
- RHEL 8 STIG Versão 1 Release 13
- Ubuntu 18.04 STIG Versão 2 Release 13
- Ubuntu 20.04 STIG Versão 1 Release 11

Linux STIG High (categoria I)

- RHEL 7 STIG Versão 3 Release 14
- RHEL 8 STIG Versão 1 Release 13
- Ubuntu 18.04 STIG Versão 2 Release 13
- Ubuntu 20.04 STIG Versão 1 Release 11

Alterações no quarto trimestre de 2023 (7/12/2023):

Versões do STIG atualizadas e STIGS aplicados para o release do quarto trimestre de 2023 da seguinte forma:

Linux STIG Low (categoria III)

- RHEL 7 STIG Versão 3 Release 13
- RHEL 8 STIG Versão 1 Release 12
- Ubuntu 18.04 STIG Versão 2 Release 12
- Ubuntu 20.04 STIG Versão 1 Release 10

Linux STIG Medium (categoria II)

- RHEL 7 STIG Versão 3 Release 13
- RHEL 8 STIG Versão 1 Release 12
- Ubuntu 18.04 STIG Versão 2 Release 12
- Ubuntu 20.04 STIG Versão 1 Release 10

Linux STIG High (categoria I)

- RHEL 7 STIG Versão 3 Release 13
- RHEL 8 STIG Versão 1 Release 12
- Ubuntu 18.04 STIG Versão 2 Release 12
- Ubuntu 20.04 STIG Versão 1 Release 10

Alterações no terceiro trimestre de 2023 - 04/10/2023:

Versões do STIG atualizadas e STIGS aplicados para o release do terceiro trimestre de 2023 da seguinte forma:

Linux STIG Low (categoria III)

- RHEL 7 STIG Versão 3 Release 12
- RHEL 8 STIG Versão 1 Release 11
- Ubuntu 18.04 STIG Versão 2 Release 11
- Ubuntu 20.04 STIG Versão 1 Release 9

Linux STIG Medium (categoria II)

- RHEL 7 STIG Versão 3 Release 12
- RHEL 8 STIG Versão 1 Release 11
- Ubuntu 18.04 STIG Versão 2 Release 11
- Ubuntu 20.04 STIG Versão 1 Release 9

Linux STIG High (categoria I)

- RHEL 7 STIG Versão 3 Release 12
- RHEL 8 STIG Versão 1 Release 11
- Ubuntu 18.04 STIG Versão 2 Release 11
- Ubuntu 20.04 STIG Versão 1 Release 9

Alterações no segundo trimestre de 2023 - 03/05/2023:

Versões do STIG atualizadas e STIGS aplicados para o release do segundo trimestre de 2023 da seguinte forma:

Linux STIG Low (categoria III)

- RHEL 7 STIG Versão 3 Release 11
- RHEL 8 STIG Versão 1 Release 10

- Ubuntu 18.04 STIG Versão 2 Release 11
- Ubuntu 20.04 STIG Versão 1 Release 8

Linux STIG Medium (categoria II)

- RHEL 7 STIG Versão 3 Release 11
- RHEL 8 STIG Versão 1 Release 10
- Ubuntu 18.04 STIG Versão 2 Release 11
- Ubuntu 20.04 STIG Versão 1 Release 8

Linux STIG High (categoria I)

- RHEL 7 STIG Versão 3 Release 11
- RHEL 8 STIG Versão 1 Release 10
- Ubuntu 18.04 STIG Versão 2 Release 11
- Ubuntu 20.04 STIG Versão 1 Release 8

Alterações no primeiro trimestre de 2023 - 27/03/2023:

Versões do STIG atualizadas e STIGS aplicados para o release do primeiro trimestre de 2023 da seguinte forma:

Linux STIG Low (categoria III)

- RHEL 7 STIG Versão 3 Release 10
- RHEL 8 STIG Versão 1 Release 9
- Ubuntu 18.04 STIG Versão 2 Release 10
- Ubuntu 20.04 STIG Versão 1 Release 7

Linux STIG Medium (categoria II)

- RHEL 7 STIG Versão 3 Release 10
- RHEL 8 STIG Versão 1 Release 9
- Ubuntu 18.04 STIG Versão 2 Release 10

- Ubuntu 20.04 STIG Versão 1 Release 7

Linux STIG High (categoria I)

- RHEL 7 STIG Versão 3 Release 10
- RHEL 8 STIG Versão 1 Release 9
- Ubuntu 18.04 STIG Versão 2 Release 10
- Ubuntu 20.04 STIG Versão 1 Release 7

Alterações no quarto trimestre de 2022 - 01/02/2023:

Versões do STIG atualizadas e STIGS aplicados para o release do quarto trimestre de 2022 da seguinte forma:

Linux STIG Low (categoria III)

- RHEL 7 STIG Versão 3 Release 9
- RHEL 8 STIG Versão 1 Release 8
- Ubuntu 18.04 STIG Versão 2 Release 9
- Ubuntu 20.04 STIG Versão 1 Release 6

Linux STIG Medium (categoria II)

- RHEL 7 STIG Versão 3 Release 9
- RHEL 8 STIG Versão 1 Release 8
- Ubuntu 18.04 STIG Versão 2 Release 9
- Ubuntu 20.04 STIG Versão 1 Release 6

Linux STIG High (categoria I)

- RHEL 7 STIG Versão 3 Release 9
- RHEL 8 STIG Versão 1 Release 8
- Ubuntu 18.04 STIG Versão 2 Release 9
- Ubuntu 20.04 STIG Versão 1 Release 6

Alterações no terceiro trimestre de 2022 - 30/09/2022 (sem alterações):

Não houve alterações no componente STIGS do Linux para o release do terceiro trimestre de 2022.

Alterações no segundo trimestre de 2022 - 02/08/2022:

Suporte do Ubuntu introduzido, versões do STIG atualizadas e STIGS aplicados para o release do segundo trimestre de 2022 da seguinte forma:

Linux STIG Low (categoria III)

- RHEL 7 STIG Versão 3 Release 7
- RHEL 8 STIG Versão 1 Release 6
- Ubuntu 18.04 STIG Versão 2 Release 6 (novo)
- Ubuntu 20.04 STIG Versão 1 Release 4 (novo)

Linux STIG Medium (categoria II)

- RHEL 7 STIG Versão 3 Release 7
- RHEL 8 STIG Versão 1 Release 6
- Ubuntu 18.04 STIG Versão 2 Release 6 (novo)
- Ubuntu 20.04 STIG Versão 1 Release 4 (novo)

Linux STIG High (categoria I)

- RHEL 7 STIG Versão 3 Release 7
- RHEL 8 STIG Versão 1 Release 6
- Ubuntu 18.04 STIG Versão 2 Release 6 (novo)
- Ubuntu 20.04 STIG Versão 1 Release 4 (novo)

Alterações no primeiro trimestre de 2022 - 26/04/2022:

Refatorado para incluir melhor suporte para contêineres. Script AL2 anterior combinado com o RHEL 7. Versões do STIG atualizadas e STIGS aplicados para o release do primeiro trimestre de 2022 da seguinte forma:

Linux STIG Low (categoria III)

- RHEL 7 STIG Versão 3 Release 6
- RHEL 8 STIG Versão 1 Release 5

Linux STIG Medium (categoria II)

- RHEL 7 STIG Versão 3 Release 6
- RHEL 8 STIG Versão 1 Release 5

Linux STIG High (categoria I)

- RHEL 7 STIG Versão 3 Release 6
- RHEL 8 STIG Versão 1 Release 5

Alterações no quarto trimestre de 2021 - 20/12/2021:

Versões do STIG atualizadas e STIGS aplicados para o release do quarto trimestre de 2021 da seguinte forma:

Linux STIG Low (categoria III)

- RHEL 7 STIG Versão 3 Release 5
- RHEL 8 STIG Versão 1 Release 4

Linux STIG Medium (categoria II)

- RHEL 7 STIG Versão 3 Release 5
- RHEL 8 STIG Versão 1 Release 4

Linux STIG High (categoria I)

- RHEL 7 STIG Versão 3 Release 5
- RHEL 8 STIG Versão 1 Release 4

Alterações no terceiro trimestre de 2021 - 30/09/2021:

Versões do STIG atualizadas e STIGS aplicados para o release do terceiro trimestre de 2021 da seguinte forma:

Linux STIG Low (categoria III)

- RHEL 7 STIG Versão 3 Release 4
- RHEL 8 STIG Versão 1 Release 3

Linux STIG Medium (categoria II)

- RHEL 7 STIG Versão 3 Release 4
- RHEL 8 STIG Versão 1 Release 3

Linux STIG High (categoria I)

- RHEL 7 STIG Versão 3 Release 4
- RHEL 8 STIG Versão 1 Release 3

Histórico de versões do Windows STIG

Esta seção registra em log o histórico das versões dos pacotes de scripts do Windows que são atualizados trimestralmente. Para ver as alterações e as versões publicadas de um trimestre, escolha o título para expandir as informações. Se não houver alterações no trimestre, isso será refletido no título.

Alterações no terceiro trimestre de 2025 (4/09/2025) (nenhuma alteração):

Não houve alterações de STIGS para componentes Windows para o lançamento do terceiro trimestre de 2025.

Alterações no segundo trimestre de 2025 (26/06/2025):

Atualizadas versões de STIG e STIGS aplicados para o lançamento do segundo trimestre de 2025, como se segue:

STIG do Windows baixa (categoria III)

- STIG versão 2 lançamento 4 do Windows Server 2022

- STIG versão 3 lançamento 4 do Windows Server 2019
- STIG versão 2 lançamento 10 do Windows Server 2016
- Windows Server 2012 R2 MS STIG Versão 3 Release 5
- STIG versão 2 lançamento 6 do Microsoft .NET Framework 4.0
- STIG versão 2 lançamento 2 do Windows Firewall
- STIG versão 2 lançamento 5 do Internet Explorer 11
- STIG versão 2 lançamento 2 do Microsoft Edge (somente Windows Server 2022)

Windows STIG Medium (categoria III)

- STIG versão 2 lançamento 4 do Windows Server 2022
- STIG versão 3 lançamento 4 do Windows Server 2019
- STIG versão 2 lançamento 10 do Windows Server 2016
- Windows Server 2012 R2 MS STIG Versão 3 Release 5
- STIG versão 2 lançamento 6 do Microsoft .NET Framework 4.0
- STIG versão 2 lançamento 2 do Windows Firewall
- STIG versão 2 lançamento 5 do Internet Explorer 11
- STIG versão 2 lançamento 2 do Microsoft Edge (somente Windows Server 2022)
- STIG versão 2 lançamento 4 do Defender

STIG do Windows High (categoria I)

- STIG versão 2 lançamento 4 do Windows Server 2022
- STIG versão 3 lançamento 4 do Windows Server 2019
- STIG versão 2 lançamento 10 do Windows Server 2016
- Windows Server 2012 R2 MS STIG Versão 3 Release 5
- STIG versão 2 lançamento 6 do Microsoft .NET Framework 4.0
- STIG versão 2 lançamento 2 do Windows Firewall
- STIG versão 2 lançamento 5 do Internet Explorer 11
- STIG versão 2 lançamento 2 do Microsoft Edge (somente Windows Server 2022)
- STIG versão 2 lançamento 4 do Defender

Alterações no primeiro trimestre de 2025 (4/05/2025):

Atualizados STIGS para o STIG versão 2 lançamento 5 do Internet Explorer 11 para todos os componentes STIG para o lançamento do primeiro trimestre de 2025.

Alterações no quarto trimestre de 2024 (10/12/2024):

Atualizadas versões de STIG e aplicados STIGS para o lançamento do quarto trimestre de 2024, como se segue:

STIG do Windows baixa (categoria III)

- STIG versão 2 lançamento 2 do Windows Server 2022
- STIG versão 3 lançamento 2 do Windows Server 2019
- STIG versão 2 lançamento 9 do Windows Server 2016
- Windows Server 2012 R2 MS STIG Versão 3 Release 5
- Microsoft .NET Framework 4.0 STIG Versão 2 Release 2
- STIG versão 2 lançamento 2 do Windows Firewall
- STIG versão 2 lançamento 5 do Internet Explorer 11
- STIG versão 2 lançamento 2 do Microsoft Edge (somente Windows Server 2022)

Windows STIG Medium (categoria III)

- STIG versão 2 lançamento 2 do Windows Server 2022
- STIG versão 3 lançamento 2 do Windows Server 2019
- STIG versão 2 lançamento 9 do Windows Server 2016
- Windows Server 2012 R2 MS STIG Versão 3 Release 5
- Microsoft .NET Framework 4.0 STIG Versão 2 Release 2
- STIG versão 2 lançamento 2 do Windows Firewall
- STIG versão 2 lançamento 5 do Internet Explorer 11
- STIG versão 2 lançamento 2 do Microsoft Edge (somente Windows Server 2022)
- STIG versão 2 lançamento 4 do Defender

STIG do Windows High (categoria I)

- STIG versão 2 lançamento 2 do Windows Server 2022

- STIG versão 3 lançamento 2 do Windows Server 2019
- STIG versão 2 lançamento 9 do Windows Server 2016
- Windows Server 2012 R2 MS STIG Versão 3 Release 5
- Microsoft .NET Framework 4.0 STIG Versão 2 Release 2
- STIG versão 2 lançamento 2 do Windows Firewall
- STIG versão 2 lançamento 5 do Internet Explorer 11
- STIG versão 2 lançamento 2 do Microsoft Edge (somente Windows Server 2022)
- STIG versão 2 lançamento 4 do Defender

Alterações no terceiro trimestre de 2024 (04/10/2024) (nenhuma alteração):

Não houve alterações de STIGS para componente Windows para o lançamento do terceiro trimestre de 2024.

Alterações no segundo trimestre de 2024 (10/5/2024; sem alterações):

Não houve alterações no componente STIGS do Windows para o lançamento do segundo trimestre de 2024.

Alterações no primeiro trimestre de 2024 (23/02/2024) (nenhuma alteração):

Não houve alterações no componente STIGS do Windows para o lançamento do primeiro trimestre de 2024.

Alterações no quarto trimestre de 2023 (7/12/2023) (nenhuma alteração):

Não houve alterações no componente STIGS do Windows para o lançamento do quarto trimestre de 2023.

Alterações no terceiro trimestre de 2023 - 04/10/2023 (sem alterações):

Não houve alterações no componente STIGS do Windows para o release do terceiro trimestre de 2023.

Alterações no segundo trimestre de 2023 - 03/05/2023 (sem alterações):

Não houve alterações no componente STIGS do Windows para o release do segundo trimestre de 2023.

Alterações no primeiro trimestre de 2023 - 27/03/2023 (sem alterações):

Não houve alterações no componente STIGS do Windows para o release do primeiro trimestre de 2023.

Alterações no quarto trimestre de 2022 - 01/02/2023:

Versões do STIG atualizadas e STIGS aplicados para o release do quarto trimestre de 2022 da seguinte forma:

STIG do Windows baixa (categoria III)

- Windows Server 2022 STIG versão 1 release 1
- Windows Server 2019 STIG Versão 2 Release 5
- Windows Server 2016 STIG Versão 2 Release 5
- Windows Server 2012 R2 MS STIG Versão 3 Release 5
- Microsoft .NET Framework 4.0 STIG Versão 2 Release 2
- Windows Firewall STIG Versão 2 Release 1
- Internet Explorer 11 STIG Versão 2 Release 3
- Microsoft Edge STIG Versão 1 Release 6 (somente Windows Server 2022)

Windows STIG Medium (categoria III)

- Windows Server 2022 STIG versão 1 release 1
- Windows Server 2019 STIG Versão 2 Release 5
- Windows Server 2016 STIG Versão 2 Release 5
- Windows Server 2012 R2 MS STIG Versão 3 Release 5
- Microsoft .NET Framework 4.0 STIG Versão 2 Release 2
- Windows Firewall STIG Versão 2 Release 1
- Internet Explorer 11 STIG Versão 2 Release 3
- Microsoft Edge STIG Versão 1 Release 6 (somente Windows Server 2022)
- Defender STIG Versão 2 Release 4 (somente Windows Server 2022)

STIG do Windows High (categoria I)

- Windows Server 2022 STIG versão 1 release 1

- Windows Server 2019 STIG Versão 2 Release 5
- Windows Server 2016 STIG Versão 2 Release 5
- Windows Server 2012 R2 MS STIG Versão 3 Release 5
- Microsoft .NET Framework 4.0 STIG Versão 2 Release 2
- Windows Firewall STIG Versão 2 Release 1
- Internet Explorer 11 STIG Versão 2 Release 3
- Microsoft Edge STIG Versão 1 Release 6 (somente Windows Server 2022)
- Defender STIG Versão 2 Release 4 (somente Windows Server 2022)

Alterações no terceiro trimestre de 2022 - 30/09/2022 (sem alterações):

Não houve alterações no componente STIGS do Windows para o release do terceiro trimestre de 2022.

Alterações no segundo trimestre de 2022 - 02/08/2022:

Versões do STIG atualizadas e STIGS aplicados para o release do segundo trimestre de 2022.

STIG do Windows baixa (categoria III)

- Windows Server 2019 STIG Versão 2 Release 4
- Windows Server 2016 STIG Versão 2 Release 4
- Windows Server 2012 R2 MS STIG Versão 3 Release 3
- Microsoft .NET Framework 4.0 STIG Versão 2 Release 1
- Windows Firewall STIG Versão 2 Release 1
- Internet Explorer 11 STIG Versão 1 Release 19

Windows STIG Medium (categoria III)

- Windows Server 2019 STIG Versão 2 Release 4
- Windows Server 2016 STIG Versão 2 Release 4
- Windows Server 2012 R2 MS STIG Versão 3 Release 3
- Microsoft .NET Framework 4.0 STIG Versão 2 Release 1
- Windows Firewall STIG Versão 2 Release 1

- Internet Explorer 11 STIG Versão 1 Release 19

STIG do Windows High (categoria I)

- Windows Server 2019 STIG Versão 2 Release 4
- Windows Server 2016 STIG Versão 2 Release 4
- Windows Server 2012 R2 MS STIG Versão 3 Release 3
- Microsoft .NET Framework 4.0 STIG Versão 2 Release 1
- Windows Firewall STIG Versão 2 Release 1
- Internet Explorer 11 STIG Versão 1 Release 19

Alterações no primeiro trimestre de 2022 - 02/08/2022 (sem alterações):

Não houve alterações no componente STIGS do Windows para o release do primeiro trimestre de 2022.

Alterações no quarto trimestre de 2021 - 20/12/2021:

Versões do STIG atualizadas e STIGS aplicados para o release do quarto trimestre de 2021.

STIG do Windows baixa (categoria III)

- Windows Server 2019 STIG Versão 2 Release 3
- Windows Server 2016 STIG Versão 2 Release 3
- Windows Server 2012 R2 MS STIG Versão 3 Release 3
- Microsoft .NET Framework 4.0 STIG Versão 2 Release 1
- Windows Firewall STIG Versão 2 Release 1
- Internet Explorer 11 STIG Versão 1 Release 19

Windows STIG Medium (categoria III)

- Windows Server 2019 STIG Versão 2 Release 3
- Windows Server 2016 STIG Versão 2 Release 3
- Windows Server 2012 R2 MS STIG Versão 3 Release 3

- Microsoft .NET Framework 4.0 STIG Versão 2 Release 1
- Windows Firewall STIG Versão 2 Release 1
- Internet Explorer 11 STIG Versão 1 Release 19

STIG do Windows High (categoria I)

- Windows Server 2019 STIG Versão 2 Release 3
- Windows Server 2016 STIG Versão 2 Release 3
- Windows Server 2012 R2 MS STIG Versão 3 Release 3
- Microsoft .NET Framework 4.0 STIG Versão 2 Release 1
- Windows Firewall STIG Versão 2 Release 1
- Internet Explorer 11 STIG Versão 1 Release 19

Alterações no terceiro trimestre de 2021 - 30/09/2021:

Versões do STIG atualizadas e STIGS aplicados para o release do terceiro trimestre de 2021.

STIG do Windows baixa (categoria III)

- Windows Server 2019 STIG Versão 2 Release 2
- Windows Server 2016 STIG Versão 2 Release 2
- Windows Server 2012 R2 MS STIG Versão 3 Release 2
- Microsoft .NET Framework 4.0 STIG Versão 2 Release 1
- Windows Firewall STIG Versão 1 Release 7
- Internet Explorer 11 STIG Versão 1 Release 19

Windows STIG Medium (categoria III)

- Windows Server 2019 STIG Versão 2 Release 2
- Windows Server 2016 STIG Versão 2 Release 2
- Windows Server 2012 R2 MS STIG Versão 3 Release 2
- Microsoft .NET Framework 4.0 STIG Versão 2 Release 1
- Windows Firewall STIG Versão 1 Release 7

- Internet Explorer 11 STIG Versão 1 Release 19

STIG do Windows High (categoria I)

- Windows Server 2019 STIG Versão 2 Release 2
- Windows Server 2016 STIG Versão 2 Release 2
- Windows Server 2012 R2 MS STIG Versão 3 Release 2
- Microsoft .NET Framework 4.0 STIG Versão 2 Release 1
- Windows Firewall STIG Versão 1 Release 7
- Internet Explorer 11 STIG Versão 1 Release 19

Usar o AWS Systems Manager para aplicar configurações STIG à instância

Você pode usar o documento de comando `AWSEC2-ConfigureSTIG` do Systems Manager para aplicar as configurações STIG a uma instância existente do EC2. Você deve executar o documento de comando na instância que ele atualiza. O documento de comando aplica as configurações apropriadas com base no sistema operacional e na configuração da instância em que ele é executado.

Esta página contém detalhes sobre o documento de comando `AWSEC2-ConfigureSTIG`, incluindo parâmetros de entrada e como executá-lo no console do Systems Manager ou com `send-command` na AWS CLI.

Parâmetros de entrada de AWSEC2-ConfigureSTIG

Você pode fornecer os seguintes parâmetros de entrada para especificar como o documento de comando deve aplicar as configurações STIG à instância.

Nível (string, obrigatório)

Especifique a categoria de gravidade STIG a ser aplicada. Entre os valores válidos estão os seguintes:

- Alto
- Médio
- Baixo

Se você não especificar um valor, o sistema usará o valor padrão `High`.

InstallPackages (string, opcional, somente Linux)

Se o valor for `No`, o script não instalará nenhum pacote de software adicional. Se o valor for `Yes`, o script instalará os pacotes de software adicionais que forem necessários para máxima conformidade. O valor padrão é `No`.

SetDoDConsentBanner (string, opcional, somente Linux)

Se o valor for `No`, o banner de consentimento do DoD não será mostrado quando você anexar a uma instância que tenha um script STIG para Linux instalado. Se o valor for `Yes`, o banner de consentimento do DoD não será mostrado quando você se anexar a uma instância que tenha um dos scripts STIG para Linux instalado. Você deve aceitar o banner para poder fazer login. O valor padrão é `No`.

Para ver um exemplo do banner de consentimento, consulte o Disclaimer Department of Defense Privacy and Consent Notice que aparece quando você acessa o site do DLA Document Services.

Execute o documento de comando AWSEC2-ConfigureSTIG

Para executar o documento `AWSEC2-ConfigureSTIG`, siga as etapas para o ambiente de sua preferência.

Console

1. Abra o console AWS Systems Manager em https://console.aws.amazon.com/systems-manager/.
2. Selecione Run Command no painel de navegação. Isso mostra uma lista dos comandos que estão sendo executados atualmente na conta, se aplicável.
3. Selecione Run command. Isso abre o diálogo Executar um comando e exibe uma lista dos documentos de comandos aos quais você tem acesso.
4. Selecione `AWSEC2-ConfigureSTIG` na lista de documentos de comando. Para otimizar os resultados, você pode inserir todo ou parte do nome do documento. Você também pode filtrar pelo proprietário, por tipos de plataforma ou por tags.

   Quando você seleciona um documento de comando, os detalhes são preenchidos abaixo da lista.
5. Selecione `Default version at runtime` na lista Versão do documento.

6. Configure os Parâmetros do comando para definir como `AWSEC2-ConfigureSTIG` instalará o pacote de script e o executará para atualizar a instância. Para obter detalhes dos parâmetros, consulte Parâmetros de entrada de AWSEC2-ConfigureSTIG.
7. Em Seleção de alvos, especifique as tags ou selecione manualmente as instâncias em que a operação deve ser executada.

   > **Note**
   >
   > Se selecionar manualmente as instâncias e uma instância que você espera ver não estiver incluída na lista, consulte Onde estão minhas instâncias? para obter dicas de solução de problemas.

8. Para obter parâmetros adicionais para definir o comportamento do Run Command do Systems Manager, como, Controle da taxa, insira os valores como descrito em Executar comandos no console.
9. Escolha Executar.

   Se tiver sucesso, o documento de comando instalará o script e configurará a instância. Se a execução do comando falhou, exiba a saída do comando do Systems Manager para obter detalhes do motivo da falha.

AWS CLI

Exemplo 1: executar com os valores padrão

Execute o comando a seguir para instalar o script STIG e executá-lo com os valores padrão. Para obter mais informações sobre os parâmetros de entrada, consulte Parâmetros de entrada de AWSEC2-ConfigureSTIG.

```
aws ssm send-command \
 --document-name "AWSEC2-ConfigureSTIG" \
 --instance-ids "i-1234567890abcdef0"'
```

Exemplo 2: definir as configurações STIG de nível médio na instância.

Execute o comando a seguir para instalar o script STIG e executá-lo com o parâmetro de entrada `Level` definido como `Medium`. Para obter mais informações sobre os parâmetros de entrada, consulte Parâmetros de entrada de AWSEC2-ConfigureSTIG.

```
aws ssm send-command \
 --document-name "AWSEC2-ConfigureSTIG" \
 --instance-ids "i-1234567890abcdef0"
 --parameters '{"Level":"Medium"}'
```

Se tiver sucesso, o documento de comando instalará o script e configurará a instância. Se a execução do comando falhou, exiba a saída do comando para obter detalhes do motivo da falha.

PowerShell

Exemplo 1: executar com os valores padrão

Execute o comando a seguir para instalar o script STIG e executá-lo com os valores padrão. Para obter mais informações sobre os parâmetros de entrada, consulte Parâmetros de entrada de AWSEC2-ConfigureSTIG.

```
Send-SSMCommand -DocumentName "AWSEC2-ConfigureSTIG" -InstanceId
 "i-1234567890abcdef0"}
```

Exemplo 2: definir as configurações STIG de nível médio na instância.

Execute o comando a seguir para instalar o script STIG e executá-lo com o parâmetro de entrada `Level` definido como `Medium`. Para obter mais informações sobre os parâmetros de entrada, consulte Parâmetros de entrada de AWSEC2-ConfigureSTIG.

```
Send-SSMCommand -DocumentName "AWSEC2-ConfigureSTIG" -InstanceId
 "i-1234567890abcdef0" -Parameter @{'Level'='Medium'}
```

Se tiver sucesso, o documento de comando instalará o script e configurará a instância. Se a execução do comando falhou, exiba a saída do comando para obter detalhes do motivo da falha.

Relógio de precisão e sincronização de horas em sua instância do EC2

Uma referência de horário consistente e precisa na instância do Amazon EC2 é crucial para muitas tarefas e processos de servidor. Os timestamps nos logs do sistema desempenham um papel essencial na identificação de quando os problemas ocorreram e na ordem cronológica dos eventos. Se você usar a AWS CLI ou um SDK da AWS para fazer solicitações à instância, essas ferramentas

assinarão as solicitações em seu nome. Se as configurações de data e hora da instância não forem exatas, poderá haver uma discrepância entre a data na assinatura e a data da solicitação, levando a AWS a rejeitar suas solicitações.

Para lidar com esse aspecto importante, a Amazon oferece o Serviço de Sincronização Temporal da Amazon, que é acessível em todas as instâncias do EC2 e é usado por vários Serviços da AWS. Esse serviço usa uma frota de relógios de referência atômicos e conectados via satélite em cada Região da AWS para fornecer leituras de hora exatas e atuais do padrão global do Horário Universal Coordenado (UTC).

Para obter a melhor performance, recomendamos o uso do Serviço de Sincronização Temporal da Amazon local nas instâncias do EC2. Para fazer backup no Serviço de Sincronização Temporal da Amazon local nas instâncias ou para conectar ao Serviço de Sincronização Temporal da Amazon recursos externos ao Amazon EC2, você pode usar o Serviço de Sincronização Temporal da Amazon público localizado em `time.aws.com`. O Serviço de Sincronização Temporal da Amazon público, como o Serviço de Sincronização Temporal da Amazon local, faz automaticamente a difusão de qualquer segundo bissexto adicionado ao UTC. O Serviço de Sincronização Temporal da Amazon público é compatível globalmente com nossa frota de relógios atômicos de referência conectados via satélite em cada Região da AWS.

Carimbo de data e hora de pacotes de hardware

É possível habilitar o carimbo de data e hora de pacotes de hardware na instância para adicionar um carimbo de data e hora de precisão de 64 bits em nanossegundos a cada pacote de rede recebido. Como o carimbo de data e hora de pacotes de hardware ocorre no nível do hardware (antes que o pacote atinja o kernel, o socket ou a camada da aplicação), você evita atrasos adicionados pelo carimbo de data e hora de software. O relógio de referência subjacente do carimbo de data e hora de hardware é o relógio de hardware PTP do Amazon Time Sync Service.

Benefícios

O carimbo de data e hora de pacotes de hardware oferece os seguintes benefícios:

- Melhora a ordenação de eventos, que também pode ser usada para determinar a ordem real em que os pacotes chegam à instância do EC2, garantindo um processamento correto dos pacotes.
- Mede a latência unidirecional da rede.
- Aumenta a velocidade das transações distribuídas com maior precisão e exatidão em comparação com a maioria das soluções on-premises.

Pré-requisitos e configuração

Para habilitar o carimbo de data e hora de pacotes de hardware, sua instância deve atender aos seguintes pré-requisitos:

- Deve ser uma instância Linux.
- Atender aos requisitos para suporte ao relógio de hardware PTP.

Para conhecer as instruções de configuração, consulte o tópico Hardware Packet Timestamping na página Linux kernel driver for Elastic Network Adapter (ENA) family no GitHub.

Segundos bissextos

Os segundos bissextos, introduzidos em 1972, são ajustes ocasionais de um segundo no horário UTC para considerar as irregularidades na rotação da Terra, a fim de acomodar as diferenças entre o Tempo Atômico Internacional (TAI) e o horário solar (Ut1). Para gerenciar os segundos bissextos para os clientes, criamos a difusão de segundos bissextos no Serviço de Sincronização Temporal da Amazon. Para obter mais informações, consulte Look Before You Leap — The Coming Leap Second and AWS.

Os segundos bissextos vão acabar e apoiamos totalmente a decisão tomada na 27ª Conferência Geral sobre Pesos e Medidas de abandonar os segundos bissextos até 2035.

Para apoiar essa transição, ainda planejamos continuar a aplicar a difusão durante um evento de segundos bissextos ao acessar o Serviço de Sincronização Temporal da Amazon via conexão NTP local ou nossos consultas de NTP público (`time.aws.com`). O relógio PTP físico, no entanto, não oferece uma opção de difusão de tempo. No caso de um segundo bissexto, o relógio PTP físico adicionará o segundo bissexto de acordo com os padrões do UTC. As fontes de hora com difusão de segundo bissexto e sem difusão de segundos bissextos são iguais na maioria dos casos. Mas, como elas diferem durante um evento de segundo bissexto, não recomendamos o uso de ambas, as fontes de hora com difusão e sem difusão, na configuração do cliente de hora durante um evento de segundo bissexto.

Tópicos

- Definir a referência de horas na instância do EC2 para usar o Serviço de Sincronização Temporal da Amazon local

- Definir a referência de horas na instância do EC2 ou em qualquer dispositivo conectado à Internet para usar o Serviço de Sincronização Temporal da Amazon público
- Comparação dos carimbos de data/hora das instâncias do Linux
- Alteração do fuso horário da instância

Recursos relacionados

- Blog de computação da AWS: It's About Time: Microsecond-Accurate Clocks on Amazon EC2 Instances
- Blog da AWS sobre operações e migrações na nuvem: Manage Amazon EC2 instance clock accuracy Amazon Time Sync Service and Amazon CloudWatch – Part 1
- (Linux) https://chrony-project.org/

Definir a referência de horas na instância do EC2 para usar o Serviço de Sincronização Temporal da Amazon local

O Serviço de Sincronização Temporal da Amazon local usa o Network Time Protocol (NTP) ou fornece um relógio físico Precision Time Protocol (PTP) nas instâncias compatíveis. O relógio físico PTP permite uma conexão NTP (instâncias Linux e Windows) ou uma conexão PTP direta (apenas instâncias Linux). As conexões NTP e PTP diretas usam a mesma fonte de hora extremamente exata, mas a conexão PTP direta é mais precisa do que a conexão NTP. A conexão NTP com o Serviço de Sincronização Temporal da Amazon usa a difusão de segundos bissextos, enquanto a conexão PTP com o relógio PTP físico não usa. Para obter mais informações, consulte Segundos bissextos.

As instâncias podem acessar o Serviço de Sincronização Temporal da Amazon da seguinte forma:

- Por NTP nos seguintes endpoints de endereço IP:
  - IPv4: `169.254.169.123`
  - IPv6: `fd00:ec2::123` (Acessível somente em instâncias baseadas em Nitro.)
- (Somente para o Linux) Por meio de uma conexão PTP direta para se conectar a um relógio de hardware PTP local:
  - `PHC0`

As AMIs do Amazon Linux, as AMIs do Windows e a maioria das AMIs de parceiros configuram a instância para usar o endpoint do protocolo NTP para IPv4 por padrão. Esta é a configuração recomendada para a maioria das workloads do cliente. Nenhuma configuração adicional é necessária para instâncias iniciadas dessas AMIs, a menos que você queira usar o endpoint IPv6 ou se conectar diretamente ao relógio PTP físico.

As conexões NTP e PTP não exigem nenhuma alteração na configuração da VPC e a instância não requer acesso à Internet.

Considerações

- Há um limite de 1.024 pacotes por segundo (PPS) para serviços que usam endereços locais do link. Esse limite inclui o agregado de consultas ao DNS do Route 53 Resolver, solicitações do Serviço de metadados de instância (IMDS), solicitações do Amazon Time Service Network Time Protocol (NTP) e solicitações do Windows Licensing Service (para instâncias baseadas no Microsoft Windows).
- Somente as instâncias do Linux podem usar uma conexão PTP direta para se conectar ao relógio de hardware PTP local. As instâncias do Windows usam o protocolo NTP para se conectar ao relógio de hardware PTP local.

Conteúdo

- Conectar-se ao endpoint IPv4 do Serviço de Sincronização Temporal da Amazon
- Conectar-se ao endpoint IPv6 do Serviço de Sincronização Temporal da Amazon
- Conectar-se ao relógio PTP físico

Conectar-se ao endpoint IPv4 do Serviço de Sincronização Temporal da Amazon

É possível que a AMI já tenha configurado o Serviço de Sincronização Temporal da Amazon por padrão. Caso contrário, use os procedimentos a seguir para configurar sua instância de forma a usar o Serviço de Sincronização Temporal da Amazon local por meio do endpoint IPv4.

Para obter ajuda com a solução de problemas, consulte Solucionar problemas de sincronização de NTP em instâncias Linux ou Solucionar problemas de horário em instâncias Windows.

Amazon Linux

O AL2023 e as versões recentes do Amazon Linux 2 são configuradas para usar o endpoint IPv4 do Serviço de Sincronização Temporal da Amazon por padrão. Se você confirmar que sua instância já está configurada, poderá pular o procedimento a seguir.

Para verificar se o chrony está configurado para utilizar o endpoint IPv4

Execute o comando a seguir. Na saída, a linha que começa com ^* indica a fonte de horário preferencial.

```
chronyc sources -v | grep -F ^*
^* 169.254.169.123               3   4   377    14    +12us[+9653ns] +/-  290us
```

Para configurar o chrony para conectar-se ao endpoint IPv4 em versões mais antigas do Amazon Linux 2

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). Adicione a linha a seguir antes de todas as outras instruções `server` ou `pool` que possam estar presentes no arquivo, e salve as alterações:

   ```
   server 169.254.169.123 prefer iburst minpoll 4 maxpoll 4
   ```

4. Reinicie o daemon `chrony` (`chronyd`).

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

   ```
   Starting chronyd:                                          [  OK  ]
   ```

> **Note**
>
> No RHEL e no CentOS (até a versão 6), o nome do serviço é `chrony` em vez de `chronyd`.

5. Para configurar o `chronyd` para ser iniciado a cada inicialização do sistema, use o comando `chkconfig`.

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

6. Confirme que o `chrony` está usando o endpoint IPv4 `169.254.169.123` para sincronizar a hora.

```
[ec2-user ~]$ chronyc sources -v | grep -F ^*
```

Na saída, `^*` indica a fonte de horário preferencial.

```
^* 169.254.169.123               3   6    17    43    -30us[ -226us] +/-  287us
```

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
```

Ubuntu

Para configurar o chrony para conectar-se ao endpoint IPv4 no Ubuntu

1. Conecte-se à sua instância e use `apt` para instalar o pacote `chrony`.

```
ubuntu:~$ sudo apt install chrony
```

> **Note**
>
> Se necessário, atualize sua instância primeiro executando `sudo apt update`.

2. Abra o arquivo `/etc/chrony/chrony.conf` usando um editor de texto (como vim ou nano). Adicione a seguinte linha antes de todas as outras instruções `server` ou `pool` já presentes no arquivo, e salve as alterações:

```
server 169.254.169.123 prefer iburst minpoll 4 maxpoll 4
```

3. Reinicie o serviço `chrony`.

```
ubuntu:~$ sudo /etc/init.d/chrony restart
```

```
Restarting chrony (via systemctl): chrony.service.
```

4. Confirme que o `chrony` está usando o endpoint IPv4 `169.254.169.123` para sincronizar a hora.

```
ubuntu:~$ chronyc sources -v | grep -F ^*
```

Na saída, a linha que começa com `^*` indica a fonte de horário preferencial.

```
^* 169.254.169.123               3   6    17    12    +15us[  +57us] +/-  320us
```

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
```

SUSE Linux

A partir do SUSE Linux Enterprise Server 15, o `chrony` é a implementação padrão do NTP.

Para configurar o chrony para conectar-se ao endpoint IPv4 no SUSE Linux

1. Abra o arquivo `/etc/chrony.conf` usando um editor de texto (como vim ou nano).
2. Verifique se o arquivo contém a seguinte linha:

   ```
   server 169.254.169.123 prefer iburst minpoll 4 maxpoll 4
   ```

   Se essa linha não estiver presente, adicione-a.
3. Comente qualquer outro servidor ou linhas de consulta.
4. Abra o YaST e ative o serviço chrony.

Windows

A versão das AMIs do Windows de agosto de 2018 em diante usam o Amazon Time Sync Service por padrão. Nenhuma configuração adicional é necessária para instâncias iniciadas dessas AMIs e você pode ignorar os procedimentos a seguir.

Se você estiver usando uma AMI que não tenha o Serviço de Sincronização Temporal da Amazon configurado por padrão, primeiro verifique sua configuração atual do protocolo NTP. Se a instância já estiver usando o endpoint IPv4 do Serviço de Sincronização Temporal da Amazon, nenhuma configuração adicional será necessária. Se a instância não estiver usando o Serviço de

Sincronização Temporal da Amazon, faça o procedimento para alterar o servidor NTP para que use o Serviço de Sincronização Temporal da Amazon.

Para verificar a configuração de NTP

1. Na instância, abra uma janela de prompt de comando.
2. Obtenha a configuração de NTP atual digitando o seguinte comando:

   ```
   w32tm /query /configuration
   ```

   Esse comando retorna as definições de configuração atuais para a instância do Windows e mostrará se você está conectado ao Serviço de Sincronização Temporal da Amazon.
3. (Opcional) Obtenha o status da configuração atual digitando o seguinte comando:

   ```
   w32tm /query /status
   ```

   Esse comando retorna informações, como o último horário em que a instância foi sincronizada com o servidor NTP e o intervalo de sondagem.

Para alterar o servidor NTP para usar o Amazon Time Sync Service

1. Na janela de prompt de comando, execute o seguinte comando:

   ```
   w32tm /config /manualpeerlist:169.254.169.123 /syncfromflags:manual /update
   ```
2. Verifique suas novas configurações usando o seguinte comando:

   ```
   w32tm /query /configuration
   ```

   Na saída retornada, verifique se `NtpServer` exibe o endpoint IPv4 `169.254.169.123`.

Configurações padrão de NTP para AMIs da Amazon para o Windows

As Imagens de máquina da Amazon (AMIs) geralmente aderem aos padrões prontos para uso, exceto em casos em que alterações são necessárias para que funcionem na infraestrutura do EC2. As seguintes configurações foram determinadas para funcionar de maneira adequada

em um ambiente virtual, bem como manter qualquer desvio de relógio dentro um segundo de precisão:

- Intervalo de atualização: rege a frequência com que o serviço de hora acertará a hora do sistema para garantir sua precisão. A AWS configura o intervalo de atualização para ocorrer uma vez a cada dois minutos.
- Servidor NTP: a partir da versão de agosto de 2018, as AMIs usam o Serviço de Sincronização Temporal da Amazon por padrão. Esse serviço de horário pode ser acessado em qualquer Região da AWS no endpoint IPv4 169.254.169.123. Além disso, o sinalizador 0x9 indica que o serviço de horário está atuando como um cliente e utiliza o `SpecialPollInterval` para determinar a frequência com a qual realizar verificações com o servidor de horário configurado.
- Tipo – "NTP" significa que o serviço atua como um cliente NTP autônomo em vez de agir como parte de um domínio.
- Habilitado e InputProvider: o serviço de hora está habilitado e fornece a hora ao sistema operacional.
- Intervalo de pesquisa especial: verifica o servidor NTP configurado a cada 900 segundos (15 minutos).

Caminho de registro	Nome da chave	Dados
HKLM:\System\CurrentControlSet\services\w32time\Config	UpdateInterval	120
HKLM:\System\CurrentControlSet\services\w32time\Parameters	NtpServer	169.254.169.123,0x9
HKLM:\System\CurrentControlSet\services\w32time\Parameters	Tipo	NTP
HKLM:\System\CurrentControlSet\services\w32time\TimeProviders\NtpClient	Enabled	1

Caminho de registro	Nome da chave	Dados
HKLM:\System\CurrentControlSet\services\w32time\TimeProviders\NtpClient	InputProvider	1
HKLM:\System\CurrentControlSet\services\w32time\TimeProviders\NtpClient	SpecialPollInterval	900

Conectar-se ao endpoint IPv6 do Serviço de Sincronização Temporal da Amazon

Esta seção explica como as etapas descritas no Conectar-se ao endpoint IPv4 do Serviço de Sincronização Temporal da Amazon diferem se você estiver configurando a instância para usar o Serviço de Sincronização Temporal da Amazon local por meio do endpoint IPv6. Ela não explica todo o processo de configuração do Amazon Time Sync Service.

O endpoint IPv6 só é acessível em instâncias baseadas em Nitro.

Não recomendamos usar as entradas de endpoint IPv4 e IPv6 em conjunto. Os pacotes IPv4 e IPv6 NTP vêm do mesmo servidor local para a sua instância. Configurar ambos os endpoints IPv4 e IPv6 é desnecessário e não melhorará a precisão da hora na instância.

Linux

Dependendo da distribuição do Linux que está usando, ao chegar à etapa de edição do arquivo `chrony.conf`, você estará usando o endpoint IPv6 do Serviço de Sincronização Temporal da Amazon (`fd00:ec2::123`) em vez do endpoint IPv4 (`169.254.169.123`):

```
server fd00:ec2::123 prefer iburst minpoll 4 maxpoll 4
```

Salve o arquivo e confirme que o chrony está usando o endpoint IPv6 `fd00:ec2::123` para sincronizar a hora:

```
[ec2-user ~]$ chronyc sources -v
```

Na saída, se você vir o endpoint IPv6 `fd00:ec2::123`, a configuração estará concluída.

Windows

Ao chegar à etapa de alteração do servidor NTP para usar o Serviço de Sincronização Temporal da Amazon, você estará usando o endpoint IPv6 do Serviço de Sincronização Temporal da Amazon (`fd00:ec2::123`) em vez do endpoint IPv4 (`169.254.169.123`):

```
w32tm /config /manualpeerlist:fd00:ec2::123 /syncfromflags:manual /update
```

Verifique se as novas configurações estão usando o endpoint IPv6 `fd00:ec2::123` para sincronizar o horário:

```
w32tm /query /configuration
```

Na saída, verifique se `NtpServer` exibe o endpoint IPv6 `fd00:ec2::123`.

Conectar-se ao relógio PTP físico

O relógio de hardware baseado em PTP faz parte do AWS Nitro System, portanto, pode ser acessado diretamente em instâncias bare metal e virtualizadas do EC2 com suporte, sem a necessidade de usar recursos do cliente.

Os endpoints NTP para o relógio de hardware PTP são os mesmos do Serviço de Sincronização Temporal da Amazon normal. Se a instância tiver um relógio de hardware PTP e você tiver configurado a conexão NTP (com o endpoint IPv4 ou IPv6), a hora da instância será automaticamente obtida do relógio de hardware PTP via NTP.

Para instâncias do Linux, é possível configurar uma conexão PTP direta, o que fornecerá uma hora mais precisa do que a conexão NTP. As instâncias do Windows só são compatíveis com uma conexão NTP para o relógio de hardware PTP.

Requisitos

O relógio PTP físico está disponível em uma instância quando os seguintes requisitos são atendidos:

- Regiões da AWS com suporte: Leste dos EUA (Norte da Virgínia), Leste dos EUA (Ohio), Ásia-Pacífico (Malásia), Ásia-Pacífico (Tailândia), Ásia-Pacífico (Tóquio) e Europa (Estocolmo)
- Zonas locais compatíveis: Leste dos EUA (Cidade de Nova York)
- Famílias de instâncias suportadas:
  - Uso geral: M7a, M7g, M7i

  - Otimizadas para memória: R7a, R7g, R7i
  - Otimizadas para armazenamento: I8g, I8ge
- (Somente Linux) Driver do ENA, na versão 2.10.0 ou em versões posteriores, instalado em um sistema operacional compatível. Para obter mais informações sobre os sistemas operacionais compatíveis, consulte os pré-requisitos do driver no GitHub.

(Somente Linux) Configurar uma conexão PTP direta com o relógio de hardware PTP

Esta seção descreve como configurar a instância do Linux para usar o Serviço de Sincronização Temporal da Amazon local por meio do relógio de hardware PTP usando uma conexão PTP direta. É necessário adicionar uma entrada do servidor para o relógio de hardware PTP ao arquivo de configuração do `chrony`.

Para configurar uma conexão PTP direta com o relógio de hardware PTP (somente instâncias do Linux)

1. Pré-requisitos de instalação

   Conecte-se à sua instância do Linux e faça o seguinte:

   a. Instale o driver do kernel Linux para o Adaptador de Rede Elástica (ENA) versão 2.10.0 ou posterior.

   b. Habilite o relógio de hardware PTP.

   Para obter as instruções de instalação, consulte Linux kernel driver for Elastic Network Adapter (ENA) family no GitHub.
2. Verificar o dispositivo ENA PTP

   Verifique se o dispositivo de relógio de hardware ENA PTP aparece em sua instância.

   ```
   [ec2-user ~]$ for file in /sys/class/ptp/*; do echo -n "$file: "; cat "$file/
   clock_name"; done
   ```

   Saída esperada

   ```
   /sys/class/ptp/ptp<index>: ena-ptp-<PCI slot>
   ```

Em que:

- *index* é o índice de relógio de hardware PTP registrado no kernel.
- *PCI slot* é o slot PCI do controlador Ethernet ENA. É o mesmo slot mostrado em `lspci | grep ENA`.

Exemplo de saída

```
/sys/class/ptp/ptp0: ena-ptp-05
```

Se `ena-ptp-<PCI slot>` não estiver na saída, o driver ENA não foi instalado corretamente. Revise a etapa 1 desse procedimento para instalar o driver.

3. Configurar o link simbólico PTP

Os dispositivos PTP geralmente são nomeados `/dev/ptp0`, `/dev/ptp1` e assim por diante, e o índice depende da ordem de inicialização do hardware. A criação de um link simbólico garante que aplicações como o chrony façam referência consistentemente ao dispositivo correto, independentemente das alterações no índice.

As AMIs mais recentes do Amazon Linux 2023 incluem uma regra `udev` que cria o link simbólico `/dev/ptp_ena`, apontando para a entrada `/dev/ptp` correta associada ao host ENA.

Primeiro, verifique se o link simbólico está presente executando o seguinte comando.

```
[ec2-user ~]$ ls -l /dev/ptp*
```

Exemplo de saída

```
crw------- 1 root root 245, 0 Jan 31 2025 /dev/ptp0
lrwxrwxrwx 1 root root      4 Jan 31 2025 /dev/ptp_ena -> ptp0
```

Em que:

- `/dev/ptp<index>` é o caminho para o dispositivo PTP.
- `/dev/ptp_ena` é o link simbólico constante, que aponta para o mesmo dispositivo PTP.

Se o link simbólico `/dev/ptp_ena` estiver presente, pule para a Etapa 4 deste procedimento. Se estiver faltando, faça o seguinte:

a. Adicione a seguinte regra `udev`.

```
[ec2-user ~]$ echo "SUBSYSTEM==\"ptp\", ATTR{clock_name}==\"ena-ptp-*\",
 SYMLINK += \"ptp_ena\"" | sudo tee -a /etc/udev/rules.d/53-ec2-network-
interfaces.rules
```

b. Recarregue a regra `udev`, reiniciando a instância ou executando o comando a seguir.

```
[ec2-user ~]$ sudo udevadm control --reload-rules && udevadm trigger
```

4. Configurar o chrony

O chrony deve ser configurado para usar o link simbólico `/dev/ptp_ena` em vez de referenciar /dev/ptp*<index>* diretamente.

a. Edite o `/etc/chrony.conf` o usando um editor de texto e adicione a linha a seguir em qualquer ponto no arquivo.

```
refclock PHC /dev/ptp_ena poll 0 delay 0.000010 prefer
```

b. Reinicie o chrony.

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

5. Verificar configuração do chrony

Verifique se o chrony está usando o relógio PTP físico para sincronizar a hora nessa instância.

```
[ec2-user ~]$ chronyc sources
```

Saída esperada

```
MS Name/IP address         Stratum Poll Reach LastRx Last sample
===============================================================================
```

```
#* PHC0                           0   0    377    1   +2ns[ +1ns] +/-   5031ns
```

Na saída retornada, * indica a fonte de hora preferida. PHC0 corresponde ao relógio PTP físico. Pode ser necessário esperar alguns segundos após reiniciar o chrony para que o asterisco apareça.

Definir a referência de horas na instância do EC2 ou em qualquer dispositivo conectado à Internet para usar o Serviço de Sincronização Temporal da Amazon público

É possível configurar a instância ou qualquer dispositivo conectado à Internet, como seu computador local ou um servidor local, para usar o Serviço de Sincronização Temporal da Amazon público, que pode ser acessado pela Internet em `time.aws.com`. É possível usar o Serviço de Sincronização Temporal da Amazon público como backup para o Serviço de Sincronização Temporal da Amazon e para conectar recursos de fora da AWS ao Serviço de Sincronização Temporal da Amazon.

> **Note**
>
> Para obter a melhor performance, recomendamos usar o Serviço de Sincronização Temporal da Amazon local nas instâncias e usar o Serviço de Sincronização Temporal da Amazon público somente como backup.

Use as instruções referentes ao sistema operacional da sua instância ou do seu dispositivo.

Linux

Para definir que a instância ou dispositivo com Linux use o Serviço de Sincronização Temporal da Amazon público usando chrony ou ntpd

1. Edite o `/etc/chrony.conf` (se você usar o chrony) ou o `/etc/ntp.conf` (se você usar o ntpd) usando um de texto da seguinte maneira:

   a. Para evitar que a instância ou o dispositivo tente misturar servidores com difusão de tempo e servidores sem difusão de tempo, remova ou comente as linhas que começam com `server`, exceto qualquer conexão existente com o Serviço de Sincronização Temporal da Amazon local.

> **Important**
>
> Se você estiver configurando sua instância do EC2 para se conectar ao Serviço de Sincronização Temporal da Amazon público, não remova a linha a seguir que a instância deve se conectar ao Serviço de Sincronização Temporal da Amazon local. O Serviço de Sincronização Temporal da Amazon local é uma conexão mais direta e garantirá uma maior precisão do relógio. O Serviço de Sincronização Temporal da Amazon público só deve ser usado como backup.
>
> ```
> server 169.254.169.123 prefer iburst minpoll 4 maxpoll 4
> ```

b. Adicione a seguinte linha para se conectar ao Serviço de Sincronização Temporal da Amazon.

```
pool time.aws.com iburst
```

2. Reinicie o daemon usando um dos comandos a seguir.

   - chrony

   ```
   sudo service chronyd force-reload
   ```

   - ntpd

   ```
   sudo service ntp reload
   ```

macOS

Para definir que a instância ou dispositivo com macOS use o Serviço de Sincronização Temporal da Amazon público

1. Abra System Preferences (Preferências do sistema).
2. Escolha Date & Time (Data e hora) e, em seguida, escolha a guia Date & Time (Data e hora).
3. Para fazer alterações, escolha o ícone de cadeado e digite sua senha quando solicitado.
4. Em Definir data e hora automaticamente, insira **`time.aws.com`**.

Windows

Para definir que a instância ou dispositivo com Windows use o Serviço de Sincronização Temporal da Amazon público

1. Abra o Control Panel (Painel de controle).
2. Escolha o ícone de Date and Time (Data e hora).
3. Escolha a guia Internet Time (Horário da Internet). Essa guia não estará disponível se o PC fizer parte de um domínio. Nesse caso, a hora será sincronizada com o controlador de domínio. É possível configurar o controlador para usar o Serviço de Sincronização Temporal da Amazon público.
4. Escolha Change settings (Alterar configurações).
5. Marque a caixa de seleção em Sincronizar com um servidor de hora na Internet.
6. Ao lado de Servidor, insira **`time.aws.com`**.

Para definir que a instância ou dispositivo com Windows Server use o Serviço de Sincronização Temporal da Amazon público

- Siga as instruções da Microsoft para atualizar o registro.

Comparação dos carimbos de data/hora das instâncias do Linux

Se estiver usando o Serviço de Sincronização Temporal da Amazon, será possível comparar os carimbos de data/hora nas instâncias do Linux do Amazon EC2 com o ClockBound para determinar o horário real de um evento. O ClockBound mede a precisão do relógio da instância do EC2 e permite que você confira se um determinado carimbo de data/hora está no passado ou no futuro em relação ao relógio atual da instância. Essas informações são valiosas para determinar a ordem e a consistência de eventos e transações entre instâncias do EC2, independentemente da localização geográfica de cada instância.

O ClockBound é um daemon e uma biblioteca de código aberto. Para saber mais sobre o ClockBound, incluindo instruções de instalação, consulte Clockbound no GitHub.

O ClockBound é compatível somente com instâncias do Linux.

Se você estiver usando a conexão PTP direta com o relógio PTP físico, seu daemon de hora, como o chrony, subestimará o limite de erro do relógio. Isso ocorre porque um relógio PTP físico não passa

as informações corretas de limite de erro para o chrony, como o NTP faz. Como resultado, o daemon de sincronização de relógio pressupõe que o relógio esteja certo em UTC e que, portanto, tenha um limite de erro de `0`. Para medir o limite total de erro, o Sistema Nitro calcula o limite de erro do relógio PTP físico e o disponibiliza para a instância do EC2 via sistema de arquivos `sysfs` do driver ENA. Isso pode ser lido diretamente como um valor em nanossegundos.

Para recuperar o limite de erro do relógio de hardware PTP

1. Primeiro, obtenha a localização correta do dispositivo de relógio de hardware PTP usando um dos comandos a seguir. O caminho no comando pode ser diferente dependendo da AMI usada para iniciar a instância.

   - Para Amazon Linux 2:

     ```
     cat /sys/class/net/eth0/device/uevent | grep PCI_SLOT_NAME
     ```

   - Para Amazon Linux 2023:

     ```
     cat /sys/class/net/ens5/device/uevent | grep PCI_SLOT_NAME
     ```

   A saída é o nome do slot PCI, que é a localização do dispositivo de relógio de hardware PTP físico. Neste exemplo, o local é `0000:00:03.0`.

   ```
   PCI_SLOT_NAME=0000:00:03.0
   ```

2. Para recuperar erro do relógio de hardware PTP vinculado execute o comando a seguir. Inclua o nome do slot PCI da etapa anterior.

   ```
   cat /sys/bus/pci/devices/0000:00:03.0/phc_error_bound
   ```

   A saída é o limite de erro do relógio PTP físico, em nanossegundos.

Para calcular o limite de erro de relógio certo em um dado momento específico ao usar a conexão PTP direta com o relógio PTP físico, você deve adicionar o limite de erro do relógio do chrony ou do ClockBound no momento em que o chrony consultar o relógio PTP físico. Para obter mais informações sobre como medir e monitorar a precisão do relógio, consulte Manage Amazon EC2 instance clock accuracy using Amazon Time Sync Service and Amazon CloudWatch – Part 1.

Alteração do fuso horário da instância

As instâncias do Amazon EC2 são definidas para o fuso horário UTC (Tempo Universal Coordenado), por padrão. É possível alterar a hora de uma instância para o horário local ou para outro fuso horário em sua rede.

Use as instruções para o sistema operacional da sua instância.

Linux

> **Important**
>
> Essas informações se aplicam ao Amazon Linux. Para obter informações sobre outras distribuições, consulte a documentação específica.

Para alterar o fuso horário no Amazon Linux

1. Exiba a configuração atual de fuso horário do sistema.

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

2. Liste os fusos horários disponíveis.

   ```
   [ec2-user ~]$ timedatectl list-timezones
   ```

3. Defina o fuso horário escolhido.

   ```
   [ec2-user ~]$ sudo timedatectl set-timezone America/Vancouver
   ```

4. (Opcional) Confirme se o fuso horário atual foi atualizado para o novo fuso horário executando o comando timedatectl novamente.

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

Windows

Para alterar o fuso horário de uma instância do Windows

1. Na instância, abra uma janela de prompt de comando.

2. Identifique o fuso horário a ser usado na instância. Para obter uma lista de fusos horários, use o seguinte comando:

```
tzutil /l
```

   Esse comando retorna uma lista com todos os fusos horários disponíveis no seguinte formato:

```
display name
time zone ID
```

3. Localize o ID do fuso horário a ser atribuído à instância.
4. Exemplo: atribuir o fuso horário UTC:

```
tzutil /s "UTC"
```

   Exemplo: atribuir o horário padrão do Pacífico:

```
tzutil /s "Pacific Standard Time"
```

Quando você altera o fuso horário em uma instância do Windows, deve garantir que ele seja mantido durante as reinicializações de sistema. Caso contrário, quando a instância for reiniciada, ela voltará a usar o horário UTC. É possível conservar o horário adicionando a chave do registro RealTimeIsUniversal. Essa chave é definida por padrão em todas as instâncias da geração atual. Para verificar se a chave de registro RealTimeIsUniversal está configurada, consulte a Etapa 3 no procedimento apresentado a seguir. Se a chave não estiver definida, siga estas etapas desde o início.

Para definir a chave do Registro RealTimeIsUniversal

1. Na instância, abra uma janela de prompt de comando.
2. Use o seguinte comando para adicionar a chave de Registro:

```
reg add "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\TimeZoneInformation" /
v RealTimeIsUniversal /d 1 /t REG_DWORD /f
```

3. (Opcional) Verifique se a instância salvou a chave com êxito usando o seguinte comando:

```
reg query "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control
\TimeZoneInformation" /s
```

Esse comando retorna as subchaves da chave de Registro TimeZoneInformation. É necessário ver a chave RealTimeIsUniversal na parte inferior da lista, semelhante à chave a seguir:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\TimeZoneInformation
    Bias                            REG_DWORD     0x1e0
    DaylightBias                    REG_DWORD     0xffffffc4
    DaylightName                    REG_SZ        @tzres.dll,-211
    DaylightStart                   REG_BINARY    00000300020002000000000000000000
    StandardBias                    REG_DWORD     0x0
    StandardName                    REG_SZ        @tzres.dll,-212
    StandardStart                   REG_BINARY    00000B0001000200000000000000000
    TimeZoneKeyName                 REG_SZ        Pacific Standard Time
    DynamicDaylightTimeDisabled     REG_DWORD     0x0
    ActiveTimeBias                  REG_DWORD     0x1a4
    RealTimeIsUniversal             REG_DWORD     0x1
```

EC2 Capacity Manager

O Amazon EC2 Gerenciador de Capacidade permite que você monitore, analise e gerencie seu uso de capacidade em instâncias sob demanda, instâncias spot e reservas de capacidade em um único local. O Capacity Manager simplifica o controle de capacidade por meio de um painel unificado que agrega seus dados de uso com atualizações de hora em hora e oportunidades de otimização.

Projetado para grandes empresas e organizações com várias contas, o Capacity Manager elimina a coleta manual de dados de várias fontes. A ferramenta fornece insights profundos sobre suas Regiões da AWS. É possível detalhar métricas de capacidade detalhadas e tomar medidas imediatas para otimizar seus recursos de nuvem.

Ao habilitar a integração do AWS Organizations, é possível visualizar e analisar os dados de capacidade em todas as contas de membro da sua organização a partir de um único painel. Sem a integração do Organizations, o Capacity Manager monitora apenas os recursos dentro da Conta da AWS individual em que está ativado.

> **Note**
>
> - Você só pode ativar o Capacity Manager em uma Região da AWS por conta.
> - Todos os custos exibidos no Capacity Manager são custos estimados com base nos preços publicados sob demanda. Essas estimativas não incluem descontos como Savings Plans ou instâncias reservadas. Seus custos reais podem diferir dessas estimativas.

Recursos principais

- Painel centralizado: visualize o uso da capacidade em todas as contas e regiões com novos pontos de dados atualizados a cada hora
- Visibilidade entre contas: visualização em nível organizacional para contas de administrador
- Exportação de dados: exportação de dados de capacidade para o Amazon S3
- APIs: acesso programático a métricas e dados de capacidade
- Análise flexível: seletor de datas dinâmico para explorar o uso da capacidade em diferentes períodos dos últimos 90 dias
- Métricas e dimensões abrangentes: acesso a mais de 30 métricas em várias unidades de medição (vCPUs, instâncias, custos estimados) com amplos recursos de filtragem, incluindo ID da conta, região, família de instâncias, zona de disponibilidade, tipo de instância, plataforma, locação e dimensões específicas de reservas

Habilitação do EC2 Capacity Manager

O Capacity Manager pode ser habilitado em dois níveis diferentes, dependendo de suas necessidades. É possível habilitá-lo para que uma única Conta da AWS monitore recursos somente dentro dessa conta, ou integrá-lo ao AWS Organizations para ter visibilidade centralizada em todas as contas de membro em sua organização.

- Nível organizacional: visualize e analise os dados de capacidade em todas as contas de membro da sua organização a partir de um único painel.
- Nível de conta: monitore o uso da capacidade em uma única Conta da AWS.

Tópicos

- Habilitação do EC2 Capacity Manager com o AWS Organizations
- Habilitação do EC2 Capacity Manager no nível da conta
- Registro de um administrador delegado
- Uso de perfis vinculados ao serviço do EC2 Capacity Manager

Habilitação do EC2 Capacity Manager com o AWS Organizations

É possível habilitar o EC2 Capacity Manager with AWS Organizations para visibilidade em nível organizacional e gerenciamento de sua capacidade em todas as contas de membro. Essa integração permite monitorar, analisar e gerenciar o uso da capacidade a partir de um local centralizado.

A conta gerencial é responsável por permitir o acesso em nível organizacional e gerenciar a capacidade em toda a organização.

Habilitar o Capacity Manager com o AWS Organizations proporciona os benefícios a seguir:

- Visibilidade centralizada da capacidade: visualize o uso da capacidade em todas as contas de membro da sua organização a partir de um único painel com agregação entre regiões e contas.
- Otimização em toda a organização: identifique reservas de capacidade não utilizadas e oportunidades de otimização em todas as contas da sua organização.
- Administrador delegado: permite que contas de membro específicas gerenciem o Capacity Manager de uma organização, mantendo os controles de acesso adequados.

Se você não habilitar a integração com o AWS Organizations, só poderá monitorar recursos na Conta da AWS individual que habilitou o Capacity Manager.

Pré-requisitos

- É necessário ter uma configuração no AWS Organizations com uma conta de gerenciamento e uma ou mais contas de membro. Para obter mais informações sobre os tipos de conta, consulte Terminologia e conceitos no Guia do usuário do AWS Organizations.
- A conta gerencial deve ter permissões para as ações do IAM a seguir:
  - `organizations:EnableAwsServiceAccess`
  - `organizations:RegisterDelegatedAdministrator` (se estiver usando administração delegada)
  - `iam:CreateServiceLinkedRole`

- É necessário criar um perfil vinculado ao serviço com o caso de uso AWSEC2CapacityManagerServiceRolePolicy para permitir o acesso ao AWS Organizations. Para obter mais informações, consulte Criação de um perfil vinculado ao serviço para Capacity Manager.

Habilitação do Capacity Manager com o AWS Organizations

Usando a conta gerencial, habilite o acesso da organização no Capacity Manager.

Console

Para habilitar o acesso da organização no Capacity Manager

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Capacity Manager.
3. Escolha a guia Configurações.
4. Na seção Acesso confiável, escolha Gerenciar acesso confiável.
5. No prompt exibido, selecione Habilitar acesso confiável. Selecione Salvar.

AWS CLI

Para habilitar o acesso da organização no Capacity Manager

1. Criar um perfil vinculado ao serviço

```
aws iam create-service-linked-role --aws-service-name
 ec2.capacitymanager.amazonaws.com
```

2. Habilite o acesso ao AWS Organizations

```
aws organizations enable-aws-service-access --service-principal
 ec2.capacitymanager.amazonaws.com
```

3. Habilite o Capacity Manager com o AWS Organizations

```
aws ec2 enable-capacity-manager --organizations-access
```

Para atualizar o acesso da organização a um Capacity Manager existente, execute o comando a seguir:

```
aws ec2 update-capacity-manager-organizations-access --organizations-access
```

Verificação se o Capacity Manager está habilitado em sua organização

Console

Para verificar se o Capacity Manager está habilitado em sua organização

1. No console do Capacity Manager, escolha Configurações.
2. Na seção Acesso confiável, verifique se Acesso da organização aparece como Habilitado.
3. Verifique se o ID da organização exibe o ID da sua organização.

AWS CLI

Para verificar se o Capacity Manager está habilitado em sua organização

Execute o seguinte comando:

```
aws ec2 get-capacity-manager-attributes
```

A saída deve exibir:

```
{
    "CapacityManagerStatus": "enabled",
    "OrganizationsAccess": true,
```

```
    "IngestionStatus": "initial-ingestion-pending",
    "IngestionStatusMessage": "Capacity Manager is collecting historical data from
 2025-10-01T00:00:00Z. Data collection is in progress and may take several hours to
 complete."
}
```

Considerações

- Criação de perfil vinculado ao serviço: quando você habilita o acesso da organização por meio do console, o Gerenciador de Capacidade cria automaticamente o perfil vinculado ao serviço AWSServiceRoleForEC2CapacityManager em todas as contas de membro. Se você habilitar por meio da AWS CLI, deverá chamar `createServiceLinkedRole` manualmente.
- Agregação de dados: depois de habilitar o acesso da organização, o Capacity Manager preencherá 14 dias de dados históricos de todas as contas de membro. Normalmente, esse processo leva alguns minutos para ser concluído.
- Limitações regionais: só é possível habilitar o Capacity Manager em uma região por organização, mas ele agregará dados de todas as regiões comerciais.
- Permissões: as contas de membro não precisam realizar nenhuma ação. O Capacity Manager usa o perfil vinculado ao serviço para descobrir automaticamente os recursos em todas as contas.

Habilitação do EC2 Capacity Manager no nível da conta

Habilite o Capacity Manager no nível da conta para monitorar e analisar o uso da capacidade do EC2 em uma única conta da AWS. Depois de habilitá-lo, o Capacity Manager coletará dados sobre suas instâncias sob demanda, instâncias spot e reservas de capacidade para ajudá-lo a identificar oportunidades de otimização e rastrear padrões de uso.

Habilitação do Capacity Manager no nível da conta

Console

Para habilitar o Capacity Manager para sua conta

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Capacity Manager.
3. Na página Capacity Manager, escolha Habilitar na região.

AWS CLI

Para habilitar o Capacity Manager para sua conta

Execute o seguinte comando:

```
aws ec2 enable-capacity-manager
```

Note

- Depois de habilitar o Capacity Manager, ele coletará e agregará 14 dias de dados históricos. Esse processo pode levar algumas horas.
- Ao coletar seus dados históricos, um estado `initial-ingestion-in-progress` será exibido. Durante esse período de coleta, é possível observar lacunas em seus dados históricos. Quando a coleta de dados for concluída, um estado `ingestion-complete` será exibido.

Registro de um administrador delegado

É possível registrar um administrador delegado para o Capacity Manager. Isso permite que uma conta de membro gerencie o Capacity Manager da sua organização da AWS. Somente a conta gerencial pode remover um administrador delegado na sua organização.

Note

Não é possível desabilitar o Gerenciador de Capacidade para sua organização enquanto houver um administrador delegado registrado.

Tópicos

- Pré-requisitos
- Registro de um administrador delegado
- Para remover um administrador delegado

Pré-requisitos

Sua conta gerencial deve ter habilitado o Capacity Manager no AWS Organizations. Para obter mais informações, consulte Habilitação do EC2 Capacity Manager com o AWS Organizations.

Registro de um administrador delegado

É possível registrar um administrador delegado usando o console do Amazon EC2 ou a AWS CLI.

Console

Para registrar um administrador delegado

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Capacity Manager.
3. Escolha a guia Configurações.
4. Na seção Administrador delegado, escolha Adicionar.
5. No prompt que será exibido, insira o ID da conta do membro da organização que você deseja adicionar como administrador delegado.
6. Selecione Add delegated administrator (Adicionar administrador delegado).

AWS CLI

Para registrar um administrador delegado

Execute o seguinte comando:

```
aws organizations register-delegated-administrator \
    --account-id 123456789012 \
    --service-principal ec2.capacitymanager.amazonaws.com
```

Para remover um administrador delegado

É possível remover um administrador delegado usando o console do Amazon EC2 ou a AWS CLI.

Console

Para remover um administrador delegado

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Capacity Manager.
3. Escolha a guia Configurações.
4. Na seção Administrador delegado, escolha Gerenciar.
5. No prompt que será exibido, escolha Remover administrador delegado.

AWS CLI

Para remover um administrador delegado

Execute o seguinte comando:

```
aws organizations deregister-delegated-administrator \
    --account-id 123456789012 \
    --service-principal ec2.capacitymanager.amazonaws.com
```

Uso de perfis vinculados ao serviço do EC2 Capacity Manager

O EC2 Capacity Manager usa perfis vinculados ao serviço do AWS Identity and Access Management (IAM). Um perfil vinculado ao serviço é um tipo exclusivo de perfil do IAM vinculado diretamente ao Capacity Manager. Os perfis vinculados a serviços são predefinidos pelo Capacity Manager e incluem todas as permissões que o serviço requer para chamar outros serviços da AWS em seu nome.

Um perfil vinculado ao serviço facilita a configuração do Gerenciador de Capacidade, pois não é preciso adicionar as permissões necessárias manualmente. O Capacity Manager define as permissões dos perfis vinculados ao serviço e, exceto se definido de outra forma, somente o Capacity Manager pode assumir os perfis. As permissões definidas incluem a política de confiança e a política de permissões, que não pode ser anexada a nenhuma outra entidade do IAM.

Um perfil vinculado ao serviço poderá ser excluído somente após excluir seus atributos relacionados. Isso protege seus recursos do Capacity Manager, pois não é possível remover por engano as permissões para acessar os recursos.

Para obter mais informações sobre outros serviços que são compatíveis com perfis vinculados ao serviço, consulte Serviços da AWS que funcionam com o IAM e procure por serviços que indiquem Sim na coluna Perfis vinculados ao serviço. Escolha um Sim com um link para visualizar a documentação do perfil vinculado a esse serviço.

Permissões dos perfis vinculados ao serviço do Capacity Manager

O Capacity Manager usa o perfil vinculado ao serviço denominado AWSServiceRoleForEC2CapacityManager para permitir que você gerencie recursos de capacidade e se integrar ao AWS Organizations em seu nome.

O perfil vinculado ao serviço AWSServiceRoleForEC2CapacityManager confia nos serviços a seguir para assumir o perfil:

- `ec2.capacitymanager.amazonaws.com`

A política de permissões de perfil denominada AWSEC2CapacityManagerServiceRolePolicy permite que o Capacity Manager execute as ações a seguir:

- `organizations:DescribeOrganization`
- `organizations:ListAccounts`
- `organizations:ListChildren`
- `organizations:ListAWSServiceAccessForOrganization`
- `organizations:ListDelegatedAdministrators`

Você deve configurar permissões para permitir que seus usuários, grupos ou perfis criem, editem ou excluam um perfil vinculado ao serviço. Para obter mais informações, consulte Permissões do perfil vinculado a serviço no Guia do usuário do IAM.

Criar um perfil vinculado ao serviço no Capacity Manager

Também é possível usar o console do IAM para criar um perfil vinculado ao serviço com o caso de uso AWSEC2CapacityManagerServiceRolePolicy. Na AWS CLI ou na API do AWS, crie um perfil vinculado a serviço com o nome de serviço `ec2.capacitymanager.amazonaws.com`. Para obter

mais informações, consulte Criar uma função vinculada ao serviço no Manual do usuário do IAM. Se você excluir essa função vinculada ao serviço, será possível usar esse mesmo processo para criar a função novamente.

Edição de um perfil vinculado a serviço no Capacity Manager

O Capacity Manager não permite editar o perfil vinculado ao serviço AWSServiceRoleForEC2CapacityManager. Depois que criar um perfil vinculado ao serviço, você não poderá alterar o nome do perfil, pois várias entidades podem fazer referência a ele. No entanto, será possível editar a descrição do perfil usando o IAM. Para saber mais, consulte Editar um perfil vinculado ao serviço no Guia do usuário do IAM.

Exclusão de um perfil vinculado a serviço no Capacity Manager

Se você não precisar mais usar um atributo ou serviço que requer um perfil vinculado ao serviço, é recomendável excluí-lo. Dessa forma, você não tem uma entidade não utilizada que não seja monitorada ativamente ou mantida. No entanto, você deve limpar os recursos de sua função vinculada ao serviço antes de exclui-la manualmente.

> **Note**
>
> Se o serviço do Capacity Manager estiver usando o perfil quando você tentar excluir os atributos, a exclusão poderá falhar. Se isso acontecer, espere alguns minutos e tente a operação novamente.

Para remover recursos do Capacity Manager usados por AWSServiceRoleForEC2CapacityManager

1. Todos os administradores delegados devem ter desabilitado o Capacity Manager antes de remover o acesso da organização.
2. É necessário excluir todas as exportações de dados ativas antes de desabilitar um Capacity Manager.

Como excluir manualmente o perfil vinculado ao serviço usando o IAM

Use o console do IAM, a AWS CLI ou a API da AWS para excluir o perfil vinculado ao serviço AWSServiceRoleForEC2CapacityManager. Para saber mais, consulte Excluir um perfil vinculado ao serviço no Guia do usuário do IAM.

Regiões com suporte a perfis vinculados ao serviço do Capacity Manager

O Capacity Manager oferece suporte ao uso de perfis vinculados ao serviço em todas as regiões em que o serviço estiver disponível. Para obter mais informações, consulte Regiões e endpoints da AWS.

O Capacity Manager não oferece suporte ao uso de perfis vinculados a serviços em todas as regiões em que o serviço estiver disponível. É possível usar o perfil AWSServiceRoleForEC2CapacityManager nas regiões a seguir.

Nome da região	Identidade da região	Suporte no Capacity Manager
Leste dos EUA (Norte da Virgínia)	us-east-1	Sim
Leste dos EUA (Ohio)	us-east-2	Sim
Oeste dos EUA (N. da Califórnia)	us-west-1	Sim
Oeste dos EUA (Oregon)	us-west-2	Sim
África (Cidade do Cabo)	af-south-1	Não
Ásia-Pacífico (Hong Kong)	ap-east-1	Não
Ásia-Pacífico (Jacarta)	ap-southeast-3	Não
Ásia-Pacífico (Mumbai)	ap-south-1	Sim
Ásia Pacifico (Osaka)	ap-northeast-3	Sim
Ásia-Pacífico (Seul)	ap-northeast-2	Sim
Ásia-Pacífico (Singapura)	ap-southeast-1	Sim
Ásia-Pacífico (Sydney)	ap-southeast-2	Sim
Ásia-Pacífico (Tóquio)	ap-northeast-1	Sim
Canadá (Central)	ca-central-1	Sim

Nome da região	Identidade da região	Suporte no Capacity Manager
Europa (Frankfurt)	eu-central-1	Sim
Europa (Irlanda)	eu-west-1	Sim
Europa (Londres)	eu-west-2	Sim
Europa (Milão)	eu-south-1	Não
Europa (Paris)	eu-west-3	Sim
Europa (Estocolmo)	eu-north-1	Sim
Oriente Médio (Barém)	me-south-1	Não
Oriente Médio (Emirados Árabes Unidos)	me-central-1	Não
América do Sul (São Paulo)	sa-east-1	Sim
AWS GovCloud (Leste dos EUA)	us-gov-east-1	Não
AWS GovCloud (Oeste dos EUA)	us-gov-west-1	Não

Organização dos seus dados no Capacity Manager

O Capacity Manager usa uma combinação de métricas, pontos de dados, dimensões, intervalos de datas e períodos para organizar seus dados de capacidade. Isso pode ajudar você a analisar padrões de uso e a tomar decisões informadas sobre seus recursos.

Métricas e pontos de dados

Uma métrica representa um conjunto de pontos de dados ordenados por tempo. Por exemplo, se você quiser monitorar seu uso de spot em vCPUs, você usa a métrica `SpotTotalUsageHrsVcpu`.

A cada hora, a métrica gera um ponto de dados com registro de data e hora com o uso do spot em horas de vCPU. Por exemplo, se você usou 100 vCPUs às 10h, o Capacity Manager cria um ponto de dados com um timestamp às 10h e um valor de 100.

Para obter a lista completa de métricas que o Capacity Manager analisa, consulte Métricas do EC2 Capacity Manager.

Dimensões

As dimensões são pares de nome e valor que ajudam você a categorizar e identificar diferentes aspectos de uma métrica. Por exemplo, o nome de uma dimensão no Capacity Manager é AccountID, em que o valor é o ID real da conta. O Capacity Manager fornece dimensões para segmentar e agrupar seus dados, como família de instâncias, ARN da reserva, tipo de reserva e locação.

Para ver a lista completa de dimensões, consulte Métricas do EC2 Capacity Manager.

Intervalo de datas e período

O intervalo de datas especifica quanto tempo você deseja analisar, de uma hora a 90 dias. O período determina como o Capacity Manager agrega seus dados ao longo do tempo e quantos pontos de dados devem ser retornados. Por exemplo, se seu intervalo de datas for de uma semana e seu período for de 1 dia, o Capacity Manager retornará 7 pontos de dados. Cada ponto de dados representa um dia de dados agregados. O período deve ter um intervalo de uma hora e ser dividido uniformemente no intervalo de datas.

Tópicos

- Métricas do EC2 Capacity Manager
- Agrupamento e filtragem de dados

Métricas do EC2 Capacity Manager

O Capacity Manager oferece uma seleção abrangente de métricas para monitorar sua capacidade em diferentes tipos de recursos. As métricas podem ser medidas usando unidades diferentes, dependendo de suas necessidades de análise.

Os nomes das métricas no Capacity Manager usam quatro prefixos diferentes para categorizar o tipo de capacidade que está sendo medida:

- `Reservation`: as próprias reservas de capacidade, incluindo a capacidade reservada total, as taxas de utilização, a capacidade não utilizada e as contagens de reservas.
- `Reserved`: o uso de instâncias sob demanda coberto por suas reservas de capacidade.

- `Unreserved`: o uso de instâncias sob demanda que ocorre fora de quaisquer reservas de capacidade.
- `Spot`: especificamente para uso de instâncias spot, incluindo o tempo de execução e custos estimados. Essas métricas são separadas da capacidade baseada em reservas.

A tabela a seguir também fornece as dimensões disponíveis para cada métrica. As categorias de dimensões são divididas da forma a seguir:

- Dimensões gerais da capacidade: ID da conta, região, família de instâncias, zona de disponibilidade, tipo de instância, plataforma e locação
- Dimensões da reserva de capacidade: ID da reserva (ID da reserva de capacidade), ARN da reserva, proprietário financeiro não utilizado, tipo de reserva (ODCR/bloco de capacidade), timestamp de criação, timestamp de início, timestamp de término, estado e critérios de correspondência de instância.
- Dimensões de uso reservado: ID da reserva (CRID), ARN da reserva, tipo de reserva

Métrica	Descrição	Dimensões disponíveis	Unidades disponíveis
`ReservationAvgCommittedSize`	A quantidade média total de capacidade em um estado ativo ou programado com um compromisso. O tamanho é somado em todas as dimensões e calculado em média ao longo do tempo.	Capacidade geral e dimensões de reserva de capacidade	vCPU, instância
`ReservationAvgFutureSize`	A quantidade média de reservas de capacidade que estão programadas para serem iniciadas no futuro, mas que ainda não se tornaram ativas durante o período selecionado. O tamanho é somado em todas	Capacidade geral e dimensões de reserva de capacidade	vCPU, instância

Métrica	Descrição	Dimensões disponíveis	Unidades disponíveis
	as dimensões e calculado em média ao longo do tempo.		
`ReservationAvgUtilization`	O percentual médio da sua capacidade reservada que foi usada durante o período selecionado.	Capacidade geral e dimensões de reserva de capacidade	vCPU, instância
`ReservationMaxCommittedSize`	A capacidade total máxima em um estado ativo ou programado com um compromisso. O tamanho é somado entre as dimensões e o valor máximo é considerado para o período.	Capacidade geral e dimensões de reserva de capacidade	vCPU, instância
`ReservationMaxFutureSize`	A quantidade máxima de reservas de capacidade que estão programadas para serem iniciadas no futuro, mas que ainda não se tornaram ativas durante o período selecionado. O tamanho é somado entre as dimensões e o valor máximo é considerado para o período.	Capacidade geral e dimensões de reserva de capacidade	vCPU, instância
`ReservationMaxSize`	O tamanho máximo que sua reserva de capacidade atingiu em qualquer momento durante o período selecionado. É necessário um ID de reserva.	Capacidade geral e dimensões de reserva de capacidade	vCPU, instância

Métrica	Descrição	Dimensões disponíveis	Unidades disponíveis
`ReservationMaxUnusedSize`	A quantidade máxima de capacidade não utilizada em sua Reserva de Capacidade em qualquer momento durante o período selecionado. É necessário um ID de reserva.	Capacidade geral e dimensões de reserva de capacidade	vCPU, instância
`ReservationMaxUtilization`	O percentual máximo de utilização que sua Reserva de Capacidade alcançou em qualquer momento durante o período selecionado. É necessário um ID de reserva.	Capacidade geral e dimensões de reserva de capacidade	
`ReservationMinCommittedSize`	A quantidade mínima total de capacidade em um estado ativo ou programado com um compromisso. O tamanho é somado entre as dimensões e o valor mínimo é considerado para o período.	Capacidade geral e dimensões de reserva de capacidade	vCPU, instância
`ReservationMinFutureSize`	A quantidade mínima de reservas de capacidade que estão programadas para serem iniciadas no futuro, mas que ainda não se tornaram ativas a qualquer momento durante o período selecionado. O tamanho é somado entre as dimensões e o valor mínimo é considerado para o período.	Capacidade geral e dimensões de reserva de capacidade	vCPU, instância

Métrica	Descrição	Dimensões disponíveis	Unidades disponíveis
ReservationMinSize	O tamanho mínimo que sua reserva de capacidade atingiu em qualquer momento durante o período selecionado. É necessário um ID de reserva.	Capacidade geral e dimensões de reserva de capacidade	vCPU, instância
ReservationMinUnusedSize	A quantidade mínima de capacidade não utilizada em sua Reserva de Capacidade em qualquer momento durante o período selecionado. É necessário um ID de reserva.	Capacidade geral e dimensões de reserva de capacidade	vCPU, instância
ReservationMinUtilization	O percentual mínimo de utilização que sua Reserva de Capacidade alcançou em qualquer momento durante o período selecionado. É necessário um ID de reserva.	Capacidade geral e dimensões de reserva de capacidade	
ReservationTotalCapacityHrs	Quantidade total de capacidade que você reservou por meio de reservas de capacidade durante o período selecionado.	Capacidade geral e dimensões de reserva de capacidade	vCPU, instância
ReservationTotalCount	O número total de diferentes reservas de capacidade que você teve durante o período selecionado.	Capacidade geral e dimensões de reserva de capacidade	

Métrica	Descrição	Dimensões disponíveis	Unidades disponíveis
`ReservationTotalEstimatedCost`	Custo estimado do total de horas de capacidade reservadas durante o período selecionado.	Capacidade geral e dimensões de reserva de capacidade	
`ReservationUnusedTotalCapacityHrs`	Quantidade total de capacidade reservada que você tinha, mas não usou, durante o período selecionado.	Capacidade geral e dimensões de reserva de capacidade	vCPU, instância
`ReservationUnusedTotalEstimatedCost`	Custo estimado da capacidade reservada que você tinha, mas não usou, durante o período selecionado (calculado usando tarifas sob demanda).	Capacidade geral e dimensões de reserva de capacidade	
`ReservedTotalEstimatedCost`	Custo estimado do uso da instância sob demanda que foi coberto por uma reserva de capacidade durante o período selecionado. Isso exclui o uso de spot.	Capacidade geral e dimensões de uso reservado	
`ReservedTotalUsageHrs`	Total de horas de uso da instância sob demanda que foram cobertas por uma reserva de capacidade durante o período selecionado. Isso exclui o uso de spot.	Capacidade geral e dimensões de uso reservado	vCPU, instância

Métrica	Descrição	Dimensões disponíveis	Unidades disponíveis
SpotAvgRunTimeBeforeInterruption	Runtime médio, em horas, para instâncias interrompidas no período selecionado.	Somente dimensões de região, AZ e ID da conta	Instância
SpotInterruptionRate	Porcentagem de instâncias spot em execução que foram interrompidas no período selecionado.	Somente dimensões de região, AZ e ID da conta	vCPU, instância
SpotMaxRunTimeBeforeInterruption	Runtime máximo, em horas, para instâncias interrompidas no período selecionado.	Somente dimensões de região, AZ e ID da conta	Instância
SpotMinRunTimeBeforeInterruption	Runtime mínimo, em horas, para instâncias interrompidas no período selecionado.	Somente dimensões de região, AZ e ID da conta	Instância
SpotTotalCount	Número de instâncias spot ou vCPUs que foram executadas durante o período selecionado.	Somente dimensões de região, AZ e ID da conta	vCPU, instância
SpotTotalEstimatedCost	Custo estimado do uso da instância spot durante o período selecionado (calculado usando taxas spot publicadas).	Dimensões gerais da capacidade	
SpotTotalInterruptions	Número de instâncias spot ou vCPUs interrompidas durante o período selecionado.	Somente dimensões de região, AZ e ID da conta	vCPU, instância

Métrica	Descrição	Dimensões disponíveis	Unidades disponíveis
`SpotTotalUsageHrs`	Total de horas de uso da instância spot durante o período selecionado.	Dimensões gerais da capacidade	vCPU, instância
`UnreservedTotalEstimatedCost`	Custo estimado do uso da instância sob demanda que não foi coberto por uma reserva de capacidade durante o período selecionado. Isso exclui o uso de spot.	Dimensões gerais da capacidade	
`UnreservedTotalUsageHrs`	Total de horas de uso da instância sob demanda que não foram cobertas por uma reserva de capacidade durante o período selecionado. Isso exclui o uso de spot.	Dimensões gerais da capacidade	vCPU, instância

> **Note**
>
> Se você incluir instâncias em suas unidades, recomendamos incluir o tipo de instância em suas dimensões.

Agrupamento e filtragem de dados

O Capacity Manager agrega suas métricas com base nas dimensões e no período de datas que você escolher. Se nenhuma dimensão for escolhida, o Capacity Manager agregará os dados e retornará um ponto de dados por período no intervalo de datas. É possível agrupar seus dados em agregações menores adicionando dimensões.

- Agrupamento: divide seus dados de capacidade por dimensões, como região, família de instâncias ou ID da conta. É possível agrupar suas métricas por várias dimensões para detalhar ainda mais

seus dados. Por exemplo, se você agrupar por região e zona de disponibilidade, obterá um ponto de dados para cada combinação de região e zona de disponibilidade em que você tiver utilização.

- Filtragem: mostra somente subconjuntos específicos das dimensões que você selecionou. Por exemplo, se você agrupar por família de instâncias, obterá pontos de dados para todas as famílias em que você tiver utilização. No entanto, se você também filtrar por p5, verá somente pontos de dados para a família de instâncias p5.
- Unidades métricas: exibe os resultados por unidades diferentes, como vCPUs, instâncias ou custos estimados. Por exemplo, depois de agrupar por região e filtrar por uma família de instâncias específica, é possível visualizar os dados de maneiras diferentes. Alterne entre o total de vCPUs usadas, o número de instâncias em execução ou os custos estimados.

Como agrupar e filtrar dados no console

Para agrupar e filtrar dados no Capacity Manager

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Capacity Manager.
3. Escolha a guia do tipo de recurso que você deseja analisar: Uso, Reservas ou Spot.
4. Na seção Filtro de data, escolha um intervalo de datas, fuso horário e intervalo.
5. Na seção Filtro de dimensão, escolha uma dimensão no menu suspenso Selecionar uma dimensão.
6. Selecione as dimensões pelas quais você deseja agrupar no menu suspenso. Observe que as opções de dimensão são diferentes para cada tipo de recurso. Para obter mais informações, consulte Métricas do EC2 Capacity Manager.

   É possível adicionar várias dimensões para criar agrupamentos mais granulares.
7. Para filtrar pelas dimensões selecionadas, escolha uma opção de filtro no menu suspenso Filtrar por dimensão.
8. Na seção Agregações, escolha uma unidade para visualizar seus resultados por vCPUs, instâncias ou custos estimados.

Navegando pelo Capacity Manager no console da AWS

O console do Capacity Manager é organizado em guias que fornecem visualizações diferentes dos seus dados de capacidade:

- Painel: fornece uma visão geral de alto nível de todas as reservas de capacidade sob demanda, do uso sob demanda e no local, incluindo as principais métricas e os principais alertas para ajudar a melhorar sua postura de capacidade.
- Uso: fornece uma visão geral dos padrões de uso da sua instância para instâncias sob demanda e spot. Analise a cobertura por reservas de capacidade e identifique oportunidades de otimização por meio de agrupamento e filtragem flexíveis.
- Reservas: fornece análise da utilização da reserva de capacidade, recursos de gerenciamento e métricas detalhadas de reservas em todas as contas e regiões.
- Spot: monitora os padrões de uso de spot e fornece análise de custos para instâncias spot em todas as contas e regiões.
- Exportações de dados: gerencia a configuração de exportação de dados para o Amazon S3, incluindo agendamento, formatação e seleção de modelos.
- Configurações: fornece opções de configuração de serviços, incluindo acesso à organização e configurações regionais.

Nas guias Uso e Reservas, o Capacity Manager fornece uma estrutura de navegação hierárquica que permite detalhar desde visões gerais de alto nível até informações detalhadas sobre recursos. A compreensão desse padrão de navegação ajuda você a analisar seus dados de capacidade com eficiência e identificar oportunidades de otimização.

Tópicos

- Hierarquia de navegação
- Exibição de detalhamento e detalhes de Uso e Reservas

Hierarquia de navegação

O Capacity Manager usa uma estrutura de navegação de três níveis para Uso e Reservas:

1. Página de visão geral: resumo de alto nível com métricas agregadas.
2. Página de detalhamento: análise detalhada com opções de filtragem e agrupamento
3. Páginas de detalhes:
   - Detalhes de uso: informações sobre a combinação de dimensões selecionada, que fornecem estatísticas e dados de séries temporais para ajudá-lo a entender os padrões de uso.
   - Detalhes da reserva: informações sobre uma reserva de capacidade específica, incluindo estatísticas de utilização, padrões de uso ao longo do tempo e detalhes de configuração.

> **Note**
>
> O spot segue uma estrutura simplificada com apenas a página de visão geral.

Exibição de detalhamento e detalhes de Uso e Reservas

As guias Uso e Reservas seguem a mesma estrutura de navegação de três níveis, permitindo que você avance da visão geral às páginas de detalhamento e detalhes. Os processos para acessar as páginas de detalhamento e detalhes são semelhantes, com apenas pequenas diferenças na localização dos links de navegação em cada guia.

Para acessar as páginas de detalhamento dos recursos

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Capacity Manager.
3. Escolha a guia do tipo de recurso que você deseja analisar: Uso ou Reservas.
4. Na seção Agregações, localize o link de detalhamento:
   - Uso: na coluna Ações, escolha Exibir detalhamento.

     > **Note**
     >
     > Dependendo do tamanho da tela ou do número de dimensões aplicadas, talvez seja necessário rolar horizontalmente pela página para encontrar o link Exibir detalhamento.

   - Reservas: na coluna Reservas, escolha o número (o número é um link) da reserva que você deseja exibir.

Para acessar as páginas de detalhes

1. Na página de detalhamento, navegue até a seção relevante:
   - Uso: a seção Combinações de dimensões exclusivas.
   - Reservas: a seção Reservas.
2. Na seção relevante dos recursos escolhidos, acesse a página de detalhes.

- Uso: na coluna Ações, escolha Exibir detalhes.

> **Note**
>
> Dependendo do tamanho da tela ou do número de dimensões aplicadas, talvez seja necessário rolar horizontalmente pela página para encontrar o link Exibir detalhes.

- Reservas: na coluna ID da reserva, escolha a reserva que você deseja exibir.

Exportação dos seus dados do Capacity Manager

É possível exportar dados de capacidade do EC2 Capacity Manager para o Amazon S3 para permitir análises adicionais, criar relatórios personalizados ou integrar-se a outros serviços da AWS. É possível exportar seus dados no formato CSV ou Parquet. Nas seções a seguir, você encontrará informações sobre como exportar seus dados do Capacity Manager.

> **Note**
>
> O Capacity Manager permite apenas uma exportação de dados por Conta da AWS.

Tópicos

- Configuração de um bucket do Amazon S3 para exportações de dados
- Criação de uma exportação de dados para seus dados do Capacity Manager

Configuração de um bucket do Amazon S3 para exportações de dados

Para receber exportações de dados do Capacity Manager, você precisa ter um bucket do Amazon S3 em sua Conta da AWS para receber e armazenar seus arquivos de exportação. Ao criar uma exportação de dados no console do Capacity Manager, é possível selecionar um bucket do Amazon S3 existente que você possui ou criar um novo bucket.

Em ambos os casos, é necessário aplicar a política de bucket necessária para permitir que o Capacity Manager forneça arquivos de exportação. Editar essa política no console do Amazon S3 ou alterar o proprietário do bucket depois de criar uma exportação de dados impedirá que o Capacity Manager entregue suas exportações.

Para criar um bucket do Amazon S3, consulte Criação de um bucket do S3 no Guia do usuário do Amazon Simple Storage Service.

A política a seguir deve ser aplicada ao seu bucket do S3 para permitir que o Capacity Manager forneça exportações de dados:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "ec2.capacitymanager.amazonaws.com"
            },
            "Action": [
                "s3:PutObject",
                "s3:GetObject",
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket",
                "arn:aws:s3:::amzn-s3-demo-bucket/*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "111122223333"
                },
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:ec2:us-east-1:111122223333:capacity-
manager-data-export/*"
                }
            }
        }
    ]
}
```

Essa política de bucket ajuda a garantir que os arquivos de exportação de dados do Capacity Manager possam ser entregues com segurança ao seu bucket. Especificamente:

- Sempre que uma exportação de dados do Capacity Manager é entregue, a AWS primeiro confirma se o bucket ainda pertence à conta que configurou a exportação. Se a propriedade do bucket tiver

sido alterada, a exportação não será entregue. Isso ajuda a garantir a segurança dos dados do Capacity Manager. Essa política de bucket permite que a AWS (`"Effect": "Allow"`) verifique qual conta é proprietária do bucket (`"Action": ["s3:ListBucket"]`).

- A política concede ao serviço do Capacity Manager (`"Service": "ec2.capacitymanager.amazonaws.com"`) permissão para gravar arquivos de exportação (`"Action": "s3:PutObject"`) e ler objetos (`"Action": "s3:GetObject"`) para copiar dados para seu bucket.

Criação de uma exportação de dados para seus dados do Capacity Manager

Para criar uma exportação de dados, é possível usar a página Exportações de dados no console do Capacity Manager ou a AWS CLI.

Pré-requisitos

É necessário criar um bucket do Amazon Simple Storage Service (Amazon S3). Certifique-se dos pontos a seguir:

- O bucket do S3 deve estar na mesma Região da AWS em que você habilitou o Capacity Manager.
- Seu bucket do S3 deve ter a política de permissões necessária para que o serviço Capacity Manager entregue arquivos.

Para obter mais informações, consulte Configuração de um bucket do Amazon S3 para exportações de dados.

Procedimento

É possível exportar seus dados do Capacity Manager usando o Console da AWS ou a AWS CLI.

Console

Para criar uma exportação de dados

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Capacity Manager.
3. Escolha a guia Exportações de dados.
4. Escolha Criar exportação de dados.

5. Configure suas propriedades de exportação, local de entrega e etiquetas (opcional).
6. Escolha Criar.

AWS CLI

Para criar uma exportação de dados

Use o comando a seguir para criar uma exportação de dados com a configuração especificada:

```
aws ec2 create-capacity-manager-data-export \
    --s3-bucket-name my-exports-bucket \
    --s3-bucket-prefix capacity-data-exports \
    --schedule hourly \
    --output-format parquet/CSV \
    --tag-specifications 'ResourceType=capacity-manager-data-
export,Tags=[{Key=environment,Value=production}]'
```

Gerenciar drivers de dispositivo para a instância do Amazon EC2

Drivers de dispositivo são componentes de software que se comunicam com o hardware virtualizado da instância do Amazon EC2. Para evitar erros no sistema, problemas de desempenho e outros comportamentos inesperados, é importante manter os drivers atualizados. Isso é especialmente verdadeiro para drivers que podem ter um forte impacto no desempenho do sistema, dependendo do uso, como drivers de dispositivos de rede, gráficos e armazenamento. As novas versões de drivers podem incluir correções de defeitos ou introduzir funcionalidades expandidas que talvez você queira aproveitar para instâncias que estão em execução no momento.

Drivers de rede

As distribuições do Linux podem incorporar recursos de rede, como Adaptador de Rede Elástica (ENA) ou Elastic Fabric Adapter (EFA) no kernel. No entanto, o tempo pode variar para a implementação dos recursos do driver do kernel nas diferentes distribuições.

Os drivers de kernel ENA e EFA do Linux estão disponíveis no repositório de drivers da Amazon no GitHub. Para obter mais informações e links para os drivers disponíveis, consulte Drivers da Amazon no GitHub.

Para obter mais informações sobre drivers do ENA, consulte Habilitar redes aperfeiçoadas com o ENA em instâncias do EC2. Para obter mais informações sobre drivers do EFA, consulte os tópicos de Conceitos básicos na seção Elastic Fabric Adapter para workloads de IA/ML e HPC no Amazon EC2 deste guia.

Para instalar ou atualizar drivers de rede em instâncias do Windows, consulte os seguintes tópicos:

- Instalar o driver do ENA no Windows
- Instalar os drivers AWS PV mais recentes

  Para obter mais informações, consulte Drivers paravirtuais para as instâncias do Windows.

> **Note**
>
> O EFA não é compatível com as instâncias do Windows.

Drivers de gráficos

Para instalar ou atualizar drivers de gráficos, consulte os seguintes tópicos:

- Drivers AMD para a instância do EC2
- Drivers NVIDIA para a instância do Amazon EC2

Drivers de dispositivo de armazenamento

Para instalar ou atualizar drivers de armazenamento, consulte os seguintes tópicos:

- Para instâncias do Linux, consulte Instalar ou atualizar o driver NVMe no Guia do usuário do Amazon EBS.
- Para instâncias do Windows, consulte AWSDrivers NVMe.

Drivers AMD para a instância do EC2

Uma instância com uma GPU AMD conectada, como uma instância G4ad, deve ter o driver AMD apropriado instalado. Dependendo de suas necessidades, você pode usar uma AMI com o driver pré-instalado ou baixar um driver de Amazon S3.

Para instalar drivers NVIDIA em uma instância com uma GPU NVIDIA conectada, como uma instância G4dn, consulte Drivers NVIDIA.

Sumário

- Software AMD Radeon Pro para driver empresarial
- AMIs com o driver AMD instalado
- Download do driver AMD

Software AMD Radeon Pro para driver empresarial

O driver AMD Radeon Pro Software for Enterprise foi criado para oferecer suporte a casos de uso de gráficos de nível profissional. Usando o driver, é possível configurar suas instâncias com dois monitores 4K por GPU.

APIs compatíveis

- OpenGL, OpenCL
- Vulkan
- Framework de mídia avançada da AMD
- API de aceleração de vídeo
- DirectX 9 e posterior
- Transformação do Microsoft Hardware Media Foundation

AMIs com o driver AMD instalado

A AWS oferece diferentes imagens de máquina da Amazon (AMIs) com os drivers AMD instalados. AbraOfertas do Open Marketplace com o driver AMD.

Download do driver AMD

Se você não estiver usando uma AMI com o driver AMD instalado, é possível fazer download do driver AMD e instalá-lo em sua instância. Somente as seguintes versões de sistema operacional são compatíveis com drivers da AMD:

- Amazon Linux 2 com kernel versão 5.4
- Ubuntu 20.04

- Ubuntu 22.04
- Ubuntu 24.04
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022

Esses downloads estão disponíveis somente para clientes da AWS. Ao fazer download, você concorda que usará o software submetido a download somente para desenvolver AMIs para uso com o hardware AMD Radeon Pro V520. Após a instalação do software, estará firmado seu vínculo nos termos do AMD End User License Agreement.

Instalação do driver da AMD em sua instância Linux do Amazon Linux 2

1. Conecte-se à sua instância do Linux.
2. Instale a AWS CLI em sua instância do Linux e configure credenciais padrão. Para obter mais informações, consulte Instalar a AWS CLI no Guia do usuário da AWS Command Line Interface.

   > **Important**
   >
   > Os usuários ou perfis devem ter as permissões concedidas pela política AmazonS3ReadOnlyAccess. Para obter mais informações, consulte Políticas gerenciadas da AWS: AmazonS3ReadOnlyAccess no Guia do usuário do Amazon Simple Storage Service.

3. Instalar o kernel 5.4

   ```
   $ sudo amazon-linux-extras disable kernel-5.10
   $ sudo amazon-linux-extras enable kernel-5.4
   $ sudo yum install -y kernel
   ```

4. Instale gcc e make, caso ainda não tenham sido instalados.

   ```
   $ sudo yum install gcc make
   ```

5. Atualize o cache de pacotes e obtenha as atualizações de pacotes para sua instância.

   ```
   $ sudo amazon-linux-extras install epel -y
   $ sudo yum update -y
   ```

6. Reinicialize a instância.

```
$ sudo reboot
```

7. Reconecte-se à instância depois que ela for reinicializada.
8. Faça download do driver AMD mais recente.

```
$ aws s3 cp --recursive s3://ec2-amd-linux-drivers/latest/ .
```

9. Extraia o arquivo.

```
$ tar -xf amdgpu-pro-*rhel*.tar.xz
```

10. Mude para a pasta do driver extraído.
11. Execute o script de instalação automática para instalar a pilha completa de gráficos.

```
$ ./amdgpu-pro-install -y --opencl=pal,legacy
```

12. Reinicialize a instância.

```
$ sudo reboot
```

13. Verifique se o driver está funcionando.

```
$ sudo dmesg | grep amdgpu
```

A resposta deve ser parecida com o seguinte:

```
Initialized amdgpu
```

Instalar o driver da AMD em instância Linux Ubuntu

1. Conecte-se à sua instância do Linux.
2. Atualize o cache de pacotes e obtenha as atualizações de pacotes para sua instância.

```
$ sudo apt-get update --fix-missing && sudo apt-get upgrade -y
```

3. Instale gcc e make, caso ainda não tenham sido instalados.

```
$ sudo apt install build-essential -y
```

4. Instalar o firmware e os módulos do kernel Linux

```
$ sudo apt install linux-firmware linux-modules-extra-aws -y
```

5. Reinicializar instância

```
$ sudo reboot
```

6. Reconecte-se à instância depois que ela for reinicializada.
7. Instalar o pacote de drivers AMD Linux
   - Para Ubuntu 20.04:

```
$ wget https://repo.radeon.com/.preview/afe3e25b8f1beff0bb312e27924d63b5/amdgpu-install/5.4.02.01/ubuntu/focal/amdgpu-install_5.4.02.01.50402-1_all.deb
$ sudo dpkg --add-architecture i386
$ sudo apt install ./amdgpu-install_5.4.02.01.50402-1_all.deb
```

   - Para obter as versões posteriores do Ubuntu, visite Linux® Drivers for AMD Radeon™ Graphics e baixe e instale o pacote do Ubuntu mais recente.

```
$ sudo apt install ./amdgpu-install_{version-you-downloaded}.deb
```

8. Execute o script de instalação automática para instalar a pilha completa de gráficos.

```
$ amdgpu-install --usecase=workstation --vulkan=pro -y
```

9. Reinicialize a instância.

```
$ sudo reboot
```

10. Verifique se o driver está funcionando.

```
$ sudo dmesg | grep amdgpu
```

A resposta deve ser parecida com o seguinte:

```
Initialized amdgpu
```

Instalação do driver da AMD na instância do Windows

1. Conecte-se à instância do Windows e abra uma janela do PowerShell.
2. Configure as credenciais padrão para o AWS Tools for Windows PowerShell em sua instância do Windows. Para obter mais informações, consulte Conceitos básicos do AWS Tools for Windows PowerShell no Guia do usuário do AWS Tools for PowerShell.

   > **Important**
   >
   > Os usuários ou perfis devem ter as permissões concedidas pela política AmazonS3ReadOnlyAccess. Para obter mais informações, consulte Políticas gerenciadas da AWS: AmazonS3ReadOnlyAccess no Guia do usuário do Amazon Simple Storage Service.

3. Defina o prefixo da chave de acordo com sua versão do Windows:

   - Windows 10 e Windows 11

     ```
     $KeyPrefix = "latest/AMD_GPU_WINDOWS10"
     ```

   - Windows Server 2016

     ```
     $KeyPrefix = "archives"
     ```

   - Windows Server 2019

     ```
     $KeyPrefix = "latest/AMD_GPU_WINDOWS_2K19" # use "archives" for Windows Server
      2016
     ```

   - Windows Server 2022

     ```
     $KeyPrefix = "latest/AMD_GPU_WINDOWS_2K22"
     ```

4. Faça download dos drivers de Amazon S3 para seu desktop usando os seguintes comandos do PowerShell.

```
$Bucket = "ec2-amd-windows-drivers"
$LocalPath = "$home\Desktop\AMD"
$Objects = Get-S3Object -BucketName $Bucket -KeyPrefix $KeyPrefix -Region us-east-1
foreach ($Object in $Objects) {
$LocalFileName = $Object.Key
if ($LocalFileName -ne '' -and $Object.Size -ne 0) {
    $LocalFilePath = Join-Path $LocalPath $LocalFileName
    Copy-S3Object -BucketName $Bucket -Key $Object.Key -LocalFile $LocalFilePath -
Region us-east-1
    }
}
```

5. Descompacte o arquivo de driver obtido por download e execute o instalador usando os comandos do PowerShell a seguir.

```
Expand-Archive $LocalFilePath -DestinationPath "$home\Desktop\AMD\$KeyPrefix" -
Verbose
```

Agora, verifique o conteúdo do novo diretório. O nome do diretório pode ser recuperado usando o comando `Get-ChildItem` do PowerShell.

```
Get-ChildItem "$home\Desktop\AMD\$KeyPrefix"
```

A saída deve ser semelhante ao seguinte:

```
Directory: C:\Users\Administrator\Desktop\AMD\latest

Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----       10/13/2021  12:52 AM                210414a-365562C-Retail_End_User.2
```

Instalar os drivers:

```
pnputil /add-driver $home\Desktop\AMD\$KeyPrefix\*.inf /install /subdirs
```

6. Siga as instruções para instalar o driver e reinicialize sua instância, conforme necessário.
7. Para verificar se a GPU está funcionando corretamente, verifique o gerenciador de dispositivos. É necessário ver “AMD Radeon Pro V520 MxGPU” listado como um adaptador de exibição.

8. Para ajudar a beneficiar-se dos quatro monitores com resolução de até 4K, configure o protocolo de exibição de alta performance, Amazon DCV.

Drivers NVIDIA para a instância do Amazon EC2

Uma instância com uma GPU NVIDIA anexada, como tipos de instância da série P- ou G-, deve ter o driver NVIDIA apropriado instalado. Dependendo do tipo de instância, é possível baixar um driver NVIDIA público, um driver do Amazon S3 disponível somente para clientes da AWS ou usar uma AMI da AWS com o driver pré-instalado.

Para instalar drivers AMD em uma instância com uma GPU AMD conectada, como uma instância G4ad, consulte Drivers AMD.

Tópicos

- Tipos de drivers NVIDIA
- Drivers disponíveis por tipo de instância
- Opções de instalação
- Uso de AMIs que incluem drivers da NVIDIA
- Instalação de drivers públicos da NVIDIA
- Instalação dos drivers da NVIDIA GRID (instâncias G7e, G6, Gr6, G6e, G6f, Gr6f, G5, G4dn e G3)
- Instalação dos drivers para jogos da NVIDIA (instâncias G7e, G6, G6e, G5 e G4dn)

Tipos de drivers NVIDIA

A seguir estão os principais tipos de drivers NVIDIA que podem ser usados com as instâncias baseadas em GPU.

Drivers Tesla

Esses drivers são destinados principalmente a workloads de computação, que usam GPUs para tarefas computacionais, como cálculos de ponto flutuante paralelizados para machine learning e transformações rápidas de Fourier para aplicações de computação de alta performance.

Drivers GRID

Esses drivers são certificados para oferecer a melhor performance para aplicações de visualização profissional que renderizam conteúdo, como modelos 3D ou vídeos de alta resolução. É possível configurar os drivers GRID para oferecer suporte a dois modos. As

estações de trabalho virtuais Quadro fornecem acesso a quatro monitores de 4K por GPU. Os GRID vApps oferecem recursos de hospedagem de aplicações RDSH.

Drivers para jogos

Esses drivers contêm otimizações para jogos e são atualizados frequentemente para oferecer melhorias de performance. Eles são compatíveis com um único monitor 4K por GPU.

Modo configurado

No Windows, os drivers Tesla são configurados para serem executados no modo Tesla Compute Cluster (TCC). O driver GRID e o driver para jogos são configurados para executar no modo Windows Display Driver Model (WDDM). No modo TCC, a placa é dedicada a workloads de computação. No modo WDDM, a placa é compatível com workloads de computação e gráficos.

Painel de controle NVIDIA

O painel de controle NVIDIA é compatível com drivers GRID e para jogos. Ele não é compatível com drivers Tesla.

APIs com suporte para drivers Tesla, GRID e para jogos

- OpenCL, OpenGL e Vulkan
- NVIDIA CUDA e bibliotecas relacionadas (por exemplo, cuDNN, TensorRT, nvJPEG e cuBLAS)
- NVENC para codificação de vídeo e NVDEC para decodificação de vídeo
- APIs somente para Windows: DirectX, Direct2D, DirectX Video Acceleration e DirectX Raytracing

Drivers disponíveis por tipo de instância

A tabela a seguir resume os drivers NVIDIA para cada tipo de instância de GPU.

Tipo de instância	Driver Tesla	Driver GRID	Driver para jogos
G3	Sim	Sim	Não
G4dn	Sim	Sim	Sim
G5	Sim	Sim	Sim
G5g	Sim [1]	Não	Não

Tipo de instância	Driver Tesla	Driver GRID	Driver para jogos
G6	Sim	Sim	Sim
G6e	Sim	Sim	Sim
G6f	Não	Sim	Não
Gr6	Sim	Sim	Não
Gr6f	Não	Sim	Não
G7e	Sim	Sim	Sim
P2	Sim	Não	Não
P3	Sim	Não	Não
P4d	Sim	Não	Não
P4de	Sim	Não	Não
P5	Sim	Não	Não
P5e	Sim	Não	Não
P5en	Sim	Não	Não
P6-B200	Sim	Não	Não
P6e-GB200	Sim	Não	Não
P6-B300	Sim	Não	Não

[1] Esse driver da Tesla também oferece suporte a aplicações gráficas otimizadas, específicas da plataforma ARM64

Opções de instalação

Use uma das opções a seguir para obter os drivers NVIDIA necessários para a instância de GPU.

Opções

1. Uso de AMIs que incluem drivers da NVIDIA
2. Instalação de drivers públicos da NVIDIA
3. Instalação dos drivers da NVIDIA GRID (instâncias G7e, G6, Gr6, G6e, G6f, Gr6f, G5, G4dn e G3)
4. Instalação dos drivers para jogos da NVIDIA (instâncias G7e, G6, G6e, G5 e G4dn)

Uso de AMIs que incluem drivers da NVIDIA

A AWS e a NVIDIA oferecem imagens de máquina da Amazon (AMIs) diferentes com drivers NVIDIA instalados.

- Ofertas do Marketplace com o driver público da Tesla
- Ofertas do Marketplace com o driver GRID
- Ofertas do Marketplace com o driver para jogos

Para analisar as considerações que dependem da plataforma do seu sistema operacional (SO), escolha a guia que se aplica à sua AMI.

Linux

Para atualizar a versão do driver instalada usando uma dessas AMIs, será necessário desinstalar os pacotes do NVIDIA da instância para evitar conflitos de versão. Use este comando para desinstalar os pacotes do NVIDIA:

```
[ec2-user ~]$ sudo yum erase nvidia cuda
```

O pacote do toolkit CUDA tem dependências nos drivers NVIDIA A desinstalação dos pacotes NVIDIA apaga o toolkit CUDA. É necessário reinstalar o toolkit CUDA depois de instalar o driver NVIDIA.

Windows

Se você criar uma AMI do Windows personalizada usando uma das ofertas do AWS Marketplace, a AMI deverá ser uma imagem padronizada criada com a ferramenta Sysprep do Windows para garantir que o driver do GRID funcione. Para obter mais informações, consulte Criar uma AMI do Amazon EC2 usando o Sysprep do Windows.

Instalação de drivers públicos da NVIDIA

Se as AMIs do AWS Marketplace descritas em Uso de AMIs que incluem drivers da NVIDIA não se adequarem ao seu caso de uso, você pode instalar os drivers públicos e trazer sua própria licença. As opções de instalação são as seguintes:

- Opção 1: instalação apenas do driver
- Opção 2: instalação com o kit de ferramentas para CUDA (recomendada para distribuições Linux)

Considerações sobre o tipo de instância P6-B200 e P6-B300

As plataformas P6-B200 e P6-B300 são únicas porque expõem as placas de interface de rede (NICs) Mellanox ConnectX à instância como dispositivos PCIe. Essas NICs não atuam como interfaces de rede típicas, mas funcionam como pontes NVSwitch, fornecendo um caminho de controle para inicializar e configurar o NVFabric, que é a topologia NVLink da interconexão da GPU.

Para inicializar totalmente o sistema, o NVIDIA Fabric Manager deve configurar o `NVFabric` e estabelecer a topologia NVSwitch. Isso permite que os módulos do kernel InfiniBand se comuniquem com as NICs Mellanox ConnectX.

O NVIDIA Fabric Manager está incluso no kit de ferramentas CUDA. Recomendamos Opção 2: instalação com o kit de ferramentas para CUDA para este tipo de instância.

Opção 1: instalação apenas do driver

Para instalar um driver específico, acesse sua instância e faça o download do driver público da NVIDIA de 64 bits correspondente ao tipo de instância em http://www.nvidia.com/Download/Find.aspx. Para Tipo de produto, Série do produto e Produto, selecione as opções apresentadas na tabela a seguir.

Em seguida, siga as instruções de instalação do repositório local no NVIDIA Driver Installation Guide.

> **Note**
>
> Os tipos de instância P6-B200 e P6-B300 exigem a instalação e a configuração de pacotes adicionais incluídos no NVIDIA CUDA Toolkit. Para obter mais informações, consulte as instruções específicas para sua distribuição Linux em Opção 2: instalação com o kit de ferramentas para CUDA.

Instância	Tipo de produto	Séries de produtos	Produto	Versão mínima do driver
G3	Tesla	M-Class	M60	--
G4dn	Tesla	Série T	T4	--
G5	Tesla	A-Series	A10	470.00 ou posterior
G5g[1]	Tesla	Série T	T4G	470.82.01 ou posterior
G6	Tesla	L-Series	L4	525.0 ou posterior
G6e	Tesla	L-Series	L40S	535.0 ou posterior
Gr6	Tesla	L-Series	L4	525.0 ou posterior
G7e	Tesla	Série RTX	RTX PRO 6000 Blackwell	575.0 ou posterior
P2	Tesla	K-Series	K80	--
P3	Tesla	V-Series	V100	--
P4d	Tesla	A-Series	A100	--
P4de	Tesla	A-Series	A100	--
P5	Tesla	H-Series	H100	530 ou posterior
P5e	Tesla	H-Series	H200	550 ou posterior
P5en	Tesla	H-Series	H200	550 ou posterior
P6-B200[2]	Tesla	HGX-Series	B200	570 ou posterior

Instância	Tipo de produto	Séries de produtos	Produto	Versão mínima do driver
P6e-GB200	Tesla	HGX-Series	B200	570 ou posterior
P6-B300[2]	Tesla	HGX-Series	B300	580 ou posterior

[1] O sistema operacional para instâncias G5g é Linux aarch64.

[2] Para os tipos de instância P6-B200 e P6-B300, há requisitos adicionais de instalação para configurar o NVIDIA Fabric Manager.

Opção 2: instalação com o kit de ferramentas para CUDA

As instruções de instalação podem diferir um pouco dependendo do sistema operacional. Para instalar drivers públicos na sua instância usando o kit de ferramentas da NVIDIA CUDA, siga as instruções correspondentes ao sistema operacional da instância. Se o sistema operacional da sua instância não estiver listado, siga as instruções correspondentes ao sistema operacional e à arquitetura do tipo de instância no site do NVIDIA Developer. Para obter mais informações, consulte CUDA Toolkit Downloads.

Para obter informações sobre a arquitetura do tipo de instância ou outras especificações, consulte as especificações de computação acelerada na referência de Tipos de instâncias do Amazon EC2.

Amazon Linux 2023

Esta seção aborda a instalação do kit de ferramentas da NVIDIA CUDA em uma instância do Amazon Linux 2023. Os exemplos de comandos apresentados nesta seção são baseados na arquitetura `x86_64`.

Para obter os comandos `arm64-sbsa`, consulte CUDA Toolkit Downloads e selecione as opções que se aplicam à sua distribuição. As instruções serão exibidas depois de você concluir a seleção final.

Pré-requisito

Antes de prosseguir com a instalação do kit de ferramentas e dos drivers, execute o comando abaixo para verificar se você tem a versão adequada dos cabeçalhos do kernel e dos pacotes de desenvolvimento.

```
[ec2-user ~]$ sudo dnf install kernel-devel-$(uname -r) kernel-headers-$(uname -r) -y
```

Download do kit de ferramentas e dos drivers

Escolha o tipo de instalação a ser usado na instância e siga as etapas correspondentes.

RPM local installation

Estas instruções permitem que você faça o download do pacote do repositório do instalador do kit de ferramentas para CUDA na sua instância, depois extraia e registre o pacote especificado.

Para acessar as instruções no site do NVIDIA Developer, consulte CUDA Toolkit Downloads.

```
[ec2-user ~]$ wget https://developer.download.nvidia.com/compute/cuda/13.0.0/
local_installers/cuda-repo-amzn2023-13-0-local-13.0.0_580.65.06-1.x86_64.rpm
[ec2-user ~]$ sudo rpm -i cuda-repo-amzn2023-13-0-
local-13.0.0_580.65.06-1.x86_64.rpm
```

RPM network installation

É possível seguir estas instruções para adicionar o repositório CUDA ao gerenciador de pacotes da sua instância. Durante a execução das etapas de instalação, o gerenciador de pacotes faz download somente dos pacotes requeridos.

Para acessar as instruções no site do NVIDIA Developer, consulte CUDA Toolkit Downloads.

```
[ec2-user ~]$ wget https://developer.download.nvidia.com/compute/cuda/
repos/ubuntu2404/x86_64/cuda-keyring_1.1-1_all.deb
[ec2-user ~]$ sudo dpkg -i cuda-keyring_1.1-1_all.deb
```

As etapas finais são idênticas tanto para instalação local quanto para instalação em rede.

1. Conclusão da instalação do kit de ferramentas para CUDA

```
[ec2-user ~]$ sudo dnf clean all
[ec2-user ~]$ sudo dnf install cuda-toolkit -y
```

2. Instalação da variante de driver com módulo de kernel aberto

```
[ec2-user ~]$ sudo dnf module install nvidia-driver:open-dkms -y
```

3. Instalação do GPUDirect Storage e do Fabric Manager

```
[ec2-user ~]$ sudo dnf install nvidia-gds -y
[ec2-user ~]$ sudo dnf install nvidia-fabric-manager -y
```

4. Habilitação do Fabric Manager e da persistência do driver

```
[ec2-user ~]$ sudo systemctl enable nvidia-fabricmanager
[ec2-user ~]$ sudo systemctl enable nvidia-persistenced
```

5. (somente P6-B200 e P6-B300) Esses tipos de instância exigem a instalação e a configuração de pacotes adicionais incluídos no NVIDIA CUDA Toolkit.

   1. Instale o NVIDIA Link Subnet Manager e `ibstat`.

      ```
      [ec2-user ~]$ sudo dnf install nvlink5
      ```

   2. Habilite o carregamento automático do módulo Infiniband na inicialização.

      ```
      [ec2-user ~]$ echo "ib_umad" | sudo tee -a /etc/modules-load.d/modules.conf
      ```

6. Reinicialize a instância.

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

Ubuntu 24.04

Esta seção aborda a instalação do kit de ferramentas da NVIDIA CUDA em uma instância do Ubuntu 24.04. Os exemplos de comandos apresentados nesta seção são baseados na arquitetura `x86_64`.

Para obter os comandos `arm64-sbsa`, consulte CUDA Toolkit Downloads e selecione as opções que se aplicam à sua distribuição. As instruções serão exibidas depois de você concluir a seleção final.

Pré-requisito

Antes de prosseguir com a instalação do kit de ferramentas e dos drivers, execute o comando abaixo para verificar se você tem a versão adequada dos cabeçalhos do kernel e dos pacotes de desenvolvimento.

```
$ apt install linux-headers-$(uname -r)
```

Download do kit de ferramentas e dos drivers

Escolha o tipo de instalação a ser usado na instância e siga as etapas correspondentes.

RPM local installation

Estas instruções permitem que você faça o download do pacote do repositório do instalador do kit de ferramentas para CUDA na sua instância, depois extraia e registre o pacote especificado.

Para acessar as instruções no site do NVIDIA Developer, consulte CUDA Toolkit Downloads.

```
$ wget https://developer.download.nvidia.com/compute/cuda/repos/ubuntu2404/
x86_64/cuda-ubuntu2404.pin
$ sudo mv cuda-ubuntu2404.pin /etc/apt/preferences.d/cuda-repository-pin-600
$ wget https://developer.download.nvidia.com/compute/cuda/13.0.0/
local_installers/cuda-repo-ubuntu2404-13-0-local_13.0.0-580.65.06-1_amd64.deb
$ sudo dpkg -i cuda-repo-ubuntu2404-13-0-local_13.0.0-580.65.06-1_amd64.deb
$ sudo cp /var/cuda-repo-ubuntu2404-13-0-local/cuda-*-keyring.gpg /usr/share/
keyrings/
```

RPM network installation

É possível seguir estas instruções para adicionar o repositório CUDA ao gerenciador de pacotes da sua instância. Durante a execução das etapas de instalação, o gerenciador de pacotes faz download somente dos pacotes requeridos.

Para acessar as instruções no site do NVIDIA Developer, consulte CUDA Toolkit Downloads.

```
$ wget https://developer.download.nvidia.com/compute/cuda/repos/ubuntu2404/x86_64/
cuda-keyring_1.1-1_all.deb
$ sudo dpkg -i cuda-keyring_1.1-1_all.deb
```

As etapas finais são idênticas tanto para instalação local quanto para instalação em rede.

1. Conclusão da instalação do kit de ferramentas para CUDA

```
$ sudo apt update
$ sudo apt install cuda-toolkit -y
```

2. Instalação da variante de driver com módulo de kernel aberto

```
$ sudo apt install nvidia-open -y
```

3. Instalação do GPUDirect Storage e do Fabric Manager

```
$ sudo apt install nvidia-gds -y
$ sudo apt install nvidia-fabricmanager -y
```

4. Habilitação do Fabric Manager e da persistência do driver

```
$ sudo systemctl enable nvidia-fabricmanager
$ sudo systemctl enable nvidia-persistenced
```

5. (somente P6-B200 and P6-B300) Esses tipos de instância exigem a instalação e a configuração de pacotes adicionais incluídos no NVIDIA CUDA Toolkit.

   1. Instale o driver mais recente específico para InfiniBand e as ferramentas de diagnóstico.

      ```
      $ sudo apt install linux-modules-extra-$(uname -r) -y
      $ sudo apt install infiniband-diags -y
      ```

   2. Instale o NVIDIA Link Subnet Manager.

      ```
      $ sudo apt install nvlsm -y
      ```

6. Reinicialize a instância.

```
sudo reboot
```

7. Atualize o caminho do sistema e inclua a variável de ambiente apresentada a seguir.

```
$ export PATH=${PATH}:/usr/local/cuda-13.0/bin
$ export LD_LIBRARY_PATH=${LD_LIBRARY_PATH}:/usr/local/cuda-13.0/lib64
```

Sistemas operacionais do Windows

Para instalar o driver da NVIDIA no Windows, siga estas etapas:

1. Abra a pasta onde você fez download do driver e execute o arquivo de instalação. Siga as instruções para instalar o driver e reinicialize sua instância, conforme necessário.

2. Desabilite o adaptador de vídeo chamado Microsoft Basic Display Adapter, que está marcado com um ícone de aviso, usando o Gerenciador de dispositivos. Instale esses recursos do Windows: Media Foundation e Quality Windows Audio Video Experience.

   > **Important**
   >
   > Não desabilite o adaptador de vídeo chamado Microsoft Remote Display Adapter. Se o Microsoft Remote Display Adapter estiver desabilitado, sua conexão poderá ser interrompida e as tentativas de conexão com a instância após a reinicialização poderão falhar.

3. Verifique o gerenciador de dispositivos para certificar-se de que a GPU está funcionando corretamente.
4. Para obter a melhor performance na GPU, siga as etapas de otimização em Otimização das configurações de GPU em instâncias do Amazon EC2.

Instalação dos drivers da NVIDIA GRID (instâncias G7e, G6, Gr6, G6e, G6f, Gr6f, G5, G4dn e G3)

Esses downloads estão disponíveis somente para clientes da AWS. Ao fazer o download, para cumprir os requisitos da solução da AWS que estão mencionados no Contrato de Licença de Usuário Final (EULA) da nuvem da NVIDIA GRID, você concorda em usar o software baixado somente para desenvolver AMIs para uso com os hardwares NVIDIA L4, NVIDIA L40S, NVIDIA A10G, NVIDIA Tesla T4 ou NVIDIA Tesla M60. Você pode usar os drivers GRID para criar e usar AMIs no ambiente da AWS. Após a instalação do software, você estará vinculado aos termos do Contrato de licença de usuário final em nuvem do NVIDIA GRID. Para obter informações sobre a versão do driver NVIDIA GRID para seu sistema operacional, consulte o software NVIDIA Virtual GPU (vGPU) no site da NVIDIA.

Considerações

- As instâncias G7e exigem GRID 19.1 ou posterior para Linux e 19.3 (581.192) ou posterior para Windows.
- As instâncias G6 e Gr6 requerem o GRID 18.4 ou posterior.
- As instâncias G6e requerem o GRID 17.4 ou posterior.
- As instâncias G6 e Gr6 requerem o GRID 17.1 ou posterior.
- As instâncias G5 requerem o GRID 13.1 ou posterior (ou o GRID 12.4 ou posterior).

- A resolução de DNS fornecida pela AWS é exigida pelas instâncias G3 para que o licenciamento do GRID funcione.
- IMDSv2 só é compatível com o driver NVIDIA versão 14.0 ou superior.
- Para instâncias do Windows, se você iniciar a instância usando uma AMI do Windows personalizada, a AMI deverá ser uma imagem padronizada criada com a ferramenta Sysprep do Windows para garantir que o driver do GRID funcione. Para obter mais informações, consulte Criar uma AMI do Amazon EC2 usando o Sysprep do Windows.
- O GRID 17.0 e as versões posteriores não são compatíveis com o Windows Server 2019.
- O GRID 14.2 e as versões posteriores não são compatíveis com o Windows Server 2016.
- O GRID 17.0 e as versões posteriores não são compatíveis com as instâncias G3.
- Para instâncias do Linux, pode ser necessário instalar ou atualizar pacotes, como o gcc, caso o instalador da NVIDIA apresente falhas e você receba uma mensagem de erro. Os detalhes variam conforme as versões do sistema operacional e do kernel. Para obter mais informações, consulte o Portal de Suporte Empresarial da NVIDIA.

Pré-requisitos

- (Linux) Verifique se a AWS CLI está instalada na sua instância e configurada com as credenciais padrão. Para obter mais informações, consulte Instalar a AWS CLI no Guia do usuário da AWS Command Line Interface.
- (Windows) Configure as credenciais padrão para as AWS Tools for Windows PowerShell na sua instância. Para obter mais informações, consulte Conceitos básicos do AWS Tools for Windows PowerShell no Manual do usuário do AWS Tools for PowerShell.
- Os usuários ou perfis devem ter as permissões concedidas pela política AmazonS3ReadOnlyAccess.

Amazon Linux 2023

Para instalar o driver NVIDIA GRID na instância

1. Conecte-se à sua instância. Atualize o cache de pacotes e obtenha as atualizações de pacotes para sua instância.

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

2. Instale gcc e make, caso ainda não tenham sido instalados.

```
[ec2-user ~]$ sudo dnf install gcc make
```

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 os pacotes de cabeçalhos do kernel.

```
[ec2-user ~]$ sudo dnf install -y kernel-devel kernel-modules-extra
```

6. Faça download do utilitário de instalação do driver GRID usando o comando a seguir:

```
[ec2-user ~]$ aws s3 cp --recursive s3://ec2-linux-nvidia-drivers/latest/ .
```

   Várias versões de driver GRID são armazenadas nesse bucket. É possível visualizar todas as versões disponíveis usando o comando a seguir.

```
[ec2-user ~]$ aws s3 ls --recursive s3://ec2-linux-nvidia-drivers/
```

7. Adicione as permissões para executar o utilitário de instalação do driver usando o comando a seguir.

```
[ec2-user ~]$ chmod +x NVIDIA-Linux-x86_64*.run
```

8. Execute o script de autoinstalação conforme segue para instalar o driver GRID baixado. Por exemplo:

```
[ec2-user ~]$ sudo /bin/sh ./NVIDIA-Linux-x86_64*.run
```

   Quando solicitado, aceite o acordo de licença e especifique as opções de instalação conforme o necessário (é possível aceitar as opções padrão).

9. Verifique se o driver está funcionando. A resposta para o comando a seguir lista a versão instalada do driver NVIDIA e os detalhes das GPUs.

```
[ec2-user ~]$ nvidia-smi -q | head
```

10. Se você estiver usando o software vGPU da NVIDIA versão 14.x ou superior nas instâncias G4dn, G5 ou G5g, desabilite o GSP com os comandos a seguir. Para obter mais informações sobre por que isso é necessário, acesse a Documentação da NVIDIA.

```
[ec2-user ~]$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
[ec2-user ~]$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /
etc/modprobe.d/nvidia.conf
```

11. Reinicialize a instância.

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

12. (Opcional) Dependendo do seu caso de uso, é possível concluir as seguintes etapas opcionais. Se você não precisar dessa funcionalidade, não conclua essas etapas.

    a. Para ajudar a usufruir das quatro telas com resolução de até 4K, configure o protocolo de exibição de alta performance Amazon DCV.

    b. O modo NVIDIA Quadro Virtual Workstation é habilitado por padrão. Para ativar as aplicações virtuais GRID para recursos de hospedagem de aplicações RDSH, conclua as etapas de ativação da aplicação virtual GRID em Ativação das aplicações virtuais NVIDIA GRID em instâncias baseadas em GPU do Amazon EC2.

Amazon Linux 2

Para instalar o driver NVIDIA GRID na instância

1. Conecte-se à sua instância. Atualize o cache de pacotes e obtenha as atualizações de pacotes para sua instância.

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

2. Instale gcc e make, caso ainda não tenham sido instalados.

```
[ec2-user ~]$ sudo yum install gcc make
```

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 pacote de cabeçalhos do kernel para a versão do kernel que está em execução.

```
[ec2-user ~]$ sudo yum install -y kernel-devel-$(uname -r)
```

6. Faça download do utilitário de instalação do driver GRID usando o comando a seguir:

```
[ec2-user ~]$ aws s3 cp --recursive s3://ec2-linux-nvidia-drivers/latest/ .
```

Várias versões de driver GRID são armazenadas nesse bucket. É possível visualizar todas as versões disponíveis usando o comando a seguir.

```
[ec2-user ~]$ aws s3 ls --recursive s3://ec2-linux-nvidia-drivers/
```

7. Adicione as permissões para executar o utilitário de instalação do driver usando o comando a seguir.

```
[ec2-user ~]$ chmod +x NVIDIA-Linux-x86_64*.run
```

8. Execute o script de autoinstalação conforme segue para instalar o driver GRID baixado. Por exemplo:

```
[ec2-user ~]$ sudo /bin/sh ./NVIDIA-Linux-x86_64*.run
```

Se você estiver usando o Amazon Linux 2 com o kernel versão 5.10, use o comando a seguir para instalar o driver GRID.

```
[ec2-user ~]$ sudo CC=/usr/bin/gcc10-cc ./NVIDIA-Linux-x86_64*.run
```

Quando solicitado, aceite o acordo de licença e especifique as opções de instalação conforme o necessário (é possível aceitar as opções padrão).

9. Verifique se o driver está funcionando. A resposta para o comando a seguir lista a versão instalada do driver NVIDIA e os detalhes das GPUs.

```
[ec2-user ~]$ nvidia-smi -q | head
```

10. Se você estiver usando o software vGPU da NVIDIA versão 14.x ou superior nas instâncias G4dn, G5 ou G5g, desabilite o GSP com os comandos a seguir. Para obter mais informações sobre por que isso é necessário, acesse a Documentação da NVIDIA.

```
[ec2-user ~]$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
[ec2-user ~]$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /
etc/modprobe.d/nvidia.conf
```

11. Reinicialize a instância.

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

12. (Opcional) Dependendo do seu caso de uso, é possível concluir as seguintes etapas opcionais. Se você não precisar dessa funcionalidade, não conclua essas etapas.

    a. Para ajudar a usufruir das quatro telas com resolução de até 4K, configure o protocolo de exibição de alta performance Amazon DCV.

    b. O modo NVIDIA Quadro Virtual Workstation é habilitado por padrão. Para ativar as aplicações virtuais GRID para recursos de hospedagem de aplicações RDSH, conclua as etapas de ativação da aplicação virtual GRID em Ativação das aplicações virtuais NVIDIA GRID em instâncias baseadas em GPU do Amazon EC2.

Para CentOS 7 e Red Hat Enterprise Linux 7

Para instalar o driver NVIDIA GRID na instância

1. Conecte-se à sua instância. Atualize o cache de pacotes e obtenha as atualizações de pacotes para sua instância.

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

2. Instale gcc e make, caso ainda não tenham sido instalados.

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

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 pacote de cabeçalhos do kernel para a versão do kernel que você está executando.

```
[ec2-user ~]$ sudo yum install -y kernel-devel-$(uname -r)
```

6. Desabilite o driver de código aberto `nouveau` para placas gráficas NVIDIA.

   a. Adicione o `nouveau` ao arquivo de lista de proibição `/etc/modprobe.d/blacklist.conf`. Copie o bloco de código a seguir e cole-o em um terminal.

   ```
   [ec2-user ~]$ cat << EOF | sudo tee --append /etc/modprobe.d/blacklist.conf
   blacklist vga16fb
   blacklist nouveau
   blacklist rivafb
   blacklist nvidiafb
   blacklist rivatv
   EOF
   ```

   b. Edite o arquivo `/etc/default/grub` e adicione a linha a seguir:

   ```
   GRUB_CMDLINE_LINUX="rdblacklist=nouveau"
   ```

   c. Recompile a configuração do Grub.

   ```
   [ec2-user ~]$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
   ```

7. Faça download do utilitário de instalação do driver GRID usando o comando a seguir:

```
[ec2-user ~]$ aws s3 cp --recursive s3://ec2-linux-nvidia-drivers/latest/ .
```

   Várias versões de driver GRID são armazenadas nesse bucket. É possível visualizar todas as versões disponíveis usando o comando a seguir.

```
[ec2-user ~]$ aws s3 ls --recursive s3://ec2-linux-nvidia-drivers/
```

8. Adicione as permissões para executar o utilitário de instalação do driver usando o comando a seguir.

```
[ec2-user ~]$ chmod +x NVIDIA-Linux-x86_64*.run
```

9. Execute o script de autoinstalação conforme segue para instalar o driver GRID baixado. Por exemplo:

   ```
   [ec2-user ~]$ sudo /bin/sh ./NVIDIA-Linux-x86_64*.run
   ```

   Quando solicitado, aceite o acordo de licença e especifique as opções de instalação conforme o necessário (é possível aceitar as opções padrão).

10. Verifique se o driver está funcionando. A resposta para o comando a seguir lista a versão instalada do driver NVIDIA e os detalhes das GPUs.

    ```
    [ec2-user ~]$ nvidia-smi -q | head
    ```

11. Se você estiver usando o software vGPU da NVIDIA versão 14.x ou superior nas instâncias G4dn, G5 ou G5g, desabilite o GSP com os comandos a seguir. Para obter mais informações sobre por que isso é necessário, acesse a Documentação da NVIDIA.

    ```
    [ec2-user ~]$ sudo touch /etc/modprobe.d/nvidia.conf
    ```

    ```
    [ec2-user ~]$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /
    etc/modprobe.d/nvidia.conf
    ```

12. Reinicialize a instância.

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

13. (Opcional) Dependendo do seu caso de uso, é possível concluir as seguintes etapas opcionais. Se você não precisar dessa funcionalidade, não conclua essas etapas.

    a. Para ajudar a usufruir das quatro telas com resolução de até 4K, configure o protocolo de exibição de alta performance Amazon DCV.

    b. O modo NVIDIA Quadro Virtual Workstation é habilitado por padrão. Para ativar as aplicações virtuais GRID para recursos de hospedagem de aplicações RDSH, conclua as etapas de ativação da aplicação virtual GRID em Ativação das aplicações virtuais NVIDIA GRID em instâncias baseadas em GPU do Amazon EC2.

    c. Instale o pacote de GUI de desktop/estação de trabalho.

```
[ec2-user ~]$ sudo yum groupinstall -y "Server with GUI"
```

CentOS Stream 8 e Red Hat Enterprise Linux 8

Para instalar o driver NVIDIA GRID na instância

1. Conecte-se à sua instância. Atualize o cache de pacotes e obtenha as atualizações de pacotes para sua instância.

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

2. Instale gcc e make, caso ainda não tenham sido instalados.

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

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 pacote de cabeçalhos do kernel para a versão do kernel que você está executando.

   ```
   [ec2-user ~]$ sudo dnf install -y elfutils-libelf-devel libglvnd-devel kernel-
   devel-$(uname -r)
   ```

6. Faça download do utilitário de instalação do driver GRID usando o comando a seguir:

   ```
   [ec2-user ~]$ aws s3 cp --recursive s3://ec2-linux-nvidia-drivers/latest/ .
   ```

   Várias versões de driver GRID são armazenadas nesse bucket. É possível visualizar todas as versões disponíveis usando o comando a seguir.

   ```
   [ec2-user ~]$ aws s3 ls --recursive s3://ec2-linux-nvidia-drivers/
   ```

7. Adicione as permissões para executar o utilitário de instalação do driver usando o comando a seguir.

   ```
   [ec2-user ~]$ chmod +x NVIDIA-Linux-x86_64*.run
   ```

8. Execute o script de autoinstalação conforme segue para instalar o driver GRID baixado. Por exemplo:

```
[ec2-user ~]$ sudo /bin/sh ./NVIDIA-Linux-x86_64*.run
```

   Quando solicitado, aceite o acordo de licença e especifique as opções de instalação conforme o necessário (é possível aceitar as opções padrão).

9. Verifique se o driver está funcionando. A resposta para o comando a seguir lista a versão instalada do driver NVIDIA e os detalhes das GPUs.

```
[ec2-user ~]$ nvidia-smi -q | head
```

10. Se você estiver usando o software vGPU da NVIDIA versão 14.x ou superior nas instâncias G4dn, G5 ou G5g, desabilite o GSP com os comandos a seguir. Para obter mais informações sobre por que isso é necessário, acesse a Documentação da NVIDIA.

```
[ec2-user ~]$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
[ec2-user ~]$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /
etc/modprobe.d/nvidia.conf
```

11. Reinicialize a instância.

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

12. (Opcional) Dependendo do seu caso de uso, é possível concluir as seguintes etapas opcionais. Se você não precisar dessa funcionalidade, não conclua essas etapas.

    a. Para ajudar a usufruir das quatro telas com resolução de até 4K, configure o protocolo de exibição de alta performance Amazon DCV.

    b. O modo NVIDIA Quadro Virtual Workstation é habilitado por padrão. Para ativar as aplicações virtuais GRID para recursos de hospedagem de aplicações RDSH, conclua as etapas de ativação da aplicação virtual GRID em Ativação das aplicações virtuais NVIDIA GRID em instâncias baseadas em GPU do Amazon EC2.

    c. Instale o pacote de GUI de estação de trabalho.

```
[ec2-user ~]$ sudo dnf groupinstall -y workstation
```

Rocky Linux 8

Como instalar o driver NVIDIA GRID na instância do Linux

1. Conecte-se à sua instância. Atualize o cache de pacotes e obtenha as atualizações de pacotes para sua instância.

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

2. Instale gcc e make, caso ainda não tenham sido instalados.

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

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 pacote de cabeçalhos do kernel para a versão do kernel que você está executando.

```
[ec2-user ~]$ sudo dnf install -y elfutils-libelf-devel libglvnd-devel kernel-
devel-$(uname -r)
```

6. Faça download do utilitário de instalação do driver GRID usando o comando a seguir:

```
[ec2-user ~]$ aws s3 cp --recursive s3://ec2-linux-nvidia-drivers/latest/ .
```

   Várias versões de driver GRID são armazenadas nesse bucket. É possível visualizar todas as versões disponíveis usando o comando a seguir.

```
[ec2-user ~]$ aws s3 ls --recursive s3://ec2-linux-nvidia-drivers/
```

7. Adicione as permissões para executar o utilitário de instalação do driver usando o comando a seguir.

```
[ec2-user ~]$ chmod +x NVIDIA-Linux-x86_64*.run
```

8. Execute o script de autoinstalação conforme segue para instalar o driver GRID baixado. Por exemplo:

```
[ec2-user ~]$ sudo /bin/sh ./NVIDIA-Linux-x86_64*.run
```

Quando solicitado, aceite o acordo de licença e especifique as opções de instalação conforme o necessário (é possível aceitar as opções padrão).

9. Verifique se o driver está funcionando. A resposta para o comando a seguir lista a versão instalada do driver NVIDIA e os detalhes das GPUs.

```
[ec2-user ~]$ nvidia-smi -q | head
```

10. Se você estiver usando o software vGPU da NVIDIA versão 14.x ou superior nas instâncias G4dn, G5 ou G5g, desabilite o GSP com os comandos a seguir. Para obter mais informações sobre por que isso é necessário, acesse a Documentação da NVIDIA.

```
[ec2-user ~]$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
[ec2-user ~]$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /
etc/modprobe.d/nvidia.conf
```

11. Reinicialize a instância.

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

12. (Opcional) Dependendo do seu caso de uso, é possível concluir as seguintes etapas opcionais. Se você não precisar dessa funcionalidade, não conclua essas etapas.

    a. Para ajudar a usufruir das quatro telas com resolução de até 4K, configure o protocolo de exibição de alta performance Amazon DCV.

    b. O modo NVIDIA Quadro Virtual Workstation é habilitado por padrão. Para ativar as aplicações virtuais GRID para recursos de hospedagem de aplicações RDSH, conclua as etapas de ativação da aplicação virtual GRID em Ativação das aplicações virtuais NVIDIA GRID em instâncias baseadas em GPU do Amazon EC2.

Ubuntu e Debian

Para instalar o driver NVIDIA GRID na instância

1. Conecte-se à sua instância. Atualize o cache de pacotes e obtenha as atualizações de pacotes para sua instância.

```
$ sudo apt-get update -y
```

2. Instale gcc e make, caso ainda não tenham sido instalados.

```
$ sudo apt-get install -y gcc make
```

3. (Ubuntu) Atualize o pacote `linux-aws` para receber a versão mais recente.

```
$ sudo apt-get upgrade -y linux-aws
```

   (Debian) Atualize o pacote para receber a versão mais recente.

```
$ sudo apt-get upgrade -y
```

4. Reinicialize sua instância para carregar a versão mais recente do kernel.

```
$ sudo reboot
```

5. Reconecte-se à sua instância depois de reinicializá-la.
6. Instale o pacote de cabeçalhos do kernel para a versão do kernel que você está executando atualmente.

```
$ sudo apt-get install -y linux-headers-$(uname -r) linux-modules-extra-$(uname -r)
```

7. Desabilite o driver de código aberto `nouveau` para placas gráficas NVIDIA.

   a. Adicione o `nouveau` ao arquivo de lista de proibição `/etc/modprobe.d/blacklist.conf`. Copie o bloco de código a seguir e cole-o em um terminal.

```
$ 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.

```
$ sudo update-grub
```

8. Faça download do utilitário de instalação do driver GRID usando o comando a seguir:

```
$ aws s3 cp --recursive s3://ec2-linux-nvidia-drivers/latest/ .
```

Várias versões de driver GRID são armazenadas nesse bucket. É possível visualizar todas as versões disponíveis usando o comando a seguir.

```
$ aws s3 ls --recursive s3://ec2-linux-nvidia-drivers/
```

9. Adicione as permissões para executar o utilitário de instalação do driver usando o comando a seguir.

```
$ chmod +x NVIDIA-Linux-x86_64*.run
```

10. Execute o script de autoinstalação conforme segue para instalar o driver GRID baixado. Por exemplo:

```
$ sudo /bin/sh ./NVIDIA-Linux-x86_64*.run
```

Quando solicitado, aceite o acordo de licença e especifique as opções de instalação conforme o necessário (é possível aceitar as opções padrão).

11. Verifique se o driver está funcionando. A resposta para o comando a seguir lista a versão instalada do driver NVIDIA e os detalhes das GPUs.

```
$ nvidia-smi -q | head
```

12. Se você estiver usando o software vGPU da NVIDIA versão 14.x ou superior nas instâncias G4dn, G5 ou G5g, desabilite o GSP com os comandos a seguir. Para obter mais informações sobre por que isso é necessário, acesse a Documentação da NVIDIA.

```
$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /etc/
modprobe.d/nvidia.conf
```

13. Reinicialize a instância.

```
$ sudo reboot
```

14. (Opcional) Dependendo do seu caso de uso, é possível concluir as seguintes etapas opcionais. Se você não precisar dessa funcionalidade, não conclua essas etapas.

    a. Para ajudar a usufruir das quatro telas com resolução de até 4K, configure o protocolo de exibição de alta performance Amazon DCV.

    b. O modo NVIDIA Quadro Virtual Workstation é habilitado por padrão. Para ativar as aplicações virtuais GRID para recursos de hospedagem de aplicações RDSH, conclua as etapas de ativação da aplicação virtual GRID em Ativação das aplicações virtuais NVIDIA GRID em instâncias baseadas em GPU do Amazon EC2.

    c. Instale o pacote de GUI de desktop/estação de trabalho.

```
$ sudo apt-get install -y lightdm ubuntu-desktop
```

Sistemas operacionais do Windows

Como instalar o driver NVIDIA GRID na instância do Windows

1. Conecte-se à instância do Windows e abra uma janela do PowerShell.
2. Faça download dos drivers e do Contrato de licença de usuário final do NVIDIA GRID do Amazon S3 para o seu desktop usando os comandos do PowerShell a seguir.

```
$Bucket = "ec2-windows-nvidia-drivers"
$KeyPrefix = "latest"
$LocalPath = "$home\Desktop\NVIDIA"
$Objects = Get-S3Object -BucketName $Bucket -KeyPrefix $KeyPrefix -Region us-east-1
```

```
foreach ($Object in $Objects) {
$LocalFileName = $Object.Key
if ($LocalFileName -ne '' -and $Object.Size -ne 0) {
$LocalFilePath = Join-Path $LocalPath $LocalFileName
Copy-S3Object -BucketName $Bucket -Key $Object.Key -LocalFile $LocalFilePath -
Region us-east-1
}
}
```

Várias versões de driver NVIDIA GRID são armazenadas nesse bucket. É possível fazer download de todas as versões do Windows disponíveis no bucket removendo a opção `-KeyPrefix $KeyPrefix`. Para obter informações sobre a versão do driver NVIDIA GRID para seu sistema operacional, consulte o software NVIDIA Virtual GPU (vGPU) no site da NVIDIA.

Começando no GRID versão 11.0, é possível usar os drivers no `latest` para instâncias G3 e G4dn. Não adicionaremos versões posteriores à 11.0 ao `g4/latest`, mas manteremos a versão 11.0 e as versões anteriores específicas ao G4dn no `g4/latest`.

As instâncias G5 requerem o GRID 13.1 ou posterior (ou o GRID 12.4 ou posterior).

3. Navegue até o desktop e clique duas vezes no arquivo de instalação para executá-lo (escolha a versão do driver correspondente à versão de SO da instância). Siga as instruções para instalar o driver e reinicialize sua instância, conforme necessário. Para verificar se a GPU está funcionando corretamente, verifique o gerenciador de dispositivos.
4. (Opcional) Use o comando a seguir para desabilitar a página de licenciamento no painel de controle a fim de impedir que os usuários mudem acidentalmente o tipo de produto (a NVIDIA GRID Virtual Workstation é habilitada por padrão). Para obter mais informações, consulte Guia do usuário de licenciamento do GRID.

   PowerShell

   Execute os seguintes comandos da PowerShell para criar o valor do registro e desativar a página de licenciamento no painel de controle. O padrão do AWS Tools for PowerShell nas AMIs do Windows da AWS é a versão de 32 bits e esse comando falha. Em vez disso, use a versão de 64 bits do PowerShell incluída no sistema operacional.

   ```
   New-Item -Path "HKLM:\SOFTWARE\NVIDIA Corporation\Global" -Name GridLicensing
   New-ItemProperty -Path "HKLM:\SOFTWARE\NVIDIA Corporation\Global\GridLicensing" -
   Name "NvCplDisableManageLicensePage" -PropertyType "DWord" -Value "1"
   ```

Prompt de comando

Execute o comando de registro a seguir para criar o valor do registro para desabilitar a página de licenciamento no painel de controle. É possível executá-lo usando a janela do prompt de comando ou uma versão de 64 bits do PowerShell.

```
reg add "HKLM\SOFTWARE\NVIDIA Corporation\Global\GridLicensing" /v
 NvCplDisableManageLicensePage /t REG_DWORD /d 1
```

5. (Opcional) Dependendo do seu caso de uso, é possível concluir as seguintes etapas opcionais. Se você não precisar dessa funcionalidade, não conclua essas etapas.

   a. Para ajudar a beneficiar-se dos quatro monitores com resolução de até 4K, configure o protocolo de exibição de alta performance, Amazon DCV.

   b. O modo NVIDIA Quadro Virtual Workstation é habilitado por padrão. Para ativar as aplicações virtuais GRID para recursos de hospedagem de aplicações RDSH, conclua as etapas de ativação da aplicação virtual GRID em Ativação das aplicações virtuais NVIDIA GRID em instâncias baseadas em GPU do Amazon EC2.

Instalação dos drivers para jogos da NVIDIA (instâncias G7e, G6, G6e, G5 e G4dn)

Esses drivers estão disponíveis somente para clientes da AWS. Ao baixá-lo, você concorda em usá-lo somente para desenvolver AMIs para uso com hardware RTX PRO 6000 Blackwell, NVIDIA L4, NVIDIA L40S, NVIDIA A10G, NVIDIA Tesla T4 ou NVIDIA Tesla M60. Você pode usar os drivers GRID para criar e usar AMIs no ambiente da AWS. Após a instalação do software, você estará vinculado aos termos do Contrato de licença de usuário final em nuvem do NVIDIA GRID.

Considerações

- A resolução de DNS fornecida pela AWS é exigida pelas instâncias G3 para que o licenciamento do GRID funcione.
- IMDSv2 só é compatível com o driver NVIDIA versão 495.x ou superior.

Pré-requisitos

- (Linux) Verifique se a AWS CLI está instalada na sua instância e configurada com as credenciais padrão. Para obter mais informações, consulte Instalar a AWS CLI no Guia do usuário da AWS Command Line Interface.
- Os usuários ou perfis devem ter as permissões concedidas pela política AmazonS3ReadOnlyAccess.

Amazon Linux 2023

Como instalar o driver para jogos NVIDIA na instância

1. Conecte-se à sua instância. Atualize o cache de pacotes e obtenha as atualizações de pacotes para sua instância.

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

2. Instale gcc e make, caso ainda não tenham sido instalados.

```
[ec2-user ~]$ sudo dnf install gcc make
```

3. Reinicialize sua instância para carregar a versão mais recente do kernel.

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

4. Reconecte-se à sua instância depois que ela for reiniciada.
5. Instale os pacotes de cabeçalhos do kernel.

```
[ec2-user ~]$ sudo dnf install -y kernel-devel kernel-modules-extra kernel-devel-
$(uname -r) kernel-headers-$(uname -r) dkms
```

6. Baixe o utilitário de instalação do driver para jogos usando o comando a seguir:

```
[ec2-user ~]$ aws s3 cp --recursive s3://nvidia-gaming/linux/latest/ .
```

   Muitas versões do driver para jogos são armazenadas neste bucket. É possível visualizar todas as versões disponíveis usando o comando a seguir:

```
[ec2-user ~]$ aws s3 ls --recursive s3://nvidia-gaming/linux/
```

7. Extraia o utilitário de instalação do driver para jogos do arquivo `.zip` baixado.

```
[ec2-user ~]$ unzip latest-driver-name.zip -d nvidia-drivers
```

8. Adicione as permissões para executar o utilitário de instalação do driver usando o comando a seguir:

```
[ec2-user ~]$ chmod +x nvidia-drivers/NVIDIA-Linux-x86_64*-grid.run
```

9. Execute o instalador usando o comando a seguir:

```
[ec2-user ~]$ sudo ./nvidia-drivers/NVIDIA-Linux-x86_64*.run
```

   Quando solicitado, aceite o acordo de licença e especifique as opções de instalação conforme o necessário (é possível aceitar as opções padrão).

10. Use o comando a seguir para criar o arquivo de configuração necessário.

```
[ec2-user ~]$ cat << EOF | sudo tee -a /etc/nvidia/gridd.conf
vGamingMarketplace=2
EOF
```

11. Use o comando a seguir para fazer download e renomear o arquivo de certificação.

    - Para a versão 460.39 ou posterior:

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCertLinux_2024_02_22.cert"
```

    - Para versões de 440.68 a 445.48:

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2020_04.cert"
```

    - Para versões anteriores

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2019_09.cert"
```

12. Se você estiver usando o driver NVIDIA versão 510.x ou superior nas instâncias G4dn, G5 ou G5g, desabilite o GSP com os comandos a seguir. Para obter mais informações sobre por que isso é necessário, acesse a Documentação da NVIDIA.

```
[ec2-user ~]$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
[ec2-user ~]$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /
etc/modprobe.d/nvidia.conf
```

13. Reinicialize a instância.

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

14. Verifique a licença do NVIDIA Gaming usando o comando a seguir.

```
[ec2-user ~]$ nvidia-smi.exe -q
```

Na saída, faça uma busca por `vGPU Software Licensed Product`.

15. (Opcional) Para ajudar a usufruir de uma única tela com resolução de até 4K, configure o protocolo de exibição de alta performance Amazon DCV.

Amazon Linux 2

Como instalar o driver para jogos NVIDIA na instância

1. Conecte-se à sua instância. Atualize o cache de pacotes e obtenha as atualizações de pacotes para sua instância.

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

2. Instale gcc e make, caso ainda não tenham sido instalados.

```
[ec2-user ~]$ sudo yum install gcc make
```

3. Reinicialize sua instância para carregar a versão mais recente do kernel.

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

4. Reconecte-se à sua instância depois que ela for reiniciada.
5. Instale o pacote de cabeçalhos do kernel para a versão do kernel que você está executando atualmente.

```
[ec2-user ~]$ sudo yum install -y kernel-devel-$(uname -r)
```

6. Baixe o utilitário de instalação do driver para jogos usando o comando a seguir:

```
[ec2-user ~]$ aws s3 cp --recursive s3://nvidia-gaming/linux/latest/ .
```

Muitas versões do driver para jogos são armazenadas neste bucket. É possível visualizar todas as versões disponíveis usando o comando a seguir:

```
[ec2-user ~]$ aws s3 ls --recursive s3://nvidia-gaming/linux/
```

7. Extraia o utilitário de instalação do driver para jogos do arquivo `.zip` baixado.

```
[ec2-user ~]$ unzip latest-driver-name.zip -d nvidia-drivers
```

8. Adicione as permissões para executar o utilitário de instalação do driver usando o comando a seguir:

```
[ec2-user ~]$ chmod +x nvidia-drivers/NVIDIA-Linux-x86_64*-grid.run
```

9. Execute o instalador usando o comando a seguir:

```
[ec2-user ~]$ sudo ./nvidia-drivers/NVIDIA-Linux-x86_64*.run
```

Se você estiver usando o Amazon Linux 2 com o kernel versão 5.10, use o comando a seguir para instalar os drivers de jogos NVIDIA.

```
[ec2-user ~]$ sudo CC=/usr/bin/gcc10-cc ./NVIDIA-Linux-x86_64*.run
```

Quando solicitado, aceite o acordo de licença e especifique as opções de instalação conforme o necessário (é possível aceitar as opções padrão).

10. Use o comando a seguir para criar o arquivo de configuração necessário.

```
[ec2-user ~]$ cat << EOF | sudo tee -a /etc/nvidia/gridd.conf
vGamingMarketplace=2
EOF
```

11. Use o comando a seguir para fazer download e renomear o arquivo de certificação.

- Para a versão 460.39 ou posterior:

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCertLinux_2024_02_22.cert"
```

- Para versões de 440.68 a 445.48:

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2020_04.cert"
```

- Para versões anteriores

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2019_09.cert"
```

12. Se você estiver usando o driver NVIDIA versão 510.x ou superior nas instâncias G4dn, G5 ou G5g, desabilite o GSP com os comandos a seguir. Para obter mais informações sobre por que isso é necessário, acesse a Documentação da NVIDIA.

```
[ec2-user ~]$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
[ec2-user ~]$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /
etc/modprobe.d/nvidia.conf
```

13. Reinicialize a instância.

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

14. Verifique a licença do NVIDIA Gaming usando o comando a seguir.

```
[ec2-user ~]$ nvidia-smi.exe -q
```

Na saída, faça uma busca por `vGPU Software Licensed Product`.

15. (Opcional) Para ajudar a usufruir de uma única tela com resolução de até 4K, configure o protocolo de exibição de alta performance Amazon DCV.

Para CentOS 7 e Red Hat Enterprise Linux 7

Como instalar o driver para jogos NVIDIA na instância

1. Conecte-se à sua instância do Linux. Instale gcc e make, caso ainda não tenham sido instalados.

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

2. Atualize o cache de pacotes e obtenha as atualizações de pacotes para sua instância.

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

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 pacote de cabeçalhos do kernel para a versão do kernel que você está executando atualmente.

```
[ec2-user ~]$ sudo yum install -y unzip kernel-devel-$(uname -r)
```

6. Desabilite o driver de código aberto `nouveau` para placas gráficas NVIDIA.

   a. Adicione o `nouveau` ao arquivo de lista de proibição `/etc/modprobe.d/blacklist.conf`. Copie o bloco de código a seguir e cole-o em um terminal.

```
[ec2-user ~]$ cat << EOF | sudo tee --append /etc/modprobe.d/blacklist.conf
blacklist vga16fb
blacklist nouveau
blacklist rivafb
blacklist nvidiafb
blacklist rivatv
EOF
```

   b. Edite o arquivo `/etc/default/grub` e adicione a linha a seguir:

```
GRUB_CMDLINE_LINUX="rdblacklist=nouveau"
```

   c. Recompile a configuração do Grub.

```
[ec2-user ~]$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

7. Baixe o utilitário de instalação do driver para jogos usando o comando a seguir:

```
[ec2-user ~]$ aws s3 cp --recursive s3://nvidia-gaming/linux/latest/ .
```

   Muitas versões do driver para jogos são armazenadas neste bucket. É possível visualizar todas as versões disponíveis usando o comando a seguir:

```
[ec2-user ~]$ aws s3 ls --recursive s3://nvidia-gaming/linux/
```

8. Extraia o utilitário de instalação do driver para jogos do arquivo `.zip` baixado.

```
[ec2-user ~]$ unzip *Gaming-Linux-Guest-Drivers.zip -d nvidia-drivers
```

9. Adicione as permissões para executar o utilitário de instalação do driver usando o comando a seguir:

```
[ec2-user ~]$ chmod +x nvidia-drivers/NVIDIA-Linux-x86_64*-grid.run
```

10. Execute o instalador usando o comando a seguir:

```
[ec2-user ~]$ sudo nvidia-drivers/NVIDIA-Linux-x86_64*.run
```

    Quando solicitado, aceite o acordo de licença e especifique as opções de instalação conforme o necessário (é possível aceitar as opções padrão).

11. Use o comando a seguir para criar o arquivo de configuração necessário.

```
[ec2-user ~]$ cat << EOF | sudo tee -a /etc/nvidia/gridd.conf
vGamingMarketplace=2
EOF
```

12. Use o comando a seguir para fazer download e renomear o arquivo de certificação.
    - Para a versão 460.39 ou posterior:

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCertLinux_2024_02_22.cert"
```

    - Para versões de 440.68 a 445.48:

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2020_04.cert"
```

- Para versões anteriores

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2019_09.cert"
```

13. Se você estiver usando o driver NVIDIA versão 510.x ou superior nas instâncias G4dn, G5 ou G5g, desabilite o GSP com os comandos a seguir. Para obter mais informações sobre por que isso é necessário, acesse a Documentação da NVIDIA.

```
[ec2-user ~]$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
[ec2-user ~]$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /
etc/modprobe.d/nvidia.conf
```

14. Reinicialize a instância.

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

15. (Opcional) Para ajudar a usufruir de uma única tela com resolução de até 4K, configure o protocolo de exibição de alta performance Amazon DCV. Se você não precisar dessa funcionalidade, não conclua esta etapa.

CentOS Stream 8 e Red Hat Enterprise Linux 8

Como instalar o driver para jogos NVIDIA na instância

1. Conecte-se à sua instância do Linux. Instale gcc e make, caso ainda não tenham sido instalados.

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

2. Atualize o cache de pacotes e obtenha as atualizações de pacotes para sua instância.

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

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 pacote de cabeçalhos do kernel para a versão do kernel que você está executando atualmente.

```
[ec2-user ~]$ sudo yum install -y unzip kernel-devel-$(uname -r)
```

6. Baixe o utilitário de instalação do driver para jogos usando o comando a seguir:

```
[ec2-user ~]$ aws s3 cp --recursive s3://nvidia-gaming/linux/latest/ .
```

   Muitas versões do driver para jogos são armazenadas neste bucket. É possível visualizar todas as versões disponíveis usando o comando a seguir:

```
[ec2-user ~]$ aws s3 ls --recursive s3://nvidia-gaming/linux/
```

7. Extraia o utilitário de instalação do driver para jogos do arquivo `.zip` baixado.

```
[ec2-user ~]$ unzip *Gaming-Linux-Guest-Drivers.zip -d nvidia-drivers
```

8. Adicione as permissões para executar o utilitário de instalação do driver usando o comando a seguir:

```
[ec2-user ~]$ chmod +x nvidia-drivers/NVIDIA-Linux-x86_64*-grid.run
```

9. Execute o instalador usando o comando a seguir:

```
[ec2-user ~]$ sudo nvidia-drivers/NVIDIA-Linux-x86_64*.run
```

   Quando solicitado, aceite o acordo de licença e especifique as opções de instalação conforme o necessário (é possível aceitar as opções padrão).

10. Use o comando a seguir para criar o arquivo de configuração necessário.

```
[ec2-user ~]$ cat << EOF | sudo tee -a /etc/nvidia/gridd.conf
vGamingMarketplace=2
EOF
```

11. Use o comando a seguir para fazer download e renomear o arquivo de certificação.
    - Para a versão 460.39 ou posterior:

      ```
      [ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCertLinux_2024_02_22.cert"
      ```

    - Para versões de 440.68 a 445.48:

      ```
      [ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2020_04.cert"
      ```

    - Para versões anteriores

      ```
      [ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2019_09.cert"
      ```

12. Se você estiver usando o driver NVIDIA versão 510.x ou superior nas instâncias G4dn, G5 ou G5g, desabilite o GSP com os comandos a seguir. Para obter mais informações sobre por que isso é necessário, acesse a Documentação da NVIDIA.

    ```
    [ec2-user ~]$ sudo touch /etc/modprobe.d/nvidia.conf
    ```

    ```
    [ec2-user ~]$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /etc/modprobe.d/nvidia.conf
    ```

13. Reinicialize a instância.

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

14. (Opcional) Para ajudar a usufruir de uma única tela com resolução de até 4K, configure o protocolo de exibição de alta performance Amazon DCV.

Rocky Linux 8

Como instalar o driver para jogos NVIDIA na instância

1. Conecte-se à sua instância do Linux. Instale gcc e make, caso ainda não tenham sido instalados.

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

2. Atualize o cache de pacotes e obtenha as atualizações de pacotes para sua instância.

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

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 pacote de cabeçalhos do kernel para a versão do kernel que você está executando atualmente.

```
[ec2-user ~]$ sudo dnf install -y unzip elfutils-libelf-devel libglvnd-devel
 kernel-devel-$(uname -r)
```

6. Baixe o utilitário de instalação do driver para jogos usando o comando a seguir:

```
[ec2-user ~]$ aws s3 cp --recursive s3://nvidia-gaming/linux/latest/ .
```

   Muitas versões do driver para jogos são armazenadas neste bucket. É possível visualizar todas as versões disponíveis usando o comando a seguir:

```
[ec2-user ~]$ aws s3 ls --recursive s3://nvidia-gaming/linux/
```

7. Extraia o utilitário de instalação do driver para jogos do arquivo `.zip` baixado.

```
[ec2-user ~]$ unzip *Gaming-Linux-Guest-Drivers.zip -d nvidia-drivers
```

8. Adicione as permissões para executar o utilitário de instalação do driver usando o comando a seguir:

```
[ec2-user ~]$ chmod +x nvidia-drivers/NVIDIA-Linux-x86_64*-grid.run
```

9. Execute o instalador usando o comando a seguir:

```
[ec2-user ~]$ sudo nvidia-drivers/NVIDIA-Linux-x86_64*.run
```

Quando solicitado, aceite o acordo de licença e especifique as opções de instalação conforme o necessário (é possível aceitar as opções padrão).

10. Use o comando a seguir para criar o arquivo de configuração necessário.

```
[ec2-user ~]$ cat << EOF | sudo tee -a /etc/nvidia/gridd.conf
vGamingMarketplace=2
EOF
```

11. Use o comando a seguir para fazer download e renomear o arquivo de certificação.
    - Para a versão 460.39 ou posterior:

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCertLinux_2024_02_22.cert"
```

    - Para versões de 440.68 a 445.48:

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2020_04.cert"
```

    - Para versões anteriores

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2019_09.cert"
```

12. Se você estiver usando o driver NVIDIA versão 510.x ou superior nas instâncias G4dn, G5 ou G5g, desabilite o GSP com os comandos a seguir. Para obter mais informações sobre por que isso é necessário, acesse a Documentação da NVIDIA.

```
[ec2-user ~]$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
[ec2-user ~]$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /
etc/modprobe.d/nvidia.conf
```

13. Reinicialize a instância.

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

14. (Opcional) Para ajudar a usufruir de uma única tela com resolução de até 4K, configure o protocolo de exibição de alta performance Amazon DCV.

Ubuntu e Debian

Como instalar o driver para jogos NVIDIA na instância

1. Conecte-se à sua instância do Linux. Instale gcc e make, caso ainda não tenham sido instalados.

```
$ sudo apt-get install -y gcc make build-essential
```

2. Atualize o cache de pacotes e obtenha as atualizações de pacotes para sua instância.

```
$ sudo apt-get update -y
```

3. Atualize o pacote `linux-aws` para receber a versão mais recente.

```
$ sudo apt-get upgrade -y linux-aws
```

4. Reinicialize sua instância para carregar a versão mais recente do kernel.

```
$ sudo reboot
```

5. Reconecte-se à sua instância depois de reinicializá-la.
6. Instale o pacote de cabeçalhos do kernel para a versão do kernel que você está executando atualmente.

```
$ sudo apt install -y unzip dkms linux-headers-$(uname -r)
```

7. Desabilite o driver de código aberto `nouveau` para placas gráficas NVIDIA.

   a. Adicione o `nouveau` ao arquivo de lista de proibição `/etc/modprobe.d/blacklist.conf`. Copie o bloco de código a seguir e cole-o em um terminal.

```
$ 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.

```
$ sudo update-grub
```

8. Baixe o utilitário de instalação do driver para jogos usando o comando a seguir:

```
$ aws s3 cp --recursive s3://nvidia-gaming/linux/latest/ .
```

Muitas versões do driver para jogos são armazenadas neste bucket. É possível visualizar todas as versões disponíveis usando o comando a seguir:

```
$ aws s3 ls --recursive s3://nvidia-gaming/linux/
```

9. Extraia o utilitário de instalação do driver para jogos do arquivo `.zip` baixado.

```
$ unzip *Gaming-Linux-Guest-Drivers.zip -d nvidia-drivers
```

10. Adicione as permissões para executar o utilitário de instalação do driver usando o comando a seguir:

```
$ chmod +x nvidia-drivers/NVIDIA-Linux-x86_64*-grid.run
```

11. Execute o instalador usando o comando a seguir:

```
$ sudo nvidia-drivers/NVIDIA-Linux-x86_64*.run
```

Quando solicitado, aceite o acordo de licença e especifique as opções de instalação conforme o necessário (é possível aceitar as opções padrão).

12. Use o comando a seguir para criar o arquivo de configuração necessário.

```
$ cat << EOF | sudo tee -a /etc/nvidia/gridd.conf
vGamingMarketplace=2
EOF
```

13. Use o comando a seguir para fazer download e renomear o arquivo de certificação.

- Para a versão 460.39 ou posterior:

```
$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCertLinux_2024_02_22.cert"
```

- Para versões de 440.68 a 445.48:

```
$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2020_04.cert"
```

- Para versões anteriores

```
$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2019_09.cert"
```

14. Se você estiver usando o driver NVIDIA versão 510.x ou superior nas instâncias G4dn, G5 ou G5g, desabilite o GSP com os comandos a seguir. Para obter mais informações sobre por que isso é necessário, acesse a Documentação da NVIDIA.

```
$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /etc/
modprobe.d/nvidia.conf
```

15. Reinicialize a instância.

```
$ sudo reboot
```

16. (Opcional) Para ajudar a usufruir de uma única tela com resolução de até 4K, configure o protocolo de exibição de alta performance Amazon DCV. Se você não precisar dessa funcionalidade, não conclua esta etapa.

Sistemas operacionais do Windows

Antes de instalar um driver NVIDIA para jogos na instância, é necessário garantir que os pré-requisitos apresentados a seguir sejam atendidos, além das considerações mencionadas para todos os drivers para jogos.

- Se você iniciar a instância do Windows usando uma AMI do Windows personalizada, a AMI deverá ser uma imagem padronizada criada com a ferramenta Sysprep do Windows para garantir que o

driver de jogo funcione. Para obter mais informações, consulte Criar uma AMI do Amazon EC2 usando o Sysprep do Windows.

- Configure as credenciais padrão para o AWS Tools for Windows PowerShell em sua instância do Windows. Para obter mais informações, consulte Conceitos básicos do AWS Tools for Windows PowerShell no Guia do usuário do AWS Tools for PowerShell.

Como instalar o driver para jogos NVIDIA na instância do Windows

1. Conecte-se à instância do Windows e abra uma janela do PowerShell.
2. Faça download e instale o driver para jogos usando os seguintes comandos do PowerShell.

```
$Bucket = "nvidia-gaming"
$KeyPrefix = "windows/latest"
$LocalPath = "$home\Desktop\NVIDIA"
$Objects = Get-S3Object -BucketName $Bucket -KeyPrefix $KeyPrefix -Region us-east-1
foreach ($Object in $Objects) {
$LocalFileName = $Object.Key
if ($LocalFileName -ne '' -and $Object.Size -ne 0) {
$LocalFilePath = Join-Path $LocalPath $LocalFileName
Copy-S3Object -BucketName $Bucket -Key $Object.Key -LocalFile $LocalFilePath -
Region us-east-1
}
}
```

   Muitas versões do driver NVIDIA GRID são armazenadas neste bucket do S3. É possível baixar todas as versões disponíveis no bucket se alterar o valor da variável `$KeyPrefix` de “windows/latest” para "windows".
3. Navegue até o desktop e clique duas vezes no arquivo de instalação para executá-lo (escolha a versão do driver correspondente à versão de SO da instância). Siga as instruções para instalar o driver e reinicialize sua instância, conforme necessário. Para verificar se a GPU está funcionando corretamente, verifique o gerenciador de dispositivos.
4. Use um dos métodos a seguir para registrar o driver.

   Version 527.27 or above

   Crie a chave de registro a seguir com a versão de 64 bits do PowerShell ou a janela do prompt de comando.

chave: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\nvlddmkm\Global`

nome: VGamingMarketplace

tipo: DWord

value: 2

PowerShell

Execute o comando a seguir do PowerShell para criar esse valor de registro. O padrão do AWS Tools for PowerShell nas AMIs do Windows da AWS é a versão de 32 bits e esse comando falha. Em vez disso, use a versão de 64 bits do PowerShell incluída no sistema operacional.

```
New-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\nvlddmkm\Global"
 -Name "vGamingMarketplace" -PropertyType "DWord" -Value "2"
```

Prompt de comando

Execute o seguinte comando do registro para criar esse valor de registro. É possível executá-lo usando a janela do prompt de comando ou uma versão de 64 bits do PowerShell.

```
reg add "HKLM\SYSTEM\CurrentControlSet\Services\nvlddmkm\Global" /v
 vGamingMarketplace /t REG_DWORD /d 2
```

Earlier versions

Crie a chave de registro a seguir com a versão de 64 bits do PowerShell ou a janela do prompt de comando.

chave: `HKEY_LOCAL_MACHINE\SOFTWARE\NVIDIA Corporation\Global`

nome: VGamingMarketplace

tipo: DWord

value: 2

PowerShell

Execute o comando a seguir do PowerShell para criar esse valor de registro. O padrão do AWS Tools for PowerShell nas AMIs do Windows da AWS é a versão de 32 bits e esse comando falha. Em vez disso, use a versão de 64 bits do PowerShell incluída no sistema operacional.

```
New-ItemProperty -Path "HKLM:\SOFTWARE\NVIDIA Corporation\Global" -Name
 "vGamingMarketplace" -PropertyType "DWord" -Value "2"
```

Prompt de comando

Execute o seguinte comando do registro para criar essa chave de registro com a janela do prompt de comando. Você também pode usar esse comando na versão de 64 bits do PowerShell.

```
reg add "HKLM\SOFTWARE\NVIDIA Corporation\Global" /v vGamingMarketplace /t
 REG_DWORD /d 2
```

5. Execute o seguinte comando no PowerShell. Essa ação baixará o arquivo de certificação, renomeará o arquivo como `GridSwCert.txt` e o moverá para a pasta Public Documents (Documentos Públicos) no drive do sistema. Normalmente, o caminho da pasta é `C:\Users\Public\Documents`.

   - Para a versão 460.39 ou posterior:

     ```
     Invoke-WebRequest -Uri "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-
     Archive/GridSwCertWindows_2024_02_22.cert" -OutFile "$Env:PUBLIC\Documents
     \GridSwCert.txt"
     ```

   - Para a versão 445.87:

     ```
     Invoke-WebRequest -Uri "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-
     Archive/GridSwCert-Windows_2020_04.cert" -OutFile "$Env:PUBLIC\Documents
     \GridSwCert.txt"
     ```

   - Para versões anteriores

```
Invoke-WebRequest -Uri "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-
Archive/GridSwCert-Windows_2019_09.cert" -OutFile "$Env:PUBLIC\Documents
\GridSwCert.txt"
```

Se você receber um erro ao baixar o arquivo e estiver usando o Windows Server 2016 ou anterior, talvez seja necessário habilitar o TLS 1.2 para seu terminal PowerShell. É possível habilitar o TLS 1.2 para a sessão atual do PowerShell com o comando a seguir e tentar novamente:

```
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
```

6. Reinicie a instância.
7. Localize o arquivo `nvidia-smi.exe` na instância.

```
Get-ChildItem -Path C:\ -Recurse -Filter "nvidia-smi.exe"
```

Verifique a licença do NVIDIA Gaming usando o comando a seguir. Substitua *caminho* pelo nome da pasta que aparece na saída do comando anterior.

```
C:\Windows\System32\DriverStore\FileRepository\path\nvidia-smi.exe -q
```

A saída deve ser semelhante a esta.

```
vGPU Software Licensed Product
Product Name              : NVIDIA Cloud Gaming
License Status            : Licensed (Expiry: N/A)
```

8. (Opcional) Para ajudar a usufruir da única tela com resolução de até 4K, configure o protocolo de exibição de alta performance Amazon DCV. Se você não precisar dessa funcionalidade, não conclua esta etapa.

Instalar o driver do ENA em instâncias do Windows do EC2

Se sua instância não for baseada em uma das mais recentes imagens de máquina da Amazon (AMIs) do Windows que a Amazon fornece, use o procedimento a seguir para instalar o driver ENA atual em sua instância. Execute esta atualização em um momento conveniente para reinicializar sua

instância. Se o script de instalação não reinicializar automaticamente sua instância, recomendamos que você reinicie a instância como etapa final.

Se você usar um volume de armazenamento de instância para armazenar dados enquanto a instância estiver em execução, esses dados serão apagados quando você interromper a instância. Antes de interromper sua instância, verifique se você copiou todos os dados necessários dos volumes de armazenamento de instância para um armazenamento persistente, como o Amazon EBS ou o Amazon S3.

Pré-requisitos

Para instalar ou atualizar o driver ENA, sua instância do Windows deve atender aos seguintes pré-requisitos:

- A versão 3.0 ou posterior do PowerShell está instalada.
- Os comandos descritos nesta seção devem ser executados na versão de 64 bits do PowerShell. Não use a versão x86 do PowerShell. Essa é a versão de 32 bits do shell e não é compatível com esses comandos.

Etapa 1: fazer backup de seus dados

Recomendamos que você crie uma AMI de backup caso não consiga reverter suas alterações por meio do Gerenciador de dispositivos. Para criar uma AMI de backup com o Console de gerenciamento da AWS, siga estas etapas:

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância que requer a atualização do driver e escolha Interromper instância no menu Estado da instância.
4. Depois de interromper a instância, selecione a instância novamente. Para criar seu backup, escolha Imagem e modelos no menu Ações e escolha Criar imagem.
5. Para reiniciar sua instância, escolha Iniciar instância no menu Estado da instância.

Etapa 2: instalar ou atualizar seu driver ENA

É possível instalar ou atualizar seu driver ENA com o AWS Systems Manager Distributor ou com os cmdlets do PowerShell. Para obter mais instruções, selecione a guia que corresponde ao método que deseja utilizar.

Systems Manager Distributor

É possível usar o recurso do Systems Manager Distributor para implantar pacotes nos nós gerenciados do Systems Manager. Com o Systems Manager Distributor, você pode instalar o pacote de driver ENA uma vez ou com atualizações programadas. Para obter mais informações sobre como instalar o pacote de driver ENA (`AwsEnaNetworkDriver`) com o Systems Manager Distributor, consulte Instalar ou atualizar pacotes no Guia do usuário do AWS Systems Manager.

PowerShell

Esta seção aborda como fazer o download e instalar pacotes de drivers ENA em sua instância com cmdlets do PowerShell.

Opção 1: fazer o download e extrair a versão mais recente

1. Conecte-se à instância e faça login como administrador local.
2. Use o cmdlet invoke-webrequest para fazer o download do pacote de driver mais recente:

```
PS C:\> invoke-webrequest https://ec2-windows-drivers-
downloads.s3.amazonaws.com/ENA/Latest/AwsEnaNetworkDriver.zip -
outfile $env:USERPROFILE\AwsEnaNetworkDriver.zip
```

> **Note**
>
> Se você receber um erro ao baixar o arquivo e estiver usando o Windows Server 2016 ou anterior, talvez seja necessário habilitar o TLS 1.2 para seu terminal PowerShell. É possível habilitar o TLS 1.2 para a sessão atual do PowerShell com o comando a seguir e tentar novamente:
>
> ```
> [Net.ServicePointManager]::SecurityProtocol =
>  [Net.SecurityProtocolType]::Tls12
> ```

Como alternativa, você pode fazer o download do pacote de driver mais recente em uma janela do navegador em sua instância.

3. Use o cmdlet expand-archive para extrair o arquivo zip que você baixou para sua instância:

```
PS C:\> expand-archive $env:userprofile\AwsEnaNetworkDriver.zip -
DestinationPath $env:userprofile\AwsEnaNetworkDriver
```

Opção 2: fazer o download e extrair uma versão específica

1. Conecte-se à instância e faça login como administrador local.
2. Faça o download do pacote do driver ENA para a versão específica desejada no link da versão na tabela Histórico da versão do driver do ENA do Windows.
3. Extraia o arquivo zip para sua instância.

Instalar o driver ENA com o PowerShell

As etapas de instalação são as mesmas, independentemente de você ter feito o download do driver mais recente ou de uma versão específica. Para instalar o driver ENA, siga estas etapas:

1. Instale o driver, execute o script `install.ps1` do PowerShell do diretório do `AwsEnaNetworkDriver` em sua instância. Se você receber um erro, verifique se está usando o PowerShell 3.0 ou posterior.
2. Se o instalador não reinicializar automaticamente sua instância, execute o cmdlet Restart-Computer do PowerShell.

```
PS C:\> Restart-Computer
```

Etapa 3 (opcional): verificar a versão do driver ENA após a instalação

Para garantir que o pacote do driver ENA tenha sido instalado com êxito em sua instância, você pode verificar a nova versão da seguinte forma:

1. Conecte-se à instância e faça login como administrador local.

2. Para abrir o Gerenciador de dispositivos do Windows, insira `devmgmt.msc` na caixa Run (Executar).
3. Escolha OK. Isso abre a janela Gerenciador de dispositivos.
4. Selecione a seta à esquerda de Network adapters (Adaptadores de rede) para expandir a lista.
5. Escolha o nome ou abra o menu de contexto para Amazon Elastic Network Adapter (Adaptador do Amazon Elastic Network) e, depois, escolha Properties (Propriedades). Isso abre a caixa de diálogo Propriedades do Adaptador de Rede Elástica da Amazon.

> **Note**
>
> Todos os adaptadores ENA usam o mesmo driver. Caso tenha vários adaptadores ENA, será possível selecionar qualquer um deles para atualizar o driver de todos os adaptadores ENA.

6. Para verificar a versão atual instalada, abra a guia Driver e verifique a Versão do driver. Se a versão atual não corresponder à sua versão de destino, consulte Solução de problemas do driver do Adaptador de Rede Elástica do Windows.

Reverter a instalação de um driver ENA

Se algo der errado com a instalação, talvez seja necessário reverter o driver. Siga estas etapas para reverter para a versão anterior do driver ENA que estava instalada em sua instância.

1. Conecte-se à instância e faça login como administrador local.
2. Para abrir o Gerenciador de dispositivos do Windows, insira `devmgmt.msc` na caixa Run (Executar).
3. Escolha OK. Isso abre a janela Gerenciador de dispositivos.
4. Selecione a seta à esquerda de Network adapters (Adaptadores de rede) para expandir a lista.
5. Escolha o nome ou abra o menu de contexto para Amazon Elastic Network Adapter (Adaptador do Amazon Elastic Network) e, depois, escolha Properties (Propriedades). Isso abre a caixa de diálogo Propriedades do Adaptador de Rede Elástica da Amazon.

> **Note**
>
> Todos os adaptadores ENA usam o mesmo driver. Caso tenha vários adaptadores ENA, será possível selecionar qualquer um deles para atualizar o driver de todos os adaptadores ENA.

6. Para reverter o driver, abra a guia Driver e escolha Reverter driver. Isso abre a janela de Reversão do pacote de driver.

> **Note**
>
> Se a guia Driver não mostrar a ação Reverter driver ou se a ação não estiver disponível, isso significa que o armazenamento de drivers em sua instância não contém o pacote de driver instalado anteriormente. Para solucionar esse problema, consulte Cenários de solução de problemas e expanda a seção Versão inesperada do driver ENA instalada. Para obter mais informações sobre o processo de seleção do pacote de driver de dispositivo, consulte Como o Windows seleciona um pacote de driver para um dispositivo no site de documentação da Microsoft.

Rastrear os lançamentos da versão do driver do ENA do Windows

As AMIs do Windows incluem o driver do ENA do Windows para habilitar a rede avançada.

Nas versões 2016 e superiores do Windows Server, recomendamos usar a versão mais recente do driver. Para versões anteriores do Windows Server, consulte a tabela a seguir para determinar qual versão do driver ENA usar.

Versão Windows Server	Versão do driver ENA
Windows Server 2012 R2	2.6.0 e anterior
Windows Server 2012	2.6.0 e anterior
Windows Server 2008 R2	2.2.3 e anterior

Histórico da versão do driver do ENA do Windows

A tabela a seguir resume as alterações de cada versão.

Versão do driver	Detalhes	Data de lançamento
2.11.0	Novos recursos • Foi adicionado suporte para alocação dinâmica de filas com aumento vertical de escala de até 64 filas de E/S, sujeito aos limites do tipo de instância. Correções de bugs • Correção da falta de tratamento das condições de erro ao recuperar a largura do endereço DMA físico do dispositivo.	1.º de agosto de 2025
2.10.0	Correções de bugs • Foi corrigido o tratamento incorreto de falhas de alocação de memória durante a inicialização da fila para evitar reinicializações inesperadas. • Foi corrigida a possível configuração incorreta de descargas de rede em que os recursos do dispositivo eram ignorados.	24 de junho de 2025
2.9.0	Novos recursos • Adicionado suporte para solicitações de redefinição assíncrona iniciadas pelo dispositivo.	12 de dezembro de 2024

Versão do driver	Detalhes	Data de lançamento
	• Adicionado suporte para lidar com o valor máximo de profundidade de LLQ grande fornecido pelo dispositivo. • Adicionada a ID de evento `58001` no Visualizador de eventos do Windows para melhorar a visibilidade de transições inesperadas de estado de energia causadas pela configuração incorreta do dispositivo. Correções de bugs • Corrigido o tratamento incorreto de falhas de alocação de memória durante a inicialização do dispositivo para evitar reinicializações inesperadas. • Corrigido um problema na rotina de serviço de interrupção que poderia enfileirar um DPC durante a parada do dispositivo, evitando reinicializações inesperadas.	
2.8.0	Correções de bugs • Foi corrigida uma condição de corrida no fluxo completo do processamento da lista de buffers de rede (NBL) de saída, que poderia levar à corrupção de memória causada pela tentativa de liberar uma NBL que já havia sido lançada. • Foi corrigida a detecção incorreta do protocolo L3 ao desativar todos os descarregamentos de LSO e soma de verificação que poderiam levar a um comportam ento inesperado.	30 de setembro de 2024

Versão do driver	Detalhes	Data de lançamento
2.7.0	Novos recursos • Removido o suporte ao Windows Server 2012 (Windows 8) e ao Windows Server 2012 R2 (Windows 8.1). A AWS não oferece mais suporte a essas versões do sistema operacional. A instalação do driver falhará no Windows Server 2012 e versões anteriores. • Adicionado suporte a descarrega do cálculo da soma de verificação IPv6 Tx para o dispositivo. • Adicionado amplo suporte a Low Latency Queuing (LLQ). Isso é habilitado dinamicamente com base na recomendação do dispositivo. É possível substitui r essa configuração pela nova chave de registro "WideLLQ". • Adicionado relatório de descarte de pacotes devido a sobrecarga de Rx, o que indica espaço insuficiente no ring Rx para pacotes recebidos. • Adicionado suporte para notificações do dispositivo sobre configurações não ideais. Veja o ID de evento `59000` no visualizador de eventos do Windows. Correções de bugs • Evite a reinicialização desnecessária do dispositivo causada por pacotes Tx com cabeçalhos que excedem o tamanho máximo de cabeçalho de Low Latency Queuing (LLQ).	1º. de maio de 2024

Versão do driver	Detalhes	Data de lançamento

2.6.0	Novos recursos
	• Adiciona as métricas de performance de rede a seguir para tipos de instância que oferecem suporte ao ENA Express.
	  • `ena_srd_mode`
	  • `ena_srd_tx_pkts`
	  • `ena_srd_eligible_tx_pkts`
	  • `ena_srd_rx_pkts`
	  • `ena_srd_resource_utilization`
	• Adiciona uma métrica de performance de rede `conntrack_allowance_available` para tipos de instância baseados em Nitro.
	• Adiciona um novo motivo de reinicialização do adaptador devido à detecção de corrupção de dados RX.
	• Atualiza a infraestrutura de registro de drivers.
	
	Correções de bugs
	• Impede a reinicialização do adaptador caso a falta de CPU faça com que uma atualização das métricas de performance da rede falhe.
	•
		20 de junho de 2023

Versão do driver	Detalhes	Data de lançamento
	Impede a falsa detecção de uma interrupção no heartbeat do dispositivo. • Corrige o script de instalação do driver para ser compatível com a operação de downgrade. • Corrige a estatística de contagem de erros de recebimento.	
2.5.0	Comunicado O driver do ENA Windows versão 2.5.0 foi revertido devido à falha na inicialização da controladora de domínio Windows. O Windows Client e o Windows Server não são afetados.	17 de fevereiro de 2023

Versão do driver	Detalhes	Data de lançamento
2.4.0	Novos recursos • Acrescenta suporte para Windows Server 2022. • Remove o suporte para Windows Server 2008 R2. • Define o enfileiramento de baixa latência (LLQ) como sempre ativo para melhorar a performance em instâncias do Amazon EC2 de sexta geração. Correções de bugs • Corrige uma falha na publicação de métricas de performance de rede no sistema de contadores de performance do Windows (PCW). • Corrige uma perda de memória durante a operação de leitura da chave de registro. • Impede um loop de reinicialização infinito em caso de erro irrecuperável durante o processo de redefinição do adaptador.	28 de abril de 2022

Versão do driver	Detalhes	Data de lançamento
2.2.4	Comunicado O driver ENA Windows versão 2.2.4 foi revertido devido à possível degradação da performance nas instâncias do EC2 de sexta geração. Recomendamos que você faça o downgrade do driver usando um dos seguintes métodos: • Instalar a versão anterior 1. Baixe o pacote da versão anterior pelo link nesta tabela (versão 2.2.3). 2. Execute o script de instalação do PowerShell install.ps1. Para obter mais detalhes sobre as etapas de pré e pós-instalação, consulte Habilitar redes avançadas no Windows. • Usar o Amazon EC2 Systems Manager para uma atualização em massa • Execute uma atualização em massa por meio do documento SSM `AWS-ConfigureAWSPackage` com os seguintes parâmetros: • Name (Nome): AwsEnaNetworkDriver • Version (Versão): 2.2.3	26 de outubro de 2021

Versão do driver	Detalhes	Data de lançamento
2.2.3	Novos recursos • Adiciona suporte para novos Nitro Cards com rede de instâncias de até 400 Gbps. Correções de bugs • Corrige um comportamento de disputa entre a mudança de hora do sistema e a consulta de hora do sistema pelo driver do ENA, que causa a detecção falso-positiva de falta de resposta de HW. Comunicado O driver ENA versão 2.2.3 para Windows é a versão final compatível com Windows Server 2008 R2. Os tipos de instância atualmente disponíveis que usam ENA continuarão tendo suporte no Windows Server 2008 R2, e os drivers estarão disponíveis por download. Nenhum tipo futuro de instância será compatível com Windows Server 2008 R2 e você não poderá executar, importar ou migrar imagens do Windows Server 2008 R2 para tipos futuros de instância.	25 de março de 2021

Versão do driver	Detalhes	Data de lançamento
2.2.2	Novos recursos • Adiciona suporte para consultar métricas de performance do adaptador de rede com o CloudWatch e os Contadores de performance para consumidores do Windows. Correções de bugs • Corrige problemas de performance em instâncias bare metal.	21 de dezembro de 2020
2.2.1	Novos recursos • Adiciona um método para permitir que o host consulte o Elastic Network Adapter para obter métricas de performance da rede.	1º de outubro de 2020

Versão do driver	Detalhes	Data de lançamento
2.2.0	Novos recursos • Adiciona suporte aos tipos de hardware de próxima geração. • Melhora o tempo de inicialização da instância após retomar de uma parada de hibernação e elimina mensagens de erro de falsos positivos de ENA. Otimizações da performance • Otimiza o processamento do tráfego de entrada. • Melhora o gerenciamento de memória compartilhada em um ambiente de recursos escassos. Correções de bugs • Evita a falha do sistema após a remoção do dispositivo do ENA em um cenário raro em que há falha na redefinição do driver.	12 de agosto de 2020
2.1.5	Correções de bugs • Corrige falhas ocasionais de inicialização do adaptador de rede em instâncias bare metal.	23 de junho de 2020

Versão do driver	Detalhes	Data de lançamento
2.1.4	Correções de bugs • Evite problemas de conectividade causados por metadados de pacotes LSO corruptos chegando da pilha da rede. • Evite falha no sistema causada por uma condição de corrida rara que resulta no acesso de uma memória de pacote já liberada.	25 de novembro de 2019
2.1.2	Novos recursos • Adição de suporte para que o relatório do ID do fornecedor permita que o SO gere UUIDs baseadas em MAC. Correções de bugs • Melhoria na performance da configuração de rede DHCP durante a inicialização. • Calcule corretamente a soma de verificação L4 no tráfego IPv6 de entrada quando a unidade de transmissão máxima (MTU) exceder 4K. • Melhorias gerais na estabilidade do driver e correções de erros secundárias.	4 de novembro de 2019

Versão do driver	Detalhes	Data de lançamento
2.1.1	Correções de bugs • Previnem a chegada de pacotes LSO TCP altamente fragmentados do sistema operacional. • Lidam corretamente com o protocolo Encapsulating Security Payload (ESP) dentro do IPSec em redes IPv6.	16 de setembro de 2019

Versão do driver	Detalhes	Data de lançamento

2.1.0	O driver ENA v2.1 do Windows apresenta novos recursos do dispositivo ENA, dá um impulso à performance, adiciona novos recursos e inclui várias melhorias de estabilidade.
	
	Novos recursos
	
	• Use a chave do Registro do Windows padronizada para configuração dos frames jumbo.
	• Permitir a configuração do ID da VLAN via a GUI das propriedades do driver ENA.
	• Fluxos de recuperação melhorados
	  • Melhora no mecanismo de identificação de falhas.
	  • Adicionado suporte para parâmetros de recuperação ajustáveis.
	• Compatibilidade para até 32 filas de E/S para instâncias do EC2 mais novas, que têm mais de 8 vCPUs.
	• Redução de ~90% da presença de memória do driver.
	
	Otimizações da performance
	
	• Redução na latência do caminho de transmissão.
	• Suporte para receber o descarregamento da soma de verificação.
	•
		1 de julho de 2019

Versão do driver	Detalhes	Data de lançamento
	Otimização da performance para um sistema pesadamente carregado (uso otimizado dos mecanismos de bloqueio). • Outras melhorias para reduzir a utilização da CPU e melhorar a responsividade do sistema em carga. Correções de bugs • Corrigir a falha devido à análise inválida de cabeçalhos Tx não contíguos. • Corrija a falha do driver v1.5 durante o desvincul amento da interface de rede elástica em instâncias bare metal. • Corrigir o erro de cálculo da soma de verificação do pseudocabeçalho do LSO sobre IPv6. • Corrigir o vazamento de recursos de memória em potencial na falha da inicialização. • Desabilitar o descarregamento da soma de verificação de TCP/UDP para fragmentos de IPv4. • Corrigir para configuração da VLAN. A VLAN foi desabilitada incorretamente quando somente a prioridade da VLAN deveria ter sido desabilitada. • Habilitar a análise das mensagens do driver personali zado pelo visualizador de eventos. •	

Versão do driver	Detalhes	Data de lançamento
	Corrigir a falha em inicializar o driver devido a tratamento de timestamp inválido. • Corrigir a condição da corrida entre o processamento de dados e a desabilitação do dispositivo ENA.	
1.5.0	Atualizações • Estabilidade aprimorada e correções de performance. • Os buffers de recebimento agora podem ser configura dos até um valor de 8192 em Advanced Properties (Propriedades avançadas) de NIC do ENA. • Buffers de recebimento padrão de 1 k.	4 de outubro de 2018
1.2.3	Inclui correções de confiabilidade e unifica o suporte para o Windows Server 2008 R2 por meio do Windows Server 2016.	13 de fevereiro de 2018
1.0.8	A versão inicial. Incluída em AMIs do Windows Server 2008, do Windows Server 2012 RTM, do Windows Server 2012 R2 e do Windows Server 2016.	Julho de 2016

Inscreva-se para receber notificações da versão de drivers do ENA do Windows do Amazon SNS

O Amazon SNS pode notificá-lo quando novas versões dos drivers EC2 para Windows são lançadas. Use o procedimento a seguir para se inscrever nessas notificações.

Assinar as notificações do EC2

1. Abra o console do Amazon SNS em https://console.aws.amazon.com/sns/v3/home.
2. Na barra de navegação, altere a região para Leste dos EUA (Norte da Virgínia), se necessário. É necessário selecionar esta região porque as notificações do SNS que você está assinando estão nesta região.
3. No painel de navegação, escolha Subscriptions.
4. Selecione Create subscription.
5. Na caixa de diálogo Criar assinatura, faça o seguinte:

   a. Para o ARN do tópico, copie o seguinte ARN (nome de recurso da Amazon):

      arn:aws:sns:us-east-1:801119661308:ec2-windows-drivers

   b. Para Protocolo, selecione `Email`.

   c. Para Endpoint, insira o endereço de e-mail no qual deseja receber as notificações.

   d. Selecione Create subscription.
6. Você receberá um e-mail de confirmação. Abra o e-mail e siga as instruções para concluir a sua assinatura.

Sempre que novos drivers EC2 para Windows são lançados, nós enviamos notificações aos assinantes. Se não deseja mais receber essas notificações, use o procedimento a seguir para cancelar a assinatura.

Para cancelar a assinatura de notificações do driver do Windows para o Amazon EC2

1. Abra o console do Amazon SNS em https://console.aws.amazon.com/sns/v3/home.
2. No painel de navegação, escolha Subscriptions.
3. Selecione a caixa de seleção para a assinatura e, depois, escolha Ações, Excluir assinaturas. Quando a confirmação for solicitada, escolha Excluir.

Drivers paravirtuais para as instâncias do Windows

As AMIs do Windows contêm um conjunto de drivers para permitir acesso ao hardware virtualizado. Esses drivers são usados pelo Amazon EC2 para mapear armazenamento de instâncias e volumes do Amazon EBS para seus dispositivos. A tabela a seguir mostra as principais diferenças entre os diferentes drivers.

	Red Hat PV	Citrix PV	AWS PV
Tipo de instância	Não tem suporte para todos os tipos de instâncias. Se você especificar um tipo de instância sem suporte, a instância ficará danificada.	Com suporte para os tipos de instância Xen.	Com suporte para os tipos de instância Xen.
Volumes anexados	Oferece suporte a até 16 volumes anexados.	Oferece suporte a mais de 16 volumes anexados.	Oferece suporte a mais de 16 volumes anexados.
Rede	O driver tem problemas conhecidos em que a conexão de rede é redefinida em cargas altas, por exemplo, transferências rápidas de arquivos via FTP.		O driver configura automaticamente quadros jumbo no adaptador da rede quando está em um tipo de instância compatível. Quando a instância está em um grupo de posicionamento de cluster, isso oferece melhor performance de rede

	Red Hat PV	Citrix PV	AWS PV
			entre as instâncias que estão no grupo de posiciona mento de cluster. Para obter mais informaçõ es, consulte Grupos de posiciona mento para as instância s do Amazon EC2.

A tabela a seguir mostra quais drivers PV é necessário executar em cada versão do Windows Server no Amazon EC2.

Versão Windows Server	Versão PV driver
Windows Server 2025	Não compatível
Windows Server 2022	Versão mais recente do AWS PV
Windows Server 2019	Versão mais recente do AWS PV
Windows Server 2016	Versão mais recente do AWS PV
Windows Server 2012 R2	AWS PV versão 8.4.3
Windows Server 2012	AWS PV versão 8.4.3
Windows Server 2008 R2	AWS PV versão 8.3.5

Versão Windows Server	Versão PV driver
Windows Server 2008	Citrix PV 5.9
Windows Server 2003	Citrix PV 5.9

Tópicos

- Drivers AWS PV
- Drivers do Citrix PV
- Drivers Red Hat PV
- Assinar notificações do
- Atualizar drivers PV em instâncias do Windows do EC2
- Solução de problemas em drivers PV em instâncias do Windows

Drivers AWS PV

Os drivers AWS PV são armazenadas no diretório `%ProgramFiles%\Amazon\Xentools`. Esse diretório também contém símbolos públicos e uma ferramenta da linha de comando, `xenstore_client.exe`, que permite acessar entradas no XenStore. Por exemplo, o seguinte comando de PowerShell retorna o horário atual do Hypervisor:

```
PS C:\> [DateTime]::FromFileTimeUTC((gwmi -n root\wmi -cl
 AWSXenStoreBase).XenTime).ToString("hh:mm:ss")
11:17:00
```

Os componentes do driver AWS PV são listados no Registro do Windows em `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services`. Esses componentes do driver são os seguintes: xenbus, xeniface, xennet, xenvbd e xenvif.

Os drivers AWS PV também têm um serviço do Windows chamado LiteAgent, que é executado no modo de usuário. Ele lida com tarefas como eventos de desligamento e reinicialização a partir das APIs da AWS em instâncias de geração Xen. É possível acessar e gerenciar serviços executando `Services.msc` a partir da linha de comando. Quando executados em instâncias de geração Nitro, os drivers AWS PV não são usados e o serviço LiteAgent será interrompido automaticamente começando pela versão do driver 8.2.4. A atualização para o driver AWS PV mais recente também atualiza o LiteAgent e melhora a confiabilidade em todas as gerações de instâncias.

Instalar os drivers AWS PV mais recentes

As AMIs Windows da Amazon contêm um conjunto de drivers para permitir acesso ao hardware virtualizado. Esses drivers são usados pelo Amazon EC2 para mapear armazenamento de instâncias e volumes do Amazon EBS para seus dispositivos. Recomendamos que você instale os drivers mais recentes para melhorar a estabilidade e a performance de suas instâncias do EC2 Windows.

Opções de instalação

- Use o AWS Systems Manager para realizar a atualização automática dos drivers PV. Para obter mais informações, consulte Demonstração: atualizar drivers de PV automaticamente em instâncias do EC2 para Windows no Guia do usuário do AWS Systems Manager.
- Faça o download do pacote de drivers e execute o programa de instalação manualmente. Verifique o arquivo `readme.txt` quanto aos requisitos do sistema. Para obter informações sobre como fazer download e instalar os drivers AWS PV ou se você estiver atualizando um controlador de domínio, consulte Atualizar manualmente as instâncias do Windows Server (atualização do AWS PV).

Histórico do pacote de drivers AWS PV

A tabela a seguir mostra as alterações nos drivers AWS PV para cada versão de driver.

Versão do pacote	Detalhes	Data de lançamento
8.6.0	• Correções de estabilidade nas interações do XenStore.	27 de maio de 2025
8.5.0	• Correções de estabilidade para resolver casos raros de falhas durante a desanexação do dispositivo de rede. • Correções de estabilidade para resolver casos raros de falhas durante a desanexação do volume EBS. • Erros corrigidos no instalador de pacotes. • O instalador do PV foi atualizado para usar `Pnputil`.	31 de outubro de 2024
8.4.3	Erros corrigidos no instalador de pacotes para melhorar a experiência de atualização. Esta é a última versão que pode ser executada no Windows Server 2012 e 2012 R2. Essa versão	24 de janeiro de 2023

Versão do pacote	Detalhes	Data de lançamento
	está disponível para download, mas não tem mais suporte, pois o Windows Server 2012 e 2012 R2 foram descontinuados.	
8.4.2	Correções de estabilidade para lidar com a condição da corrida.	13 de abril de 2022
8.4.1	Instalador de pacotes aprimorado.	7 de janeiro de 2022
8.4.0	• Correções de estabilidade para resolver casos raros de E/S de disco preso. • Correções de estabilidade para resolver casos raros de falhas durante a desanexação do volume EBS. • Recurso adicionado para distribuir carga em vários núcleos para workloads que usam mais de 20.000 IOPS e experimentam degradação devido a gargalos. Para ativar esse recurso, consulte Workloads que usam mais de 20.000 IOPS de disco apresentam degradação devido a gargalos da CPU.	2 de março de 2021
8.3.5	Instalador de pacotes aprimorado. Esta é a última versão que pode ser executada no Windows Server 2008 R2. Esta versão está disponível para download, mas não tem mais suporte. O Windows Server 2008 R2 atingiu o fim da vida útil e não tem mais suporte da Microsoft.	7 de janeiro de 2022
8.3.4	Maior confiabilidade do anexo do dispositivo de rede.	4 de agosto de 2020

Versão do pacote	Detalhes	Data de lançamento
8.3.3	• Atualize para o componente voltado para o XenStore a fim de evitar a verificação de bugs durante os caminhos de manipulação de erros. • Atualize para o componente de armazenamento para evitar falhas quando um SRB inválido for enviado. Para atualizar esse driver em instâncias do Windows Server 2008 R2, é necessário primeiro verificar se os patches apropriad os estão instalados para abordar o seguinte Aviso de segurança da Microsoft: Aviso de segurança da Microsoft 3033929.	4 de fevereiro de 2020
8.3.2	Confiabilidade aprimorada de componentes da rede.	30 de julho de 2019
8.3.1	Melhora na performance e na robustez do componente de armazenamento.	12 de junho de 2019
8.2.7	Maior eficiência para oferecer suporte à migração para os tipos de instância de última geração.	20 de maio de 2019
8.2.6	Eficiência aumentada do caminho de despejo de memória.	15 de janeiro de 2019
8.2.5	Melhorias de segurança adicionais. O instalador do PowerShell agora está disponível no pacote.	12 de dezembro de 2018
8.2.4	Melhorias na confiabilidade.	2 de outubro de 2018
8.2.3	Correções de erros e melhorias na performance. Relate o ID de volume do EBS como o número de série do disco para volumes do EBS. Isso permite cenários de cluster, como o S2D.	29 de maio de 2018

Versão do pacote	Detalhes	Data de lançamento
8.2.1	Melhorias de performance de rede e de armazenamento e várias correções de solidez. Para verificar se esta versão foi instalada, consulte o valor do seguinte registro do Windows: `HKLM\Software\Amazon\PVDriver\Version 8.2.1` .	8 de março de 2018
7.4.3	Adicionado suporte para o Windows Server 2016. Correções de estabilidade para todas as versões dos sistemas operacionais Windows com suporte. *A assinatura da versão 7.4.3 do driver AWS PV expira em 29 de março de 2019. Recomendamos que você atualize para o driver AWS PV mais recente.	18 de nov de 2016
7.4.2	Correções de estabilidade para suporte do tipo de instância X1.	2 de agosto de 2016
7.4.1	• Melhoria da performance no driver AWS PV Storage. • Correções de estabilidade no driver AWS PV Storage: corrigido um problema em que as instâncias sofriam uma paralisação do sistema com o código de verificação de bugs 0x0000DEAD. • Correções de estabilidade no driver AWS PV Network. • Adicionado suporte para o Windows Server 2008R2.	12 de julho de 2016
7.3.2	• Aperfeiçoados o registro em log e o diagnóstico. • Correção de estabilidade no driver AWS PV Storage. Em alguns casos, os discos podem não ser expostos no Windows depois de anexar novamente o disco à instância. • Adicionado suporte para o Windows Server 2012.	24 de junho de 2015

Versão do pacote	Detalhes	Data de lançamento
7.3.1	Atualização TRIM: correção relativa às solicitações TRIM. Essa correção estabiliza as instâncias e melhora a performance da instância ao gerenciar um grande número de solicitações TRIM.	
7.3.0	Suporte TRIM: o driver AWS PV agora envia solicitações TRIM para o hipervisor. Os discos efêmeros processarão adequadamente as solicitações TRIM desde que o armazenam ento subjacente ofereça suporte a TRIM (SSD). Observe que o armazenamento baseado em EBS não oferece suporte a TRIM desde março de 2015.	
7.2.5	• Correção de estabilidade em drivers AWS PV Storage: em alguns casos, o driver AWS PV pode cancelar a referência de memória inválida e causar uma falha de sistema. • Correção de estabilidade ao gerar um despejo de memória: em alguns casos o driver AWS PV trava em um condição de disputa ao gravar um despejo de memória. Antes dessa versão, só era possível resolver o problema forçando o driver a interromper e reiniciar, o que fazia com que o despejo de memória fosse perdido.	
7.2.4	Manutenção do ID de dispositivo: essa correção de driver mascara o ID do dispositivo PCI da plataforma e força o sistema a sempre expor o mesmo ID de dispositivo, mesmo que a instância seja movida. De uma forma mais geral, a correção afeta como o hipervisor expõe dispositivos virtuais. A correção também inclui modificações ao coinstalador dos drivers AWS PV de forma que o sistema mantenha dispositivos virtuais mapeados.	

Versão do pacote	Detalhes	Data de lançamento
7.2.2	• Carga dos drivers AWS PV no modo Directory Services Restore Mode (DSRM): o modo Directory Services Restore é uma opção de inicialização do modo de segurança para controladores de domínio do Windows Server. • Manutenção do ID do dispositivo quando o dispositivo de adaptador de rede virtual é anexado novamente: essa correção força o sistema a verificar o mapeamento de endereço MAC e a manter o ID do dispositivo. Essa correção garante que os adaptadores retenham suas configurações estáticas se os adaptadores forem anexados novamente.	
7.2.1	• Execução no modo de segurança: corrigido o problema em que o driver não era carregado no modo de segurança . Anteriormente, os drivers AWS PV só instanciavam em sistemas de execução normal. • Adição de discos aos grupos de armazenamento do Microsoft Windows: anteriormente, sintetizávamos as consultas da página 83. A correção desabilitou o suporte da página 83. Isso não afeta os grupos de armazenamento que são usados em um ambiente de cluster porque os discos PV não são discos de cluster válidos.	
7.2.0	Base: A versão base do AWS PV.	

Drivers do Citrix PV

Os drivers Citrix PV são armazenados no diretório `%ProgramFiles%\Citrix\XenTools` (instâncias de 32 bits) ou `%ProgramFiles(x86)%\Citrix\XenTools` (instâncias de 64 bits).

Os componentes do driver Citrix PV são listados no Registro do Windows em `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services`. Esses componentes de driver são os seguintes: xenevtchn, xeniface, xennet, Xennet6, xensvc, xenvbd e xenvif.

O Citrix também tem um componente de driver chamado XenGuestAgent, que é executado como um serviço do Windows. Ele lida com tarefas como eventos de desligamento e reinicialização a partir da API. É possível acessar e gerenciar serviços executando `Services.msc` a partir da linha de comando.

Se você estiver encontrando erros de redes ao executar determinadas workloads, precisará desabilitar o recurso de descarregamento de TCP para o driver Citrix PV. Para obter mais informações, consulte Descarregamento de TCP.

Drivers Red Hat PV

Os drivers Red Hat têm suporte para instâncias herdadas, mas não são recomendados em instâncias mais novas com mais de 12 GB de RAM devido às limitações do driver. As instâncias com mais de 12 GB de RAM que executam drivers Red Hat podem não ser iniciadas e se tornar inacessíveis. Recomendamos atualizar os drivers Red Hat para drivers Citrix PV e, em seguida, atualizar os drivers Citrix PV para drivers AWS PV.

Os arquivos de origem para os drivers Red Hat estão no diretório `%ProgramFiles%\RedHat` (instâncias de 32 bits) ou `%ProgramFiles(x86)%\RedHat` (instâncias de 64 bits). Os dois drivers são `rhelnet`, o driver de rede paravirtualizado Red Hat e `rhelscsi`, o driver miniporta SCSI Red Hat.

Assinar notificações do

O Amazon SNS pode notificá-lo quando novas versões dos drivers EC2 para Windows são lançadas. É possível se inscrever para receber essas notificações.

> **Note**
>
> Você deve especificar a região na qual o tópico do SNS foi criado.

Sempre que novos drivers EC2 para Windows são lançados, nós enviamos notificações aos assinantes. Se não desejar mais receber essas notificações, você poderá se desinscrever. Para obter mais informações, consulte Excluir um tópico e uma assinatura do SNS.

Console

Para assinar as notificações do

1. Abra o console do Amazon SNS em https://console.aws.amazon.com/sns/v3/home.

2. Na barra de navegação, altere a região para Leste dos EUA (Norte da Virgínia), se necessário. É necessário selecionar esta região porque as notificações do SNS que você está assinando estão nesta região.
3. No painel de navegação, escolha Subscriptions.
4. Selecione Create subscription.
5. Na caixa de diálogo Criar assinatura, faça o seguinte:
   a. Para o ARN do tópico, copie o seguinte ARN (nome de recurso da Amazon):

      arn:aws:sns:us-east-1:801119661308:ec2-windows-drivers
   b. Para Protocolo, selecione `Email`.
   c. Para Endpoint, digite um endereço de e-mail que é possível usar para receber as notificações.
   d. Selecione Create subscription.
6. Você receberá um e-mail de confirmação. Abra o e-mail e siga as instruções para concluir a sua assinatura.

AWS CLI

Para assinar as notificações do

Use o seguinte comando.

```
aws sns subscribe \
    --topic-arn arn:aws:sns:us-east-1:801119661308:ec2-windows-drivers \
    --region us-east-1 \
    --protocol email \
    --notification-endpoint YourUserName@YourDomainName.ext
```

PowerShell

Para assinar as notificações do

Use o seguinte comando.

```
Connect-SNSNotification `
    -TopicArn 'arn:aws:sns:us-east-1:801119661308:ec2-windows-drivers' `
```

```
    -Region us-east-1 `
    -Protocol email `
    -Endpoint "YourUserName@YourDomainName.ext"
```

Atualizar drivers PV em instâncias do Windows do EC2

Recomendamos que você instale os drivers de PV mais recentes para melhorar a estabilidade e a performance de suas instâncias do EC2 Windows. As instruções desta página ajudam você a fazer download do pacote do driver e executar o programa de instalação.

Para verificar qual driver sua instância do Windows usa

Abra o Gerenciador de dispositivos e visualize Adaptadores de rede. Verifique se o driver do PV é um dos seguintes:

- AWS PV Network Device
- Citrix PV Ethernet Adapter
- Driver Red Hat PV NIC

Requisitos do sistema

Verifique o arquivo `readme.txt` no download quanto aos requisitos do sistema.

Conteúdo

- Atualizar instâncias do Windows Server (atualização do AWS PV) com o Distributor
- Atualizar manualmente as instâncias do Windows Server (atualização do AWS PV)
- Atualizar um controlador de domínio (atualização do AWS PV)
- Atualizar instâncias do Windows Server 2008 e 2008 R2 (atualização do Red Hat para Citrix PV)
- Atualizar o serviço de agente convidado do Citrix Xen

Atualizar instâncias do Windows Server (atualização do AWS PV) com o Distributor

É possível usar o Distributor, um recurso do AWS Systems Manager, para instalar ou atualizar o pacote de drivers do AWS PV. É possível executar a instalação ou atualização uma vez, ou pode executar essas operações de acordo com um cronograma. A opção `In-place update` para Tipo de instalação não é compatível com esse pacote do Distributor.

> **Important**
>
> Se sua instância for um controlador de domínio, consulte Atualizar um controlador de domínio (atualização do AWS PV). O processo de atualização dessas instâncias do controlador de domínio é diferente das edições padrão do Windows.

1. Recomendamos que você crie um backup, caso precise reverter suas alterações.

   > **Tip**
   >
   > Em vez de criar a AMI no console do Amazon EC2, será possível usar o Systems Manager Automation para criar a AMI usando o runbook `AWS-CreateImage`. Para obter mais informações, consulte AWS-CreateImage no Guia do usuário de referência de runbook do AWS Systems Manager Automation.

   a. Quando você interrompe uma instância, os dados em todos os volumes de armazenamento de instâncias são apagados. Antes de interromper uma instância, verifique se você copiou todos os dados necessários dos volumes de armazenamento de instâncias para um armazenamento persistente, como o Amazon EBS ou o Amazon S3.

   b. No painel de navegação, escolha Instances (Instâncias).

   c. Selecione a instância que requer a atualização do driver e escolha Instance state (Estado da instância), Stop Instance (Parar instância).

   d. Depois que a instância for interrompida, selecione a instância, escolha Actions (Ações), Image and templates (Imagem e modelos) e escolha Create image (Criar imagem).

   e. Escolha Instance state (Estado da instância) e Start instance (Iniciar instância).

2. Conectar-se à instância usando o Desktop Remoto. Para obter mais informações, consulte the section called “Conectar-se usando um cliente RDP”.

3. Recomendamos que você deixe offline todos os discos que não sejam do sistema e anote quaisquer mapeamentos de letras de unidade para os discos secundários no Gerenciamento de Disco antes de executar esta atualização. Essa etapa não será necessária se você executar uma atualização no local dos drivers AWS PV. Também recomendamos definir serviços não essenciais como inicialização Manual no console de Services.

4. Para obter instruções sobre como instalar ou atualizar o pacote de drivers do AWS PV usando o Distributor, consulte os procedimentos em Instalar ou atualizar pacotes no Guia do usuário do AWS Systems Manager.
5. Em Nome, escolha AWSPVDriver.
6. Em Tipo de instalação, escolha Desinstalar e reinstalar.
7. Configure os outros parâmetros do pacote conforme necessário e execute a instalação ou a atualização seguindo o procedimento indicado em Step 4.

   Após executar o pacote do Distributor, a instância será reinicializada automaticamente e, em seguida, atualizará o driver. A instância não estará disponível por até 15 minutos.
8. Depois que atualização terminar e a instância for aprovada nas duas verificações de integridade no console do Amazon EC2, conecte-se à instância usando o Remote Desktop e verifique se o novo driver foi instalado.
9. Quando estiver conectado, execute o seguinte comando do PowerShell:

   ```
   Get-ItemProperty HKLM:\SOFTWARE\Amazon\PVDriver
   ```
10. Verifique se a versão do driver é a mesma que a versão mais recente listada na tabela Histórico de versões do driver. Para obter mais informações, consulte Histórico do pacote de drivers AWS PV Abrir o gerenciamento de disco para revisar todos os volumes secundários offline e colocá-los on-line de acordo com as letras de unidade indicadas em Step 3.

Se você desabilitou anteriormente o Descarregamento de TCP usando Netsh para drivers Citrix PV, recomendamos reabilitar esse recurso depois de fazer a atualização para drivers AWS PV. Os problemas de descarregamento de TCP com os drivers Citrix não estão presentes nos drivers AWS PV. Como resultado, o descarregamento de TCP proporciona um melhor performance com os drivers AWS PV.

Se você aplicou anteriormente um endereço IP estático ou a configuração de DNS à interface de rede, pode ser necessário reaplicar o endereço IP estático ou a configuração de DNS depois de atualizar os drivers AWS PV.

Atualizar manualmente as instâncias do Windows Server (atualização do AWS PV)

Use o seguinte procedimento para executar uma atualização no local dos drivers AWS PV ou fazer uma atualização de drivers Citrix PV para drivers AWS PV no Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019 ou Windows

Server 2022. Essa atualização não está disponível para drivers Red Hat nem outras versões do Windows Server.

Algumas versões mais antigas do Windows Server não podem usar os drivers mais recentes. Para verificar qual versão de driver usar para seu sistema operacional, consulte a tabela de versões dos drivers em Drivers paravirtuais para as instâncias do Windows.

> **Important**
>
> Se sua instância for um controlador de domínio, consulte Atualizar um controlador de domínio (atualização do AWS PV). O processo de atualização dessas instâncias do controlador de domínio é diferente das edições padrão do Windows.

Para atualizar manualmente os drivers do AWS PV

1. Recomendamos que você crie um backup, caso precise reverter suas alterações.

   > **Tip**
   >
   > Em vez de criar a AMI no console do Amazon EC2, será possível usar o Systems Manager Automation para criar a AMI usando o runbook `AWS-CreateImage`. Para obter mais informações, consulte AWS-CreateImage no Guia do usuário de referência de runbook do AWS Systems Manager Automation.

   a. Quando você interrompe uma instância, os dados em todos os volumes de armazenamento de instâncias são apagados. Antes de interromper uma instância, verifique se você copiou todos os dados necessários dos volumes de armazenamento de instâncias para um armazenamento persistente, como o Amazon EBS ou o Amazon S3.
   b. No painel de navegação, escolha Instances (Instâncias).
   c. Selecione a instância que requer a atualização do driver e escolha Instance state (Estado da instância), Stop Instance (Parar instância).
   d. Depois que a instância for interrompida, selecione a instância, escolha Actions (Ações), Image and templates (Imagem e modelos) e escolha Create image (Criar imagem).
   e. Escolha Instance state (Estado da instância) e Start instance (Iniciar instância).
2. Conectar-se à instância usando o Desktop Remoto.

3. Recomendamos que você deixe offline todos os discos que não sejam do sistema e anote quaisquer mapeamentos de letras de unidade para os discos secundários no Gerenciamento de Disco antes de executar esta atualização. Essa etapa não será necessária se você executar uma atualização no local dos drivers AWS PV. Também recomendamos definir serviços não essenciais como inicialização Manual no console de Services.
4. Faça o download dos drivers para a sua instância usando uma das seguintes opções:
   - Navegador: faça o download do pacote de drivers mais recente para a instância e extraia o arquivo zip.
   - PowerShell: execute os seguintes comandos:

     ```
     Invoke-WebRequest https://s3.amazonaws.com/ec2-windows-drivers-downloads/AWSPV/Latest/AWSPVDriver.zip -outfile $env:USERPROFILE\pv_driver.zip
     Expand-Archive $env:userprofile\pv_driver.zip -DestinationPath $env:userprofile\pv_drivers
     ```

     Se você receber um erro ao baixar o arquivo e estiver usando o Windows Server 2016 ou anterior, talvez seja necessário habilitar o TLS 1.2 para seu terminal PowerShell. É possível habilitar o TLS 1.2 para a sessão atual do PowerShell com o comando a seguir e tentar novamente:

     ```
     [Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
     ```
5. Executar `AWSPVDriverSetup.msi`.

Depois de executar o MSI, a instância é reinicializada automaticamente e, em seguida, atualiza o driver. A instância não estará disponível por até 15 minutos. Após o término da atualização e a instância passar nas duas verificações de integridade no console do Amazon EC2, será possível verificar se o novo driver foi instalado conectando-se à instância usando o Remote Desktop e executando o seguinte comando do PowerShell:

```
Get-ItemProperty HKLM:\SOFTWARE\Amazon\PVDriver
```

Verifique se a versão do driver é a mesma que a versão mais recente listada na tabela Histórico de versões do driver. Para obter mais informações, consulte Histórico do pacote de drivers AWS PV Abrir o gerenciamento de disco para revisar todos os volumes secundários offline e colocá-los on-line de acordo com as letras de unidade indicadas em Step 3.

Se você desabilitou anteriormente o Descarregamento de TCP usando Netsh para drivers Citrix PV, recomendamos reabilitar esse recurso depois de fazer a atualização para drivers AWS PV. Os problemas de descarregamento de TCP com os drivers Citrix não estão presentes nos drivers AWS PV. Como resultado, o descarregamento de TCP proporciona um melhor performance com os drivers AWS PV.

Se você aplicou anteriormente um endereço IP estático ou a configuração de DNS à interface de rede, pode ser necessário reaplicar o endereço IP estático ou a configuração de DNS depois de atualizar os drivers AWS PV.

Atualizar um controlador de domínio (atualização do AWS PV)

Use o procedimento a seguir em um controlador de domínio para executar uma atualização no local dos drivers AWS PV ou atualizar drivers Citrix PV para drivers AWS PV. Para garantir que suas funções FSMO permaneçam operacionais durante a atualização, recomendamos que você transfira essas funções para outros controladores de domínio antes de iniciar a atualização. Para obter mais informações, consulte Como visualizar e transferir funções FSMO no site do Microsoft Learn.

Para atualizar um controlador de domínio

1. Recomendamos que você crie um backup do seu controlador de domínio no caso de precisar reverter suas alterações. O uso de uma AMI como backup não é aceito. Para obter mais informações, consulte Considerações de backup e restauração na documentação da Microsoft.
2. Execute o comando a seguir para configurar o Windows para ser iniciado no Modo de Restauração dos Serviços de Diretório (DSRM):

   > **Warning**
   >
   > Antes de executar esse comando, confirme a senha do DSRM. Você precisará dessas informações para fazer login na sua instância depois que a atualização estiver concluída e a instância tiver sido reiniciada automaticamente.

   ```
   bcdedit /set {default} safeboot dsrepair
   ```

   PowerShell:

   ```
   PS C:\> bcdedit /set "{default}" safeboot dsrepair
   ```

O sistema deve ser inicializado no DSRM porque o utilitário de atualização remove os drivers de armazenamento Citrix PV para que possa instalar os drivers AWS PV. Por isso, recomendamos que anote quaisquer mapeamentos de letras e pastas de unidade para os discos secundários no Gerenciamento de Disco. Quando os drivers de armazenamento Citrix PV não estiverem presentes, as unidades secundárias não serão detectadas. Os controladores de domínio que usam uma pasta NTDS em unidades secundárias não serão inicializados porque o disco secundário não será detectado.

> **Warning**
>
> Depois de executar esse comando não reinicialize o sistema manualmente. O sistema ficará inacessível porque os drivers Citrix PV não oferecem suporte a DSRM.

3. Execute o comando a seguir para adicionar **`DisableDCCheck`** ao registro:

```
reg add HKLM\SOFTWARE\Wow6432Node\Amazon\AWSPVDriverSetup /v DisableDCCheck /t
 REG_SZ /d true
```

4. Faça o download do pacote de drivers mais recente para a instância e extraia o arquivo zip.
5. Executar `AWSPVDriverSetup.msi`.

   Depois de executar o MSI, a instância é reinicializada automaticamente e, em seguida, atualiza o driver. A instância não estará disponível por até 15 minutos.
6. Após o término da atualização e a instância passar nas duas verificações de integridade no console do Amazon EC2, conecte-se à instância usando o Remote Desktop. Abra o Gerenciamento de disco para revisar todos os volumes secundários offline e colocá-los online correspondendo ao mapeamento de letras e pastas de unidade observado anteriormente.

   É necessário se conectar à instância especificando o nome do usuário no seguinte formato: hostname\administrator. Por exemplo, Win2k12TestBox\administrador.
7. Execute o comando a seguir para remover a configuração de inicialização do DSRM:

```
bcdedit /deletevalue safeboot
```

8. Reinicialize a instância.
9. Para concluir o processo de atualização, verifique se o novo driver foi instalado. Em Device Manager (Gerenciador de dispositivos), em Storage Controllers (Controladores de

armazenamento), localize AWS PV Storage Host Adapter (Adaptador host de armazenamento do PV). Verifique se a versão do driver é a mesma que a versão mais recente listada na tabela Histórico de versões do driver. Para obter mais informações, consulte Histórico do pacote de drivers AWS PV.

10. Execute o comando a seguir para excluir **`DisableDCCheck`** do registro:

```
reg delete HKLM\SOFTWARE\Wow6432Node\Amazon\AWSPVDriverSetup /v DisableDCCheck
```

> **Note**
>
> Se você desabilitou anteriormente o Descarregamento de TCP usando Netsh para drivers Citrix PV, recomendamos reabilitar esse recurso depois de fazer a atualização para drivers AWS PV. Os problemas de descarregamento de TCP com os drivers Citrix não estão presentes nos drivers AWS PV. Como resultado, o descarregamento de TCP proporciona um melhor performance com os drivers AWS PV.

Atualizar instâncias do Windows Server 2008 e 2008 R2 (atualização do Red Hat para Citrix PV)

Antes você começar a atualizar seus drivers Red Hat para drivers Citrix PV, faça o seguinte:

- Instale a versão mais recente do serviço EC2Config. Para obter mais informações, consulte Instalar a versão mais recente do EC2Config.
- Verifique se você tem o Windows PowerShell 3.0 instalado. Para verificar a versão que você instalou, execute o seguinte comando em uma janela do PowerShell:

  ```
  PS C:\> $PSVersionTable.PSVersion
  ```

  O Windows PowerShell 3.0 está incluído no pacote de instalação do Windows Management Framework (WMF) versão 3.0. Se você precisar instalar o Windows PowerShell 3.0, consulte Windows Management Framework 3.0 no Centro de Download da Microsoft.
- Faça backup de suas informações importantes sobre a instância ou crie uma AMI da instância. Para obter mais informações sobre a criação de uma AMI, consulte Criação de uma AMI baseada no Amazon EBS.

> **Tip**
>
> Em vez de criar a AMI no console do Amazon EC2, será possível usar o Systems Manager Automation para criar a AMI usando o runbook `AWS-CreateImage`. Para obter mais informações, consulte AWS-CreateImage no Guia do usuário de referência de runbook do AWS Systems Manager Automation.

Se você criar uma AMI, certifique-se de fazer o seguinte:

- Escreva sua senha.
- Não execute a ferramenta Sysprep manualmente nem usando o serviço EC2Config.
- Defina o adaptador de Ethernet para obter um endereço IP usando automaticamente o DHCP.

Para atualizar drivers Red Hat

1. Conecte-se à instância e faça login como administrador local. Para obter mais informações sobre como se conectar à sua instância, consulte Conectar-se à instância do Windows no usando RDP.
2. Em sua instância, faça download do pacote de atualização do Citrix PV.
3. Extraia o conteúdo dos pacotes de atualização para um local de sua escolha.
4. Clique duas vezes no arquivo Upgrade.bat. Se receber um aviso de segurança, selecione Executar.
5. Na caixa de diálogo Atualizar drivers, revise as informações e selecione Sim se você estiver pronto para iniciar a atualização.
6. Na caixa de diálogo Desinstalador dos drivers paravirtualizados Red Hat para Windows, selecione Sim para remover o software Red Hat. Sua instância será recarregada.

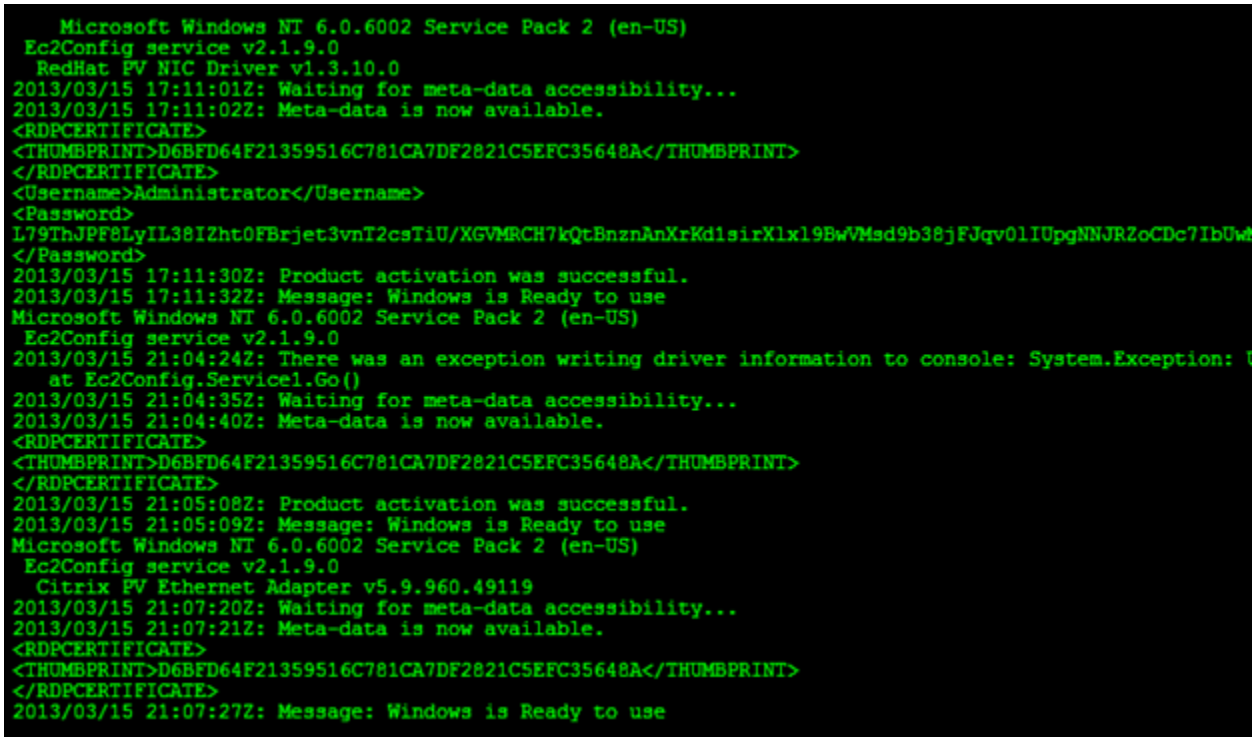
> **Note**
>
> Se você não vir a caixa de diálogo do desinstalador, selecione Red Hat paravirtualizado na barra de tarefas do Windows.

7. Verifique se a instância foi reinicializada e está pronta para uso.

   a. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.

   b. Na página Instances (Instâncias), selecione Actions (Ações), Monitor and troubleshoot (Monitorar e solucionar problemas) e, em seguida, escolha Get system log (Obter log do sistema).

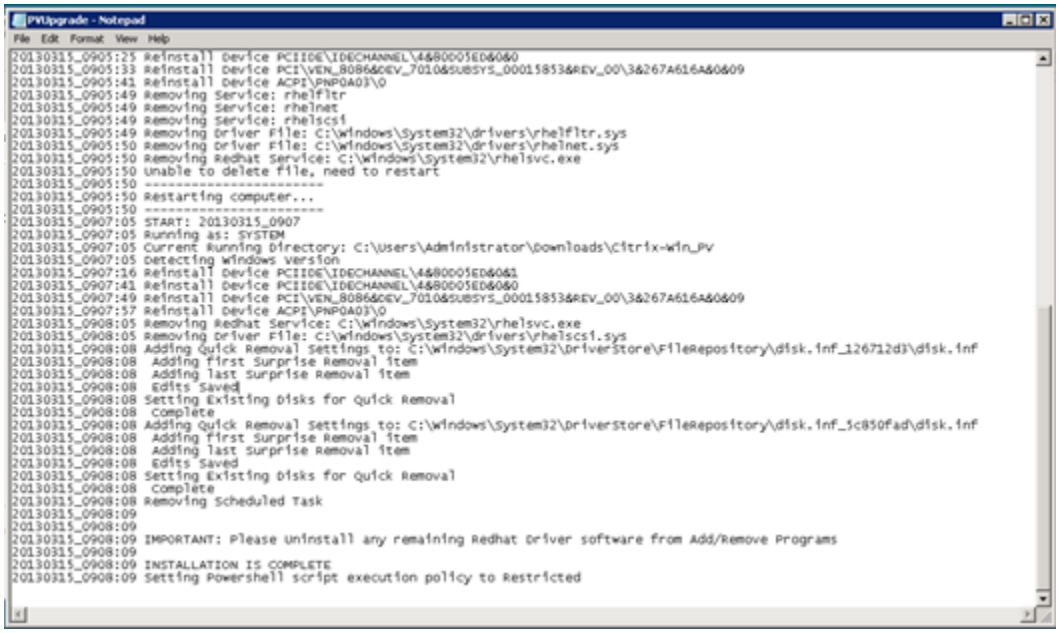
   c. As operações de atualização devem ter reiniciado o servidor 3 ou 4 vezes. É possível ver isso no arquivo de log pelo número de vezes em que `Windows is Ready to use` é exibido.



8. Conecte-se à instância e faça login como administrador local.

9. Feche a caixa de diálogo Desinstalador dos drivers Xen paravirtualizados Red Hat para Windows.

10. Verifique se a instalação foi concluída. Navegue até a pasta `Citrix-WIN_PV` que você extraiu anteriormente, abra o arquivo `PVUpgrade.log` e verifique o texto `INSTALLATION IS COMPLETE`.



Atualizar o serviço de agente convidado do Citrix Xen

Se você estiver usando drivers Citrix PV no Windows Server, será possível atualizar o serviço de agente de convidado do Citrix Xen. Esse serviço do Windows gerencia tarefas como eventos de desligamento e reinicialização a partir da API. É possível executar esse pacote de atualização em qualquer versão do Windows Server, desde que a instância esteja executando drivers Citrix PV.

> **Important**
>
> Para Windows Server 2008 R2 e posterior, recomendamos atualizar para drivers AWS PV que incluem a atualização do agente convidado.

Antes de começar a atualizar seus drivers, faça backup de suas informações importantes sobre a instância ou crie uma AMI a partir da instância. Para obter mais informações sobre a criação de uma AMI, consulte Criação de uma AMI baseada no Amazon EBS.

> **Tip**
>
> Em vez de criar a AMI no console do Amazon EC2, será possível usar o Systems Manager Automation para criar a AMI usando o runbook `AWS-CreateImage`. Para obter mais

informações, consulte AWS-CreateImage no Guia do usuário de referência de runbook do AWS Systems Manager Automation.

Se você criar uma AMI, certifique-se de fazer o seguinte:

- Não habilite a ferramenta Sysprep no serviço EC2Config.
- Escreva sua senha.
- Defina o adaptador de Ethernet como DHCP.

Para atualizar seu serviço de agente convidado do Citrix Xen

1. Conecte-se à instância e faça login como administrador local. Para obter mais informações sobre como se conectar à sua instância, consulte Conectar-se à instância do Windows no usando RDP.
2. Em sua instância, faça download do pacote de atualização do Citrix.
3. Extraia o conteúdo dos pacotes de atualização para um local de sua escolha.
4. Clique duas vezes no arquivo Upgrade.bat. Se receber um aviso de segurança, selecione Executar.
5. Na caixa de diálogo Atualizar drivers, revise as informações e selecione Sim se você estiver pronto para iniciar a atualização.
6. Quando a atualização estiver concluída, o arquivo `PVUpgrade.log` será aberto e conterá o texto `UPGRADE IS COMPLETE`.
7. Reinicie a instância.

Solução de problemas em drivers PV em instâncias do Windows

Veja a seguir soluções para problemas que podem ser encontrados com imagens do Amazon EC2 e drivers de PV mais antigos.

Tópicos

- O Windows Server 2012 R2 perde a conectividade de rede e armazenamento após a reinicialização de uma instância
- Descarregamento de TCP
- Sincronização de horário

- Workloads que usam mais de 20.000 IOPS de disco apresentam degradação devido a gargalos da CPU

O Windows Server 2012 R2 perde a conectividade de rede e armazenamento após a reinicialização de uma instância

> **Important**
>
> Esse problema ocorre somente com AMIs disponibilizadas antes de setembro de 2014.

As Imagens de máquina da Amazon (AMIs) do Windows Server 2012 R2 disponibilizadas antes de 10 de setembro de 2014 podem perder conectividade de rede e armazenamento após a reinicialização da instância. O erro no log do sistema do Console de gerenciamento da AWS indica: "Dificuldade em detectar detalhes do driver PV para a saída do console". A perda de conectividade é causada pelo recurso Limpeza de plug and play. Esse recurso verifica e desabilita dispositivos inativos do sistema a cada 30 dias. O recurso identifica incorretamente o dispositivo de rede EC2 como inativo e o remove do sistema. Quando isso ocorre, a instância perde a conectividade de rede após uma reinicialização.

Para sistemas que você suspeita estar sendo afetados por esse problema, é possível fazer download e executar uma atualização de driver no local. Caso não seja possível executar a atualização de driver no local, é possível executar um script auxiliar. O script determina se sua instância foi afetada. Se ela tiver sido afetada, e o dispositivo de rede do Amazon EC2 não tiver sido removido, o script desabilitará a verificação da Limpeza de plug and play. Se o dispositivo de rede tiver sido removido, o script reparará o dispositivo, desabilitará a verificação do recurso Limpeza de plug and play e permitirá que sua instância seja reinicializada com a conectividade de rede habilitada.

Tópicos

- Escolher como corrigir problemas
- Método 1 – Redes aprimoradas
- Método 2 – Configuração do Registro
- Executar o script de correção

Escolher como corrigir problemas

Há dois métodos para restaurar a conectividade de rede e de armazenamento em uma instância afetada por esse problema. Escolha um dos seguintes métodos:

Método	Pré-requisitos	Visão geral do procedimento
Método 1 – Redes aprimoradas	As redes aprimoradas só estão disponíveis em uma nuvem privada virtual (VPC) que exija um tipo de instância C3. Se o servidor não usar atualmente o tipo de instância C3, altere-o temporariamente.	Você altera o tipo de instância do servidor em uma instância C3. Em seguida, as redes aprimoradas permitem a você se conectar à instância afetada e corrigir o problema. Depois de corrigir o problema, você altera a instância de volta para o tipo original. Esse método é geralmente mais rápido do que o método 2 e tem menos probabilidade de resultar em erro do usuário. Haverá cobranças adicionais pelo período de execução da instância C3.
Método 2 – Configuração do Registro	Capacidade de criar ou acessar um segundo servidor. Capacidade de alterar as configurações do Registro.	Você desanexa o volume raiz da instância afetada, anexa-o a outra instância, conecta-se e faz alterações no Registro. Haverá cobranças adicionais pelo período de execução do servidor adicional. Esse método é mais lento do que o método 1, mas ele funcionou em situações nas quais o método 1 não resolveu o problema.

Método 1 – Redes aprimoradas

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Localize a instância afetada. Selecione a instância e escolha Instance state (Estado da instância) e, em seguida, escolha Stop instance (Interromper instância).

   > **Warning**
   >
   > Quando você interrompe uma instância, os dados em todos os volumes de armazenamento de instâncias são apagados. Para manter dados longe dos volumes de armazenamento de instância, faça backup no armazenamento persistente.

4. Depois de interromper a instância, crie um backup. Selecione a instância e escolha Actions (Ações), Image and templates (Imagem e modelos) e escolha Create image (Criar imagem).
5. Altere o tipo de instância para qualquer tipo de instância C3.
6. Inicie a instância.
7. Conecte-se à instância usando o Desktop Remoto e faça download do pacote de atualização de drivers AWS PV na instância.
8. Extraia o conteúdo da pasta e execute `AWSPVDriverSetup.msi`.

   Depois de executar o MSI, a instância é reinicializada automaticamente e, em seguida, atualiza os drivers. A instância não estará disponível por até 15 minutos.
9. Após o término da atualização e a instância passar nas duas verificações de integridade no console do Amazon EC2, conecte-se à instância usando o Remote Desktop e verifique se os novos drivers foram instalados. Em Device Manager (Gerenciador de dispositivos), em Storage Controllers (Controladores de armazenamento), localize AWS PV Storage Host Adapter (Adaptador host de armazenamento do PV). Verifique se a versão do driver é a mesma que a versão mais recente listada na tabela Histórico de versões do driver. Para obter mais informações, consulte Histórico do pacote de drivers AWS PV.
10. Interrompa a instância e altere-a de volta para seu tipo original.
11. Inicie a instância e retome o uso normal.

Método 2 – Configuração do Registro

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

2. No painel de navegação, escolha Instances (Instâncias).
3. Localize a instância afetada. Selecione a instância, escolha Instance state (Estado da instância) e, em seguida, escolha Stop instance (Interromper instância).

> **Warning**
>
> Quando você interrompe uma instância, os dados em todos os volumes de armazenamento de instâncias são apagados. Para manter dados longe dos volumes de armazenamento de instância, faça backup no armazenamento persistente.

4. Escolha Launch instance (Executar instâncias) e crie uma instância temporária Windows Server 2008 ou Windows Server 2012 na mesma zona de disponibilidade que a instância afetada. Não crie uma instância do Windows Server 2012 R2.

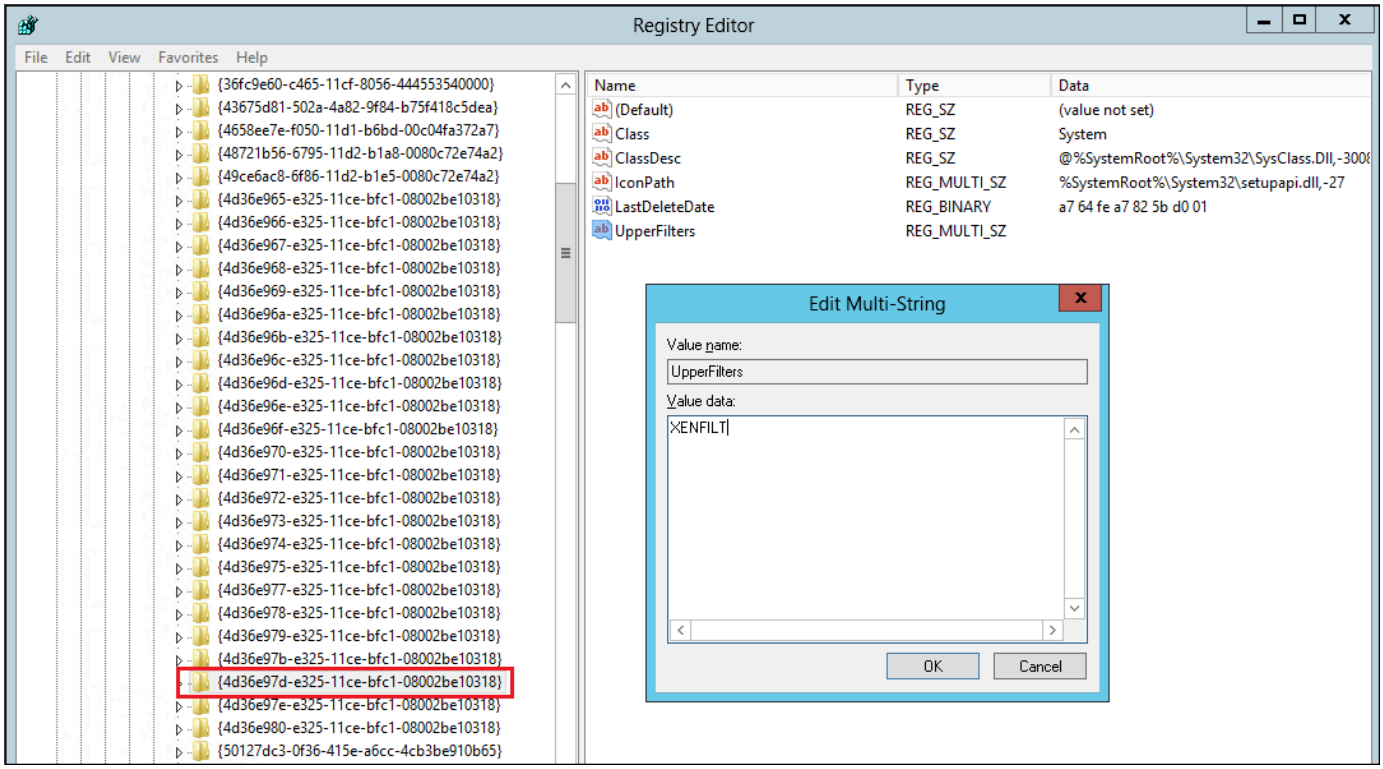
> **Important**
>
> Se você não criar a instância na mesma zona de disponibilidade que a instância afetada, não conseguirá associar o volume do dispositivo raiz da instância afetada à nova instância.

5. No painel de navegação, escolha Volumes.
6. Localize o volume do dispositivo raiz da instância afetada. Desanexe o volume e anexe o volume à instância temporária criada anteriormente. Associe-a com o nome do padrão do dispositivo (xvdf).
7. Use o Desktop Remoto para se conectar à instância temporária e use em utilitário Gerenciamento de Disco para disponibilizar o volume para uso.
8. Na instância temporária, abra a caixa de diálogo Run (Executar), digite **`regedit`** e pressione Enter.
9. No painel de navegação do Editor de Registro, escolha HKEY_Local_Machine e no menu Arquivo escolha Carregar Hive.
10. Na caixa de diálogo Carregar Hive, navegue até Volume afetado\Windows\System32\config \System e digite um nome temporário na caixa de diálogo Nome da chave. Por exemplo, digite OldSys.
11. No painel de navegação do Editor de Registro, localize as seguintes chaves:

HKEY_LOCAL_MACHINE***your_temporary_key_name**\ControlSet001\Control\Class\4d36e97d-e325-11ce-bfc1-08002be10318

HKEY_LOCAL_MACHINE***your_temporary_key_name**\ControlSet001\Control\Class\4d36e96a-e325-11ce-bfc1-08002be10318

12. Para cada chave, clique duas vezes em UpperFilters, digite um valor de XENFILT e, em seguida, selecione OK.



13. Localize a seguinte chave:

HKEY_LOCAL_MACHINE***your_temporary_key_name**\ControlSet001\Services\XENBUS\Parameters

14. Crie uma nova string (REG_SZ) com o nome ActiveDevice e o seguinte valor:

PCI\VEN_5853&DEV_0001&SUBSYS_00015853&REV_01

15. Localize a seguinte chave:

HKEY_LOCAL_MACHINE***your_temporary_key_name**\ControlSet001\Services\XENBUS

16. Altere a contagem de 0 para 1.
17. Localize e exclua as seguintes chaves:

HKEY_LOCAL_MACHINE***your_temporary_key_name**\ControlSet001\Services\xenvbd\StartOverride

HKEY_LOCAL_MACHINE ***your_temporary_key_name**\ControlSet001\Services\xenfilt\StartOverride

18. No painel de navegação do Editor de Registro, escolha a chave temporária que você criou quando abriu pela primeira vez o Editor de Registro.
19. No menu Arquivo, escolha Descarregar Hive.
20. No utilitário de Gerenciamento de Disco, escolha a unidade que você associou anteriormente, abra o menu contextual (botão direito do mouse) e escolha Offline.
21. No console do Amazon EC2, desanexe o volume afetado de instância temporária e reanexe-o à sua instância do Windows Server 2012 R2 com o nome de dispositivo /dev/sda1. Especifique o nome desse dispositivo para designar o volume como volume do dispositivo raiz.
22. Inicie a instância.
23. Conecte-se à instância usando o Desktop Remoto e faça download do pacote de atualização de drivers AWS PV na instância.
24. Extraia o conteúdo da pasta e execute `AWSPVDriverSetup.msi`.

    Depois de executar o MSI, a instância é reinicializada automaticamente e, em seguida, atualiza os drivers. A instância não estará disponível por até 15 minutos.
25. Após o término da atualização e a instância passar nas duas verificações de integridade no console do Amazon EC2, conecte-se à instância usando o Remote Desktop e verifique se os novos drivers foram instalados. Em Device Manager (Gerenciador de dispositivos), em Storage Controllers (Controladores de armazenamento), localize AWS PV Storage Host Adapter (Adaptador host de armazenamento do PV). Verifique se a versão do driver é a mesma que a versão mais recente listada na tabela Histórico de versões do driver. Para obter mais informações, consulte Histórico do pacote de drivers AWS PV.
26. Exclua ou interrompa a instância temporária que você criou nesse procedimento.

Executar o script de correção

Caso não seja possível executar uma atualização de driver no local nem migrar para uma instância mais nova, é possível executar o script de correção para corrigir os problemas causados pela tarefa da Limpeza de plug and play.

Para executar o script de correção

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Escolha a instância para a qual você deseja executar o script de correção. Escolha Instance State (Estado da instância) e, em seguida, escolha Stop Instance (Interromper instância).

   > **Warning**
   >
   > Quando você interrompe uma instância, os dados em todos os volumes de armazenamento de instâncias são apagados. Para manter dados longe dos volumes de armazenamento de instância, faça backup no armazenamento persistente.

4. Depois de interromper a instância, crie um backup. Selecione a instância, escolha Actions (Ações), Image and templates (Imagem e modelos) e, em seguida, escolha Create image (Criar imagem).
5. Escolha Instance state (Estado da instância) e, em seguida, escolha Start Instance (Iniciar instância).
6. Conecte-se à instância usando o Desktop Remoto e, em seguida, faça download da pasta RemediateDriverIssue.zip na instância.
7. Extraia o conteúdo da pasta.
8. Execute o script de correção de acordo com as instruções no arquivo Readme.txt. O arquivo está localizado na pasta onde você extraiu o RemediateDriverIssue.zip.

Descarregamento de TCP

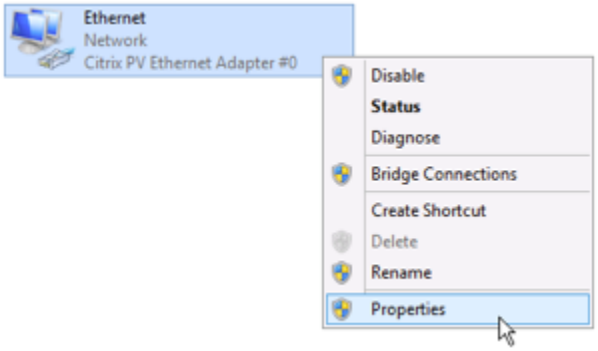
> **Important**
>
> Esse problema não se aplica a instâncias que executam drivers de rede AWS PV ou Intel.

Por padrão, o descarregamento TCP é habilitado para os drivers Citrix PV em AMIs do Windows. Se você encontrar erros no nível do transporte ou na transmissão de pacotes (conforme esteja visível no monitor de performance do Windows)—por exemplo, quando você estiver executando determinadas workloads do SQL—talvez seja necessário desabilitar esse recurso.

> **Warning**
>
> Desabilitar o descarregamento TCP pode reduzir a performance de rede de sua instância.

Para desabilitar o descarregamento TCP para Windows Server 2012 e 2008

1. Conecte-se à instância e faça login como administrador local.
2. Se você estiver usando o Windows Server 2012, pressione Ctrl+Esc para acessar a tela Iniciar e, em seguida, selecione Painel de controle. Se você estiver usando o Windows Server 2008, escolha Iniciar e selecione Painel de controle.
3. Escolha Rede e Internet e, em seguida, Central de Rede e Compartilhamento.
4. Selecione Alterar configurações de adaptador.
5. Clique com o botão direito do mouse em Adaptador de rede Citrix PV Ethernet nº 0 e selecione Propriedades.



6. Na caixa de diálogo Propriedades de conexão de área local, selecione Configurar para abrir a caixa de diálogo Propriedades do adaptador Citrix PV Ethernet nº 0.
7. Na guia Avançado, desabilite cada uma das propriedades, exceto Valor correto da soma de verificação TCP/UDP. Para desabilitar uma propriedade, seleciona-a em Propriedade e escolha Desabilitado em Valor.
8. Escolha OK.
9. Execute os comandos a seguir em uma janela do prompt de comando.

```
netsh int ip set global taskoffload=disabled
netsh int tcp set global chimney=disabled
netsh int tcp set global rss=disabled
netsh int tcp set global netdma=disabled
```

10. Reinicialize a instância.

Sincronização de horário

Antes da versão de 13/02/2013, a AMI do Windows, o agente convidado do Citrix Xen poderiam definir a hora do sistema incorretamente. Isso pode fazer com que seu locação de DHCP expire. Se você tiver problemas para se conectar à sua instância, talvez precise atualizar o agente.

Para determinar se você tem o agente convidado do Citrix Xen atualizado, verifique se a data do arquivo `C:\Program Files\Citrix\XenGuestAgent.exe` é a partir de março de 2013. Se a data nesse arquivo for anterior, atualize o serviço do agente convidado do Citrix Xen. Para obter mais informações, consulte Atualizar o serviço de agente convidado do Citrix Xen.

Workloads que usam mais de 20.000 IOPS de disco apresentam degradação devido a gargalos da CPU

É possível ser afetado por esse problema se estiver usando instâncias do Windows que executam os drivers AWS PV que usam mais de 20.000 IOPS, e se você encontrar o código `0x9E: USER_MODE_HEALTH_MONITOR` de verificação de bugs.

As leituras e gravações de disco (E/S) nos drivers AWS PV ocorrem em duas fases: Preparação de E/S e Conclusão de E/S. Por padrão, a fase de preparação é executada em um único núcleo arbitrário. A fase de conclusão é executada no núcleo `0`. A quantidade de computação necessária para processar uma E/S varia de acordo com o tamanho e outras propriedades. Algumas E/S usam mais computação na fase de preparação, e outras na fase de conclusão. Quando uma instância gera mais de 20.000 IOPS, a fase de preparação ou conclusão pode resultar em um gargalo, em que a CPU na qual ela é executada está com 100% de capacidade. Se a fase de preparação ou conclusão se torna ou não um gargalo depende das propriedades de E/S usadas pela aplicação.

Começando nos drivers AWS PV 8.4.0, a carga da fase de preparação e de conclusão podem ser distribuídas por vários núcleos, eliminando gargalos. Cada aplicação usa diferentes propriedades de E/S. Portanto, a adoção de uma das configurações a seguir pode aumentar, reduzir ou não afetar a performance da aplicação. Depois de aplicar qualquer uma dessas configurações, monitore a aplicação para verificar se ela está proporcionando a performance desejada.

1. Pré-requisitos

   Antes de iniciar este procedimento de solução de problemas, verifique os seguintes pré-requisitos:

- A instância usa drivers AWS PV versão 8.4.0 ou posterior. Para atualizar, consulte Atualizar drivers PV em instâncias do Windows do EC2.
- Você tem acesso RDP à instância. Para conhecer as etapas para se conectar à instância baseada no Windows usando RDP, consulte Conexão com a instância do Windows usando um cliente RDP.
- Você tem acesso de administrador na instância.

2. Observe a carga da CPU na instância

   É possível usar o Gerenciador de Tarefas do Windows para visualizar a carga em cada CPU, a fim de determinar possíveis gargalos na E/S do disco.

   1. Verifique se a aplicação está executando e lidando com o tráfego semelhante à workload de produção.
   2. Conecte-se à sua instância usando RDP.
   3. Clique no menu Start (Iniciar) na sua instância.
   4. Insira `Task Manager` no menu Iniciar para abrir o Gerenciador de Tarefas.
   5. Se o Gerenciador de tarefas mostrar a exibição Summary (Resumo), clique em More details (Mais detalhes) para expandir a exibição detalhada.
   6. Escolha a guia Performance.
   7. Selecione a CPU no painel esquerdo.
   8. Clique com o botão direito do mouse no gráfico do painel principal e selecione Change graph to (Alterar gráfico para) > Logical processors (Processadores lógicos) para exibir cada núcleo individual.
   9. Dependendo de quantos núcleos estiverem na instância, com o passar do tempo será possível ver linhas exibindo a carga da CPU, ou poderá ver somente um número.
      - Se forem exibidos gráficos da carga ao longo do tempo, procure CPUs onde a caixa esteja quase totalmente sombreada.
      - Se um número for exibido em cada núcleo, procure por núcleos que consistentemente mostrem 95% ou mais.
   10. Observe se o núcleo `0` ou um núcleo diferente está experimentando uma carga pesada.

3. Escolha qual configuração aplicar

Nome da configuração	Quando aplicar esta configuração	Observações
Default configuration	A workload está gerando menos de 20.000 IOPS, ou outras configurações não melhoraram a performance ou a estabilidade.	Para essa configuração, a E/S ocorre em alguns núcleos, o que pode beneficiar workloads menores, aumentando a localidade do cache e reduzindo a comutação de contexto.
Allow driver to choose whether to distribute completion	A workload está gerando mais de 20.000 IOPS e uma carga moderada ou alta é observada no núcleo `0`.	Essa configuração é recomendada para todas as instâncias Xen que usam o PV 8.4.0 ou posterior, e que usam mais de 20.000 IOPS, independentemente de problemas serem encontrados ou não.
Distribute both preparation and completion	A workload está gerando mais de 20.000 IOPS. Ou a permissão para o driver escolher a distribuição não melhorou a performance, ou um núcleo diferente de `0` está experimentando uma alta carga.	Esta configuração permite a distribuição da preparação de E/S e da conclusão de E/S.

> **Note**
>
> Recomendamos que você não distribua a preparação de E/S sem também distribuir a conclusão de E/S (configuração `DpcRedirection` sem configuração

`NotifierDistributed`) porque a fase de conclusão é sensível à sobrecarga na fase de preparação, quando a fase de preparação estiver ocorrendo em paralelo.

Valores de chave do Registro

- NotifierDistributed

  Valor `0` ou não presente — A fase de conclusão será executada no núcleo `0`.

  Valor 1 — O driver escolhe executar a fase de conclusão, o núcleo `0` ou um núcleo adicional por disco conectado.

  Valor 2 — O driver executa a fase de conclusão em um núcleo adicional por disco conectado.
- DpcRedirection

  Valor `0` ou não presente — A fase de preparação será executada em um único núcleo arbitrário.

  Valor 1 — A fase de preparação é distribuída entre vários núcleos.

Configuração padrão

Aplique a configuração padrão com as versões de driver AWS PV anteriores à 8.4.0 ou se a degradação da performance ou da estabilidade for observada após a aplicação de uma das outras configurações nesta seção.

1. Conecte-se à sua instância usando RDP.
2. Abra um novo prompt de comando do PowerShell como um administrador.
3. Execute os seguintes comandos para remover as chaves de registro `NotifierDistributed` e `DpcRedirection`.

```
Remove-ItemProperty -Path HKLM:\System\CurrentControlSet\Services\xenvbd
\Parameters -Name NotifierDistributed
```

```
Remove-ItemProperty -Path HKLM:\System\CurrentControlSet\Services\xenvbd
\Parameters -Name DpcRedirection
```

4. Reinicie a instância.

Permitir que o driver escolha se deseja distribuir a conclusão

Defina a chave de registro `NotiferDistributed` para permitir que o driver de armazenamento PV escolha se deve ou não distribuir a conclusão de E/S.

1. Conecte-se à sua instância usando RDP.
2. Abra um novo prompt de comando do PowerShell como um administrador.
3. Use o comando a seguir para adicionar a chave de registro `NotiferDistributed`.

```
Set-ItemProperty -Type DWORD -Path HKLM:\System\CurrentControlSet\Services\xenvbd
\Parameters -Value 0x00000001 -Name NotifierDistributed
```

4. Reinicie a instância.

Distribuir a preparação e a conclusão

Defina as chaves de registro `NotifierDistributed` e `DpcRedirection` para sempre distribuir as fases de preparação e conclusão.

1. Conecte-se à sua instância usando RDP.
2. Abra um novo prompt de comando do PowerShell como um administrador.
3. Execute os seguintes comandos para definir as chaves de registro `NotifierDistributed` e `DpcRedirection`.

```
Set-ItemProperty -Type DWORD -Path HKLM:\System\CurrentControlSet\Services\xenvbd
\Parameters -Value 0x00000002 -Name NotifierDistributed
```

```
Set-ItemProperty -Type DWORD -Path HKLM:\System\CurrentControlSet\Services\xenvbd
\Parameters -Value 0x00000001 -Name DpcRedirection
```

4. Reinicie a instância.

AWSDrivers NVMe

Os volumes do Amazon EBS e volumes de armazenamento de instâncias são expostos como dispositivos de blocos NVMe em instâncias baseadas em Nitro. Para utilizar totalmente a performance e as capacidades dos recursos do Amazon EBS para volumes expostos como dispositivos de blocos NVMe, a instância deve ter o driver AWS NVMe instalado. Todas as AMIs Windows AWS da geração atual vêm com o driver AWS NVMe instalado por padrão.

Para obter mais informações sobre o EBS e o NVMe, consulte Amazon EBS e NVMe no Guia do usuário do Amazon EBS. Para obter mais informações sobre armazenamento de instâncias em SSD e o NVMe, consulte Volumes de armazenamento de instância SSD para instâncias do EC2.

Instâncias do Linux

As seguintes AMIs incluem os drivers NVMe necessários:

- Amazon Linux 2
- Amazon Linux AMI 2018.03
- Ubuntu 14.04 ou posterior com kernel `linux-aws`

> **Note**
>
> Os tipos de instância baseados no AWS Graviton requerem o Ubuntu 18.04 ou posterior com kernel `linux-aws`

- Red Hat Enterprise Linux 7.4 ou posterior
- SUSE Linux Enterprise Server 12 SP2 ou posterior
- CentOS 7.4.1708 ou posterior
- FreeBSD 11.1 ou posterior
- Debian GNU/Linux 9 ou posterior

Como confirmar se a instância tem o driver NVMe

É possível confirmar se sua instância tem o driver NVMe usando o comando a seguir.

- Amazon Linux, RHEL, CentOS e SUSE Linux Enterprise Server

```
$ modinfo nvme
```

  Se a instância tiver o driver NVMe, o comando retornará informações sobre o driver.

- Amazon Linux 2 e Ubuntu

```
$ ls /sys/module/ | grep nvme
```

  Se a instância tiver o driver NVMe, o comando retornará os drivers instalados.

Como atualizar o driver NVMe

Se sua instância tiver o driver NVMe, será possível atualizar o driver para a versão mais recente usando o procedimento a seguir.

1. Conecte-se à sua instância.
2. Atualize o cache de pacotes para obter as atualizações de pacotes necessárias da seguinte forma:

   - Para Amazon Linux 2, Amazon Linux, CentOS e Red Hat Enterprise Linux:

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

   - Para Ubuntu e Debian:

     ```
     [ec2-user ~]$ sudo apt-get update -y
     ```

3. Ubuntu 16.04 ou posterior incluem o pacote `linux-aws`, que contém os drivers NVMe e ENA exigidos pelas instâncias baseadas em Nitro. Atualize o pacote `linux-aws` para receber a versão mais recente da seguinte forma:

   ```
   [ec2-user ~]$ sudo apt-get install --only-upgrade -y linux-aws
   ```

   Para o Ubuntu 14.04, é possível instalar o pacote mais recente `linux-aws` da seguinte maneira:

   ```
   [ec2-user ~]$ sudo apt-get install linux-aws
   ```

4. Reinicialize sua instância para carregar a versão mais recente do kernel.

```
sudo reboot
```

5. Reconecte-se à sua instância depois de reinicializá-la.

Instâncias do Windows

PowerShell

Se você não iniciou sua instância usando uma das últimas AMIs da AWS para o Windows, que são fornecidas pela Amazon, use o procedimento apresentado a seguir para instalar o driver atual da AWS NVMe na sua instância. É necessário reiniciar a instância após a instalação. O script de instalação reiniciará sua instância ou você deverá reiniciá-la como a etapa final.

Pré-requisitos

- A versão 3.0 ou posterior do PowerShell está instalada.
- Os comandos descritos nesta seção devem ser executados na versão de 64 bits do PowerShell. Não use a versão x86 do PowerShell. Essa é a versão de 32 bits do shell e não é compatível com esses comandos.

Para fazer download e instalar o driver AWS NVMe mais recente

1. Recomendamos que você crie uma AMI como backup da seguinte forma, caso precise reverter suas alterações.

   a. Quando você interrompe uma instância, os dados em todos os volumes de armazenamento de instâncias são apagados. Antes de interromper uma instância, verifique se você copiou todos os dados necessários dos volumes de armazenamento de instâncias para um armazenamento persistente, como o Amazon EBS ou o Amazon S3.
   b. No painel de navegação, escolha Instances (Instâncias).
   c. Selecione a instância que requer a atualização do driver e escolha Instance state (Estado da instância), Stop Instance (Parar instância).
   d. Depois que a instância for interrompida, selecione a instância, escolha Actions (Ações), Image and templates (Imagem e modelos) e escolha Create image (Criar imagem).
   e. Escolha Instance state (Estado da instância) e Start instance (Iniciar instância).

2. Conecte-se à instância e faça login como administrador local.
3. Faça o download dos drivers para a sua instância usando uma das seguintes opções:
   - Navegador: faça o download do pacote de drivers mais recente para a instância e extraia o arquivo zip.
   - PowerShell: execute os seguintes comandos:

     ```
     Invoke-WebRequest https://s3.amazonaws.com/ec2-windows-drivers-downloads/
     NVMe/Latest/AWSNVMe.zip -outfile $env:USERPROFILE\nvme_driver.zip
     Expand-Archive $env:userprofile\nvme_driver.zip -DestinationPath
      $env:userprofile\nvme_driver
     ```

     Se você receber um erro ao baixar o arquivo e estiver usando o Windows Server 2016 ou anterior, talvez seja necessário habilitar o TLS 1.2 para seu terminal PowerShell. É possível habilitar o TLS 1.2 para a sessão atual do PowerShell com o comando a seguir e tentar novamente:

     ```
     [Net.ServicePointManager]::SecurityProtocol =
      [Net.SecurityProtocolType]::Tls12
     ```
4. Instale o driver em sua instância executando o script do PowerShell `install.ps1` do diretório `nvme_driver` (`.\install.ps1`). Se você receber um erro, verifique se está usando o PowerShell 3.0 ou posterior.

   a. (Opcional) A partir da versão AWS NVMe`1.5.0`, as reservas persistentes Small Computer System Interface (SCSI) são suportadas para o Windows Server 2016 e versões posteriores. Esse recurso adiciona suporte ao Windows Server Failover Clustering com armazenamento compartilhado do Amazon EBS. Por padrão, esse recurso não está ativado durante a instalação.

   É possível ativar o recurso ao executar o `install.ps1` script para instalar o driver especificando o `EnableSCSIPersistentReservations` parâmetro com um valor de`$true`.

   ```
   PS C:\> .\install.ps1 -EnableSCSIPersistentReservations $true
   ```

   É possível desativar o recurso ao executar o `install.ps1` script para instalar o driver especificando o `EnableSCSIPersistentReservations` parâmetro com um valor de`$false`.

```
PS C:\> .\install.ps1 -EnableSCSIPersistentReservations $false
```

b. Começando com o AWS NVMe`1.5.0`, o `install.ps1` script sempre instala a `ebsnvme-id` ferramenta com o driver.

(Opcional) Para as versões `1.4.0`1.4.1,`1.4.2`, e, o `install.ps1` script permite que você especifique se a `ebsnvme-id` ferramenta deve ser instalada com o driver.

i. Para instalar a ferramenta `ebsnvme-id`, especifique `InstallEBSNVMeIdTool 'Yes'`.

ii. Se você não quiser instalar a ferramenta, especifique `InstallEBSNVMeIdTool 'No'`.

Se você não especificar `InstallEBSNVMeIdTool` e a ferramenta já está presente em `C:\ProgramData\Amazon\Tools`, o pacote atualizará a ferramenta por padrão. Se a ferramenta não estiver presente, o `install.ps1` não atualizará a ferramenta por padrão.

Se você não quiser instalar a ferramenta como parte do pacote, e quiser instalá-la mais tarde, você pode encontrar a versão mais recente ou a ferramenta no pacote do driver. Como alternativa, você pode baixar a versão `1.0.0` do Amazon S3:

Baixe a `ebsnvme-id` ferramenta.

5. Se o instalador não reinicializar sua instância, reinicie-a.

Distributor

É possível usar o distribuidor, um recurso do AWS Systems Manager, para instalar o pacote de drivers do NVMe uma vez ou com atualizações programadas.

Para instalar o driver AWS NVMe mais recente

1. Para obter instruções sobre como instalar o pacote de drivers do NVMe usando o distribuidor, consulte os procedimentos em Instalar ou atualizar pacotes no Guia do usuário do Amazon EC2 Systems Manager.
2. Em Tipo de instalação, escolha Desinstalar e reinstalar.
3. Em Nome, escolha AWSNVMe.

4. (Opcional) Em Argumentos adicionais, é possível personalizar a instalação especificando valores. Os valores devem ser formatados usando uma sintaxe JSON válida. Para obter exemplos de como passar argumentos adicionais para o pacote `aws configure`, consulte a Referência de plugin de documento do comando.

   a. Começando com o AWS NVMe`1.5.0`, o driver oferece suporte a reservas persistentes SCSI para Windows Server 2016 e versões posteriores. Por padrão, esse recurso não está ativado durante a instalação.

      - Para habilitar esse recurso, especifique `{"SSM_EnableSCSIPersistentReservations": "true"}`.
      - Se você não quiser habilitar esse recurso, especifique `{"SSM_EnableSCSIPersistentReservations": "false"}`.

   b. Começando com o AWS NVMe`1.5.0`, o `install.ps1` script sempre instalará a `ebsnvme-id` ferramenta.

      (Opcional) Para as versões`1.4.0`,,`1.4.1`, e`1.4.2`,, o `install.ps1` script permite que você especifique se a ferramenta ebsnvme-id deve ser instalada com o driver.

      - Para instalar a ferramenta ebsnvme-id, especifique `{"SSM_InstallEBSNVMeIdTool": "Yes"}`.
      - Se você não quiser instalar a ferramenta, especifique `{"SSM_InstallEBSNVMeIdTool": "No"}`.

      Se `SSM_InstallEBSNVMeIdTool` não for especificado em Additional Arguments (Argumentos adicionais) e a ferramenta já está presente em `C:\ProgramData\Amazon\Tools`, o pacote atualizará a ferramenta por padrão. Se a ferramenta não estiver presente, o pacote não atualizará a ferramenta por padrão.

      Se você não quiser instalar a ferramenta como parte do pacote, e quiser instalá-la mais tarde, você pode encontrar a versão mais recente da ferramenta no pacote do driver. Como alternativa, você pode baixar a versão `1.0.0` do Amazon S3:

      Baixe a `ebsnvme-id` ferramenta.

5. Se o instalador não reinicializar sua instância, reinicie-a.

Configurar reservas persistentes SCSI para instâncias do Windows

Depois que a versão do driver AWS NVMe `1.5.0` ou posterior for instalada, será possível habilitar ou desabilitar as reservas persistentes de SCSI usando o registro do Windows para Windows Server 2016 e versões posteriores. Você deve reiniciar a instância de banco de dados antes que a alteração entre em vigor.

É possível habilitar reservas persistentes de SCSI com o comando a seguir, que define `EnableSCSIPersistentReservations` o como um valor de`1`.

```
PS C:\> $registryPath = "HKLM:\SYSTEM\CurrentControlSet\Services\AWSNVMe\Parameters
\Device"
Set-ItemProperty -Path $registryPath -Name EnableSCSIPersistentReservations -Value 1
```

É possível desativar as reservas persistentes de SCSI com o comando a seguir, que define `EnableSCSIPersistentReservations` o como um valor de`0`.

```
PS C:\> $registryPath = "HKLM:\SYSTEM\CurrentControlSet\Services\AWSNVMe\Parameters
\Device"
Set-ItemProperty -Path $registryPath -Name EnableSCSIPersistentReservations -Value 0
```

Histórico da versão do driver AWS NVMe para Windows

A tabela a seguir mostra quais drivers AWS NVMe são executados em cada versão do Windows Server no Amazon EC2.

Versão Windows Server	Versão do driver AWS NVME
Windows Server 2025	versão mais recente
Windows Server 2022	versão mais recente
Windows Server 2019	versão mais recente
Windows Server 2016	versão mais recente
Windows Server 2012 R2	versão 1.5.1 e versões anteriores
Windows Server 2012	versão 1.5.1 e versões anteriores

Versão Windows Server	Versão do driver AWS NVME
Windows Server 2008 R2	versão 1.3.2 e versões anteriores
Windows Server 2008	versão 1.3.2 e versões anteriores

A tabela a seguir descreve as versões lançadas do driver AWS NVMe.

Versão do pacote	Versão do driver	Detalhes	Data de lançamento
1.8.0	1.8.0	• Suporte adicionado para IOCTLs para operar com dispositivos que implementam gerenciamento dinâmico de namespace. Para obter mais informações, consulte IOCTL_SCSI_MINIPORT IOCTL na documentação da Microsoft. • Correções de erros no comando Get Log Page e na geração do número de série.	16 de janeiro de 2026
1.7.0	1.7.0	• Adicionada compatibilidade com o comando NVMe Get Log Page. • Adicionadas estatísticas de performance detalhadas para os volumes de armazenamento de instância do EBS e do EC2 • Correções de erros do comando Identify Namespace.	17 de setembro de 2025
1.6.0	1.6.0	• Atualização do script de instalação para usar PnPUtil. •	25 de outubro de 2024

Versão do pacote	Versão do driver	Detalhes	Data de lançamento
		Atualização de ebsnvme-id.exe para usar NVMe IOCTL.	
1.5.1	1.5.0	Correção do script de instalação para criar uma pasta para a ferramenta `ebsnvme-id` se ela não estiver presente.	17 de novembro de 2023
1.5.0	1.5.0	Foi adicionado suporte para reservas persistentes da Small Computer System Interface (SCSI) para instâncias que executam o Windows Server 2016 e versões posteriores. A ferramenta ebsnvme-id (`ebsnvme-id.exe`) agora é instalada por padrão.	31 de agosto de 2023
1.4.2	1.4.2	Corrigido um erro em que o Driver do AWS NVMe não oferecia suporte a volumes de armazenamento em instâncias D3.	16 de março de 2023
1.4.1	1.4.1	Relatórios Namespace Preferred Write Granularity (NPGW) para volumes do EBS que suportem esse recurso de NVMe opcional. Para obter mais informações, consulte a seção 8.25, “Melhorando a performance por meio do tamanho da E/S e aderência ao alinhamento”, na Especificação básica do NVMe, versão 1.4.	20 de maio de 2022

Versão do pacote	Versão do driver	Detalhes	Data de lançamento
1.4.0	1.4.0	• Adicionado suporte para IOCTLs, que permitem que as aplicações interajam com dispositivos NVMe. Esse suporte permite que as aplicações obtenham a lista de `IdentifyController` , `IdentifyNamespace` e `NameSpace` do dispositivo NVMe. Para obter mais informações, consulte Consultas específicas do protocolo na documentação da Microsoft. • A versão 1.4.0 do driver e a ferramenta `ebsnvme-id` mais recente (`ebsnvme-id.exe`) são combinadas em um único pacote. Essa combinação permite instalar o driver e a ferramenta de um único pacote. Para obter mais detalhes, consulte AWSDrivers NVMe. • Correções de bugs e aprimoramentos em confiabilidade.	23 de novembro de 2021
1.3.2	1.3.2	Corrigido o problema com a modificação de volumes do EBS processando a E/S ativamente, o que pode resultar em dados corrompidos. Os clientes que não modificam volumes do EBS online (por exemplo, redimensionando ou alterando o tipo) não são afetados. Esta é a última versão que pode ser executada no Windows Server 2008 e 2008 R2. Esta versão está disponível para download, mas não tem mais suporte. O Windows Server 2008 e 2008 R2 chegaram ao fim da vida útil e não contam mais com suporte da Microsoft.	10 de setembro de 2019

Versão do pacote	Versão do driver	Detalhes	Data de lançamento
1.3.1	1.3.1	Melhorias de confiabilidade.	21 de maio de 2019
1.3.0	1.3.0	Melhorias de otimização do dispositivo.	31 de agosto de 2018
1.2.0	1.2.0	Melhorias na performance e confiabilidade para dispositivos NVMe da AWS em todas as instâncias compatíveis, incluindo instâncias bare metal.	13 de junho de 2018
>1.0.0	>1.0.0	Driver NVMe da AWS para tipos de instâncias compatíveis executando Windows Server.	12 de fevereiro de 2018

Assinar notificações do

O Amazon SNS pode notificá-lo quando novas versões dos drivers EC2 para Windows são lançadas. Use o procedimento a seguir para se inscrever nessas notificações.

Como assinar as notificações do EC2 no console

1. Abra o console do Amazon SNS em https://console.aws.amazon.com/sns/v3/home.
2. Na barra de navegação, altere a região para Leste dos EUA (Norte da Virgínia), se necessário. É necessário selecionar esta região porque as notificações do SNS que você está assinando estão nesta região.
3. No painel de navegação, escolha Subscriptions.
4. Selecione Create subscription.
5. Na caixa de diálogo Criar assinatura, faça o seguinte:

    a. Para o ARN do tópico, copie o seguinte ARN (nome de recurso da Amazon):

    arn:aws:sns:us-east-1:801119661308:ec2-windows-drivers

b. Para Protocolo, selecione `Email`.

c. Para Endpoint, digite um endereço de e-mail que é possível usar para receber as notificações.

d. Selecione Create subscription.

6. Você receberá um e-mail de confirmação. Abra o e-mail e siga as instruções para concluir a sua assinatura.

Sempre que novos drivers EC2 para Windows são lançados, nós enviamos notificações aos assinantes. Se não deseja mais receber essas notificações, use o procedimento a seguir para cancelar a assinatura.

Para cancelar a assinatura de notificações do driver Amazon EC2 para Windows

1. Abra o console do Amazon SNS em https://console.aws.amazon.com/sns/v3/home.
2. No painel de navegação, escolha Subscriptions.
3. Selecione a caixa de seleção para a assinatura e, depois, escolha Ações, Excluir assinaturas. Quando a confirmação for solicitada, escolha Excluir.

Para assinar as notificações do EC2 usando a AWS CLI

Para assinar as notificações do EC2 com a AWS CLI, use o comando a seguir.

```
aws sns subscribe --topic-arn arn:aws:sns:us-east-1:801119661308:ec2-windows-drivers --
protocol email --notification-endpoint YourUserName@YourDomainName.ext
```

Para assinar as notificações do EC2 usando o AWS Tools for Windows PowerShell

Para assinar as notificações do EC2 com AWS Tools for Windows PowerShell, use o comando a seguir.

```
Connect-SNSNotification -TopicArn 'arn:aws:sns:us-east-1:801119661308:ec2-windows-
drivers' -Protocol email -Region us-east-1 -Endpoint 'YourUserName@YourDomainName.ext'
```

Configurar a instância do Windows do Amazon EC2

Após executar uma instância do Windows, será possível fazer login como administrador para realizar configurações adicionais para definições do sistema e recursos do Windows. O Utilitários de solução de problemas de problemas do EC2 pode ajudar com a resolução de problemas em sua instância.

É possível configurar os agentes de execução e outros recursos específicos do Windows, conforme a seguir.

Agentes de inicialização do Windows

Cada AMI do Windows da AWS (e muitas outras AMIs disponíveis no AWS Marketplace) inclui um agente de execução do Windows pré-configurado com configurações padrão. Os agentes de execução realizam tarefas durante a inicialização da instância e serão executados se uma instância for interrompida e, posteriormente, iniciada ou reiniciada.

EC2 Fast Launch para Windows

Cada instância Windows do Amazon EC2 deve passar pelas etapas padrão de execução do sistema operacional Windows (SO), que incluem várias reinicializações, e frequentemente levam 15 minutos ou mais para serem concluídas. As AMIs do Windows Server do Amazon EC2 que têm o atributo EC2 Fast Launch habilitado concluem algumas dessas etapas e são reinicializadas com antecedência para reduzir o tempo necessário para iniciar uma instância.

Configurações de sistema específicas do Windows

A lista a seguir inclui algumas configurações do sistema que se aplicam somente aos sistemas operacionais Windows:

Alterar a senha de administrador do Windows

Quando se conectar a uma instância do Windows, especifique uma conta de usuário e uma senha que tenha permissão para acessar a instância. A primeira vez que se conectar a uma instância, você deverá usar a conta de administrador e fornecer a senha padrão. Quando você se conectar a uma instância pela primeira vez, recomendamos alterar a senha de administrador de seu valor padrão.

Adicionar componentes do Sistema Windows

Os sistemas operacionais do Windows Server incluem muitos componentes opcionais. Não é prático incluir todos os componentes opcionais em cada AMI do Windows Server do AWS.

Em vez disso, nós fornecemos snapshots do EBS de mídia de instalação que têm os arquivos necessários para configurar ou instalar componentes na instância do Windows.

Instalação do WSL no Windows

O Subsistema do Windows para Linux (WSL) é um download gratuito que pode ser instalado na sua instância do Windows. Ao instalar o WSL, você pode executar ferramentas de linha de comando do Linux diretamente na sua instância do Windows e usar as ferramentas do Linux para o desenvolvimento de scripts, junto com a sua área de trabalho tradicional do Windows. É possível alternar facilmente entre Linux e Windows em uma única instância do Windows, o que pode ser útil em um ambiente de desenvolvimento.

Drivers de dispositivos da AWS para instâncias do Windows

É possível atualizar os drivers de dispositivos da AWS para suas instâncias do Windows. Para obter mais informações, consulte the section called “Gerenciamento de drivers de dispositivo”.

A tabela a seguir resume os drivers com suporte para instâncias baseadas em Nitro por versão do Windows.

Versão	Driver de armazenamento	Driver de rede aprimorada
Windows Server 2025	Versão mais recente do AWS NVMe	Versão mais recente do ENA
Windows Server 2022	Versão mais recente do AWS NVMe	Versão mais recente do ENA
Windows Server 2019	Versão mais recente do AWS NVMe	Versão mais recente do ENA
Windows Server 2016	Versão mais recente do AWS NVMe	Versão mais recente do ENA
Windows Server 2012 R2	AWS NVMe versão 1.5.1	ENA versão 2.6.0
Windows Server 2008 R2	AWS NVMe versão 1.3.2	ENA versão 2.2.3

A tabela a seguir resume os drivers com suporte para instâncias baseadas em Xen por versão do Windows.

Versão	Driver de armazenamento	Driver de rede aprimorada
Windows Server 2022	AWSVersão mais recente do PV	• Versão mais recente do ENA [1] • Intel VF [2] • AWS Versão mais recente do PV [3]
Windows Server 2019	AWSVersão mais recente do PV	• Versão mais recente do ENA [1] • Intel VF [2] • AWS Versão mais recente do PV [3]
Windows Server 2016	AWSVersão mais recente do PV	• Versão mais recente do ENA [1] • Intel VF [2] • AWS Versão mais recente do PV [3]
Windows Server 2012 R2	AWS PV versão 8.4.3	• ENA versão 2.6.0 [1] • Intel VF [2] • AWS PV versão 8.4.3 [3]
Windows Server 2008 R2	AWS PV versão 8.3.5	• ENA versão 2.2.3 [1] • Intel VF [2] • AWS PV versão 8.3.5 [3]

[1] Para tipos de instância G3, H1, I3, `m4.16xlarge`, P2, P3, P3dn e R4.

[2] Para tipos de instância C3, C4, D2, I2, M4 (excluindo `m4.16xlarge`) e R3.

[3] Para tipos de instância C1, M1, M2, M3, T1, T2, X1 e X1e.

Agentes de inicialização do Windows em instâncias do Windows do Amazon EC2

Cada AMI do Windows da AWS inclui um agente de execução do Windows pré-configurado com configurações padrão. Os agentes de execução realizam tarefas durante a inicialização da instância e serão executados se uma instância for interrompida e, posteriormente, iniciada ou reiniciada. Para obter informações sobre um agente específico, consulte as páginas de detalhes na lista a seguir.

Para obter mais informações sobre as AMIs do AWS Windows, consulte a Referência da AMI do AWS Windows.

- Usar o agente do EC2Launch v2 para realizar tarefas durante a execução da instância EC2 Windows
- Usar o agente do EC2Launch v1 para realizar tarefas durante a execução da instância EC2 Windows
- Usar o serviço EC2Config para realizar tarefas durante a execução da instância herdada do sistema operacional Windows do EC2

Conteúdo

- Comparação entre os agentes de inicialização do Amazon EC2
- Configurar o sufixo DNS para agentes de execução do EC2 Windows
- Assinar as notificações do agente de execução do EC2 Windows
- Administração do Serviço do Windows para agentes do EC2Launch v2 e EC2Config

Comparação entre os agentes de inicialização do Amazon EC2

A tabela a seguir mostra as principais diferenças funcionais entre EC2Config, EC2Launch v1 e EC2Launch v2.

Recurso	EC2Config	EC2Launch v1	EC2Launch v2
Executar como	Windows Service	Scripts PowerShell	Windows Service

Recurso	EC2Config	EC2Launch v1	EC2Launch v2
Suporte	Somente SO herdado	Versões do Windows Server: • 2016 • 2019 (LTSC e SAC)	Versões do Windows Server: • 2016 • 2019 (LTSC e SAC) • 2022 • 2025
Arquivo de configuração	XML	JSON	JSON/YAML
Definir nome de usuário do administrador	Não	Não	Sim
Dados de usuários compactados	Não	Não	Sim
Dados de usuário local incorporados na AMI	Não	Não	Sim, configurável
Configuração de tarefa nos dados do usuário	Não	Não	Sim
Papel de parede configurável	Não	Não	Sim
Personalizar a ordem de execução de tarefas	Não	Não	Sim
Tarefas configuráveis	15	9	20 na execução

Recurso	EC2Config	EC2Launch v1	EC2Launch v2
Oferece suporte ao Visualizador de eventos do Windows	Sim	Não	Sim
Número dos tipos de eventos do Visualizador de eventos	2	0	30

> **Note**
>
> A documentação do EC2Config é fornecida somente para referência histórica. As versões do sistema operacional em que ele é executado não têm mais suporte pela Microsoft. É altamente recomendável atualizar para o serviço de execução mais recente.

Configurar o sufixo DNS para agentes de execução do EC2 Windows

Com os agentes de inicialização do Amazon EC2, é possível configurar uma lista de sufixos DNS que as instâncias do Windows usam para a resolução de nomes de domínio. Os agentes de inicialização substituem as configurações padrão do Windows na chave de registro `System\CurrentControlSet\Services\Tcpip\Parameters\SearchList` ao adicionar os seguintes valores à lista de pesquisa de sufixos DNS:

- O domínio da instância
- Os sufixos que resultam da devolução do domínio da instância
- O domínio NV
- Os domínios especificados por cada placa de interface de rede

Todos os agentes de inicialização são compatíveis com a configuração de sufixo DNS. Para obter mais informações, consulte a versão específica do seu agente de inicialização:

- Para obter informações sobre a tarefa `setDnsSuffix` e como configurar sufixos DNS no EC2Launch v2, consulte setDnsSuffix.

- Para obter informações sobre a configuração da lista de sufixos DNS e como habilitar ou desabilitar a devolução para o EC2Launch v1, consulte Configurar o agente do EC2Launch v1 na instância do Windows.
- Para obter informações sobre a configuração da lista de sufixos DNS e como habilitar ou desabilitar a devolução para o EC2Config, consulte Arquivos de configurações do EC2Config.

Devolução de nome de domínio

A devolução de nome de domínio é um comportamento do Active Directory que permite que computadores em um domínio secundário acessem recursos no domínio principal sem a necessidade de usar um nome de domínio totalmente qualificado. Por padrão, a devolução de nome de domínio continua até que restem somente dois nós na progressão do nome de domínio.

Os agentes de inicialização executarão a devolução no nome de domínio se a instância estiver conectada a um domínio e adicionarão os resultados à lista de pesquisa de sufixos DNS mantida na chave do registro **`System\CurrentControlSet\Services\Tcpip\Parameters\SearchList`**. Os agentes usam as configurações das chaves de registro apresentadas a seguir para determinar o comportamento de devolução.

- **`System\CurrentControlSet\Services\Tcpip\Parameters\UseDomainNameDevolution`**
  - Quando não há definição, desabilita a devolução.
  - Quando está definida como `1`, habilita a devolução (padrão).
  - Quando está definida como `0`, desabilita a devolução.
- **`System\CurrentControlSet\Services\Dnscache\Parameters\DomainNameDevolutionLevel`**
  - Quando não há definição, use o nível de 2 (padrão).
  - Quando está definida como `3` ou valores superiores, use o valor para definir o nível.

Quando você desabilita a devolução ou altera as configurações de devolução para um nível superior, a chave do registro `System\CurrentControlSet\Services\Tcpip\Parameters\SearchList` ainda contém os sufixos que foram adicionados anteriormente. Eles não são removidos automaticamente. É possível atualizar a lista de forma manual ou limpá-la e deixar seu agente executar o processo para configurar a nova lista.

> **Note**
>
> Para limpar a lista de sufixos DNS do registro, você pode executar o comando apresentado a seguir.
>
> ```
> PS C:\> Invoke-CimMethod -ClassName Win32_NetworkAdapterConfiguration -
> MethodName "SetDNSSuffixSearchOrder" -Arguments @{ DNSDomainSuffixSearchOrder =
>  $null } | Out-Null
> ```

Exemplos de devolução

Os exemplos apresentados a seguir demonstram a progressão do nome de domínio por meio do processo de devolução.

`corp.example.com`

- Progride para `example.com`

`locale.region.corp.example.com`

1. Progride para `region.corp.example.com`
2. Progride para `corp.example.com`
3. Progride para `example.com`

`locale.region.corp.example.com` com uma configuração de `DomainNameDevolutionLevel=3`

1. Progride para `region.corp.example.com`
2. Progride para `corp.example.com` A progressão é interrompida aqui devido à configuração do nível.

Assinar as notificações do agente de execução do EC2 Windows

O Amazon SNS pode notificar você quando novas versões dos agentes de execução do EC2 forem liberadas. Use o procedimento a seguir para se inscrever nessas notificações.

Inscrever-se nas notificações do EC2Config

1. Abra o console do Amazon SNS em https://console.aws.amazon.com/sns/v3/home.
2. Na barra de navegação, altere a região para Leste dos EUA (Norte da Virgínia), se necessário. É necessário selecionar esta Região porque as notificações do SNS que você está assinando foram criadas nesta Região.
3. No painel de navegação, escolha Subscriptions.
4. Selecione Create subscription.
5. Na caixa de diálogo Criar assinatura, faça o seguinte:

    a. Para ARN do tópico, use o seguinte nome do recurso da Amazon (ARN) que corresponda ao agente do qual você deseja receber as notificações:

    - EC2Launch v2:

    ```
    arn:aws:sns:us-east-1:309726204594:amazon-ec2launch-v2
    ```

    - EC2Launch ou EC2Config:

    ```
    arn:aws:sns:us-east-1:801119661308:ec2-windows-ec2config
    ```

    b. Para Protocolo, selecione `Email`.

    c. Para Endpoint, insira o endereço de e-mail no qual deseja receber as notificações.

    d. Selecione Create subscription.
6. Você receberá um e-mail solicitando que você confirme sua assinatura. Abra o e-mail e siga as instruções para concluir a sua assinatura.

Sempre que uma nova versão do agente de execução é liberada, nós enviamos notificações aos assinantes. Se não deseja mais receber essas notificações, use o procedimento a seguir para cancelar a assinatura.

Cancelar a assinatura das notificações do agente de execução

1. Abra o console do Amazon SNS.
2. No painel de navegação, escolha Subscriptions.
3. Selecione a assinatura e escolha Actions (Ações), Delete subscriptions (Excluir assinaturas). Quando a confirmação for solicitada, escolha Excluir.

Administração do Serviço do Windows para agentes do EC2Launch v2 e EC2Config

Caso esteja conectado à instância como um usuário com direitos administrativos, você pode gerenciar os agentes de execução do EC2Launch v2 e do EC2Config da mesma forma como com qualquer outro serviço do Windows. O EC2Launch v1 é um conjunto de scripts do PowerShell gerenciado por meio de tarefas agendadas por padrão. Esta seção aborda a administração de serviços para o EC2Launch v2 e o EC2Config.

Para aplicar as configurações atualizadas à instância, você pode parar e reiniciar o agente do EC2Launch v2 ou o agente de execução do serviço do EC2Config na interface do Microsoft Management Console (MMC) para Serviços. Da mesma forma, ao instalar uma nova versão do agente de execução, você deve primeiro interromper o agente e reiniciá-lo quando a instalação estiver concluída.

> **Note**
>
> Você deve abrir a interface de Serviços do MMC como administrador para selecionar essas ações. Para fazer isso, você pode selecionar Executar como administrador no menu de contexto. Como alternativa, para abrir a interface usando o teclado, siga estas etapas:
>
> 1. Usando a tecla `Tab` ou as teclas de seta, selecione o item de menu Serviços no menu Ferramentas administrativas.
> 2. Use a seguinte combinação de teclas para abrir como administrador: `Ctrl` + `Shift` + `Enter`.

Os procedimentos a seguir listam as etapas para interromper e iniciar o agente de execução na instância.

Interromper o agente de execução

1. Execute e conecte-se à sua instância do Windows.
2. Selecione Ferramentas administrativas no menu Iniciar do Windows.
3. Abra o console de Serviços como administrador, conforme descrito no início desta seção.
4. Na lista de serviços, selecione o agente que está sendo executado na instância (EC2Launch ou EC2Config) e escolha Interromper no menu Ação. Também é possível usar o menu de contexto para interromper o agente.

Reiniciar o agente de execução

1. Execute e conecte-se à sua instância do Windows.
2. Selecione Ferramentas administrativas no menu Iniciar do Windows.
3. Abra o console de Serviços como administrador, conforme descrito no início desta seção.
4. Na lista de serviços, selecione o agente que está sendo executado na instância (EC2Launch ou EC2Config) e escolha Interromper ou Reiniciar no menu Ação. Também é possível usar o menu de contexto para reiniciar o agente.

Caso não precise atualizar as configurações, criar sua própria AMI ou usar o AWS Systems Manager, será possível excluir e desinstalar o agente de execução.

Excluir

A exclusão de um serviço remove a subchave do registro.

Desinstalar

Desinstalar um serviço elimina os arquivos, a subchave do registro e todos os atalhos do serviço.

Excluir o agente de execução

1. Execute e conecte-se à sua instância do Windows.
2. Inicie uma janela de prompt de comando do Windows.
3. Execute um dos comandos a seguir para excluir o agente de execução.
   - Execute o seguinte comando para excluir o EC2Launch ou o EC2Launch v2:

     ```
     sc delete ec2launch
     ```
   - Execute o seguinte comando para excluir o serviço do EC2Config:

     ```
     sc delete ec2config
     ```

Desinstalar o agente de execução

1. Execute e conecte-se à sua instância do Windows.
2. Escolha Sistema Windows e, em seguida, Painel de controle no menu Iniciar do Windows.

3. Escolha Programas e recursos para abrir a lista de programas que estão instalados na instância.
4. Selecione o agente de execução na lista (Amazon EC2Launch ou EC2ConfigService) e escolha Desinstalar no menu Arquivo. Como alternativa, você pode usar o menu de contexto.

> **Note**
>
> É possível ver qual versão do agente de execução está instalada na coluna Versão.

Usar o agente do EC2Launch v2 para realizar tarefas durante a execução da instância EC2 Windows

Todas as instâncias compatíveis do Amazon EC2 iniciadas em AMIs da AWS com o Windows Server 2022 e o Windows Server 2025 incluem o agente de inicialização do EC2Launch v2 (`EC2Launch.exe`) por padrão. Também fornecemos AMIs do Windows Server 2016 e 2019 com o EC2Launch v2 instalado como o agente padrão de execução. Essas AMIs são fornecidas além das AMIs do Windows Server 2016 e 2019 que incluem o EC2Launch v1. É possível procurar por AMIs do Windows que incluam o EC2Launch v2 por padrão inserindo o seguinte prefixo em sua pesquisa na página AMIs no console do Amazon EC2: `EC2LaunchV2-Windows_Server-*`.

Para comparar os recursos da versão do agente de inicialização, consulte Comparação entre os agentes de inicialização do Amazon EC2.

O EC2Launch v2 executa tarefas durante o startup da instância e é executado se uma instância for interrompida e iniciada posteriormente, ou reiniciada. O EC2Launch v2 também pode executar tarefas sob demanda. Algumas dessas tarefas são automaticamente habilitadas, enquanto outras precisam ser habilitadas manualmente. O serviço EC2Launch v2 é compatível com todos os recursos EC2Config e EC2Launch.

Esse serviço usa um arquivo de configuração para controlar sua operação. É possível atualizar o arquivo de configuração usando uma ferramenta gráfica ou editando-o diretamente como único arquivo .yml (`agent-config.yml`). Para obter mais informações sobre localizações de arquivos, consulte Estrutura de diretório do EC2Launch v2.

O EC2Launch v2 publica logs de eventos do Windows para ajudá-lo a solucionar erros e definir gatilhos. Para obter mais informações, consulte Logs de eventos do Windows.

Versões compatíveis do SO

O agente do EC2Launch v2 é compatível com as seguintes versões do sistema operacional (SO) do Windows Server abaixo:

- Windows Server 2025
- Windows Server 2022
- Windows Server 2019 (canal de manutenção de longo prazo e canal semestral)
- Windows Server 2016

Tarefas que são executadas por padrão

Por padrão, o agente EC2Launch v2 executa as tarefas apresentadas a seguir uma única vez durante a primeira inicialização da instância. As tarefas são organizadas de acordo com a ordem em que são executadas durante a fase de inicialização.

Fase de `Boot`

- extendRootPartition

Fase de `PreReady`

- activateWindows
- setDnsSuffix
- setAdminAccount
- setWallpaper

Fase de `PostReady`

- startSsm

Conceitos do EC2Launch v2

É útil entender os conceitos a seguir ao considerar o EC2Launch v2.

agent-config

`agent-config`O é um arquivo localizado na pasta de configuração do EC2Launch v2. Ele inclui a configuração para os estágios de inicialização, rede, PreReady e PostReady. Este arquivo é

usado para especificar a configuração de uma instância para tarefas que devem ser executadas quando a AMI é inicializada pela primeira vez ou em ocasiões posteriores.

Por padrão, a instalação do EC2Launch v2 instala um arquivo `agent-config` que inclui configurações recomendadas usadas nas AMIs padrão do Amazon Windows. É possível atualizar o arquivo de configuração de modo a alterar a experiência de inicialização padrão para sua AMI especificada pelo EC2Launch v2. Para obter mais informações sobre localizações de arquivos, consulte Estrutura de diretório do EC2Launch v2.

Frequência

A frequência da tarefa determina quando as tarefas devem ser executadas, dependendo do contexto de inicialização. A maioria das tarefas tem apenas uma frequência permitida. É possível especificar uma frequência para as tarefas `executeScript`.

Você verá as seguintes frequências no Configuração de tarefas do EC2Launch v2.

- Uma vez — a tarefa é executada uma vez, mediante a inicialização da AMI pela primeira vez (Sysprep concluído).
- Sempre: a tarefa é executada toda vez que o agente de inicialização é executado. O agente de inicialização é executado quando:
  - uma instância inicia ou reinicia
  - o serviço EC2Launch é executado
  - `EC2Launch.exe run`O é invocado

Estágio

Um estágio é um agrupamento lógico de tarefas que o agente EC2Launch v2 executa. Algumas tarefas podem ser executadas apenas em um estágio específico. Outras podem ser executadas em vários estágios. Ao usar `agent-config.yml`, você deve especificar uma lista de estágios e uma lista das tarefas de cada estágio.

O serviço executa as etapas nesta ordem:

Etapa 1: Boot

Etapa 2: Network

Etapa 3: PreReady

O Windows está pronto

Após a conclusão do estágio PreReady, o serviço envia a mensagem `Windows is ready` para o console do Amazon EC2.

Etapa 4: PostReady

Os dados do usuário são executados durante o estágio PostReady. Algumas versões de script são executadas antes do estágio PostReady do arquivo `agent-config.yml` e outras depois, da seguinte forma:

Antes do `agent-config.yml`

- Dados de usuário em YAML versão 1.1
- Dados de usuário em XML

Depois de `agent-config.yml`

- Dados do usuário em YAML versão 1.0 (versão antiga para compatibilidade com versões anteriores)

Para obter exemplos dos estágios e das tarefas, consulte Exemplo: `agent-config.yml`.

Ao usar dados do usuário, você deve especificar uma lista de tarefas para o agente de inicialização executar. O estágio está implícito. Para obter exemplos de tarefas, consulte Exemplo: dados do usuário.

O EC2Launch v2 executa a lista de tarefas na ordem especificada em `agent-config.yml` e nos dados do usuário. Os estágios são executados sequencialmente. O próximo estágio começa após a conclusão do estágio anterior. As tarefas também são executadas sequencialmente.

Tarefa

É possível invocar uma tarefa para realizar uma ação em uma instância. É possível configurar tarefas no arquivo `agent-config.yml` ou por meio de dados do usuário. Para obter uma lista das tarefas disponíveis no EC2Launch v2, consulte Tarefas do EC2Launch v2. Para obter o esquema e os detalhes de configuração da tarefa, consulte Configuração de tarefas do EC2Launch v2.

Dados do usuário

Os dados do usuário são dados que podem ser configurados ao iniciar uma instância. É possível atualizar os dados do usuário para alterar de maneira dinâmica como as AMIs personalizadas ou AMIs de início rápido são configuradas. O EC2Launch v2 suporta 60 kB de comprimento de entrada de dados do usuário. Os dados do usuário incluem apenas o estágio do UserData e,

portanto, são executados após o arquivo `agent-config`. É possível inserir dados do usuário ao executar uma instância usando o assistente de execução de instância ou pode modificar os dados do usuário no console do EC2. Para obter mais informações sobre como trabalhar com dados do usuário, consult Como o Amazon EC2 lida com os dados dos usuários para instâncias do Windows.

Visão geral da tarefa do EC2Launch v2

O EC2Launch v2 pode executar as seguintes tarefas em cada inicialização:

- Configurar papel de parede novo e opcionalmente personalizado que renderiza informações sobre a instância.
- Definir os atributos para a conta de administrador criada na máquina local.
- Adicionar sufixos DNS à lista de sufixos de pesquisa. Somente sufixos que ainda não existem são adicionados à lista.
- Definir letras de unidade para quaisquer volumes adicionais e estendê-las para usar o espaço disponível.
- Gravar arquivos da configuração no disco.
- Executar scripts especificados no arquivo de configuração do EC2Launch v2 ou de `user-data`. Os scripts de `user-data` podem ser em texto simples ou compactados e fornecidos no formato base64.
- Executar um programa com os argumentos fornecidos.
- Definir o nome do computador.
- Enviar informações de instância para o console do Amazon EC2.
- Enviar a impressão digital do certificado RDP ao console do Amazon EC2.
- Estenda dinamicamente a partição do sistema operacional para incluir qualquer espaço não particionado.
- Executar dados do usuário. Para obter mais informações sobre como especificar os dados do usuário, consulte Configuração de tarefas do EC2Launch v2.
- Defina rotas estáticas não persistentes para alcançar o serviço de metadados e os servidores AWS KMS.
- Definir partições que não sejam de inicialização como `mbr` ou `gpt`.
- Iniciar o serviço Systems Manager após o Sysprep.
- Otimizar as configurações do ENA.

- Ativar o OpenSSH para versões posteriores do Windows.
- Ativar os frames jumbo.
- Defina o Sysprep para execução com o EC2Launch v2.
- Publicar logs de eventos do Windows.

Estrutura de diretório do EC2Launch v2

O EC2Launch v2 deve ser instalado nos seguintes diretórios:

- Binários de serviço: `%ProgramFiles%\Amazon\EC2Launch`
- Dados de serviço (configurações, arquivos de log e arquivos de estado): `%ProgramData%\Amazon\EC2Launch`

> **Note**
>
> Por padrão, o Windows oculta os arquivos e as pastas sob `C:\ProgramData`. Para visualizar os diretórios e arquivos do EC2Launch v2, digite o caminho no Windows Explorer ou altere as propriedades da pasta para os arquivos e as pastas ocultos.

O diretório `%ProgramFiles%\Amazon\EC2Launch` contém binários e bibliotecas compatíveis. Ele inclui os seguintes subdiretórios:

- `settings`
  - `EC2LaunchSettingsUI.exe`: interface de usuário para modificar o arquivo `agent-config.yml`
  - `YamlDotNet.dll`: DLL para oferecer suporte a algumas operações na interface do usuário
- `tools`
  - `ebsnvme-id.exe`: ferramenta para examinar os metadados dos volumes do EBS na instância
  - `AWSAcpiSpcrReader.exe`: ferramenta para determinar a porta COM correta a ser usada
  - `EC2LaunchEventMessage.dll`: DLL para oferecer suporte ao registro de eventos do Windows para o EC2Launch
- `service`
  - `EC2LaunchService.exe`: serviço do Windows executável que é iniciado quando o agente de inicialização é executado como um serviço

- `EC2AgentTelemetry.dll`: DLL para dar suporte à telemetria do agente EC2
- `EC2Launch.exe`: executável principal do EC2Launch
- `EC2LaunchAgentAttribution.txt`: atribuição para código usado dentro do EC2 Launch

O diretório `%ProgramData%\Amazon\EC2Launch` contém os seguintes subdiretórios. Todos os dados produzidos pelo serviço, incluindo logs, configuração e estado, são armazenados neste diretório.

- `config`: configuração

  O arquivo de configuração do serviço é armazenado neste diretório como `agent-config.yml`. Esse arquivo pode ser atualizado de modo a modificar, adicionar ou remover tarefas padrão executadas pelo serviço. A permissão para criar arquivos neste diretório é restrita à conta de administrador para evitar o escalonamento de privilégios.
- `log`: logs de instância

  Os logs do serviço (`agent.log`), o console (`console.log`), a performance (`bench.log`), os erros (`err.log`) e a telemetria (`telemetry.log`) são armazenados neste diretório. Os arquivos de log são anexados a execuções subsequentes do serviço.
- `state`: dados de estado do serviço

  O estado usado pelo serviço para determinar quais tarefas devem ser executadas é armazenado aqui. Há um arquivo `.run-once` que indica se o serviço já foi executado após Sysprep (portanto, as tarefas com frequência de uma vez serão ignoradas na próxima execução). Esse subdiretório inclui `state.json` e `previous-state.json` para rastrear o status de cada tarefa.
- `sysprep`: Sysprep

  Esse diretório contém arquivos usados para determinar quais operações executar pelo Sysprep ao criar uma AMI do Windows personalizada que pode ser reutilizada.
- `wallpaper`: papel de parede

  As imagens de papel de parede são armazenadas nesse diretório.

Telemetria

Telemetria é informação adicional que ajuda a AWS a entender melhor suas necessidades, diagnosticar problemas e fornecer recursos para melhorar sua experiência com os Serviços da AWS.

EC2Launch versão v2 `2.1.592` e, posteriormente, coletar telemetria, como métricas de uso e erros. Esses dados são coletados da instância do Amazon EC2 na qual o EC2Launch v2 é executado. Isso inclui todas as AMIs do Windows de propriedade da AWS.

Os seguintes tipos de telemetria são coletados pelo EC2Launch v2:

- Informações de uso: comandos do agente, método de instalação e frequência de execução programada.
- Erros e informações de diagnóstico: códigos de erro da instalação do agente, códigos de erro de execução e pilhas de chamada como erro.

Exemplos de dados coletados da versão 2.0.592 até a 2.1.1:

```
2025/07/18 22:38:52Z: EC2LaunchTelemetry: IsTelemetryEnabled=true
2025/07/18 22:38:52Z: EC2LaunchTelemetry: AgentOsArch=windows_amd64
2025/07/18 22:38:52Z: EC2LaunchTelemetry: IsAgentScheduledPerBoot=true
2025/07/18 22:38:52Z: EC2LaunchTelemetry: AgentCommandErrorCode=0
2025/07/18 22:38:52Z: EC2LaunchTelemetry: AdminPasswordTypeCode=0
2025/07/18 22:38:52Z: EC2LaunchTelemetry: IpConflictDetectionCode=0
2025/07/18 22:38:52Z: EC2LaunchTelemetry: AgentErrorLocation=addroutes.go:49
```

A partir da versão 2.2.63, os dados de telemetria do EC2 Agent são formatados como um objeto JSON:

```
{"type":"EC2AgentTelemetry","agentId":"WindowsLaunchAgentV2" ... }
```

A telemetria está habilitada por padrão. É possível desativar a coleta de telemetria a qualquer momento.

Desativar telemetria em uma instância

Para desativar a telemetria para uma única instância, é possível definir uma variável de ambiente do sistema ou usar o MSI para modificar a instalação.

Para desabilitar a telemetria definindo uma variável de ambiente do sistema, execute o seguinte comando como administrador:

```
setx /M EC2LAUNCH_TELEMETRY 0
```

Para desabilitar a telemetria usando o MSI, execute o comando a seguir depois de baixar o MSI,

```
msiexec /i ".\AmazonEC2Launch.msi" Remove="Telemetry" /q
```

Mais tópicos do EC2Launch v2

- Instalar a versão mais recente do EC2Launch v2
- Definição das configurações do EC2Launch v2 para instâncias do Windows
- Definições de tarefas para tarefas de inicialização do EC2Launch v2
- Solucionar problemas com o agente do EC2Launch v2
- Históricos de versões do EC2Launch v2

Instalar a versão mais recente do EC2Launch v2

É possível usar um dos seguintes métodos para instalar o agente EC2Launch v2 em sua instância do EC2:

- Fazer download do agente do Amazon S3 e instalá-lo com o Windows PowerShell. Para URLs de downloads, consulte Downloads do EC2Launch v2 no Amazon S3.
- Instalar com o SSM Distributor.
- Instalar de um componente do EC2 Image Builder ao criar uma imagem personalizada.
- Iniciar sua instância de uma AMI que tenha o EC2Launch v2 pré-instalado.

> **Warning**
>
> O AmazonEC2Launch.msi desinstala versões anteriores dos serviços de execução do EC2, como EC2Launch (v1) ou EC2Config.

Para as etapas de instalação, selecione a guia que corresponde ao seu método preferido.

PowerShell

Para instalar a versão mais recente do agente do EC2Launch v2 com o Windows PowerShell, siga estas etapas.

1. Crie um diretório local.

```
New-Item -Path "$env:USERPROFILE\Desktop\EC2Launchv2" -ItemType Directory
```

2. Defina o URL do seu local de download. Execute o comando a seguir com o URL do Amazon S3 que será usado. Para URLs de downloads, consulte Downloads do EC2Launch v2 no Amazon S3.

```
$Url = "Amazon S3 URL/AmazonEC2Launch.msi"
```

3. Use o comando a seguir para fazer download do agente e executar a instalação

```
$DownloadFile = "$env:USERPROFILE\Desktop\EC2Launchv2\" + $(Split-Path -Path
 $Url -Leaf)
Invoke-WebRequest -Uri $Url -OutFile $DownloadFile
msiexec /i "$DownloadFile"
```

> **Note**
>
> Se você receber um erro ao baixar o arquivo e estiver usando o Windows Server 2016 ou anterior, talvez seja necessário habilitar o TLS 1.2 para seu terminal PowerShell. É possível habilitar o TLS 1.2 para a sessão atual do PowerShell com o comando a seguir e tentar novamente:
>
> ```
> [Net.ServicePointManager]::SecurityProtocol =
>  [Net.SecurityProtocolType]::Tls12
> ```

4. O comando msiexec instala o EC2Launch v2 no seguinte local nas instâncias do Windows Server: `%ProgramFiles%\Amazon\EC2Launch`. Para verificar se a instalação foi executada, você pode verificar o sistema de arquivos local na sua instância.

AWS Systems Manager Distributor

Para configurar atualizações automáticas para o EC2Launch v2 com a Configuração rápida do AWS Systems Manager, consulte Instalar e atualizar automaticamente com o Distributor Quick Setup.

Você também pode realizar uma instalação única do pacote `AWSEC2Launch-Agent` a partir do Distribuidor do AWS Systems Manager. Para obter instruções sobre como instalar um pacote com

o Systems Manager Distributor, consulte Instalar ou atualizar pacotes no Guia do usuário do AWS Systems Manager SSM.

EC2 Image Builder component

É possível instalar o componente `ec2launch-v2-windows` ao criar uma imagem personalizada com o EC2 Image Builder. Para instruções sobre como criar uma imagem personalizada com o EC2 Image Builder, consulte Create an image pipeline using the EC2 Image Builder console wizard no Guia do usuário do EC2 Image Builder.

AMI

O EC2Launch v2 é pré-instalado por padrão nas seguintes AMIs do Windows Server 2022 e sistemas operacionais superiores:

- Windows_Server-*version*-English-Full-Base
- Windows_Server-*version*-English-Core-Base
- Windows_Server-*version*-English-Core-EKS_Optimized
- AMIs da *versão* do Windows Server com todos os outros idiomas
- AMIs da *versão* do Windows Server com SQL instalado

O EC2Launch v2 também vem pré-instalado nas AMIs do Windows Server a seguir. Essas AMIs podem ser encontradas no console do Amazon EC2. Também é possível usar o seguinte prefixo de pesquisa: `EC2LaunchV2-` na AWS CLI.

- EC2LaunchV2-Windows_Server-2019-English-Core-Base
- EC2LaunchV2-Windows_Server-2019-English-Full-Base
- EC2LaunchV2-Windows_Server-2016-English-Core-Base
- EC2LaunchV2-Windows_Server-2016-English-Full-Base

Instalar e atualizar o EC2Launch v2 automaticamente com o AWS Systems Manager Distributor Quick Setup

Com o AWS Systems Manager Distributor Quick Setup, você pode configurar atualizações automáticas para o EC2Launch v2. O processo a seguir configura uma Associação do Systems Manager na sua instância que atualiza automaticamente o agente EC2Launch v2 em uma frequência que você especifica. A associação criada pelo Distributor Quick Setup pode incluir instâncias dentro de uma região e Conta da AWS ou instâncias dentro de uma Organização da AWS. Para obter

mais informações sobre como configurar uma organização, consulte Tutorial: Criar e configurar uma organização, no Guia do usuário do AWS Organizations.

Antes de começar, certifique-se de que as suas instâncias atendam a todos os pré-requisitos.

Pré-requisitos

Para configurar atualizações automáticas com o Distributor Quick Setup, suas instâncias devem atender aos seguintes pré-requisitos.

- Você tem pelo menos uma instância em execução que oferece suporte ao EC2Launch v2. Consulte os sistemas operacionais compatíveis com o EC2Launch v2.
- Você executou as tarefas de configuração do Systems Manager nas suas instâncias. Para obter mais informações, consulte Configurar o Systems Manager, no Guia do usuário do AWS Systems Manager.
- O EC2Launch v2 deve ser o único agente de inicialização instalado na sua instância. Se você tiver mais de um agente de inicialização instalado, sua configuração do Distributor Quick Setup falhará. Antes de configurar o EC2Launch v2 com o Distributor Quick Setup, desinstale os agentes de inicialização EC2Config ou EC2Launch v1, se existirem.

Configurar o Distributor Quick Setup para o EC2Launch v2

Para criar uma configuração para o EC2Launch v2 com o Distributor Quick Setup, use as seguintes configurações ao concluir as etapas de Implantação do pacote do Distributor:

- Pacotes de software: agente Amazon EC2Launch v2.
- Frequência de atualização: selecione uma frequência na lista.
- Destinos: escolha entre as opções de implantação disponíveis.

Para verificar o status da sua configuração, navegue até a guia Configurações do Systems Manager Quick Setup no Console de gerenciamento da AWS.

1. Abra o console AWS Systems Manager em https://console.aws.amazon.com/systems-manager/.
2. No painel de navegação, escolha Configuração rápida.
3. Na guia Configurações, selecione a linha associada à configuração que você criou. A guia Configurações lista suas configurações e inclui um resumo dos principais detalhes, como Região, Status da implantação e Status da associação.

> **Note**
>
> O nome da associação para cada configuração do EC2Launch v2 Distributor começa com o seguinte prefixo: `AWS-QuickSetup-Distributor-EC2Launch-Agent-`.

4. Para visualizar detalhes, selecione a configuração e escolha Visualizar detalhes.

Para obter mais informações e etapas para a solução de problemas, consulte Solução de problemas com resultados do Quick Setup, no Guia do usuário do AWS Systems Manager.

Downloads do EC2Launch v2 no Amazon S3

Para instalar a versão mais recente do EC2Launch v2, baixe o instalador do local a seguir:

- https://s3.amazonaws.com/amazon-ec2launch-v2/windows/amd64/latest/AmazonEC2Launch.msi

Configurar opções de instalação

Ao instalar ou atualizar o EC2Launch v2, será possível configurar as opções de instalação com a caixa de diálogo de instalação do EC2Launch v2 ou com o comando msiexec em um shell de linha de comando.

Na primeira vez que o instalador do EC2Launch v2 é executado em uma instância, ele inicializa as configurações do agente de execução em sua instância da seguinte forma:

- Ele cria o caminho local e grava nele o arquivo do agente de execução. Algumas vezes, isso é chamado de instalação limpa.
- Ele cria a variável de ambiente `EC2LAUNCH_TELEMETRY`, se ela ainda não existir, e a define com base na sua configuração.

Para obter detalhes de configuração, selecione a guia que corresponde ao método de configuração que você usará.

Amazon EC2Launch Setup dialog

Ao instalar ou atualizar o EC2Launch v2, será possível configurar as opções de instalação a seguir na caixa de diálogo de instalação do EC2Launch v2.

Opções de Instalação básica

Enviar telemetria

Quando você inclui esse recurso na caixa de diálogo de configuração, o instalador define a variável de ambiente `EC2LAUNCH_TELEMETRY` para o valor `1`. Se você desabilitar a opção Enviar telemetria, o instalador definirá a variável de ambiente com um valor de `0`.

Quando o agente EC2Launch v2 é executado, ele lê a variável de ambiente `EC2LAUNCH_TELEMETRY` para determinar se os dados de telemetria devem ser carregados. Se o valor for igual a `1`, ele carregará os dados. Caso contrário, os dados não serão carregados.

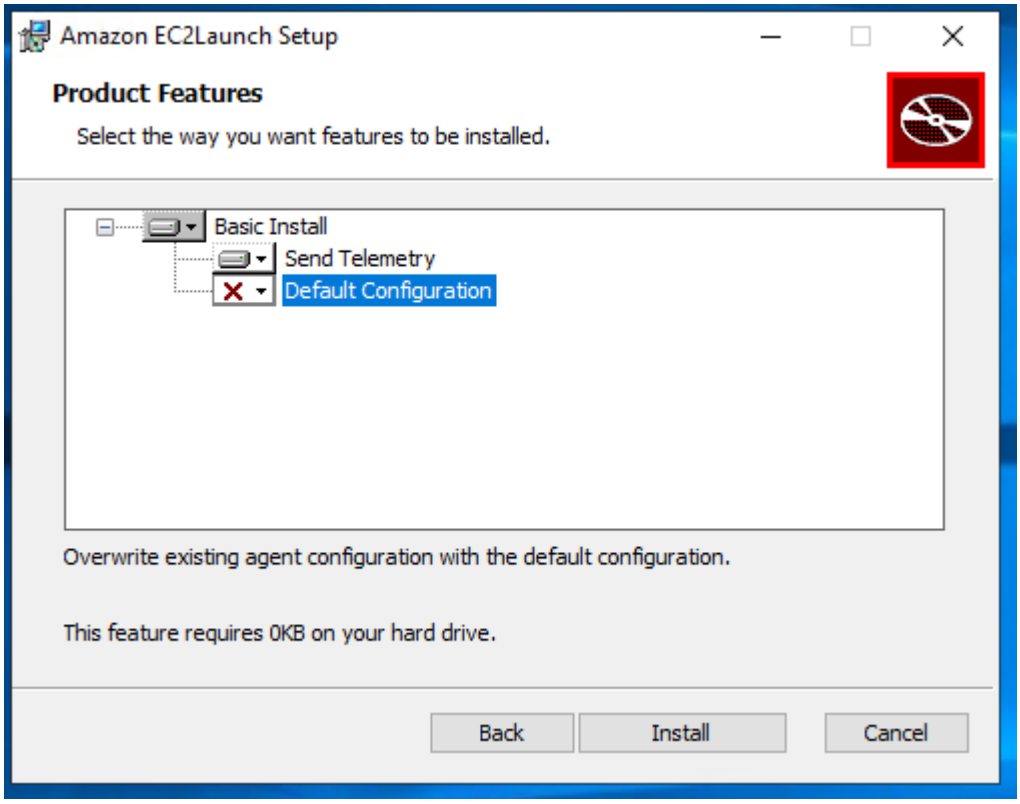
Configuração padrão

A configuração padrão do EC2Launch v2 é sobrescrever o agente de inicialização local, caso ele já exista. Na primeira vez que você executa uma instalação em uma instância, a configuração padrão realiza uma instalação limpa. Se a configuração padrão for desabilitada na instalação inicial, a instalação falhará.

Se você executar a instalação novamente na instância, poderá desabilitar a configuração padrão para realizar uma atualização que não substitua o arquivo `%ProgramData%/Amazon/EC2Launch/config/agent-config.yml`.

Exemplo: atualizar o EC2Launch v2 com telemetria

O exemplo a seguir mostra a caixa de diálogo de configuração do EC2Launch v2 configurada para atualizar a instalação atual e habilitar a telemetria. Essa configuração realiza uma instalação sem substituir o arquivo de configuração do agente e define a variável de ambiente `EC2LAUNCH_TELEMETRY` para o valor `1`.



Command line

Ao instalar ou atualizar o EC2Launch v2, será possível configurar as seguintes opções de instalação com o comando msiexec em um shell de linha de comando.

Valores do parâmetro **`ADDLOCAL`**

Básico (obrigatório)

Instale o agente de execução. Se esse valor não estiver presente no parâmetro `ADDLOCAL`, a instalação terminará.

Limpa

Quando o valor `Clean` é incluído no parâmetro `ADDLOCAL`, o instalador grava o arquivo de configuração do agente no seguinte local: `%ProgramData%/Amazon/EC2Launch/config/agent-config.yml`. Se o arquivo de configuração do agente já existir, ele sobrescreverá o arquivo.

Quando o valor `Clean` é deixado de fora do parâmetro `ADDLOCAL`, o instalador executa uma atualização que não substitui o arquivo de configuração do agente.

Telemetria

Quando o valor `Telemetry` é incluído no parâmetro `ADDLOCAL`, o instalador define a variável de ambiente `EC2LAUNCH_TELEMETRY` para o valor `1`.

Quando o valor `Telemetry` é deixado de fora do parâmetro `ADDLOCAL`, o instalador define a variável de ambiente para o valor `0`.

Quando o agente EC2Launch v2 é executado, ele lê a variável de ambiente `EC2LAUNCH_TELEMETRY` para determinar se os dados de telemetria devem ser carregados. Se o valor for igual a 1, ele carregará os dados. Caso contrário, os dados não serão carregados.

Exemplo: instalar o EC2Launch v2 com telemetria

```
& msiexec /i "C:\Users\Administrator\Desktop\EC2Launchv2\AmazonEC2Launch.msi"
 ADDLOCAL="Basic,Clean,Telemetry" /q
```

Verificar a versão do EC2Launch v2

Use o procedimento a seguir para verificar a versão do EC2Launch v2 que está instalada nas suas instâncias.

PowerShell

Verifique a versão instalada do EC2Launch v2 com o Windows PowerShell.

1. Execute uma instância pela AMI e conecte-se a ela.
2. Execute o comando a seguir no Windows PowerShell a seguir para verificar a versão instalada do EC2Launch v2.

   ```
   & "C:\Program Files\Amazon\EC2Launch\EC2Launch.exe" version
   ```

Windows Control Panel

Verifique a versão instalada do EC2Launch v2 no Painel de Controle do Windows conforme descrito a seguir.

1. Execute uma instância pela AMI e conecte-se a ela.
2. Abra o Painel de Controle do Windows e selecione Programas e Recursos.
3. Procure `Amazon EC2Launch` na lista de programas instalados. O número da versão aparece na coluna Versão.

Para visualizar as atualizações mais recentes das AMIs do AWS Windows, consulte o histórico de versões da AMI do Windows na Referência da AMI do AWS Windows.

Para obter a versão mais recente do EC2Launch v2, consulte Histórico de versões do EC2Launch v2.

É possível receber notificações quando novas versões do serviço EC2Launch v2 forem liberadas. Para obter mais informações, consulte Assinar as notificações do agente de execução do EC2 Windows.

Definição das configurações do EC2Launch v2 para instâncias do Windows

Esta seção contém informações sobre como definir configurações para o EC2Launch v2.

Os tópicos incluem:

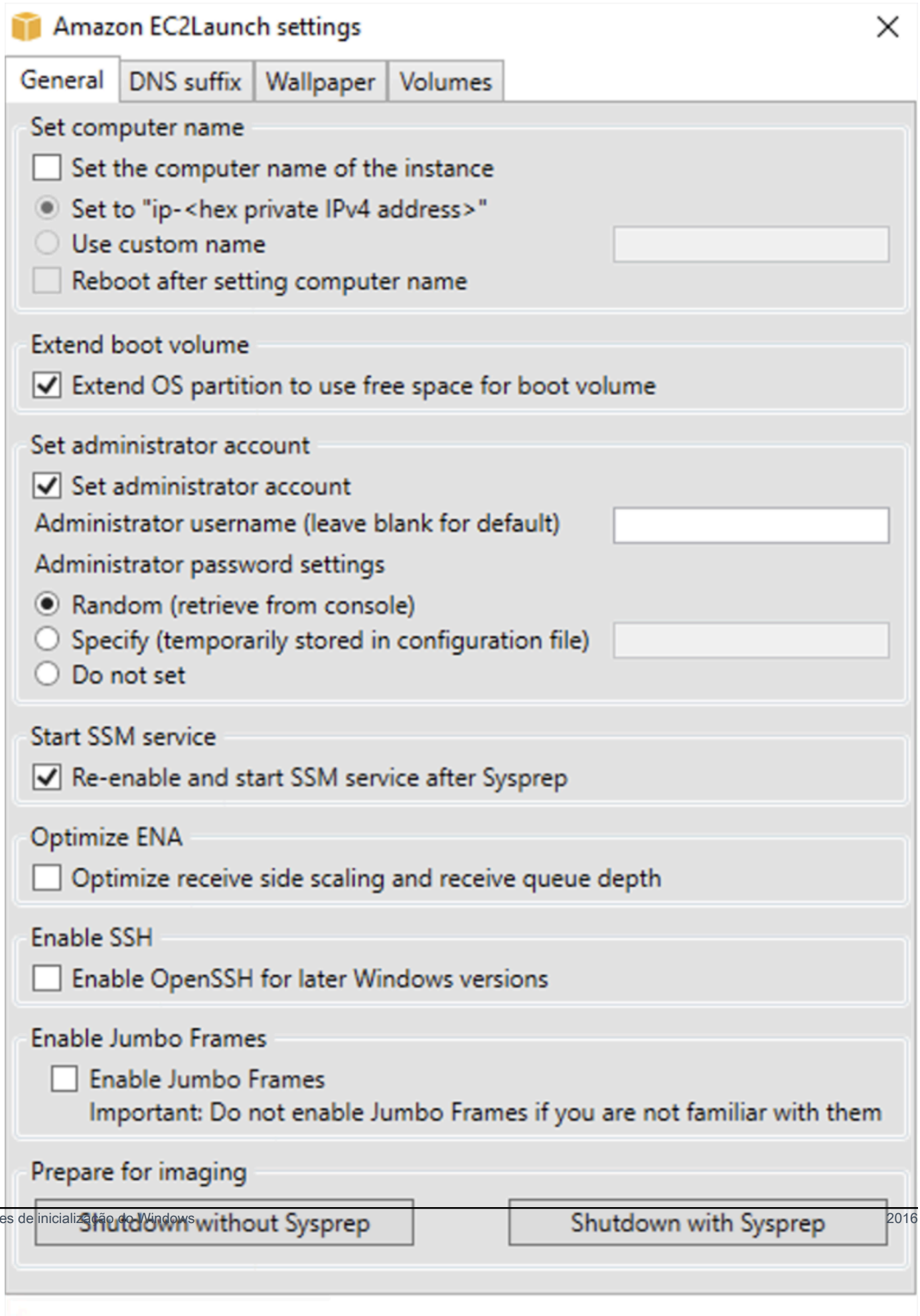
- Alterar configurações usando a caixa de diálogo de configurações do EC2Launch v2
- Configurar o EC2Launch v2 com a CLI
- Configuração de tarefas do EC2Launch v2
- Códigos de saída e reinicializações do EC2Launch v2
- EC2Launch v2 e Sysprep

Alterar configurações usando a caixa de diálogo de configurações do EC2Launch v2

O procedimento a seguir descreve como usar a caixa de diálogo de configurações do EC2Launch v2 para habilitar ou desabilitar configurações.

> **Note**
>
> Se você configurar de forma imprópria tarefas personalizadas no arquivo agent-config.yml e tentar abrir a caixa de diálogo de configurações Amazon EC2Launch, receberá um erro. Por obter um exemplo de esquema, consulte Exemplo: `agent-config.yml`.

1. Execute e conecte-se à sua instância do Windows.
2. No menu Iniciar, escolha Todos os programas e navegue até as Configurações do EC2Launch. Antes de escolher Desligar com Sysprep ou Desligar sem Sysprep, salve as alterações que deseja aplicar ao executar o desligamento.


Amazon EC2Launch settings
General
DNS suffix
Wallpaper
Volumes
Set computer name
Set the computer name of the instance
Set to "ip-<hex private IPv4 address>"
Use custom name
Reboot after setting computer name
Extend boot volume
Extend OS partition to use free space for boot volume
Set administrator account
Set administrator account
Administrator username (leave blank for default)
Administrator password settings
Random (retrieve from console)
Specify (temporarily stored in configuration file)
Do not set
Start SSM service
Re-enable and start SSM service after Sysprep
Optimize ENA
Optimize receive side scaling and receive queue depth
Enable SSH
Enable OpenSSH for later Windows versions
Enable Jumbo Frames
Enable Jumbo Frames
Important: Do not enable Jumbo Frames if you are not familiar with them
Prepare for imaging
Shutdown without Sysprep
Shutdown with Sysprep

3. Na guia Geral da caixa de diálogo Configurações do EC2Launch, é possível habilitar ou desabilitar as configurações a seguir.

   a. Definir o nome do computador

      Se essa configuração estiver habilitada (por padrão, ela fica desabilitada), o nome do host atual será comparado com o nome de host desejado em cada inicialização. Se os nomes de host não corresponderem, o nome do host será redefinido e o sistema, opcionalmente, reinicializa para ficar com o novo nome de host. Se um nome de host personalizado não for especificado, ele será gerado usando o endereço IPv4 privado formatado hexadecimal, por exemplo, `ip-AC1F4E6`. Para impedir a modificação de um nome de host existente, não habilite essa configuração.

   b. Estender o volume de inicialização

      Essa configuração amplia dinamicamente o `Disk 0`/`Volume 0` para incluir qualquer espaço não particionado. Isto pode ser útil quando a instância é inicializada usando um volume raiz com tamanho personalizado.

   c. Definir a conta do administrador

      Quando habilitado, é possível definir os atributos de nome de usuário e senha para a conta de administrador criada em sua máquina local. Se esse recurso não estiver habilitado, uma conta de administrador não será criada no sistema após o Sysprep. Forneça uma senha em `adminPassword` somente se `adminPasswordtype` for `Specify`.

      Os tipos de senha são definidos da seguinte maneira:

      i. `Random`

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

      ii. `Specify`

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

iii. `Do not set`

O EC2Launch usa a senha especificada no arquivo unattend.xml. Se você não especificar uma senha em unattend.xml, a conta de administrador será desativada.

d. Iniciar o serviço SSM

Quando selecionado, o serviço Systems Manager é habilitado para começar após o Sysprep. O EC2Launch v2 executa todas as tarefas descritas anteriormente e o SSM Agent processa recursos do Systems Manager, como Run Command e State Manager.

É possível usar Run Command para atualizar suas instâncias existentes e usar a versão mais recente do serviço do EC2Launch v2 e do SSM Agent. Para obter mais informações, consulte Atualizar o SSM Agent usando o Run Command no Guia do usuário do AWS Systems Manager.

e. Otimizar ENA

Quando selecionadas, as configurações do ENA são definidas para garantir que as configurações Receive Side Scaling (Receber dimensionamento lateral) e Receive Queue Depth (Receber profundidade da fila) sejam otimizadas para a AWS. Para obter mais informações, consulte Configurar a afinidade de CPU do Receive Side Scaling.

f. Habilitar SSH

Essa configuração habilita o OpenSSH para versões posteriores do Windows a fim de permitir a administração remota do sistema.

g. Ativar os frames jumbo

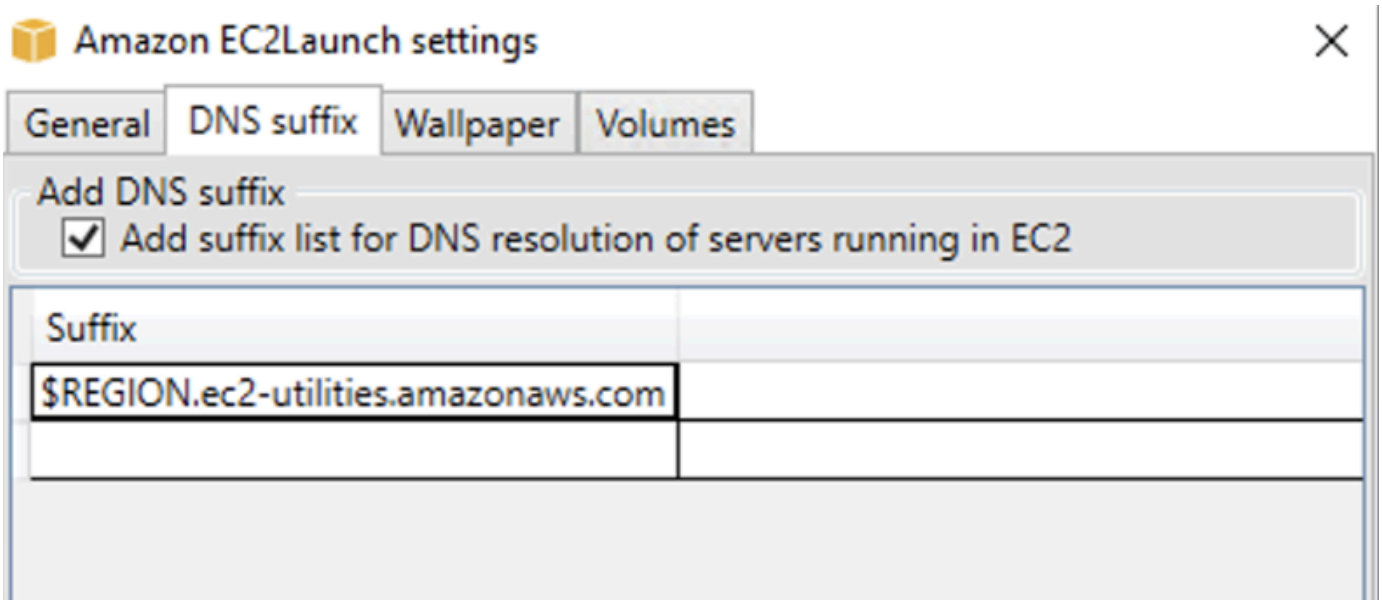
Selecione para ativar frames jumbo. Os frames jumbo podem ter efeitos não intencionais sobre suas comunicações de rede, portanto, certifique-se de entender como eles afetarão seu sistema antes de ativá-los. Para obter mais informações sobre os frames jumbo, consulte Frames jumbo (9001 MTU).

h. Preparar para imagens

Selecione se deseja que sua instância do EC2 seja desligada com ou sem Sysprep. Quando quiser executar o Sysprep com o EC2Launch v2, escolha Shutdown with Sysprep (Desligar com Sysprep).

4. Na guia Sufixo DNS, é possível selecionar se deseja adicionar uma lista de sufixos DNS para resolução DNS de servidores em execução no EC2, sem fornecer o nome de domínio totalmente

qualificado. Os sufixos DNS podem conter as variáveis `$REGION` e `$AZ`. Somente sufixos que ainda não existem serão adicionados à lista.

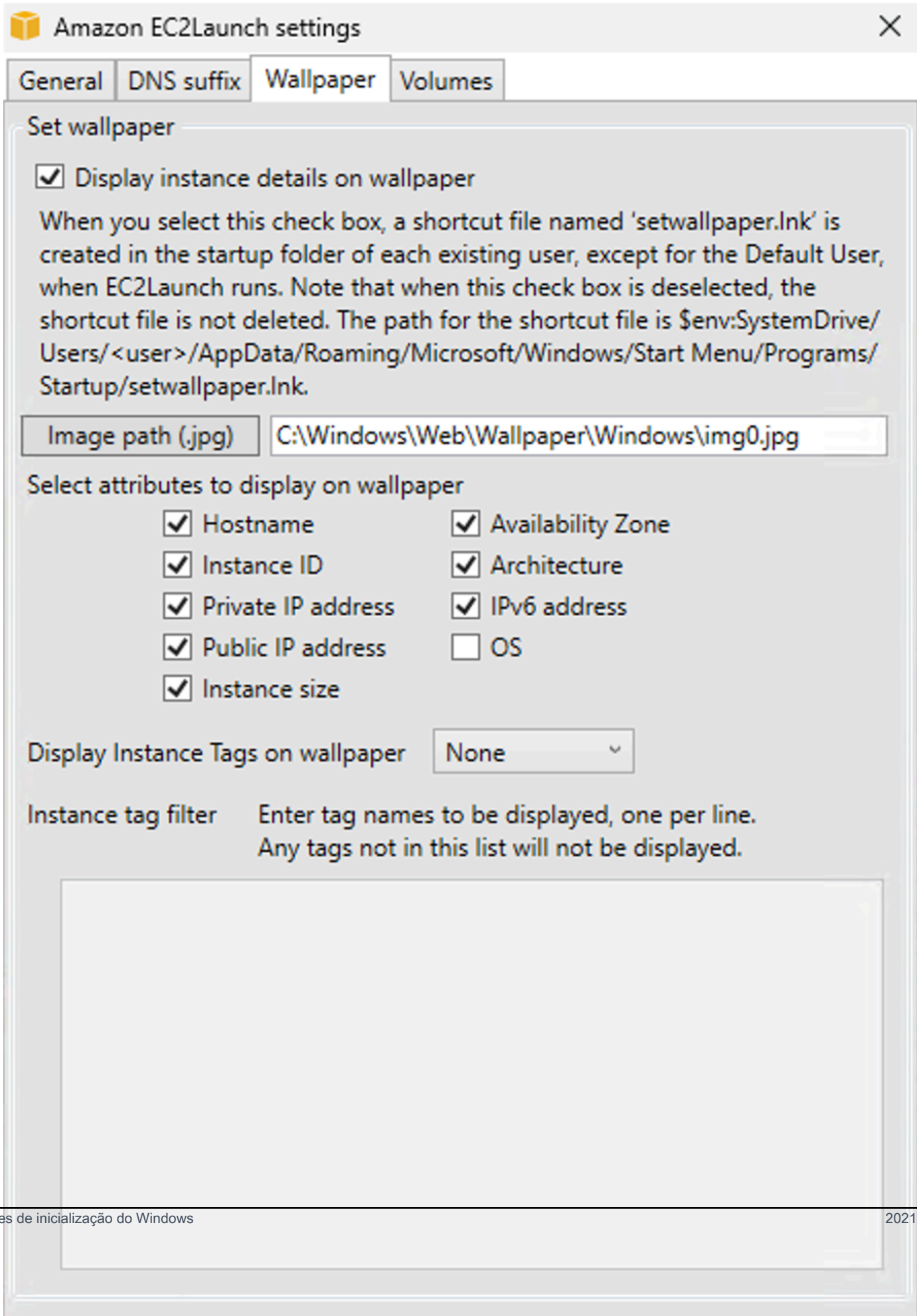


5. Na guia Papel de parede, você pode configurar o papel de parede da instância com uma imagem de fundo e especificar os detalhes da instância a serem exibidos no papel de parede. O Amazon EC2 gera os detalhes toda vez que você faz login.

   É possível configurar o papel de parede com os seguintes controles.

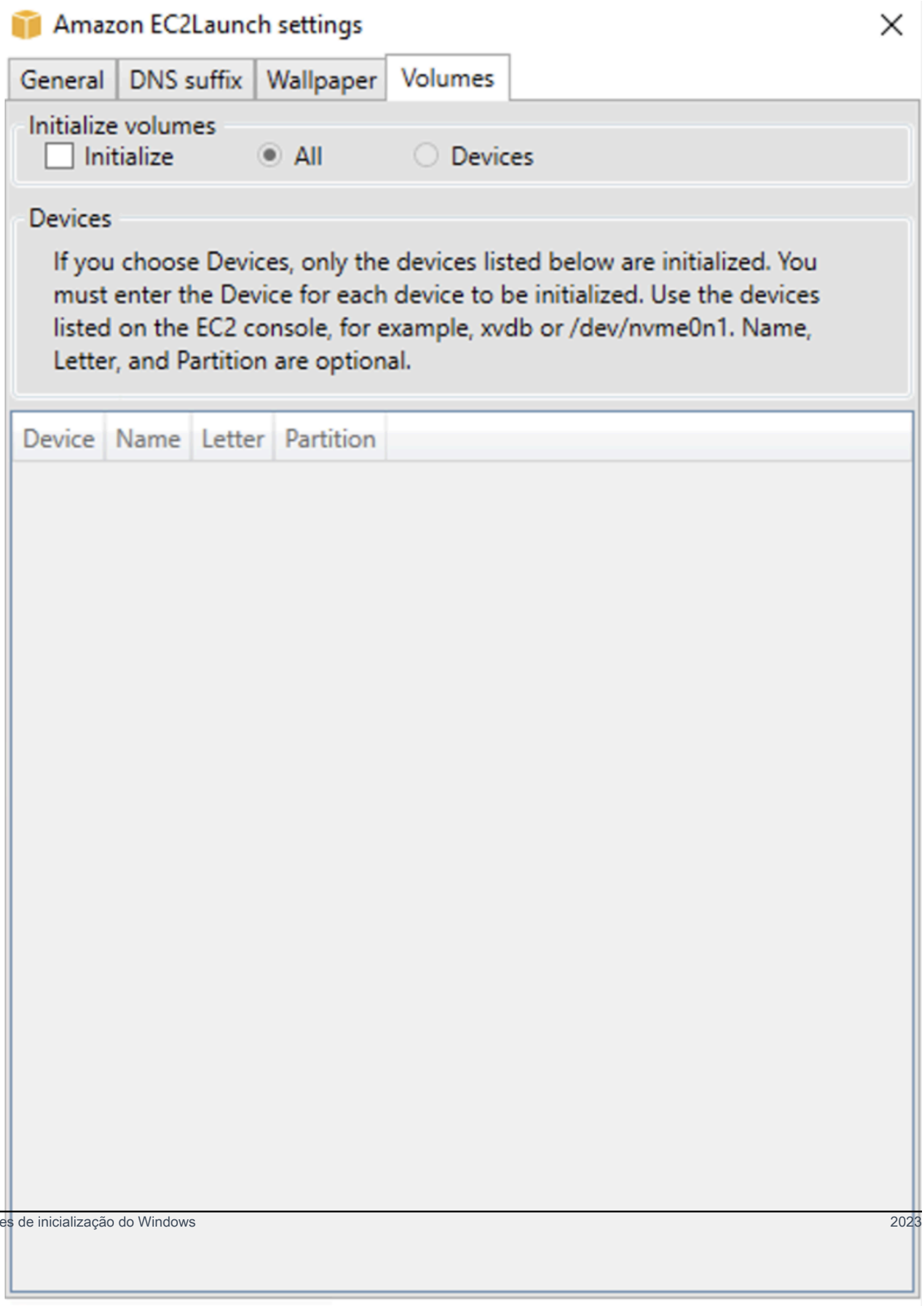
   - Exibir detalhes da instância no papel de parede: essa caixa de seleção ativa ou desativa a exibição de detalhes da instância no papel de parede.
   - Caminho da imagem (.jpg): especifique o caminho até a imagem a ser usada como plano de fundo do papel de parede.
   - Selecionar atributos a serem exibidos no papel de parede: marque as caixas de seleção dos detalhes da instância que você deseja que apareçam no papel de parede. Desmarque as caixas de seleção dos detalhes da instância selecionados anteriormente que você deseja remover do papel de parede.
   - Exibir tags de instância no papel de parede: selecione uma das seguintes configurações para exibir tags de instância no papel de parede:
     - Nenhuma: não exiba nenhuma tag de instância no papel de parede.
     - Mostrar todas: exiba todas as tags de instância no papel de parede.
     - Mostrar filtradas: exibe as tags de instância especificadas no papel de parede. Quando você selecionar essa configuração, será possível adicionar tags de instância que você deseje exibir no seu papel de parede na caixa Filtro de tag de instância.

> **Note**
>
> Você deve habilitar as tags nos metadados para mostrá-las no papel de parede. Para obter mais informações sobre tags e metadados da instância, consulte Visualizar tags para as instâncias do EC2 usando os metadados de instância.


Amazon EC2Launch settings
General
DNS suffix
Wallpaper
Volumes
Set wallpaper
Display instance details on wallpaper
When you select this check box, a shortcut file named 'setwallpaper.lnk' is created in the startup folder of each existing user, except for the Default User, when EC2Launch runs. Note that when this check box is deselected, the shortcut file is not deleted. The path for the shortcut file is $env:SystemDrive/Users/<user>/AppData/Roaming/Microsoft/Windows/Start Menu/Programs/Startup/setwallpaper.lnk.
Image path (.jpg)
C:\Windows\Web\Wallpaper\Windows\img0.jpg
Select attributes to display on wallpaper
Hostname
Instance ID
Private IP address
Public IP address
Instance size
Availability Zone
Architecture
IPv6 address
OS
Display Instance Tags on wallpaper
None
Instance tag filter
Enter tag names to be displayed, one per line.
Any tags not in this list will not be displayed.

6. Na guia Volumes, selecione se deseja inicializar os volumes anexados à instância. A ativação define letras de unidade para quaisquer volumes adicionais e estende-as para usar o espaço disponível. Se você selecionar Todos, todos os volumes de armazenamento serão inicializados. Se você selecionar Dispositivos, somente os dispositivos especificados na lista serão inicializados. É preciso inserir cada dispositivo a ser inicializado. Use os dispositivos listados no console do EC2, por exemplo, `xvdb` ou `/dev/nvme0n1`. A lista suspensa exibe os volumes de armazenamento anexados à instância. Para inserir um dispositivo que não está anexado à instância, insira-o no campo de texto.

   Nome, Letra e Partição são campos opcionais. Se nenhum valor for especificado para Partição, os volumes de armazenamento com mais de 2 TB serão inicializados com o tipo de partição `gpt` e os com menos de 2 TB serão inicializados com o tipo de partição `mbr`. Se os dispositivos estiverem configurados e um dispositivo não NTFS contiver uma tabela de partição ou os primeiros 4 KB do disco contiverem dados, o disco será ignorado e a ação será registrada.


Amazon EC2Launch settings
General
DNS suffix
Wallpaper
Volumes
Initialize volumes
Initialize
All
Devices
Devices
If you choose Devices, only the devices listed below are initialized. You must enter the Device for each device to be initialized. Use the devices listed on the EC2 console, for example, xvdb or /dev/nvme0n1. Name, Letter, and Partition are optional.
Device
Name
Letter
Partition

Configurar o EC2Launch v2 com a CLI

É possível usar a Interface de Linhas de Comando (CLI) para definir suas configurações do EC2Launch e gerenciar o serviço. A seção a seguir contém descrições e informações de uso dos comandos da CLI que podem ser usados para gerenciamento do EC2Launch v2.

Comandos

- collect-logs
- get-agent-config
- list-volumes
- reset
- executar
- status
- sysprep
- validar
- version
- wallpaper

collect-logs

Coleta arquivos de log para o EC2Launch, compacta os arquivos e os coloca em um diretório especificado.

Exemplo do

```
ec2launch collect-logs -o C:\Mylogs.zip
```

Usage

`ec2launch collect-logs [flags]`

Sinalizadores

`-h`, `--help`

ajuda para `collect-logs`

`-o, --output string`

caminho para arquivos de log de saída compactados

get-agent-config

Imprime `agent-config.yml` no formato especificado (JSON ou YAML). Se nenhum formato for especificado, `agent-config.yml` será impresso no formato especificado anteriormente.

Exemplo do

```
ec2launch get-agent-config -f json
```

Usage

`ec2launch get-agent-config [flags]`

Sinalizadores

`-h, --help`

ajuda para `get-agent-config`

`-f, --format string`

formato de saída do arquivo `agent-config`: `json`, `yaml`

list-volumes

Lista todos os volumes de armazenamento anexados à instância, incluindo volumes temporários e do EBS.

Exemplo do

```
ec2launch list-volumes
```

Usage

`ec2launch list-volumes`

Sinalizadores

`-h, --help`

ajuda para `list-volumes`

reset

O objetivo principal dessa tarefa é redefinir o agente para a próxima vez que ele for executado. Para fazer isso, o comando reset exclui todos os dados de estado do agente do EC2Launch v2 do `EC2Launch` diretório local (consulte Estrutura de diretório do EC2Launch v2). Opcionalmente, a redefinição exclui os logs do serviço e do Sysprep.

O comportamento do script depende do modo em que o agente executa os scripts: em linha ou desanexados.

Em linha (padrão)

O agente EC2Launch v2 executa os scripts um de cada vez (`detach: false`) Essa é a configuração padrão.

> **Note**
>
> Quando seu script em linha emite um comando reset ou sysprep, ele é executado imediatamente e redefine o agente. A tarefa atual é concluída e, em seguida, o agente é desligado sem executar mais nenhuma tarefa.
> Por exemplo, se a tarefa que emite o comando tivesse sido seguida por uma tarefa `startSsm` (incluída por padrão após a execução dos dados do usuário), a tarefa não executaria e o serviço Systems Manager nunca seria iniciado.

Desanexados

O agente do EC2Launch v2 executa scripts simultaneamente com outras tarefas (`detach: true`).

> **Note**
>
> Quando seu script desanexado emite um comando reset ou sysprep, esses comandos aguardam a conclusão do agente antes de serem executados. As tarefas após executeScript ainda serão executadas.

Exemplo do

```
ec2launch reset -c
```

Usage

`ec2launch reset [flags]`

Sinalizadores

`-c`, `--clean`

limpa os logs da instância antes de `reset`

`-h`, `--help`

ajuda para `reset`

executar

Executa o EC2Launch v2.

Exemplo do

```
ec2launch run
```

Usage

`ec2launch run [flags]`

Sinalizadores

`-h`, `--help`

ajuda para `run`

status

Obtém o status do agente EC2Launch v2. Opcionalmente, bloqueia o processo até que o agente seja concluído. O código de saída do processo determina o estado do agente:

- `0`: o agente foi executado de forma bem-sucedida.

- 1: o agente foi executado e apresentou falha.
- 2: o agente ainda está em execução.
- 3: o agente está em um estado desconhecido. O estado do agente é não está em execução ou foi interrompido.
- 4: ocorreu um erro ao tentar recuperar o estado do agente.
- 5: o agente não está em execução e o status da última execução conhecida é desconhecido. Isso pode significar uma das seguintes opções:
  - tanto o `state.json` quanto o `previous-state.json` foram excluídos.
  - o `previous-state.json` está corrompido.

  Este é o estado do agente após executar o comando `reset`.

Exemplo do:

```
ec2launch status -b
```

Usage

`ec2launch status [flags]`

Sinalizadores

`-b,--block`

bloqueia o processo até que o agente conclua a execução

`-h,--help`

ajuda para `status`

sysprep

O objetivo principal dessa tarefa é redefinir o agente para a próxima vez que ele for executado. Para fazer isso, o comando sysprep redefine o estado do agente, atualiza o arquivo `unattend.xml`, desabilita o RDP e executa o Sysprep.

O comportamento do script depende do modo em que o agente executa os scripts: em linha ou desanexados.

Em linha (padrão)

O agente EC2Launch v2 executa os scripts um de cada vez (`detach: false`) Essa é a configuração padrão.

> **Note**
>
> Quando seu script em linha emite um comando reset ou sysprep, ele é executado imediatamente e redefine o agente. A tarefa atual é concluída e, em seguida, o agente é desligado sem executar mais nenhuma tarefa.
> Por exemplo, se a tarefa que emite o comando tivesse sido seguida por uma tarefa `startSsm` (incluída por padrão após a execução dos dados do usuário), a tarefa não executaria e o serviço Systems Manager nunca seria iniciado.

Desanexados

O agente do EC2Launch v2 executa scripts simultaneamente com outras tarefas (`detach: true`).

> **Note**
>
> Quando seu script desanexado emite um comando reset ou sysprep, esses comandos aguardam a conclusão do agente antes de serem executados. As tarefas após executeScript ainda serão executadas.

Exemplo do:

```
ec2launch sysprep
```

Usage

`ec2launch sysprep [flags]`

Sinalizadores

`-c,--clean`

limpa os logs da instância antes de `sysprep`

`-h,--help`

ajuda para Sysprep

`-s,--shutdown`

desliga a instância após `sysprep`

validar

Valida o arquivo `agent-config` `C:\ProgramData\Amazon\EC2Launch\config\agent-config.yml`.

Exemplo do

```
ec2launch validate
```

Usage

`ec2launch validate [flags]`

Sinalizadores

`-h , --help`

ajuda para `validate`

version

Obtém a versão executável.

Exemplo do

```
ec2launch version
```

Usage

`ec2launch version [flags]`

Sinalizadores

`-h, --help`

ajuda para `version`

wallpaper

Define o novo papel de parede para o caminho de papel de parede fornecido (arquivo .jpg) e exibe os detalhes da instância selecionada.

Sintaxe

```
ec2launch wallpaper ^
--path="C:\ProgramData\Amazon\EC2Launch\wallpaper\Ec2Wallpaper.jpg" ^
--all-tags ^
--
attributes=hostName,instanceId,privateIpAddress,publicIpAddress,ipv6Address,instanceSize,availa
```

Entradas

Parâmetros

--allowed-tags [***`tag-name-1`***, ***`tag-name-n`***]

(Opcional) Matriz JSON codificada em Base64 de nomes de tags de instância para exibição no papel de parede. É possível usar essa tag ou `--all-tags`, mas não ambas.

--attributes ***`attribute-string-1`***, ***`attribute-string-n`***

(Opcional) uma lista separada por vírgulas de strings de atributo `wallpaper` para aplicar configurações ao papel de parede.

[--path | -p] ***`path-string`***

(Obrigatório) Especifica o caminho do arquivo da imagem do plano de fundo do `wallpaper`.

Sinalizadores

--all-tags

(Opcional) Exibe todas as tags de instância no papel de parede. É possível usar essa tag ou `--allowed-tags`, mas não ambas.

[--help | -h]

Exibe a ajuda referente ao comando wallpaper.

Configuração de tarefas do EC2Launch v2

Esta seção inclui o esquema, tarefas, detalhes e exemplos de configuração para `agent-config.yml` e dados do usuário.

Tarefas e exemplos

- Esquema: agent-config.yml
- Configurar scripts de dados do usuário do EC2Launch v2 que são executados durante a execução ou reinicialização

Esquema: **`agent-config.yml`**

Veja a estrutura do arquivo `agent-config.yml` abaixo. Não é possível repetir uma tarefa na mesma etapa. Para obter as propriedades da tarefa, consulte as descrições da tarefa a seguir.

Estrutura do documento: agent-config.yml

JSON

```
{
 "version": "1.1",
 "config": [
  {
   "stage": "string",
   "tasks": [
    {
     "task": "string",
     "inputs": {
      ...
     }
    },
    ...
   ]
  },
  ...
 ]
```

```
}
```

YAML

```
version: 1.1
config:
- stage: string
  tasks:
  - task: string
 inputs:
   ...
  ...
...
```

Exemplo: **`agent-config.yml`**

O exemplo a seguir mostra as configurações do arquivo de configuração `agent-config.yml`.

```
version: 1.1
config:
- stage: boot
  tasks:
  - task: extendRootPartition
- stage: preReady
  tasks:
  - task: activateWindows
    inputs:
      activation:
        type: amazon
  - task: setDnsSuffix
    inputs:
      suffixes:
      - $REGION.ec2-utilities.amazonaws.com
  - task: setAdminAccount
    inputs:
      password:
        type: random
  - task: setWallpaper
    inputs:
      path: C:\ProgramData\Amazon\EC2Launch\wallpaper\Ec2Wallpaper.jpg
      attributes:
      - hostName
      - instanceId
```

```
      - privateIpAddress
      - publicIpAddress
      - instanceSize
      - availabilityZone
      - architecture
- stage: postReady
  tasks:
  - task: startSsm
```

Configurar scripts de dados do usuário do EC2Launch v2 que são executados durante a execução ou reinicialização

Os exemplos de JSON e YAML a seguir mostram a estrutura do documento para dados do usuário. O Amazon EC2 analisa cada tarefa nomeada na matriz `tasks` que você especifica no documento. Cada tarefa tem seu próprio conjunto de propriedades e requisitos. Para obter detalhes, consulte Definições de tarefas para tarefas de inicialização do EC2Launch v2.

> **Note**
>
> Uma tarefa só deve aparecer uma vez na matriz de tarefas de dados do usuário.

Estrutura do documento: dados do usuário

JSON

```
{
 "version": "1.1",
 "tasks": [
  {
   "task": "string",
   "inputs": {
    ...
   },
  },
  ...
 ]
}
```

YAML

```
version: 1.1
```

```
tasks:
- task: string
  inputs:
    ...
...
```

Exemplo: dados do usuário

Para obter mais informações sobre as funções de usuário, consulte Como o Amazon EC2 lida com os dados dos usuários para instâncias do Windows.

O exemplo de documento YAML a seguir mostra um script do PowerShell que o EC2Launch v2 executa como dados do usuário para criar um arquivo.

```
version: 1.1
tasks:
- task: executeScript
  inputs:
  - frequency: always
    type: powershell
    runAs: localSystem
    content: |-
      New-Item -Path 'C:\PowerShellTest.txt' -ItemType File
```

É possível usar um formato XML para os dados do usuário que seja compatível com as versões anteriores do agente de inicialização. O EC2Launch v2 executa o script como uma tarefa `executeScript` no estágio `UserData`. Para atender ao comportamento do EC2Launch v1 e do EC2Config, o script de dados do usuário é executado por padrão como um processo anexado/em linha.

É possível adicionar tags opcionais para personalizar a execução do seu script. Por exemplo, para executar o script de dados do usuário quando a instância é reinicializada, além de uma vez quando a instância é iniciada, é possível usar a seguinte tag:

```
<persist>true</persist>
```

Exemplo do:

```
<powershell>
  $file = $env:SystemRoot + "\Temp" + (Get-Date).ToString("MM-dd-yy-hh-mm")
```

```
  New-Item $file -ItemType file
</powershell>
<persist>true</persist>
```

É possível especificar um ou mais argumentos do PowerShell com tag `<powershellArguments>`. Se nenhum argumento for passado, o EC2Launch v2 adicionará o seguinte argumento por padrão: `-ExecutionPolicy Unrestricted`.

Exemplo do:

```
<powershell>
  $file = $env:SystemRoot + "\Temp" + (Get-Date).ToString("MM-dd-yy-hh-mm")
  New-Item $file -ItemType file
</powershell>
<powershellArguments>-ExecutionPolicy Unrestricted -NoProfile -NonInteractive</
powershellArguments>
```

Para executar um script de dados de usuário XML como um processo separado, adicione a seguinte tag aos dados do usuário.

`<detach>true</detach>`

Exemplo do:

```
<powershell>
  $file = $env:SystemRoot + "\Temp" + (Get-Date).ToString("MM-dd-yy-hh-mm")
  New-Item $file -ItemType file
</powershell>
<detach>true</detach>
```

> **Note**
>
> A tag de desanexação não é compatível com agentes de inicialização anteriores.

Log de alterações: dados do usuário

A tabela a seguir lista as alterações nos dados do usuário e as faz referência cruzada à versão do agente EC2Launch v2 aplicável.

Versão de dados do usuário	Detalhes	Introduzida em
1.1	• As tarefas de dados do usuário são executadas antes do estágio `PostReady` no arquivo de configuração do agente. • Executa dados do usuário antes de iniciar o Systems Manager Agent (mesmo comportamento do EC2Launch v1 e do EC2Config).*	EC2Launch v2 versão 2.0.1245
1,0	• Será descontinuada. • As tarefas de dados do usuário são executadas depois do estágio `PostReady` no arquivo de configuração do agente. Isso não é compatível com versões anteriores do EC2Launch v1. • Impactado por uma condição de corrida entre o início do Systems Manager Agent e as tarefas de dados do usuário.	EC2Launch v2 versão 2.0.0

* Quando usado com o arquivo `agent-config.yml` padrão.

Códigos de saída e reinicializações do EC2Launch v2

É possível usar EC2Launch v2 para definir como os códigos de saída são manipulados por seus scripts. Por padrão, o código de saída do último comando executado em um script é relatado como o código de saída de todo o script. Por exemplo, se um script incluir três comandos e o primeiro comando falhar, mas os seguintes forem bem-sucedidos, o status de execução será relatado como `success` porque o comando final foi bem-sucedido.

Se quiser que um script reinicialize uma instância, você deverá especificar `exit 3010` em seu script, mesmo quando a reinicialização for a última etapa do script. O `exit 3010` instrui o EC2Launch v2 a reiniciar a instância e chamar o script novamente até que ele retorne um código de saída que não seja `3010` ou até que a contagem máxima de reinicializações seja atingida. O EC2Launch v2 permite um máximo de 5 reinicializações por tarefa. Se você tentar reiniciar uma

instância a partir de um script usando um mecanismo diferente, como `Restart-Computer`, o status de execução do script será inconsistente. Por exemplo, ele pode ficar preso em um loop de reinicialização ou não executar a reinicialização.

Se você estiver usando um formato de dados de usuário XML compatível com agentes mais antigos, os dados do usuário poderão ser executados mais vezes do que o pretendido. Para obter mais informações, consulte O serviço executa dados do usuário mais de uma vez na seção Solução de problemas.

EC2Launch v2 e Sysprep

O serviço EC2Launch v2 executa o Sysprep, uma ferramenta da Microsoft que permite a criação de uma AMI personalizada do Windows que pode ser reutilizada. Quando o EC2Launch v2 acessa o Sysprep, ela usa os arquivos em `%ProgramData%\Amazon\EC2Launch` para determinar quais operações devem ser executadas. É possível editar esses arquivos indiretamente usando a caixa de diálogo Configurações do EC2Launch ou diretamente usando um editor de YAML ou um editor de texto. Contudo, há algumas configurações avançadas que não estão disponíveis na caixa de diálogo Configurações do EC2Launch, portanto, é necessário editar as entradas diretamente.

Se você criar AMIs com base em uma instância depois de atualizar suas configurações, as configurações novas serão aplicadas a qualquer instância executada pela nova AMI. Para obter informações sobre como criar uma AMI, consulte Criação de uma AMI baseada no Amazon EBS.

Definições de tarefas para tarefas de inicialização do EC2Launch v2

Cada tarefa que o EC2Launch v2 inicia durante a inicialização ou startup tem seu próprio conjunto de propriedades e requisitos. Os detalhes da tarefa incluem configurações da frequência com que uma tarefa é executada: uma vez ou sempre, em qual estágio do processo de inicialização do agente ela é executada, a sintaxe e exemplos de documentos YAML. Para obter mais informações, revise os detalhes da tarefa mostrados nesta referência.

Tarefas do EC2Launch v2

- activateWindows
- enableJumboFrames
- enableOpenSsh
- executeProgram
- executeScript
- extendRootPartition

- initializeVolume
- optimizeEna
- setAdminAccount
- setDnsSuffix
- setHostName
- setWallpaper
- startSsm
- sysprep
- writeFile

activateWindows

Ativa o Windows em relação a um conjunto de servidores de AWS KMS. A ativação será ignorada se a instância for detectada como traga a sua própria licença (BYOL).

Frequência — uma vez

AllowedStages — `[PreReady]`

Entradas —

`activation`: (mapa)

`type`: (string) tipo de ativação a usar, defina como `amazon`

Exemplo do

```
task: activateWindows
  inputs:
    activation:
    type: amazon
```

enableJumboFrames

Habilita frames jumbo, que aumentam a MTU (unidade de transmissão máxima) do adaptador de rede. Para obter mais informações, consulte Frames jumbo (9001 MTU).

Frequência — sempre

AllowedStages — `[PostReady, UserData]`

Entradas — nenhuma

Exemplo do

```
task: enableJumboFrames
```

enableOpenSsh

Habilita o Windows OpenSSH e adiciona a chave pública da instância à pasta de chaves autorizadas.

Frequência — uma vez

AllowedStages — `[PreReady, UserData]`

Entradas — nenhuma

Exemplo do

O exemplo a seguir mostra como habilitar o OpenSSH em uma instância e adicionar a chave pública da instância à pasta de chaves autorizadas. Essa configuração funciona somente em instâncias que executam o Windows Server 2019 e versões posteriores.

```
task: enableOpenSsh
```

executeProgram

Executa um programa com argumentos opcionais e uma frequência especificada.

Estágios: você pode executar a tarefa `executeProgram` durante os estágios `PreReady`, `PostReady` e `UserData`.

Frequência: configurável. Consulte Entradas.

Entradas

Esta seção contém um ou mais programas para a tarefa executeProgram executar (entradas). Cada etapa pode incluir as seguintes definições configuráveis:

frequência (string)

(Obrigatório) Especifique exatamente um dos seguintes valores:

- `once`
- `always`

caminho (string)

(Obrigatório) O caminho do arquivo para que o executável seja executado.

argumentos (lista de strings)

(Opcional) Uma lista de argumentos separados por vírgula para fornecer ao programa como entrada.

runAs (string)

(Obrigatório) Deve ser definido como `localSystem`

Output

Todas as tarefas gravam entradas do arquivo de log no arquivo `agent.log`. A saída adicional da tarefa `executeProgram` é armazenada separadamente em uma pasta com nome dinâmico, da seguinte forma:

`%LocalAppData%\Temp\`*`EC2Launch#########\outputfilename.tmp`*

O caminho exato para os arquivos de saída está incluído no arquivo `agent.log`, por exemplo:

```
Program file is created at: C:\Windows\system32\config\systemprofile\AppData\Local
\Temp\EC2Launch123456789\ExecuteProgramInputs.tmp
Output file is created at: C:\Windows\system32\config\systemprofile\AppData\Local
\Temp\EC2Launch123456789\Output.tmp
Error file is created at: C:\Windows\system32\config\systemprofile\AppData\Local
\Temp\EC2Launch123456789\Err.tmp
```

Arquivos de saída para a tarefa **`executeProgram`**

`ExecuteProgramInputs.tmp`

Contém o caminho para o executável e todos os parâmetros de entrada que a tarefa `executeProgram` transmite para ele quando é executada.

`Output.tmp`

Contém a saída de runtime do programa que a tarefa `executeProgram` executa.

`Err.tmp`

Contém as mensagens de erro de runtime do programa que a tarefa `executeProgram` executa.

Exemplos

Os exemplos a seguir mostram como executar um arquivo executável de um diretório local em uma instância com a tarefa `executeProgram`.

Exemplo 1: configurar executável com um argumento

Este exemplo mostra uma tarefa `executeProgram` que executa um executável de configuração no modo silencioso.

```
task: executeProgram
  inputs:
    - frequency: always
      path: C:\Users\Administrator\Desktop\setup.exe
      arguments: ['-quiet']
```

Exemplo 2: VLC executável com dois argumentos

Este exemplo mostra uma tarefa `executeProgram` que executa um arquivo VLC executável com dois argumentos transmitidos como parâmetros de entrada.

```
task: executeProgram
  inputs:
    - frequency: always
      path: C:\vlc-3.0.11-win64.exe
      arguments: ['/L=1033','/S']
      runAs: localSystem
```

executeScript

Executa um script com argumentos opcionais e uma frequência especificada. O comportamento do script depende do modo em que o agente executa os scripts: em linha ou desanexados.

Em linha (padrão)

O agente EC2Launch v2 executa os scripts um de cada vez (`detach: false`) Essa é a configuração padrão.

> **Note**
>
> Quando seu script em linha emite um comando reset ou sysprep, ele é executado imediatamente e redefine o agente. A tarefa atual é concluída e, em seguida, o agente é desligado sem executar mais nenhuma tarefa.
> Por exemplo, se a tarefa que emite o comando tivesse sido seguida por uma tarefa `startSsm` (incluída por padrão após a execução dos dados do usuário), a tarefa não executaria e o serviço Systems Manager nunca seria iniciado.

Desanexados

O agente do EC2Launch v2 executa scripts simultaneamente com outras tarefas (`detach: true`).

> **Note**
>
> Quando seu script desanexado emite um comando reset ou sysprep, esses comandos aguardam a conclusão do agente antes de serem executados. As tarefas após executeScript ainda serão executadas.

Estágios: você pode executar a tarefa `executeScript` durante os estágios `PreReady`, `PostReady` e `UserData`.

Frequência: configurável. Consulte Entradas.

Entradas

Esta seção contém um ou mais scripts para a tarefa executeScript executar (entradas). Cada etapa pode incluir as seguintes definições configuráveis:

frequência (string)

(Obrigatório) Especifique exatamente um dos seguintes valores:

- `once`

- `always`

tipo (string)

(Obrigatório) Especifique exatamente um dos seguintes valores:

- `batch`
- `powershell`

argumentos (lista de strings)

(Opcional) Uma lista de argumentos de string a serem transmitidos ao shell (não ao script do PowerShell). Esse parâmetro não é compatível com `type: batch`. Se nenhum argumento for passado, o EC2Launch v2 adicionará o seguinte argumento por padrão: `-ExecutionPolicy Unrestricted`.

conteúdo (string)

(Obrigatório) Conteúdo de script

runAs (string)

(Obrigatório) Especifique exatamente um dos seguintes valores:

- `admin`
- `localSystem`

desanexar (booleano)

(Opcional) O agente do EC2Launch v2 assume como padrão a execução de um script por vez (`detach: false`). Para executar o script simultaneamente com outras tarefas, defina o valor como `true` (`detach: true`).

> **Note**
>
> Os códigos de saída de script (incluindo `3010`) não têm efeito quando `detach` é definido como `true`.

Output

Todas as tarefas gravam entradas do arquivo de log no arquivo `agent.log`. A saída adicional do script que a tarefa `executeScript` executa é armazenada separadamente em uma pasta com nome dinâmico, da seguinte forma:

`%LocalAppData%\Temp\EC2Launch########\outputfilename.ext`

O caminho exato para os arquivos de saída está incluído no arquivo `agent.log`, por exemplo:

```
Program file is created at: C:\Windows\system32\config\systemprofile\AppData\Local
\Temp\EC2Launch123456789\UserScript.ps1
Output file is created at: C:\Windows\system32\config\systemprofile\AppData\Local
\Temp\EC2Launch123456789\Output.tmp
Error file is created at: C:\Windows\system32\config\systemprofile\AppData\Local
\Temp\EC2Launch123456789\Err.tmp
```

Arquivos de saída para a tarefa **`executeScript`**

`UserScript.ext`

Contém o script que a tarefa `executeScript` executou. A extensão do arquivo depende do tipo de script especificado no parâmetro `type` da tarefa `executeScript`, da seguinte forma:

- Se o tipo for `batch`, então a extensão do arquivo será `.bat`.
- Se o tipo for `powershell`, então a extensão do arquivo será `.ps1`.

`Output.tmp`

Contém a saída de runtime do script que a tarefa `executeScript` executa.

`Err.tmp`

Contém as mensagens de erro de runtime do script que a tarefa `executeScript` executa.

Exemplos

Os exemplos a seguir mostram como executar um script em linha com a tarefa `executeScript`.

Exemplo 1: arquivo de texto de saída Hello world

Este exemplo mostra uma tarefa `executeScript` que executa um script do PowerShell para criar um arquivo de texto "Hello world" na unidade `C:`.

```
task: executeScript
  inputs:
    - frequency: always
      type: powershell
      runAs: admin
```

```
      content: |-
        New-Item -Path 'C:\PowerShellTest.txt' -ItemType File
        Set-Content 'C:\PowerShellTest.txt' "Hello world"
```

Exemplo 2: execução de dois scripts

Este exemplo mostra que a tarefa `executeScript` pode executar mais de um script, e o tipo de script não precisa necessariamente corresponder.

O primeiro script (`type: powershell`) grava um resumo dos processos atualmente em execução na instância em um arquivo de texto localizado na unidade `C:`.

O segundo script (`batch`) grava as informações do sistema no arquivo `Output.tmp`.

```
task: executeScript
  inputs:
    - frequency: always
      type: powershell
      runAs: localSystem
      content: |
        Get-Process | Out-File -FilePath C:\Process.txt
    - frequency: always
      type: batch
      runAs: localSystem
      content: |
        systeminfo
```

Exemplo 3: configuração do sistema idempotente com reinicializações

Este exemplo mostra uma tarefa `executeScript` que executa um script idempotente para realizar a seguinte configuração do sistema com uma reinicialização entre cada etapa:

- Renomear o computador.
- Juntar o computador ao domínio.
- Habilitar Telnet.

O script garante que cada operação seja executada apenas uma vez. Isso evita um loop de reinicialização e torna o script idempotente.

```
task: executeScript
  inputs:
```

```
    - frequency: always
      type: powershell
      runAs: localSystem
      content: |-
        $name = $env:ComputerName
        if ($name -ne $desiredName) {
          Rename-Computer -NewName $desiredName
          exit 3010
        }
        $domain = Get-ADDomain
        if ($domain -ne $desiredDomain)
        {
          Add-Computer -DomainName $desiredDomain
          exit 3010
        }
        $telnet = Get-WindowsFeature -Name Telnet-Client
        if (-not $telnet.Installed)
        {
          Install-WindowsFeature -Name "Telnet-Client"
          exit 3010
        }
```

extendRootPartition

Estende o volume raiz para usar todo o espaço disponível no disco.

Frequência — uma vez

AllowedStages — `[Boot]`

Entradas — nenhuma

Exemplo do

```
task: extendRootPartition
```

initializeVolume

Inicializa volumes vazios que estão anexados à instância para que eles sejam ativados e particionados. O agente de inicialização ignorará a inicialização se detectar que o volume não está vazio. Um volume será considerado vazio se os primeiros 4 KiB estiverem vazios ou se o volume não tiver um layout de unidade reconhecível pelo Windows.

O parâmetro de entrada `letter` sempre é aplicado quando essa tarefa é executada, quer a unidade tenha sido inicializada ou não.

A tarefa `initializeVolume` realiza as ações a seguir.

- Defina os atributos de disco `offline` e `readonly` como falsos.
- Crie uma partição. Se nenhum tipo de partição for especificado no parâmetro de entrada `partition`, os seguintes padrões serão aplicados:
  - Se o tamanho do disco for menor do que 2 TB, defina o tipo de partição com `mbr`.
  - Se o tamanho do disco for 2 TB ou mais, defina o tipo de partição com `gpt`.
- Formate o volume como NTFS.
- Defina o rótulo do volume como se segue:
  - Use o valor `name` do parâmetro de entrada, se especificado.
  - Se o volume for efêmero e nenhum nome estiver especificado, defina o rótulo do volume como `Temporary Storage Z`.
- Se o volume for efêmero (SSD ou HDD, não Amazon EBS), crie um arquivo `Important.txt` na raiz do volume com o seguinte conteúdo:

```
This is an 'Instance Store' disk and is provided at no additional charge.

*This disk offers increased performance since it is local to the host
*The number of Instance Store disks available to an instance vary by instance type
*DATA ON THIS DRIVE WILL BE LOST IN CASES OF IMPAIRMENT OR STOPPING THE INSTANCE.
 PLEASE ENSURE THAT ANY IMPORTANT DATA IS BACKED UP FREQUENTLY

For more information, please refer to: Armazenamento em bloco temporário do
 armazenamento de instância para instâncias do EC2.
```

- Defina a letra da unidade como o valor especificado no parâmetro de entrada `letter`.

Estágios: você pode executar a tarefa `initializeVolume` durante os estágios `PostReady` e `UserData`.

Frequência: sempre.

Entradas

Você pode configurar os parâmetros de runtime seguinte forma:

dispositivos (lista de mapas)

(Condicional) Configuração de cada dispositivo iniciado pelo agente de inicialização. É obrigatório quando o parâmetro de entrada `initialize` está definido como `devices`.

- dispositivo (string, obrigatório): identifica o dispositivo durante a criação da instância. Por exemplo, `xvdb`, `xvdf` ou `\dev\nvme0n1`.
- letra (string, opcional): um caractere. A letra de unidade a ser atribuída.
- nome (string, opcional): o nome do volume a ser atribuído.
- partição (string, opcional): especifique um dos seguintes valores para o tipo de partição a ser criada ou deixe o agente de inicialização usar o padrão de acordo com o tamanho do volume:
  - mbr
  - gpt

inicializar (string)

(Obrigatório) Especifique exatamente um dos seguintes valores:

- `all`
- `devices`

Exemplos

Os exemplos a seguir mostram exemplos de configurações de entrada para a tarefa `initializeVolume`.

Exemplo 1: inicializar dois volumes em uma instância

Este exemplo mostra uma tarefa `initializeVolume` que inicializa dois volumes secundários em uma instância. O dispositivo denominado `DataVolume2` no exemplo é efêmero.

```
task: initializeVolume
inputs:
  initialize: devices
  devices:
  - device: xvdb
    name: DataVolume1
    letter: D
    partition: mbr
```

```
  - device: /dev/nvme0n1
    name: DataVolume2
    letter: E
    partition: gpt
```

Exemplo 2: inicializar volumes do EBS anexados a uma instância

Este exemplo mostra uma tarefa `initializeVolume` que inicializa todos os volumes vazios do EBS que estão conectados à instância.

```
task: initializeVolume
inputs:
  initialize: all
```

optimizeEna

Otimiza as configurações do ENA com base no tipo de instância atual; pode reinicializar a instância.

Frequência — sempre

AllowedStages — `[PostReady, UserData]`

Entradas — nenhuma

Exemplo do

```
task: optimizeEna
```

setAdminAccount

Define atributos para a conta de administrador padrão criada na máquina local.

Frequência — uma vez

AllowedStages — `[PreReady]`

Entradas —

`name`: (string) nome da conta de administrador

`password`: (mapa)

`type`: (string) estratégia para definir a senha como `static`, `random` ou `doNothing`

`data`: (string) armazena dados se o campo `type` for estático

Exemplo do

```
task: setAdminAccount
inputs:
  name: Administrator
  password:
  type: random
```

setDnsSuffix

Adiciona sufixos DNS à lista de sufixos de pesquisa. Somente sufixos que ainda não existem são adicionados à lista. Para obter mais informações sobre como os agentes de inicialização definem os sufixos DNS, consulte Configurar o sufixo DNS para agentes de execução do EC2 Windows.

Frequência — sempre

AllowedStages — `[PreReady]`

Entradas —

`suffixes`: (lista de strings) lista de um ou mais sufixos DNS válidos; variáveis de substituição válidas são `$REGION` e `$AZ`

Exemplo do

```
task: setDnsSuffix
inputs:
  suffixes:
  - $REGION.ec2-utilities.amazonaws.com
```

setHostName

Define o nome do host do computador como uma string personalizada ou, se o `hostName` não for especificado, o endereço IPv4 privado.

Frequência — sempre

AllowedStages — `[PostReady, UserData]`

Entradas —

`hostName`: (string) nome do host opcional, que deve ser formatado conforme o seguinte.

- Ele deve ter 15 caracteres ou menos
- Ele deve conter apenas caracteres alfanuméricos (a-z, A-Z, 0-9) e hífen (-).
- Ele não deve consistir inteiramente em caracteres numéricos.

`reboot`: (booliano) indica se uma reinicialização é permitida quando o nome de host é alterado

Exemplo do

```
task: setHostName
inputs:
  reboot: true
```

setWallpaper

Cria o arquivo de atalho `setwallpaper.lnk` na pasta de startup de cada usuário existente, exceto para `Default User`. Esse arquivo de atalho é executado quando o usuário faz login pela primeira vez após a inicialização da instância. Ele configura a instância com um papel de parede personalizado que exibe os atributos da instância.

O caminho de arquivo de atalho é:

```
$env:SystemDrive/Users/<user>/AppData/Roaming/Microsoft/Windows/Start Menu/Programs/
Startup/setwallpaper.lnk
```

> **Note**
>
> Quando você remover a tarefa `setWallpaper`, não exclua esse arquivo de atalho. Para obter mais informações, consulte `setWallpaper`A tarefa não está ativada, mas o papel de parede é redefinido na reinicialização.

Estágios: é possível configurar o papel de parede durante os estágios `PreReady` e `UserData`.

Frequência: `always`

Configuração do papel de parede

Você pode usar as definições a seguir para configurar o papel de parede.

Entradas

Parâmetros de entrada que você fornece e atributos que você pode definir para configurar o papel de parede:

caminho (string)

(Obrigatório) O caminho do nome do arquivo da imagem local no formato .jpg a ser usada como imagem do papel de parede.

atributos (lista de strings)

(Opcional) Você pode adicionar um ou mais dos seguintes atributos ao papel de parede:

- `architecture`
- `availabilityZone`
- `hostName`
- `instanceId`
- `instanceSize`
- `privateIpAddress`
- `publicIpAddress`
- `ipv6Address`

instanceTags

(Opcional) Você pode usar exatamente uma das seguintes opções para essa configuração.

- AllTags (string): adicione todas as tags de instância ao papel de parede.

```
instanceTags: AllTags
```

- InstanceTags (lista de strings): especifique uma lista de nomes de tags de instância para adicionar ao papel de parede. Por exemplo:

```
instanceTags:
  - Tag 1
```

```
  - Tag 2
```

Exemplo

O exemplo a seguir mostra as entradas da configuração do papel de parede que definem o caminho do arquivo da imagem de fundo do papel de parede, junto com as tags de instância denominadas `Tag 1` e `Tag 2`, e os atributos que incluem o nome do host, o ID da instância e os endereços IP públicos e privados da instância.

```
task: setWallpaper
inputs:
  path: C:\ProgramData\Amazon\EC2Launch\wallpaper\Ec2Wallpaper.jpg
  attributes:
  - hostName
  - instanceId
  - privateIpAddress
  - publicIpAddress
  instanceTags:
  - Tag 1
  - Tag 2
```

> **Note**
>
> Você deve habilitar as tags nos metadados para mostrá-las no papel de parede. Para obter mais informações sobre tags e metadados da instância, consulte Visualizar tags para as instâncias do EC2 usando os metadados de instância.

startSsm

Iniciar o serviço Systems Manager (SSM) após o Sysprep.

Frequência — sempre

AllowedStages — `[PostReady, UserData]`

Entradas — nenhuma

Exemplo do

```
task: startSsm
```

sysprep

Redefine o estado do serviço, atualiza `unattend.xml`, desativa o RDP e executa Sysprep. Esta tarefa só é executada depois que todas as outras tarefas forem concluídas

Frequência — uma vez

AllowedStages — `[UserData]`

Entradas —

`clean`: (booliano) limpa os logs de instância antes de executar o Sysprep

`shutdown`: (booliano) desliga a instância depois de executar o Sysprep

Exemplo do

```
task: sysprep
inputs:
clean: true
shutdown: true
```

writeFile

Grava um arquivo em um destino.

Frequência — visualizar Entradas

AllowedStages — `[PostReady, UserData]`

Entradas —

`frequency`: (string) `once` ou `always`

`destination`: (string) caminho no qual gravar o conteúdo

`content`: (string) texto a gravar no destino

Exemplo de

```
task: writeFile
inputs:
  - frequency: once
  destination: C:\Users\Administrator\Desktop\booted.txt
  content: Windows Has Booted
```

Solucionar problemas com o agente do EC2Launch v2

Esta seção mostra cenários comuns de solução de problemas para o EC2Launch v2, informações sobre como visualizar logs de eventos do Windows e saída e mensagens do log do console.

Tópicos de solução de problemas

- Cenários comuns de solução de problemas
- Logs de eventos do Windows
- Saída do log do console do EC2Launch v2

Cenários comuns de solução de problemas

Esta seção mostra cenários comuns de solução de problemas e etapas para resolução.

Cenários

- Falha no serviço ao definir o papel de parede
- Falha no serviço ao executar dados do usuário
- O serviço executa uma tarefa apenas uma vez
- Falha no serviço ao executar uma tarefa
- O serviço executa dados do usuário mais de uma vez
- As tarefas agendadas do EC2Launch v1 não conseguem ser executadas após a migração para o EC2Launch v2
- O serviço inicializa um volume do EBS que não está vazio
- setWallpaperA tarefa não está ativada, mas o papel de parede é redefinido na reinicialização
- Serviço preso no status em execução
- Um agent-config.yml inválido impede a abertura da caixa de diálogo de configurações do EC2Launch v2
- task:executeScript should be unique and only invoked once

Falha no serviço ao definir o papel de parede

Resolução

1. Verifique se `%AppData%\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\setwallpaper.lnk` existe.

2. Verifique `%ProgramData%\Amazon\EC2Launch\log\agent.log` para saber se ocorreram erros.

Falha no serviço ao executar dados do usuário

Causa possível: a falha no serviço pode ter ocorrido antes da execução dos dados do usuário.

Resolução

1. Verifique `%ProgramData%\Amazon\EC2Launch\state\previous-state.json`.
2. Veja se `boot`, `network`, `preReady` e `postReadyLocalData` foram todos marcados como sucesso.
3. Se um dos estágios falhar, verifique se há erros específicos `%ProgramData%\Amazon\EC2Launch\log\agent.log`.

O serviço executa uma tarefa apenas uma vez

Resolução

1. Verifique a frequência da tarefa.
2. Se o serviço já tiver sido executado após Sysprep e a frequência da tarefa estiver definida como `once`, a tarefa não será executada novamente.
3. Defina a frequência da tarefa como `always` se você quiser que ela execute a tarefa sempre que o EC2Launch v2 for executado.

Falha no serviço ao executar uma tarefa

Resolução

1. Verifique as entradas mais recentes em `%ProgramData%\Amazon\EC2Launch\log\agent.log`.
2. Se não ocorrerem erros, tente executar o serviço manualmente a partir de `"%ProgramFiles%\Amazon\EC2Launch\EC2Launch.exe" run` para ver se as tarefas foram bem-sucedidas.

O serviço executa dados do usuário mais de uma vez

Resolução

Os dados do usuário são tratados de forma diferente entre o EC2Launch v1 e o EC2Launch v2. O EC2Launch v1 executa dados do usuário como uma tarefa programada na instância quando `persist` for definido como `true`. Se `persist` estiver definido como `false`, a tarefa não será programada mesmo quando ela sair com uma reinicialização ou for interrompida durante a execução.

EC2Launch v2 executa dados do usuário como uma tarefa de agente e rastreia seu estado de execução. Se os dados do usuário emitirem uma reinicialização do computador ou se os dados do usuário tiverem sido interrompidos durante a execução, o estado de execução persistirá `pending` e os dados do usuário serão executados novamente na próxima inicialização da instância. Se você quiser impedir que o script de dados do usuário seja executado mais de uma vez, torne o script idempotente.

O exemplo a seguir de script idempotente define o nome do computador e se junta a um domínio.

```
<powershell>
  $name = $env:computername
  if ($name -ne $desiredName) {
 Rename-Computer -NewName $desiredName
  }
  $domain = Get-ADDomain
  if ($domain -ne $desiredDomain)
  {
 Add-Computer -DomainName $desiredDomain
  }
  $telnet = Get-WindowsFeature -Name Telnet-Client
  if (-not $telnet.Installed)
  {
 Install-WindowsFeature -Name "Telnet-Client"
  }
</powershell>
<persist>false</persist>
```

As tarefas agendadas do EC2Launch v1 não conseguem ser executadas após a migração para o EC2Launch v2

Resolução

A ferramenta de migração não detecta qualquer tarefa agendada vinculada aos scripts do EC2Launch v1; portanto, ela não configura automaticamente essas tarefas no EC2Launch v2. Para configurar essas tarefas, edite o arquivo `agent-config.yml` ou use a caixa de diálogo de

configurações do EC2Launch v2. Por exemplo, se uma instância tiver uma tarefa agendada que executa `InitializeDisks.ps1`, depois de executar a ferramenta de migração, você deverá especificar os volumes que deseja inicializar na caixa de diálogo de configurações do EC2Launch v2. Consulte a Etapa 6 do procedimento para Alterar configurações usando a caixa de diálogo de configurações do EC2Launch v2.

O serviço inicializa um volume do EBS que não está vazio

Resolução

Antes de inicializar um volume, o EC2Launch v2 tenta detectar se ele está vazio. Se um volume não estiver vazio, ele ignorará a inicialização. Quaisquer volumes detectados como não vazios não são inicializados. Um volume é considerado vazio se seus primeiros 4 KiB estiverem vazios ou se o volume não tiver um layout de unidade reconhecível pelo Windows. Um volume que foi inicializado e formatado em um sistema Linux não tem um layout de unidade reconhecível pelo Windows, por exemplo MBR ou GPT. Portanto, ele será considerado vazio e será inicializado. Se você quiser preservar esses dados, não confie na detecção de unidade vazia do EC2Launch v2. Em vez disso, especifique os volumes que você gostaria de inicializar na caixa de diálogo de configurações do EC2Launch v2 (consulte a etapa 6) ou no `agent-config.yml`.

`setWallpaper`A tarefa não está ativada, mas o papel de parede é redefinido na reinicialização

A tarefa `setWallpaper` cria o arquivo de atalho `setwallpaper.lnk` na pasta de startup de cada usuário existente. Esse arquivo de atalho é executado quando o usuário faz login pela primeira vez após a inicialização da instância. Ele configura a instância com um papel de parede personalizado que exibe os atributos da instância. Remover a tarefa `setWallpaper` não exclui esse arquivo de atalho. Exclua esse arquivo manualmente ou excluí-lo usando um script.

O caminho do atalho é:

`$env:SystemDrive/Users/<user>/AppData/Roaming/Microsoft/Windows/Start Menu/Programs/Startup/setwallpaper.lnk`

Resolução

Exclua esse arquivo manualmente ou exclua-o usando um script.

Exemplo de script PowerShell para excluir arquivo de atalho

```
foreach ($userDir in (Get-ChildItem "C:\Users" -Force -Directory).FullName)
{
```

```
 $startupPath = Join-Path $userDir -ChildPath "AppData\Roaming\Microsoft\Windows\Start
 Menu\Programs\Startup"
 if (Test-Path $startupPath)
 {
  $wallpaperSetupPath = Join-Path $startupPath -ChildPath "setwallpaper.lnk"
  if (Test-Path $wallpaperSetupPath)
  {
   Remove-Item $wallpaperSetupPath -Force -Confirm:$false
  }
 }
}
```

Serviço preso no status em execução

Descrição

O EC2Launch v2 é bloqueado com mensagens de log (`agent.log`) semelhantes às seguintes:

```
2022-02-24 08:08:58 Info:
 ********************************************************************************
2022-02-24 08:08:58 Info: EC2Launch Service starting
2022-02-24 08:08:58 Info: Windows event custom log exists: Amazon EC2Launch
2022-02-24 08:08:58 Info: ACPI SPCR table not supported. Bailing Out
2022-02-24 08:08:58 Info: Serial port is in use. Waiting for Serial Port...
2022-02-24 08:09:00 Info: ACPI SPCR table not supported. Use default console port.
2022-02-24 08:09:02 Info: ACPI SPCR table not supported. Use default console port.
2022-02-24 08:09:04 Info: ACPI SPCR table not supported. Use default console port.
2022-02-24 08:09:06 Info: ACPI SPCR table not supported. Use default console port.
```

Possível causa

O SAC está habilitado e usando a porta serial. Para mais informações, consulte Use SAC to troubleshoot your Windows instance (Usar o SAC para solucionar problemas de instâncias do Windows).

Resolução

Tente as seguintes etapas para resolver esse problema:

- Desative o serviço que está usando a porta serial.
- Se quiser que o serviço continue usando a porta serial, crie scripts personalizados para executar tarefas do agente de execução e invoque-os como tarefas agendadas.

Um `agent-config.yml` inválido impede a abertura da caixa de diálogo de configurações do EC2Launch v2

Descrição

As configurações do EC2Launch v2 tentam analisar o arquivo `agent-config.yml` antes de abrir a caixa de diálogo. Se o arquivo de configuração YAML não seguir o esquema compatível, a caixa de diálogo exibirá o seguinte erro:

```
Unable to parse configuration file agent-config.yml. Review configuration file. Exiting application.
```

Resolução

1. Verifique se o arquivo de configuração segue o esquema compatível.
2. Para começar do zero, copie o arquivo de configuração padrão no `agent-config.yml`. Você pode usar o exemplo `agent-config.yml` fornecido na seção Configuração da tarefa.
3. Também é possível recomeçar excluindo o `agent-config.yml`. As configurações do EC2Launch v2 geram um arquivo de configuração vazio.

`task:executeScript should be unique and only invoked once`

Descrição

Não é possível repetir uma tarefa na mesma etapa.

Resolução

Algumas tarefas devem ser inseridas como uma matriz, como executeScript e executeProgram. Para obter um exemplo de como escrever o script como uma matriz, consulte executeScript.

Logs de eventos do Windows

O EC2Launch v2 publica logs de eventos do Windows para eventos importantes, como a inicialização do serviço, o Windows pronto, e o sucesso e a falha da tarefa. Identificadores de eventos identificam exclusivamente um evento específico. Cada evento contém informações de estágio, tarefa e nível e uma descrição. É possível definir gatilhos para eventos específicos usando o identificador de eventos.

Os IDs de evento fornecem informações sobre um evento e identificam alguns eventos de forma exclusiva. O dígito menos significativo de um ID de evento indica a gravidade de um evento.

Evento	Dígito menos significativo
Success	. . .0
Informational	. . .1
Warning	. . .2
Error	. . .3

Os eventos relacionados ao serviço, gerados quando o serviço é iniciado ou interrompido, incluem um identificador de evento de um dígito.

Evento	Identificador de um dígito
Success	0
Informational	1
Warning	2
Error	3

As mensagens de evento para eventos do `EC2LaunchService.exe` começam com `Service:`. As mensagens de evento para eventos do `EC2Launch.exe` não começam com `Service:`.

Os IDs de evento de quatro dígitos incluem informações sobre o estado, a tarefa e a gravidade de um evento.

Tópicos

- Formato de ID do evento
- Exemplos de ID de evento
- Esquema de log de eventos do Windows

Formato de ID do evento

A tabela a seguir mostra o formato de um identificador de eventos do EC2Launch v2.

3	2 1	0
S	T	L

As letras e números na tabela representam o tipo de evento e as definições a seguir.

Tipo de evento	Definição
S (Estágio)	0 - Mensagem de nível de serviço 1 - Inicialização 2 - Rede 3 - PreReady 5 - O Windows está pronto 6 - PostReady 7 - Dados do usuário
T (Tarefa)	As tarefas representadas pelos dois valores correspondentes são diferentes para cada estágio. Para visualizar a lista completa de eventos, consulte Esquema de log de eventos do Windows.
L (Nível do evento)	0 - Êxito 1 - Informativo 2 - Aviso 3 - Erro

Exemplos de ID de evento

Veja a seguir alguns exemplos de IDs de evento.

- `5000` - o Windows está pronto para ser usado
- `3010` - êxito ao ativar a tarefa do Windows no estágio PreReady
- `6013` - A tarefa Definir papel de parede no estágio PostReady Local Data encontrou um erro

Esquema de log de eventos do Windows

MessageId/ID do evento	Mensagem do evento
`. . .0`	`Success`
`. . .1`	`Informational`
`. . .2`	`Warning`
`. . .3`	`Error`
x	`EC2Launch service-level logs`
0	`EC2Launch service exited successfully`
1	`EC2Launch service informational logs`
2	`EC2Launch service warning logs`
3	`EC2Launch service error logs`
10	`Replace state.json with previous-state.json`
100	`Serial Port`
200	`Sysprep`
300	`PrimaryNic`

MessageId/ID do evento	Mensagem do evento
400	Metadata
x000	Stage (1 digit), Task (2 digits), Status (1 digit)
1000	Boot
1010	Boot - extend_root_partition
2000	Network
2010	Network - add_routes
3000	PreReady
3010	PreReady - activate_windows
3020	PreReady - install_egpu_manager
3030	PreReady - set_monitor_on
3040	PreReady - set_hibernation
3050	PreReady - set_admin_account
3060	PreReady - set_dns_suffix
3070	PreReady - set_wallpaper
3080	PreReady - set_update_schedule
3090	PreReady - output_log
3100	PreReady - enable_open_ssh
5000	Windows is Ready to use
6000	PostReadyLocalData
7000	PostReadyUserData

MessageId/ID do evento	Mensagem do evento
6010/7010	PostReadyLocal/UserData - set_wallpaper
6020/7020	PostReadyLocal/UserData - set_update_schedule
6030/7030	PostReadyLocal/UserData - set_hostname
6040/7040	PostReadyLocal/UserData - execute_program
6050/7050	PostReadyLocal/UserData - execute_script
6060/7060	PostReadyLocal/UserData - manage_package
6070/7070	PostReadyLocal/UserData - initialize_volume
6080/7080	PostReadyLocal/UserData - write_file
6090/7090	PostReadyLocal/UserData - start_ssm
7100	PostReadyUserData - enable_open_ssh
6110/7110	PostReadyLocal/UserData - enable_jumbo_frames

Saída do log do console do EC2Launch v2

Esta seção contém uma saída de log do console de exemplo para EC2Launch v2 e lista todas as mensagens de erro de log do console do EC2Launch v2 para ajudar você a solucionar problemas.

Para obter mais informações sobre a saída do console da instância e como acessá-la, consulte the section called “Saída do console da instância”.

Outputs

- Saída do log do console do EC2Launch v2
- Mensagens de log do console do EC2Launch v2

Saída do log do console do EC2Launch v2

Veja a seguir um exemplo de saída de log do console para EC2Launch v2. Alguns valores nesse exemplo são substituídos por texto representativo entre chaves.

```
2025/07/22 21:26:53Z: Windows sysprep configuration complete.
2025/07/22 21:26:53Z: Message: Waiting for access to metadata...
2025/07/22 21:26:53Z: Message: Meta-data is now available.
2025/07/22 21:26:53Z: AMI Origin Version: 2024.12.13
2025/07/22 21:26:53Z: AMI Origin Name: Windows_Server-2022-English-Full-Base
2025/07/22 21:26:53Z: OS: Microsoft Windows NT 10.0.20348
2025/07/22 21:26:53Z: OsVersion: 10.0
2025/07/22 21:26:53Z: OsProductName: Windows Server 2022 Datacenter
2025/07/22 21:26:53Z: OsBuildLabEx: 20348.1.amd64fre.fe_release.210507-1500
2025/07/22 21:26:53Z: OsCurrentBuild: 20348
2025/07/22 21:26:53Z: OsReleaseId: 2009
2025/07/22 21:26:53Z: Language: en-US
2025/07/22 21:26:53Z: TimeZone: UTC
2025/07/22 21:26:53Z: Offset: UTC +0000
2025/07/22 21:26:53Z: Launch: EC2 Launch v2.2.63
2025/07/22 21:26:53Z: AMI-ID: ami-1234567890abcdef1
2025/07/22 21:26:53Z: Instance-ID: i-1234567890abcdef0
2025/07/22 21:26:54Z: Instance Type: t3.xlarge
2025/07/22 21:26:54Z: Driver: AWS NVMe Driver v1.6.0.35
2025/07/22 21:26:54Z: SubComponent: 1.6.0.35; EnableSCSIPersistentReservations: 0
2025/07/22 21:26:54Z: Driver: AWS PV Driver Package v8.5.0
2025/07/22 21:26:55Z: Driver: Amazon Elastic Network Adapter v2.8.0.0
2025/07/22 21:26:55Z: HOSTNAME: EC2AMAZ-9FJG5CC
2025/07/22 21:26:55Z: RDPCERTIFICATE-SUBJECTNAME: {certificate subject name}
2025/07/22 21:26:55Z: RDPCERTIFICATE-THUMBPRINT: {thumbprint hash}
2025/07/22 21:26:56Z: SSM: Amazon SSM Agent v3.3.2746.0
2025/07/22 21:26:57Z: User data format: no_user_data
2025/07/22 21:26:57Z: EC2LaunchTelemetry: IsTelemetryEnabled=true
2025/07/22 21:26:57Z: EC2LaunchTelemetry: AgentOsArch=windows_amd64
2025/07/22 21:26:57Z: EC2LaunchTelemetry: IsAgentScheduledPerBoot=true
```

```
2025/07/22 21:26:57Z: EC2LaunchTelemetry: AgentCommandErrorCode=1
2025/07/22 21:26:57Z: EC2LaunchTelemetry: AdminPasswordTypeCode=0
2025/07/22 21:26:57Z: EC2LaunchTelemetry: AgentErrorLocation=execute_windows.go:410
2025/07/22 21:26:57Z: EC2LaunchTelemetry: IpConflictDetectionCode=0
2025/07/22 21:26:57Z: Message: Windows is Ready to use
{"type":"EC2AgentTelemetry","agentId":"WindowsLaunchAgentV2", ...}
{"type":"EC2AgentTelemetry","agentId":"WindowsLaunchAgentV2", ...}
```

Mensagens de log do console do EC2Launch v2

Veja a seguir uma lista de todas as mensagens de log do console do EC2Launch v2.

```
Error EC2Launch service is stopping. {error message}
```

Detalhes do erro do serviço interrompido:

- `Error setting up EC2Launch agent folders`
- `See instance logs for detail`
- `Error stopping service`
- `Error initializing service`

```
Windows sysprep configuration complete
```

```
Invalid administrator username: {invalid username}
```

```
Invalid administrator password
Username: {username}
Password: <Password>{encrypted password}</Password>
```

A mensagem a seguir é um bloco de informações contendo detalhes da AMI:

```
AMI Origin Version: {amiVersion}
AMI Origin Name: {amiName}
Microsoft Windows NT {currentVersion}.{currentBuildNumber}
OsVersion: {currentVersion}
OsProductName: {productName}
OsBuildLabEx: {buildLabEx}
```

```
OsCurrentBuild: {currentBuild}
OsReleaseId: {releaseId}
Language: {language}
TimeZone: {timeZone}
Offset: UTC {offset}
Launch agent: EC2Launch {BuildVersion}
AMI-ID: {amiId}
Instance-ID: {instanceId}
Instance Type: {instanceType}
HOSTNAME: {computer name}
RDPCERTIFICATE-SUBJECTNAME: {certificate subject name}
RDPCERTIFICATE-THUMBPRINT: {thumbprint hash}
SqlServerBilling: {sql billing}
SqlServerInstall: {sql patch leve, edition type}
Driver: AWS NVMe Driver {version}
Driver: Inbox NVMe Driver {version}
Driver: AWS PV Driver Package {version}
Microsoft-Hyper-V is installed.
Unable to get service status for vmms
Microsoft-Hyper-V is {status}
SSM: Amazon SSM Agent {version}
AWS VSS Version: {version}
```

```
Windows sysprep configuration complete.
Windows is being configured. 'SysprepState is {state}'
Windows is still being configured. 'SysprepState is {state}'
Windows is Ready to use
Waiting for access to metadata...
Meta-data is now available.
Metadata is not available for this instance.
Timed out waiting for access to metadata.
User data format: {format}
```

As mensagens de telemetria do EC2Launch v2 incluem os valores das propriedades de telemetria de inicialização. A partir da versão 2.2.63, os dados de telemetria do EC2 Agent são formatados como um objeto JSON.

```
EC2LaunchTelemetry: {telemetry property}
```

```
{"type":"EC2AgentTelemetry","agentId":"WindowsLaunchAgentV2" ... }
```

Históricos de versões do EC2Launch v2

Históricos de versões

- Histórico de versões do EC2Launch v2

Histórico de versões do EC2Launch v2

Para garantir que você tenha o agente de lançamento mais recente instalado, consulte Instalar a versão mais recente do EC2Launch v2. Receba notificações quando novas versões do atendente do EC2Launch v2 são disponibilizadas. Para obter mais informações, consulte Assinar as notificações do agente de execução do EC2 Windows.

A tabela a seguir descreve as versões disponíveis do EC2Launch v2.

Versão	Detalhes	Data de lançamento
2.3.108	• Foi adicionada a exibição do endereço IPv6 ao papel de parede. Para atributos de memória e rede, consulte AWSDocumentação.	29 de dezembro de 2025
2.3.56	• Correção de um problema em que rotas de rede persistentes pré-configuradas não eram tratadas adequadamente pelo EC2Launch v2.	4 de novembro de 2025
2.3.5	• Detecção avançada de interface de rede primária usando IMDS ao adicionar rotas.	15 de setembro de 2025
2.2.63	• Atualização do agente de lançamento para melhorar Telemetria.	29 de julho de 2025
2.1.1	• Adicionada total compatibilidade com IPv6.	14 de maio de 2025
2.0.2107	•	27 de março de 2025

Versão	Detalhes	Data de lançamento
	Adição aprimorada de rotas para lidar com cenários nos quais os endereços IPv4 ou IPv6 não estão disponíveis na interface.	
2.0.2081	• Correção de um problema em que as informações do certifica do RDP não eram recuperadas ou validadas adequadamente. Funcionalidade adicionada para iniciar automaticamente os Serviços de Área de Trabalho Remota, se necessário. • As permissões do serviço EC2Launch v2 foram ajustadas para corrigir um problema que ocorria ao consultar o status do serviço.	4 de fevereiro de 2025
2.0.2046	• Caminho do papel de parede atualizado no arquivo `agent-config.yml` para usar o caminho padrão do papel de parede do sistema operacional. • Telemetria adicionada para monitorar os locais onde ocorreram erros do atendente. • Mensagens de log do atendente atualizadas.	3 de outubro de 2024
2.0.1981	• Mensagens de erro do comando `EC2Launch.exe` da CLI atualizadas para usuários que não são administradores.	6 de agosto de 2024
2.0.1948	• Adicionada telemetria para monitorar o uso das opções de senha do administrador. • Modificadas as permissões do EC2Launch.	1º de julho de 2024

Versão	Detalhes	Data de lançamento
2.0.1924	• Atualização da interface do usuário de configurações do EC2Launch. • Atualização do comando da CLI para o papel de parede. • Atualização do instalador do EC2Launch.	10 de junho de 2024
2.0.1914	• Adição de rotas com endereços de gateway não especific ados (`0.0.0.0` para IPv4 ou`::` para IPv6). • Sempre adicione as rotas IPv4 e IPv6. • Correção de um problema em que o nome de usuário `Administrator` era adicionado ao arquivo `agent-con fig.yml` quando não estava especificado. • Modificação das permissões do EC2Launch v2.	5 de junho de 2024

Versão	Detalhes	Data de lançamento
2.0.1881	• Adicionada uma opção de senha criptografada à tarefa `setAdminAccount` . • Adicionado o comando da CLI para criptografar senha estática em agent-config.yml. • Corrigido um problema em que os dados de usuário do XML não adicionavam argumentos do PowerShell quando executados com permissões de administrador. Para mais informações, consulte Como o Amazon EC2 lida com os dados dos usuários para instâncias do Windows. • Ajustados os argumentos do PowerShell para a tarefa `executeScript` e os scripts de dados de usuário quando executados com permissões `LocalSystem` . Quando os argumentos estão em branco, o atendente usa o seguinte valor padrão: `-ExecutionPolicy Unrestricted` . • Evitada a impressão de versões duplicadas do driver no log do console.	8 de maio de 2024

Versão	Detalhes	Data de lançamento
2.0.1815	• Ajuste do tratamento de erros para gerar uma falha em problemas críticos de configuração antes da execução de sysprep. • Corrigido um problema em que tarefas de papel de parede e nome de host podiam usar um endereço IP incorreto em instâncias com vários endereços IP atribuídos à interface de rede primária. • As tarefas de papel de parede e nome de host foram alteradas para obter primeiro o IP privado do IMDS e, em seguida, retornar ao WMI caso o IMDS esteja desativado. • Corrigido um problema com a tarefa `initializeVolume` em que os volumes `sc1` não eram inicializados devido a um erro transitório.	6 de março de 2024
2.0.1739	• Correção de um problema que impedia a captura de códigos de saída por tarefas `executeScript` executadas como o usuário Administrador do Windows.	17 de janeiro de 2024

Versão	Detalhes	Data de lançamento
2.0.1702	• Permissões `Telemetry.log` restritas para `read-execute` somente para usuários padrão. • Configurado o serviço EC2Launch Windows para reiniciar em caso de falha na inicialização. • Falhas `add-routes` tornadas acionáveis ao registrar em log a saída `route.exe stderr`. • Corrigido um problema que ocorre quando as métricas de rota estão fora do intervalo [1, 9999]. • Adicionado suporte a papéis de parede para vários novos tipos de instâncias. • Corrigido um problema causado por scripts de dados do usuário executados como usuário administrador do Windows e que enviam a saída para `stderr`.	4 de janeiro de 2024

Versão	Detalhes	Data de lançamento
2.0.1643	• Atualização da ferramenta `ebsnvme-id.exe` para a versão 1.1.0.7. • Correção de um problema com o Receive Side Scaling (Dimensionamento Lateral de Recebimento, RSS) e as configurações de profundidade da fila de recebimento em tipos de instância de metal que começam com 'metal-*', como metal-48x1. • Remoção de evento de telemetria que relata comandos de dados de usuários em XML que bloqueiam o atendente. • Atualização da tarefa `setDnsSuffix` para limitar a devolução de nomes de domínio com base na entrada do registro: `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Dnscache\Parameters\DomainNameDevolutionLevel` . • Inclusão de uma tarefa pública e uma CLI que adiciona rotas de rede. • Observação: essa é a última versão que oferece suporte oficial ao Windows Server 2012. • Observação: essa é a última versão que oferece suporte oficial a sistemas operacionais de 32 bits.	4 de outubro de 2023
2.0.1580	• Alterou a forma como o atendente de inicialização lida com erros quando se modifica as permissões do arquivo de log. • Foi adicionado um tempo limite para conexão com a porta serial. O tempo limite permite que o atendente de lançamento continue em execução caso a porta serial esteja em uso.	5 de setembro de 2023

Versão	Detalhes	Data de lançamento

2.0.1521	• A sinalização –`block` dos comandos `EC2Launch .exe` , reset e sysprep foi descontinuada.
	• Atualização de `EC2Launch.exe` para detectar e lidar com os comandos reset e sysprep usados em tarefas `executeScript` em linha. Esses comandos fazem com que o atendente pare de ser executado depois que a tarefa `executeScript` os executa.
	• Scripts de dados de usuário em XML atualizados para serem executados em linha de forma automática.
	• Permite que scripts XML de dados de usuário sejam executados separadamente com a nova tag `detach`. Para obter mais detalhes, consulte Scripts de dados do usuário.
	• As alterações a seguir foram implementadas no log do atendente.
	  • Mensagens de log do atendente atualizadas.
	  • Conteúdo de `executeScript` e saída removidos do log do atendente.
	  • Argumentos de `executeProgram` e saída removidos do log do atendente.
	• As alterações a seguir foram implementadas no log do console.
	  • Valor `EnableSCSIPersistentReservations` adicionado ao log do console.
		3 de julho de 2023

Versão	Detalhes	Data de lançamento
2.0.1303	• Foram acrescentadas linhas adicionais de tratamento de erros e de logs ao acrescentar rotas de rede. • Tarefas `executeScript` e `executeProgram` permitidas no estágio PreReady. • Tarefa `executeProgram` atualizada para gerar arquivos de saída semelhantes à saída da tarefa executeScript. Para mais informações, consulte executeProgram. • Foi adicionada a telemetria para monitorar o uso dos comandos do atendente de bloqueio nos dados de usuário XML.	3 de maio de 2023
2.0.1245	• Maior visibilidade de falhas registrando em log pilhas de chamadas de falha em texto não criptografado. • Foi adicionado o serviço EventLog como uma dependência de startup para corrigir uma falha quando o serviço Amazon EC2Launch é iniciado mais rápido do que o serviço EventLog. • Foi feito com que os dados do usuário XML fossem executados antes do estágio PostReady a partir do arquivo de configuração do atendente (como EC2Launch v1 e EC2Config). • Foram adicionados dados do usuário YAML versão 1.1 para fazer com que os dados do usuário sejam executados antes do estágio PostReady a partir do arquivo de configuração do atendente (os dados do usuário YAML versão 1.0 são executados após o estágio PostReady a partir do arquivo de configuração do atendente).	8 de março de 2023

Versão	Detalhes	Data de lançamento
2.0.1173	• Adiciona um recurso opcional para exibir tags de instância no papel de parede. Para mais informações, consulte setWallpaper. • Adiciona o tratamento de erros quando o grupo de segurança do Elastic Graphics não está configurado corretamente. • Corrige um tempo limite quando o Instance Metadata Service não está habilitado.	6 de fevereiro de 2023
2.0.1121	• Corrige um problema em que um erro 404 é impresso no papel de parede quando nenhum endereço IPv4 público é atribuído. • Corrige um problema em que o sistema de arquivos do volume é formatado como `RAW` em vez de `NTFS` quando a letra da unidade do dispositivo é definida como `D`. • Corrige um problema em que os volumes de SSD NVMe estão identificados incorretamente como volumes do EBS. • Corrige um erro ao ativar o Windows quando o IMDS está desativado.	4 de janeiro de 2023

Versão	Detalhes	Data de lançamento
2.0.1082	• Corrige um problema em que o campo `setWallpaper` : `privateIpAddress` : fica em branco quando o IMDS está desabilitado. • Corrige um problema com a configuração de hostname para o endereço IPv4 privado quando o IMDS está desabilitado. • Corrige um problema com a inicialização de volumes no Windows Server 2012. • Corrige um problema com a configuração de frames jumbo. • Corrige um erro quando nenhuma chave SSH é especificada na inicialização da instância. • Corrige um erro no Windows Server 2012 quando o Windows não tem uma chave de registro “ReleaseId”.	7 de dezembro de 2022
2.0.1011	• Corrige a lógica para encontrar o adaptador de rede quando o PnPDeviceID está vazio.	11 de novembro de 2022
2.0.1009	• Usa informações do segmento PCI para selecionar a porta do console.	8 de novembro de 2022

Versão	Detalhes	Data de lançamento
2.0.982	• Adiciona lógica de nova tentativa para obtenção de informaçõ es de RDP. • Corrige erros durante a inicialização do volume em instâncias `d2.8xlarge` . • Corrige um problema que permite selecionar um adaptador de rede incorreto após uma reinicialização. • Remove a mensagem de erro de alarme falso quando o ACPI SPCR está indisponível.	31 de outubro de 2022
2.0.863	• Atualiza a lógica de espera IMDS para que sejam feitas somente solicitações IMDSv2. • Adiciona lógica para atribuir a letra da unidade a volumes que já foram inicializados, mas não montados. • Imprime uma mensagem de erro mais específica quando não há suporte ao tipo do par de chaves. • Corrige o erro do código de reinicialização 3010. • Adiciona a verificação de dados do usuário com codificação base64 inválida.	6 de julho de 2022
2.0.698	• Corrige o erro de digitação na saída do log ao executar scripts.	30 de janeiro de 2022

Versão	Detalhes	Data de lançamento
2.0.674	• A telemetria carrega o controle de privacidade habilitado/desabilitado. • Corrige o bug `index out of bounds`. • Remove atalhos de papel de parede durante `sysprep`.	15 de novembro de 2021
2.0.651	• Adiciona lógica para desinstalar atendentes herdados durante a instalação do EC2Launch v2. • Corrige o problema de CLI `list-volume` quando o volume raiz não está listado como volume 0.	7 de outubro de 2021
2.0.592	• Corrige o bug para relatar corretamente o status do estágio. • Remove alarmes falsos de mensagens de erro quando os arquivos de log são fechados. • Adiciona telemetria.	31 de agosto de 2021
2.0.548	• Adiciona zeros à esquerda para nome de host IP hexadecimal. • Corrige permissões de arquivo para a tarefa `enableOpenSsh` . • Corrige a falha no comando sysprep.	4 de agosto de 2021

Versão	Detalhes	Data de lançamento
2.0.470	• Corrige o erro na etapa de rede para esperar que o DHCP atribua um IP à instância. • Correções de erros com `setDnsSuffix` quando a chave de registro `SearchList` não existe. • Corrige o bug na lógica de devolução de DNS em `setDnsSuffix` . • Adiciona roteamentos de rede após reinicializações intermediárias. • Permite que `initializeVolume` volte a escrever volumes existentes. • Remove informações adicionais do subcomando da versão.	20 de julho de 2021
2.0.285	• Adiciona opção de executar scripts de usuário em um processo desanexado. • Os dados de usuário herdados (dados de usuário XML) agora são executados em um processo desvinculado, que é um comportamento semelhante ao atendente de inicialização anterior. • Adiciona o sinalizador CLI ao `sysprep` e aos comandos `reset`, o que os permite bloquear até que o serviço pare. • Restringe as permissões da pasta de configuração.	8 de março de 2021

Versão	Detalhes	Data de lançamento
2.0.207	• Adiciona o campo `hostName` opcional à tarefa `setHostName`. • Corrige bugs de reinicialização. As tarefas de reinicialização `executeScript` e `executeProgram` serão marcadas como em execução. • Adiciona mais códigos de retorno ao comando de status. • Adiciona o serviço de bootstrap para corrigir problema de startup ao executar no tipo de instância `t2.nano`. • Corrige o modo de instalação limpa para remover arquivos não rastreados pelo instalador.	2 de fevereiro de 2021
2.0.160	• Corrige o comando `validate` para detectar nomes de estágios inválidos. • Adiciona o comando `w32tm resync` na tarefa `addroutes`. • Corrige o problema com a alteração da ordem de pesquisa de sufixos DNS. • Adiciona condições de verificação para informar melhor os dados inválidos do usuário.	4 de dezembro de 2020
2.0.153	Adiciona a funcionalidade Sysprep em UserData.	3 de novembro de 2020

Versão	Detalhes	Data de lançamento
2.0.146	• Corrige o problema com RootExtend em AMIs em outros idiomas. • Concede permissão de gravação ao grupo de usuários para os arquivos de log. • Cria partição MS Reserved para volumes GPT. • Adiciona o comando list-volumes e o menu suspenso de volume nas configurações do Amazon EC2Launch. • Adiciona comando get-agent-config para imprimir o arquivo agent-config.yml no formato yaml ou json. • Apaga a senha estática caso nenhuma chave pública seja detectada.	6 de outubro de 2020
2.0.124	• Adiciona a opção para exibir a versão do SO no papel de parede. • Inicializa volumes criptografados do EBS. • Adiciona rotas para VPCs sem nome DNS local.	10 de setembro de 2020
2.0.104	• Cria a lista de pesquisa de sufixos DNS, caso ela não exista. • Ignora a hibernação caso não seja solicitado.	12 de agosto de 2020
2.0.0	Versão inicial.	30 de junho de 2020

Usar o agente do EC2Launch v1 para realizar tarefas durante a execução da instância EC2 Windows

As AMIs gerenciadas pela Amazon para o Windows Server 2016 e 2019 incluem um conjunto de scripts do Windows PowerShell chamados EC2Launch. O EC2Launch executa tarefas durante a inicialização inicial da instância. Para obter informações sobre as versões do EC2Launch incluídas nas AMIs da AWS para o Windows, consulte AWS Windows AMI Reference.

> **Note**
>
> O agente de inicialização mais recente para o Windows Server 2016 e versões posteriores do sistema operacional é o EC2Launch v2, que substitui tanto o EC2Config quanto o EC2Launch, e está pré-instalado nas AMIs da AWS para o Windows Server 2016 e 2019 com nomes que começam com `EC2LaunchV2-Windows_Server-*`. Você também instalar manualmente e configurar o agente no Windows Server 2016 e 2019. Para obter mais informações, consulte Instalar o EC2Launch v2.
> Para usar o EC2Launch com IMDSv2, a versão deve ser a 1.3.2002730 ou posterior.

É possível usar o comando do Windows PowerShell a seguir para verificar a versão instalada do EC2Launch.

```
Test-ModuleManifest -Path "C:\ProgramData\Amazon\EC2-Windows\Launch\Module
\Ec2Launch.psd1" | Select Version
```

Tarefas do EC2Launch

Por padrão, o EC2Launch executa as seguintes tarefas durante a primeira inicialização da instância:

- Configura novo papel de parede que produz informações sobre a instância.
- Define o nome do computador para o endereço IPv4 privado da instância.
- Envia informações da instância ao console do Amazon EC2.
- Envia a impressão digital do certificado RDP ao console do EC2.
- Define uma senha aleatória para a conta do administrador.
- Adiciona sufixos DNS.
- Estende dinamicamente a partição do sistema operacional para incluir qualquer espaço não particionado.

- Executa dados do usuário (se especificado). Para obter mais informações sobre como especificar os dados do usuário, consulte Executar comandos ao iniciar uma instância do EC2 com entrada de dados do usuário.
- Define rotas estáticas persistentes para alcançar o serviço de metadados e os servidores AWS KMS.

> **Important**
>
> Se uma AMI personalizada for criada a partir dessa instância, essas rotas serão capturadas como parte da configuração do sistema operacional e quaisquer novas instâncias iniciadas a partir da AMI manterão as mesmas rotas, independentemente do posicionamento da sub-rede. Para atualizar as rotas, consulte Para atualizar rotas de metadados/KMS para o Server 2016 e posterior ao iniciar uma AMI personalizada.

As seguintes tarefas ajudam a manter a compatibilidade com versões anteriores do serviço do EC2Config. Também é possível configurar o EC2Launch para executar essas tarefas durante o startup:

- Inicializar volumes de EBS secundários.
- Enviar logs de eventos do Windows aos logs do console do EC2.
- Enviar a mensagem O Windows está pronto para uso ao console do EC2.

Estrutura de diretório do EC2Launch

Por padrão, o EC2Launch é instalado nas AMIs do Windows Server 2016 e posterior no diretório raiz `C:\ProgramData\Amazon\EC2-Windows\Launch`.

> **Note**
>
> Por padrão, o Windows oculta os arquivos e as pastas sob `C:\ProgramData`. Para visualizar os diretórios e arquivos do EC2Launch, digite o caminho no Windows Explorer ou altere as propriedades da pasta para os arquivos e as pastas ocultos.

O diretório `Launch` contém os seguintes subdiretórios.

- `Scripts` — contém os scripts do PowerShell que compõem o EC2Launch.

- `Module` — contém o módulo para compilação dos scripts relacionados ao Amazon EC2.
- `Config` — contém arquivos script de configuração que é possível personalizar.
- `Sysprep` — contém recursos de Sysprep.
- `Settings`: contém uma aplicação para a interface gráfica do usuário do Sysprep.
- `Library` – Contém bibliotecas compartilhadas para agentes de inicialização do EC2.
- `Log`: contém subdiretórios para scripts e os arquivos de log que são gerados pelos scripts.

Telemetria

Telemetria é informação adicional que ajuda o AWS a entender melhor suas necessidades, diagnosticar problemas e fornecer recursos para melhorar sua experiência com os serviços da AWS.

O EC2Launch versão `1.3.2003498` e posteriores coleta telemetria, como métricas de uso e erros. Esses dados são coletados na instância do Amazon EC2 na qual o EC2Launch é executado. Isso inclui todas as AMIs do Windows de propriedade da AWS.

Os seguintes tipos de telemetria são coletados pelo EC2Launch:

- Informações de uso: comandos do agente, método de instalação e frequência de execução programada.
- Erros e informações de diagnóstico: instalação do agente e execução dos códigos de erro.

Exemplos de dados coletados pelo:

```
2021/07/15 21:44:12Z: EC2LaunchTelemetry: IsAgentScheduledPerBoot=true
2021/07/15 21:44:12Z: EC2LaunchTelemetry: IsUserDataScheduledPerBoot=true
2021/07/15 21:44:12Z: EC2LaunchTelemetry: AgentCommandCode=1
2021/07/15 21:44:12Z: EC2LaunchTelemetry: AgentCommandErrorCode=5
2021/07/15 21:44:12Z: EC2LaunchTelemetry: AgentInstallCode=2
2021/07/15 21:44:12Z: EC2LaunchTelemetry: AgentInstallErrorCode=0
```

A telemetria está habilitada por padrão. É possível desativar a coleta de telemetria a qualquer momento. Se a telemetria estiver habilitada, o EC2Launch enviará dados de telemetria sem notificações adicionais do cliente.

Sua escolha de habilitar ou desabilitar a telemetria é coletada.

É possível optar por habilitar ou desabilitar a coleta de telemetria. Sua seleção de optar por habilitar ou desabilitar telemetria é coletada para garantir que atenderemos à sua opção de telemetria.

Visibilidade de telemetria

Quando a telemetria é ativada, ela aparece na saída do console do Amazon EC2 da seguinte maneira:

```
2021/07/15 21:44:12Z: Telemetry: <Data>
```

Desativar telemetria em uma instância

Para desativar a telemetria definindo uma variável de ambiente do sistema, execute o seguinte comando como administrador:

```
setx /M EC2LAUNCH_TELEMETRY 0
```

Para desabilitar a telemetria durante a instalação, execute `install.ps1` da seguinte forma:

```
. .\install.ps1 -EnableTelemetry:$false
```

Mais tópicos do EC2Launch

- Instalar a versão mais recente do EC2Launch
- Configurar o agente do EC2Launch v1 na instância do Windows
- Histórico de versões do EC2Launch

Instalar a versão mais recente do EC2Launch

Use o seguinte procedimento para baixar e instalar a versão mais recente do EC2Launch em suas instâncias.

Para fazer download e instalar a versão mais recente do EC2Launch

1. Se você já tiver instalado e configurado o EC2Launch em uma instância, faça um backup do arquivo de configuração do EC2Launch. O processo de instalação não preserva as alterações feitas nesse arquivo. Por padrão, o arquivo está localizado no diretório `C:\ProgramData\Amazon\EC2-Windows\Launch\Config`.

2. Faça download do EC2-Windows-Launch.zip em um diretório na instância.
3. Faça download do install.ps1 no mesmo diretório onde você baixou o `EC2-Windows-Launch.zip`.
4. Executar `install.ps1`
5. Se você fez um backup do arquivo de configuração do EC2Launch, copie-o no diretório `C:\ProgramData\Amazon\EC2-Windows\Launch\Config`.

Para baixar e instalar a versão mais recente do EC2Launch usando o PowerShell

Se você já tiver instalado e configurado o EC2Launch em uma instância, faça um backup do arquivo de configuração do EC2Launch. O processo de instalação não preserva as alterações feitas nesse arquivo. Por padrão, o arquivo está localizado no diretório `C:\ProgramData\Amazon\EC2-Windows\Launch\Config`.

Para instalar a versão mais recente do EC2Launch usando o PowerShell, execute os seguintes comandos em uma janela do PowerShell como administrador:

```
mkdir $env:USERPROFILE\Desktop\EC2Launch
$Url = "https://s3.amazonaws.com/ec2-downloads-windows/EC2Launch/latest/EC2-Windows-Launch.zip"
$DownloadZipFile = "$env:USERPROFILE\Desktop\EC2Launch\" + $(Split-Path -Path $Url -Leaf)
Invoke-WebRequest -Uri $Url -OutFile $DownloadZipFile
$Url = "https://s3.amazonaws.com/ec2-downloads-windows/EC2Launch/latest/install.ps1"
$DownloadZipFile = "$env:USERPROFILE\Desktop\EC2Launch\" + $(Split-Path -Path $Url -Leaf)
Invoke-WebRequest -Uri $Url -OutFile $DownloadZipFile
& $env:USERPROFILE\Desktop\EC2Launch\install.ps1
```

> **Note**
>
> Se você receber um erro ao baixar o arquivo e estiver usando o Windows Server 2016, talvez seja necessário habilitar o TLS 1.2 para seu terminal PowerShell. É possível habilitar o TLS 1.2 para a sessão atual do PowerShell com o comando a seguir e tentar novamente:
>
> ```
> [Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
> ```

Verifique a instalação conferindo o agente de inicialização. Execute os seguintes comandos em uma janela do PowerShell como administrador:

```
Import-Module C:\ProgramData\Amazon\EC2-Windows\Launch\Module\Ec2Launch.psm1
Import-LocalizedData -BaseDirectory C:\ProgramData\Amazon\EC2-Windows\Launch\Module\ -
FileName 'Ec2Launch.psd1' -BindingVariable moduleManifest
$moduleManifest.Get_Item('ModuleVersion')
```

Configurar o agente do EC2Launch v1 na instância do Windows

Quando a instância tiver sido inicializada pela primeira vez, é possível configurar o EC2Launch para iniciar novamente e executar diferentes tarefas de startup.

Tarefas

- Configurar as tarefas de inicialização
- Programar o EC2Launch para ser executado em cada inicialização
- Inicializar unidades e mapear as letras de unidades
- Enviar logs de eventos do Windows ao console do EC2
- Enviar a mensagem O Windows está pronto após uma inicialização bem-sucedida

Configurar as tarefas de inicialização

Especifique as configurações no arquivo `LaunchConfig.json` para ativar ou desativar as seguintes tarefas de inicialização:

- Defina o nome do computador para o endereço IPv4 privado da instância.
- Defina o monitor para ficar sempre ligado.
- Configurar novo papel de parede.
- Adicionar a lista de sufixos DNS.

> **Note**
>
> Isso adiciona uma pesquisa de sufixo DNS para o domínio apresentado a seguir e configura outros sufixos padrão. Para obter mais informações sobre como os agentes de inicialização definem os sufixos DNS, consulte Configurar o sufixo DNS para agentes de execução do EC2 Windows.

```
region.ec2-utilities.amazonaws.com
```

- Estender o tamanho do volume de inicialização.
- Defina a senha de administrador.

Para definir as configurações de inicialização

1. Na instância a ser configurada, abra o seguinte arquivo em um editor de texto: `C:\ProgramData\Amazon\EC2-Windows\Launch\Config\LaunchConfig.json`.
2. Atualize as seguintes configurações conforme necessário e salve suas alterações. Forneça uma senha em `adminPassword` somente se `adminPasswordtype` for `Specify`.

```
{
 "setComputerName": false,
 "setMonitorAlwaysOn": true,
 "setWallpaper": true,
 "addDnsSuffixList": true,
 "extendBootVolumeSize": true,
 "handleUserData": true,
 "adminPasswordType": "Random | Specify | DoNothing",
 "adminPassword": "password that adheres to your security policy (optional)"
}
```

Os tipos de senha são definidos da seguinte maneira:

`Random`

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

`Specify`

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

`DoNothing`

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

3. No Windows PowerShell, execute o seguinte comando para programar a execução do script como uma tarefa agendada do Windows. O script é executado uma vez durante a próxima inicialização e desativa essas tarefas para que não sejam executadas novamente.

```
C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeInstance.ps1 -Schedule
```

Programar o EC2Launch para ser executado em cada inicialização

É possível programar o EC2Launch para ser executado em cada inicialização e não apenas na inicialização inicial.

Para programar o EC2Launch para ser executado em cada inicialização:

1. Abra o Windows PowerShell e execute o seguinte comando:

```
C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeInstance.ps1 -
SchedulePerBoot
```

2. Ou execute o executável com o seguinte comando:

```
C:\ProgramData\Amazon\EC2-Windows\Launch\Settings\Ec2LaunchSettings.exe
```

Em seguida, selecione `Run EC2Launch on every boot`. É possível especificar que sua instância do EC2 seja `Shutdown without Sysprep` ou `Shutdown with Sysprep`.

> **Note**
>
> Quando você habilita o EC2Launch para ser executado em cada inicialização, acontecerá o seguinte na próxima vez que o EC2Launch for executado:
>
> - Se o `AdminPasswordType` ainda estiver definido como `Random`, o EC2Launch gerará uma nova senha na próxima inicialização. Após a reinicialização, o `AdminPasswordType` é automaticamente definido como `DoNothing`para impedir que o EC2Launch gere novas senhas em inicializações subsequentes. Para evitar que o EC2Launch gere uma nova

senha na primeira inicialização, defina manualmente o `AdminPasswordType` como `DoNothing` antes de reiniciar.

- `HandleUserData` será redefinido como `false` a menos que os dados do usuário tenham `persist` definido como `true`. Para obter mais informações, consulte the section called "Scripts de dados do usuário".

Inicializar unidades e mapear as letras de unidades

Especifique as configurações no arquivo `DriveLetterMappingConfig.json` para mapear letras de unidades para volumes na instância do EC2. O script inicializa drives que ainda não foram inicializados e particionados. Para obter mais informações sobre como obter detalhes do volume no Windows, consulte Get-Volume na documentação da Microsoft.

Para mapear letras de unidade a volumes

1. Abra o arquivo `C:\ProgramData\Amazon\EC2-Windows\Launch\Config\DriveLetterMappingConfig.json` em um editor de textos.
2. Especifique as seguintes configurações de volume e salve suas alterações:

```
{
 "driveLetterMapping": [
  {
   "volumeName": "sample volume",
   "driveLetter": "H"
  }
 ]
}
```

3. Abra o Windows PowerShell e use o seguinte comando para executar o script do EC2Launch que inicializa os discos:

```
C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeDisks.ps1
```

Para inicializar os discos sempre que a instância for inicializada, adicione o sinalizador `-Schedule` da seguinte forma:

```
C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeDisks.ps1 -Schedule
```

Enviar logs de eventos do Windows ao console do EC2

Especifique configurações no arquivo `EventLogConfig.json` para enviar logs de eventos do Windows aos logs do console do EC2.

Para definir as configurações para enviar logs de eventos do Windows

1. Na instância, abra o arquivo `C:\ProgramData\Amazon\EC2-Windows\Launch\Config\EventLogConfig.json` em um editor de texto.
2. Configure as seguintes configurações de log e salve suas alterações:

```
{
 "events": [
  {
   "logName": "System",
   "source": "An event source (optional)",
   "level": "Error | Warning | Information",
   "numEntries": 3
  }
 ]
}
```

3. No Windows PowerShell, execute o seguinte comando para que o sistema agende o script para execução como uma tarefa agendada do Windows sempre que a instância for inicializada.

```
C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\SendEventLogs.ps1 -Schedule
```

   Os logs podem demorar três minutos ou mais para aparecerem no console do EC2.

Enviar a mensagem O Windows está pronto após uma inicialização bem-sucedida

O serviço de EC2Config envia a mensagem “O Windows está pronto” ao console do EC2 após cada inicialização. O EC2Launch envia essa mensagem somente após a primeira inicialização. Para compatibilidade com versões anteriores do serviço de EC2Config, é possível agendar o EC2Launch para enviar essa mensagem após cada inicialização. Na instância, abra o Windows PowerShell e execute o seguinte comando. O sistema agenda o script para ser executado como uma tarefa agendada do Windows.

```
C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\SendWindowsIsReady.ps1 -Schedule
```

Histórico de versões do EC2Launch

> **Important**
>
> A partir de 1.º de janeiro de 2025, há suporte somente às duas versões mais recentes. Ao lançar uma nova versão, a versão mais antiga com suporte será automaticamente marcada como privada e deixará de estar disponível para download.

Para fazer download e instalar a versão mais recente do EC2Launch, consulte Instalar a versão mais recente do EC2Launch.

É possível receber notificações quando novas versões do agente do EC2Launch forem liberadas. Para obter mais informações, consulte Assinar as notificações do agente de execução do EC2 Windows.

As versões apresentadas a seguir do agente EC2Launch são compatíveis e estão disponíveis para download.

Versão	Detalhes	Data de lançamento
1.4.183	• A lógica do programa de instalação foi atualizada para evitar uma instalação incompatível no Windows Server 2022. • Atualizado para imprimir a versão do driver EC2WinUtil no log do console da instância.	4 de fevereiro de 2026
1.4.6	• Mensagens de log do atendente atualizadas.	13 de outubro de 2025

As versões anteriores do EC2Launch, apresentadas a seguir, não estão mais disponíveis para download.

Versão	Detalhes	Data de lançamento
1.3.2005119	• Correção de um problema em que `Invoke-Userdata` não funcionava quando chamado sem parâmetros.	11 de fevereiro de 2025
1.3.2005065	• Correção de um problema em que as informações do certifica do RDP não eram recuperadas ou validadas adequadamente. Funcionalidade adicionada para iniciar automaticamente os Serviços de Área de Trabalho Remota, se necessário.	22 de outubro de 2024
1.3.2005008	• `Set-Wallpaper` atualizado para retornar para um fundo de cor sólida se a imagem de papel de parede padrão não for encontrada.	6 de agosto de 2024
1.3.2004959	• A lógica do programa de instalação foi atualizada para evitar uma instalação incompatível no Windows Server 2025 ou posterior.	2 de julho de 2024
1.3.2004891	• Corrigido um problema em que `HandleUserData` não estava definido como `false` conforme o esperado. • Adicionou uma opção de senha `Encrypted` a `LaunchConfig.json` . • Comportamento de `Settings UI` alterado para criptografar a senha especificada pelo usuário por padrão. • Adicionado `SetAdminPasswordConfig.ps1` para converter a opção de senha `Specify` para a opção de senha `Encrypted` no arquivo de configuração do agente.	31 de maio de 2024
1.3.2004617	• Correção de um erro ao definir o papel de parede.	15 de janeiro de 2024

Versão	Detalhes	Data de lançamento
1.3.2004592	• Atualizadas permissões de acesso definidas por install.ps1 para `%ProgramData%\Amazon\EC2-Windows\Launch` . • Restringido o acesso a pastas/arquivos do EC2Launch para leitura e execução somente para contas de usuário padrão. • Alterado o agente para parar de esperar que o serviço de metadados de instância (IMDS) inicialize se o IMDS não estiver habilitado para a instância. • Adicionado um tempo limite de cinco minutos ao ser aguardada a inicialização do IMDS. • Alterado o agente para gravar a telemetria no log do console da instância antes da mensagem `Windows is Ready`, em vez de depois. • Adicionado suporte a papéis de parede para vários novos tipos de instâncias. Para obter mais informações sobre as permissões de acesso e as permissões de conta de usuário dos diretórios do EC2Launch, consulte the section called “Estrutura de diretório do EC2Launch”.	2 de janeiro de 2024
1.3.2004491	• Adicionada telemetria para monitorar o uso da opção Especificar senha do administrador.	9 de novembro de 2023
1.3.2004462	• Adicionada uma descarga após cada gravação no console de série.	18 de outubro de 2023

Versão	Detalhes	Data de lançamento
1.3.2004438	• Limitação da devolução de nomes de domínio com base na entrada do registro: `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Dnscache\Parameters\DomainNameDevolutionLevel` . • Limitação das permissões `UserdataExecution.log` apenas para `Administrators` . • Mensagens de erro adicionadas no log de eventos do Windows quando ocorre falha na inicialização.	4 de outubro de 2023
1.3.2004256	• Valor `EnableSCSIPersistentReservations` adicionado ao log do console. • Adição da capacidade de realização de novas tentativas a Get-ConsolePort.	7 de julho de 2023
1.3.2004052	• Corrigido um erro que ocorria quando nenhuma chave SSH era especificada na inicialização da instância. • Atualizado para tentar iniciar novamente o serviço AmazonSSMAgent Windows em caso de falha. • Atualizado para falhar SysprepInstance.ps1 se BeforeSysprep.cmd falhar com um código de saída diferente de zero.	8 de março de 2023
1.3.2003975	• Foi corrigido o problema que afetava as compilações do Packer AMI, em que `SysprepInstance.ps1` retorna um `$LastErrorCode` de 1.	24 de dezembro de 2022

Versão	Detalhes	Data de lançamento
1.3.2003961	• Foi corrigido um problema em que senhas de administrador especificadas explicitamente eram substituídas por uma senha aleatória em instâncias de inicialização rápida. • Foi corrigido um problema em que o SSM Agent apresentava falha ao iniciar em tipos de instância menores. • Foi corrigido um problema em que o log do console da instância continha `RDPCERTIFICATE-THUMBPRINT: 0000000000000000000000` em vez de um valor de impressão digital válido do certificado RDP.	6 de dezembro de 2022
1.3.2003923	• Corrige a lógica para encontrar o adaptador de rede quando o PnPDeviceID está vazio.	9 de novembro de 2022
1.3.2003919	• Atualizado Get-ConsolePort para usar as informações do segmento PCI. • Corrigido um problema que permite selecionar um adaptador de rede incorreto após a reinicialização. • Corrigida a lógica de tempo limite do Start-SSM-Agent. • Corrigida a compatibilidade com versões anteriores do alias da função Send-AdminCredentials.	8 de novembro de 2022
1.3.2003857	• Prioriza adaptadores com um gateway padrão quando o adaptador da rede primária é selecionado. • Criptografia de senha na memória estendida.	3 de outubro de 2022

Versão	Detalhes	Data de lançamento
1.3.2003824	• Foi corrigido o erro durante `setComputerName` . • Foi adicionada a lógica para ignorar a ativação do Windows quando um código de faturamento BYOL for detectado. • Foi adicionada criptografia de senha na memória. • Foi corrigido o erro durante a inicialização do volume em `m6id.4xlarge` .	30 de agosto de 2022
1.3.2003691	• Atualizada a lógica de espera IMDS para fazer somente solicitações IMDSv2. • Correção de bug que afeta a instalação da eGPU.	21 de junho de 2022
1.3.2003639	• Adicionada a lógica de espera do adaptador de rede para impedir o uso antes da inicialização. • Problemas secundários corrigidos.	10 de maio de 2022
1.3.2003498	• Telemetria adicionada. • Atalho adicionado à UI de Configurações. • Scripts PowerShell formatados. • Corrigido o problema de desligamento antes da conclusão do Beforesysprep.cmd.	31 de janeiro de 2022
1.3.2003411	Alterou-se a lógica de geração de senha para excluir senhas com baixa complexidade.	4 de agosto de 2021

Versão	Detalhes	Data de lançamento
1.3.2003364	Install-EGPumanager atualizado com suporte a IMDSv2.	7 de junho de 2021
1.3.2003312	• Linhas de log adicionadas antes e depois da configuração de `setMonitorAlwaysOn` . • Incluída a versão do pacote do AWS Nitro Enclaves no log do console.	04 de maio de 2021
1.3.2003284	Modelo de permissão aprimorado com atualização do local para armazenar dados do usuário em `LocalAppData` .	23 de março de 2021
1.3.2003236	• Método atualizado para definir a senha do usuário em `Set-AdminAccount` e `Randomize-LocalAdminPassword` . • `InitializeDisks` fixos para verificar se o disco está definido como somente leitura antes de configurá-lo para gravável.	11 de fevereiro de 2021
1.3.2003210	Correção de localização para `install.ps1` .	7 de janeiro de 2021
1.3.2003205	Correção de segurança do `install.ps1` para atualizar permissões no diretório `%ProgramData%AmazonEC2-WindowsLaunchModuleScripts` .	28 de dezembro de 2020
1.3.2003189	Adição do `w32tm resync` depois de adicionar rotas.	4 de dezembro de 2020
1.3.2003155	Informações de tipo de instância atualizadas.	25 de agosto de 2020

Versão	Detalhes	Data de lançamento
1.3.2003150	`OsCurrentBuild` e `OsReleaseId` adicionados à saída do console.	22 de abril de 2020
1.3.2003040	Lógica de fallback de versão 1 IMDS corrigida.	7 de abril de 2020
1.3.2002730	Suporte adicionado para IMDS V2.	3 de março de 2020
1.3.2002240	Problemas secundários corrigidos.	31 de outubro de 2019
1.3.2001660	Corrigido o problema de login automático para usuários sem a senha depois da primeira execução do Sysprep.	2 de julho de 2019
1.3.2001360	Problemas secundários corrigidos.	27 de março de 2019
1.3.2001220	Todos os scripts do PowerShell assinados.	28 de fevereiro de 2019
1.3.2001200	Corrigido o problema com InitializeDisks.ps1 em que a execução do script em um nó em um Cluster de Failover do Windows Server formaria unidades em nós remotos cuja letra da unidade correspondesse à letra da unidade local.	27 de fevereiro de 2019
1.3.2001160	Corrigido o papel de parede ausente no Windows 2019.	22 de fevereiro de 2019
1.3.2001040	• Plugin adicionado para configurar o monitor para nunca desligar para corrigir problemas de ACPI. • Edição e versão do SQL Server gravadas no console.	21 de janeiro de 2019

Versão	Detalhes	Data de lançamento
1.3.2000930	Correção para adição de rotas a metadados em ENIs habilitadas para IPv6.	2 de janeiro de 2019
1.3.2000760	• Configuração padrão para RSS e configurações de fila de recebimento para dispositivos ENA adicionadas • Hibernação desabilitada durante Sysprep.	5 de dezembro de 2018
1.3.2000630	• Adição da rota 169.254.169.253/32 para servidor DNS. • Adicionado filtro de configuração de usuário administrador. • Melhorias feitas na hibernação de instâncias. • Adicionada opção para programar o EC2Launch para ser executado em cada inicialização.	9 de novembro de 2018
1.3.2000430.0	• Rota 169.254.169.123/32 adicionada ao serviço de horário do AMZN. • Rota 169.254.169.249/32 adicionada ao serviço de licença do GRID. • Adicionado tempo limite de 25 segundos ao tentar iniciar o Systems Manager.	19 de setembro de 2018
1.3.200039.0	• Corrigida a letra incorreta de unidade para volumes EBS NVME. • Adicionado log adicional para versões do driver NVME.	15 de agosto de 2018
1.3.2000080	Problemas secundários corrigidos.	

Versão	Detalhes	Data de lançamento
1.3.610	Problema corrigido com redirecionamento de saída e erros para os arquivos de dados do usuário.	
1.3.590	• Tipos de instâncias ausentes adicionadas ao papel de parede. • Problema corrigido com mapeamento de letra de unidade e instalação de disco.	
1.3.580	• `Get-Metadata` corrigido para usar as configurações do proxy do sistema padrão para solicitações da Web. • Adicionou um argumento especial para NVMe na inicialização do disco. • Problemas secundários corrigidos.	
1.3.550	Adicionou uma opção `-NoShutdown` para ativar o Sysprep sem desligamento.	
1.3.540	Problemas secundários corrigidos.	
1.3.530	Problemas secundários corrigidos.	
1.3.521	Problemas secundários corrigidos.	
1.3.0	• Problema de tamanho de hexadecimal corrigido para alteração de nome do computador. • Possível loop de reinicialização corrigido para alteração de nome do computador. • Problema de configuração de papel de parede corrigido.	

Versão	Detalhes	Data de lançamento
1.2.0	• Atualização para exibir informações sobre o sistema operacional (SO) instalado no log do sistema do EC2. • Atualização para exibir a versão do EC2Launch e do SSM Agent no log do sistema do EC2. • Problemas secundários corrigidos.	
1.1.2	• Atualização para exibir informações do driver de ENA no log do sistema do EC2. • Atualização para excluir o Hyper-V da lógica primária do filtro NIC. • O servidor e a porta do AWS KMS foram adicionados à chave do registro para ativação do KMS. • Configuração de papel de parede aprimorada para vários usuários. • Atualização para limpar rotas no armazenamento persistente. • Atualização para remover o z da zona de disponibilidade na lista de sufixos DNS. • Atualização para resolver um problema com a tag <runAsLocalSystem> nos dados do usuário.	
1.1.1	Versão inicial.	

Usar o serviço EC2Config para realizar tarefas durante a execução da instância herdada do sistema operacional Windows do EC2

> **Note**
>
> O EC2Config atingiu o fim do suporte. As versões do sistema operacional em que ele é executado não têm mais suporte pela Microsoft. É altamente recomendável atualizar para o agente de execução mais recente.
> O agente de inicialização mais recente do Windows Server 2022 e versões posteriores do sistema operacional é o EC2Launch v2, que substitui o EC2Config e o EC2Launch e vem pré-instalado nas AMIs do Windows Server 2022 e 2025 da AWS. Você também instalar manualmente e configurar o agente no Windows Server 2016 e 2019. Para obter mais informações, consulte Instalar o EC2Launch v2.

As AMIs do Windows para versões do Windows Server anteriores ao Windows Server 2016 incluem um serviço opcional: EC2Config (`EC2Config.exe`). O EC2Config é iniciado quando a instância inicia e executa tarefas durante o startup e sempre você iniciar ou para iniciar a instância. O EC2Config também executa tarefas sob demanda. Algumas dessas tarefas são automaticamente habilitadas, enquanto outras precisam ser habilitadas manualmente. Embora opcional, esse serviço dá acesso a recursos avançados que não estariam disponíveis de outra forma. Esse serviço é executado na conta LocalSystem.

O serviço EC2Config executa o Sysprep, uma ferramenta da Microsoft que permite a criação de uma AMI personalizada do Windows que pode ser reutilizada. Quando o EC2Config acessa o Sysprep, ela usa os arquivos em `%ProgramFiles%\Amazon\EC2ConfigService\Settings` para determinar quais operações devem ser executadas. É possível editar esses arquivos indiretamente usando a caixa de diálogo EC2 Service Properties do sistema, ou usando diretamente um editor de XML ou texto. Contudo, há algumas configurações avançadas que não estão disponíveis na caixa de diálogo Propriedades do serviço do EC2 do serviço, portanto, é necessário editar as entradas diretamente.

Se você criar AMIs com base em uma instância depois de atualizar suas configurações, as configurações novas serão aplicadas a qualquer instância executada pela nova AMI. Para obter informações sobre como criar uma AMI, consulte Criação de uma AMI baseada no Amazon EBS.

O EC2Config usa arquivos de configurações para controlar sua operação. É possível atualizar esses arquivos de configurações usando uma ferramenta gráfica ou editando diretamente arquivos XML.

Os arquivos binários de serviço e adicionais estão contidos no diretório `%ProgramFiles%\Amazon\EC2ConfigService`.

Conteúdo

- EC2Config e AWS Systems Manager
- Tarefas do EC2Config
- Arquivos de configurações do EC2Config
- Instalar a versão mais recente do EC2Config
- Configurar as definições do proxy .NET para o serviço EC2Config
- Definir as propriedades do serviço EC2Config na caixa de diálogo do sistema na instância EC2 Windows
- Solucionar problemas com o agente de execução do EC2Config
- Histórico de versões do EC2Config

EC2Config e AWS Systems Manager

O serviço EC2Config processa solicitações de Systems Manager nas instâncias criadas com base em AMIs para versões do Windows Server anteriores ao Windows Server 2016 que foram publicadas antes de novembro de 2016.

Instâncias criadas com base em AMIs para versões do Windows Server anteriores ao Windows Server 2016, publicadas depois de novembro de 2016 incluem o serviço EC2Config e SSM Agent. O EC2Config executa todas as tarefas descritas anteriormente e o SSM Agent processa recursos do Systems Manager, como Run Command e o State Manager.

É possível usar Run Command para atualizar suas instâncias existentes e usar a versão mais recente do serviço EC2Config e do SSM Agent. Para obter mais informações, consulte Atualizar o SSM Agent usando o Run Command no Manual do usuário do AWS Systems Manager.

Tarefas do EC2Config

O EC2Config executa tarefas de startup iniciais quando a instância é iniciada pela primeira vez; depois, as desabilita. Para executar novamente essas tarefas, é necessário explicitamente habilitá-las antes de fechar a instância ou executar manualmente o Sysprep. Essas tarefas são as seguintes:

- Defina uma senha aleatória e criptografada para a conta do administrador.
- Gerencie e instale o certificado do host usado para abrir a Conexão de Desktop Remoto.

- Estenda dinamicamente a partição do sistema operacional para incluir qualquer espaço não particionado.
- Execute os dados de usuário especificado (e Cloud-Init, se instalado). Para obter mais informações sobre como especificar os dados do usuário, consulte Executar comandos ao iniciar uma instância do EC2 com entrada de dados do usuário.

O EC2Config executa as tarefas a seguir sempre que a instância for iniciada:

- Altere o nome do host para corresponder ao endereço IP privado na notação Hex (essa tarefa está desabilitada por padrão e deverá ser ativada para execução no início da instância).
- Configure o servidor de gerenciamento de chaves (AWS KMS), verifique o status de ativação do Windows e ative o Windows, conforme necessário.
- Monte todos os volumes do Amazon EBS e volumes de armazenamento de instâncias e mapeie os nomes dos volumes para as letras de unidade.
- Grave entradas do log de eventos no console para ajudar a solucionar problemas (essa tarefa fica desabilitada por padrão e deve ser ativada para execução no início da instância).
- Escreva para o console que o Windows está pronto.
- Adicione uma rota personalizada para o adaptador de rede primária para habilitar os endereços IP a seguir quando uma única NIC ou várias NICs estiverem conectadas: `169.254.169.250`, `169.254.169.251` e `169.254.169.254`. Esses endereços são usados pelo Windows Activation e ao acessar metadados de instância.

> **Note**
>
> Se o sistema operacional Windows estiver configurado para usar IPv4, esses endereços locais de link IPv4 poderão ser usados. Se o sistema operacional Windows tiver a pilha de protocolos de rede IPv4 desabilitada e usar IPv6 em seu lugar, adicione `[fd00:ec2::250]` em vez de `169.254.169.250` e `169.254.169.251`. Depois, adicione `[fd00:ec2::254]` em vez de `169.254.169.254`.

O EC2Config executa a tarefa a seguir sempre que um usuário faz login:

- Exibe informações do papel de parede do segundo plano do desktop.

Enquanto a instância estiver sendo executada, é possível solicitar que o EC2Config execute a seguinte tarefa sob demanda:

- Execute Sysprep e feche a instância, de modo que você possa criar as AMIs a partir dela. Para obter mais informações, consulte Criar uma AMI do Amazon EC2 usando o Sysprep do Windows.

Arquivos de configurações do EC2Config

Os arquivos de configurações controlam a operação do serviço EC2Config. Esses arquivos estão localizados no diretório `C:\Program Files\Amazon\Ec2ConfigService\Settings`:

- `ActivationSettings.xml`—Controla a ativação do produto usando um servidor de gerenciamento de chaves (AWS KMS).
- `AWS.EC2.Windows.CloudWatch.json`: controla quais contadores de performance enviar ao CloudWatch e quais logs enviar ao CloudWatch Logs.
- `BundleConfig.xml`—Controla como o EC2Config prepara uma instância com armazenamento de instâncias para criação da AMI.
- `Config.xml`—Controla as configurações primárias.
- `DriveLetterConfig.xml`—Controla os mapeamentos da letra de unidade.
- `EventLogConfig.xml`—Controla as informações do log de eventos exibidas no console enquanto a instância está inicializando.
- `WallpaperSettings.xml`—Controla as informações exibidas na tela de fundo do desktop.

ActivationSettings.xml

Esse arquivo contém as configurações que controlam a ativação do produto. Quando o Windows inicializa, o serviço EC2Config verifica se o Windows já está ativado. Se o Windows ainda não estiver ativado, ele tentará ativar o Windows procurando pelo servidor AWS KMS específico.

- `SetAutodiscover` indica se é necessário detectar um AWS KMS automaticamente.
- `TargetKMSServer`—armazena o endereço IP privado de um AWS KMS. O AWS KMS deve estar na mesma região que a instância.
- `DiscoverFromZone` descobre o servidor AWS KMS da zona de DNS especificada.
- `ReadFromUserData` obtém o servidor AWS KMS de UserData.

- `LegacySearchZones` descobre o servidor AWS KMS da zona de DNS especificada.
- `DoActivate`—Tenta a ativação usando as configurações especificadas na seção. Esse valor pode ser `true` ou `false`.
- `LogResultToConsole`—Exibe o resultado para o console.

BundleConfig.xml

Este arquivo contém configurações que controlam como o EC2Config prepara uma instância para criação da AMI.

- `AutoSysprep`—Indica se o Sysprep deve ser usado automaticamente. Altere o valor para `Yes` para usar o Sysprep.
- `SetRDPCertificate`: define um certificado autoassinado para o servidor de Desktop Remoto. Isso permite que você use RDP com segurança nas instâncias. Altere o valor para `Yes` se as novas instâncias precisarem ter o certificado.

  Essa configuração não é usada para instâncias com versões do sistema operacional anteriores ao Windows Server 2016, pois estas podem gerar seus próprios certificados.
- `SetPasswordAfterSysprep`—Define uma senha aleatória em uma instância recém-executada, criptografa-a com a chave de execução do usuário e gera a senha criptografada no console. Altere o valor dessa configuração para `No` se as novas instâncias não forem definidas como uma senha criptografada aleatória.

Config.xml

Plugins

- `Ec2SetPassword`—Gera uma senha criptografada aleatória sempre que você executar uma instância. Esse recurso é desabilitado por padrão após a primeira execução, de forma que as reinicializações dessa instância não alterem uma senha definida pelo usuário. Altere essa configuração para `Enabled` para continuar a gerar senhas sempre que você executar uma instância.

  Essa configuração é importante se você estiver planejando criar um AMI a partir da sua instância.
- `Ec2SetComputerName`—Define o nome do host da instância para um nome exclusivo baseado no endereço IP da instância e reinicializa a instância. Ao configurar seu próprio nome de host ou impedir a modificação de um nome de host existente, é preciso desabilitar essa configuração.

- `Ec2InitializeDrives`—Inicializa e formata todos os volumes durante o startup. Esse recurso está habilitado por padrão.
- `Ec2EventLog`—Exibe entradas no log de eventos do console. Por padrão, são exibidas as três entradas de erro mais recentes do log de eventos do sistema. Para especificar as entradas no log de evento a serem exibidas, edite o arquivo `EventLogConfig.xml` localizado no diretório `EC2ConfigService\Settings`. Para obter informações sobre as configurações nesse arquivo, consulte Eventlog Key.
- `Ec2ConfigureRDP`—Define um certificado autoatribuído na instância, de forma que os usuários possam acessar com segurança a instância usando o Desktop Remoto. Essa configuração não é usada para instâncias com versões do sistema operacional anteriores ao Windows Server 2016, pois estas podem gerar seus próprios certificados.
- `Ec2OutputRDPCert`—Exibe informações do certificado de Desktop Remoto ao console, de forma que o usuário possa verificá-las contra o thumbprint.
- `Ec2SetDriveLetter`— Define as letras de unidade dos volumes montados com base em configurações definidas pelo usuário. Por padrão, quando um volume do Amazon EBS estiver associado a uma instância, ele poderá ser montado usando a letra de unidade na instância. Para especificar os mapeamentos da sua letra de unidade, edite o arquivo `DriveLetterConfig.xml` localizado no diretório `EC2ConfigService\Settings`.
- `Ec2WindowsActivate`— O plugin lida com ativação do Windows. Verifica para ver se o Windows está ativado. Caso contrário, atualiza as configurações do cliente AWS KMS e, então, ativa o Windows.

  Para modificar as configurações do AWS KMS, edite o arquivo `ActivationSettings.xml` localizado no diretório `EC2ConfigService\Settings`.
- `Ec2DynamicBootVolumeSize`—Estende o disco 0/Volume 0 para incluir qualquer espaço não particionado.
- `Ec2HandleUserData`—Cria e executa scripts criados pelo usuário na primeira execução de uma instância depois que o Sysprep for executado. Os comandos encapsulados nas tag do script são salvos em um arquivo em lote, e os comandos encapsulados nas tags do PowerShell são salvos em um arquivo .ps1 (corresponde à caixa de seleção Dados do usuário na caixa de diálogo Propriedades do serviço EC2 do sistema).
- `Ec2ElasticGpuSetup`—Instala o pacote de software para GPU elástica se a instância estiver associada a uma GPU elástica.

- `Ec2FeatureLogging`—Envia a instalação do recurso do Windows e o status do serviço correspondente ao console. Válido somente para o recurso Microsoft Hyper-V e o serviço vmms correspondente.

Configurações globais

- `ManageShutdown`: garante que instâncias iniciadas usando AMIs baseadas no Amazon S3 não sejam encerradas enquanto o Sysprep estiver em execução.
- `SetDnsSuffixList`—Define o sufixo DNS do adaptador de rede para Amazon EC2. Isso permite resolução do DNS dos servidores em execução no Amazon EC2 sem fornecer o nome de domínio totalmente qualificado.

> **Note**
>
> Isso adiciona uma pesquisa de sufixo DNS para o domínio apresentado a seguir e configura outros sufixos padrão. Para obter mais informações sobre como os agentes de inicialização definem os sufixos DNS, consulte Configurar o sufixo DNS para agentes de execução do EC2 Windows.
>
> ```
> region.ec2-utilities.amazonaws.com
> ```

- `WaitForMetaDataAvailable`—Assegura que o serviço EC2Config aguardará os metadados estarem acessíveis e redes estarem disponíveis antes de continuar com a inicialização. Essa verificação garante que o EC2Config possa obter informações dos metadados para ativação e outros plugins.
- `ShouldAddRoutes`—Adiciona uma rota personalizada para o adaptador de rede primária para habilitar os endereços IP a seguir quando múltiplos NICs estiverem associados: 169.254.169.250, 169.254.169.251 e 169.254.169.254. Esses endereços são usados pelo Windows Activation e ao acessar metadados de instância.
- `RemoveCredentialsfromSyspreponStartup`—Remove a senha do administrador de `Sysprep.xml` da próxima vez que o serviço iniciar. Para garantir que essa senha persista, edite essa configuração.

DriveLetterConfig.xml

Esse arquivo contém configurações que controlam os mapeamentos de letra da unidade. Por padrão, um volume pode ser mapeado para qualquer letra de unidade disponível. É possível montar um volume em uma letra de unidade específica, da seguinte forma.

```
<?xml version="1.0" standalone="yes"?>
<DriveLetterMapping>
  <Mapping>
    <VolumeName></VolumeName>
    <DriveLetter></DriveLetter>
  </Mapping>
  . . .
  <Mapping>
    <VolumeName></VolumeName>
    <DriveLetter></DriveLetter>
  </Mapping>
</DriveLetterMapping>
```

- `VolumeName`—A etiqueta de volume. Por exemplo, *`My Volume`*. Para especificar um mapeamento para um volume de armazenamento de instâncias, use a etiqueta `Temporary Storage X`, onde `X` é um número de 0 a 25.
- `DriveLetter`—A letra de unidade. Por exemplo, *`M:`*. O mapeamento falhará se a letra de unidade já estiver em uso.

EventLogConfig.xml

Este arquivo contém configurações que controlam as informações do log de eventos exibidas no console enquanto a instância estiver sendo inicializada. Por padrão, exibimos as três entradas de erro mais recentes do log de eventos do sistema.

- `Category`—A chave de log do evento a ser monitorada.
- `ErrorType`—O tipo de evento (por exemplo, `Error`, `Warning`, `Information`.)
- `NumEntries`—O número de eventos armazenados para essa categoria.
- `LastMessageTime`—Para impedir que a mesma mensagem seja enviada repetidamente, o serviço atualizará esse valor sempre que enviar uma mensagem.
- `AppName`: a origem do evento ou a aplicação que o registrou.

WallpaperSettings.xml

Esse arquivo contém as configurações que controlam as informações exibidas na tela de fundo do desktop. As informações a seguir são exibidas por padrão.

- `Hostname`—Exibe o nome do computador.
- `Instance ID`—Exibe o ID da instância.
- `Public IP Address`—Exibe o endereço IP público da instância.
- `Private IP Address`—Exibe o endereço IP privado da instância.
- `Availability Zone`—Exibe a zona de disponibilidade na qual a instância está em execução.
- `Instance Size`—Exibe o tipo de instância.
- `Architecture`: exibe a configuração da variável de ambiente `PROCESSOR_ARCHITECTURE`.

É possível remover qualquer informação exibida por padrão ao excluir essa entrada. É possível adicionar metadados de instância adicionais para exibir da forma a seguir.

```
<WallpaperInformation>
  <name>display_name</name>
  <source>metadata</source>
  <identifier>meta-data/path</identifier>
</WallpaperInformation>
```

É possível adicionar variáveis do ambiente do sistema para exibir da forma a seguir.

```
<WallpaperInformation>
  <name>display_name</name>
  <source>EnvironmentVariable</source>
  <identifier>variable-name</identifier>
</WallpaperInformation>
```

InitializeDrivesSettings.xml

Esse arquivo contém as configurações que controlam como o EC2Config inicializa as unidades.

Por padrão, o EC2Config inicializa as unidades que não foram trazidas online com o sistema operacional. É possível personalizar o plugin conforme a seguir.

```
<InitializeDrivesSettings>
```

```
    <SettingsGroup>setting</SettingsGroup>
</InitializeDrivesSettings>
```

Use um grupo de configurações para especificar como deseja inicializar as unidades:

FormatWithTRIM

Permite o comando TRIM ao formatar as unidades. Após uma unidade ser formatada e inicializada, o sistema restaurará a configuração de TRIM.

A partir do EC2Config versão 3.18, o comando TRIM é desativado durante a operação de formatação do disco, por padrão. Isso aprimora o tempo de formatação. Use essa configuração para permitir a TRIM durante a operação de formatação do disco para o EC2Config versão 3.18 e posterior.

FormatWithoutTRIM

Desabilita o comando TRIM ao formatar as unidades e melhorar o tempo de formatação no Windows. Após uma unidade ser formatada e inicializada, o sistema restaurará a configuração de TRIM.

DisableInitializeDrives

Desabilita a formatação de novas unidades. Use essa configuração para inicializar as unidades manualmente.

Instalar a versão mais recente do EC2Config

> **Note**
>
> O agente de inicialização mais recente do Windows Server 2022 e versões posteriores do sistema operacional é o EC2Launch v2, que substitui o EC2Config e o EC2Launch. O EC2Launch v2 vem pré-instalado nas AMIs Windows Server 2022 e 2025 da AWS. Você também instalar manualmente e configurar o agente no Windows Server 2016 e 2019. Para obter mais informações, consulte Instalar o EC2Launch v2.

Para obter informações sobre como receber notificações para atualizações do EC2Config, consulte Assinar as notificações do agente de execução do EC2 Windows. Para obter informações sobre alterações em cada versão, consulte Histórico de versões do EC2Config.

Antes de começar

- Verifique que você tem .NET framework 3.5 SP1 ou posterior.
- Por padrão, a configuração substitui os arquivos de configuração durante a instalação e reinicia o serviço EC2Config quando a instalação é concluída. Se você tiver alterado as configurações do serviço EC2Config, copie o arquivo `config.xml` do diretório `%Program Files%\Amazon \Ec2ConfigService\Settings`. Após atualizar o serviço EC2Config, será possível restaurar esse arquivo para reter as alterações nas configurações.

Verificar a versão do EC2Config

Use o procedimento a seguir para verificar a versão do EC2Config que está instalada em suas instâncias.

Para verificar a versão instalada do EC2Config

1. Execute uma instância pela AMI e conecte-se a ela.
2. No Painel de Controle, selecione Programas e Recursos.
3. Na lista de programas instalados, procure `Ec2ConfigService`. O número da versão aparece na coluna Versão.

Atualizar o EC2Config

Use o seguinte procedimento para fazer download e instalar a versão mais recente do EC2Config em suas instâncias.

Para fazer download e instalar a versão mais recente do EC2Config

1. Faça download e descompacte o instalador do EC2Config.
2. Execute `EC2Install.exe`. Para uma lista completa de opções, execute `EC2Install` com a opção `/?`. Por padrão, a configuração exibe os prompts. Para executar o comando sem prompts, use a opção `/quiet`.

> **Important**
>
> Para manter as configurações personalizadas do arquivo `config.xml` que você salvou, execute `EC2Install` com a opção `/norestart`, restaure as configurações e reinicie o serviço EC2Config manualmente.

3. Se você estiver executando o EC2Config versão 4.0 ou superior, reinicie o SSM Agent na instância do snap-in do Microsoft Services.

> **Note**
>
> As informações da versão atualizada do EC2Config não serão exibidas no log do sistema da instância ou na verificação do Trusted Advisor até que você reinicialize ou interrompa e inicie a instância.

Para baixar e instalar a versão mais recente do EC2Config usando o PowerShell

Para baixar, descompactar e instalar a versão mais recente do EC2Config usando o PowerShell, execute os seguintes comandos em uma janela do PowerShell:

```
$Url = "https://s3.amazonaws.com/ec2-downloads-windows/EC2Config/EC2Install.zip"
$DownloadZipFile = "$env:USERPROFILE\Desktop\" + $(Split-Path -Path $Url -Leaf)
$ExtractPath = "$env:USERPROFILE\Desktop\"
Invoke-WebRequest -Uri $Url -OutFile $DownloadZipFile
$ExtractShell = New-Object -ComObject Shell.Application
$ExtractFiles = $ExtractShell.Namespace($DownloadZipFile).Items()
$ExtractShell.NameSpace($ExtractPath).CopyHere($ExtractFiles)
Start-Process $ExtractPath
Start-Process `
    -FilePath $env:USERPROFILE\Desktop\EC2Install.exe `
    -ArgumentList "/S"
```

> **Note**
>
> Se você receber um erro ao baixar o arquivo e estiver usando o Windows Server 2016 ou anterior, talvez seja necessário habilitar o TLS 1.2 para seu terminal PowerShell. É possível habilitar o TLS 1.2 para a sessão atual do PowerShell com o comando a seguir e tentar novamente:

```
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
```

Verifique a instalação conferindo `C:\Program Files\Amazon\` para o diretório do `Ec2ConfigService`.

Configurar as definições do proxy .NET para o serviço EC2Config

É possível configurar o serviço EC2Config para se comunicar por meio de um proxy usando um dos seguintes métodos: AWS SDK for .NET, o elemento `system.net` as políticas de grupo da Microsoft e o Internet Explorer. O uso do AWS SDK para .NET é o método preferido, pois é possível especificar credenciais de login.

Métodos

- Configurar definições de proxy usando a opção AWS SDK for .NET (Preferencial)
- Definir as configurações de proxy usando o elemento system.net
- Definir as configurações de proxy usando as políticas do grupo Microsoft e o Internet Explorer

Configurar definições de proxy usando a opção AWS SDK for .NET (Preferencial)

É possível configurar as configurações de proxy para o serviço EC2Config ao especificar o elemento `proxy` no arquivo `Ec2Config.exe.config`. Para obter mais informações, consulte Referência de arquivos de configuração do AWS SDK for .NET.

Para especificar o elemento de proxy em Ec2Config.exe.config

1. Edite o arquivo `Ec2Config.exe.config` em uma instância onde deseja que o serviço EC2Config se comunica através de um proxy. Por padrão, o arquivo está localizado no seguinte diretório: `%ProgramFiles%\Amazon\Ec2ConfigService`.
2. Adicione o elemento `aws` a seguir para o `configSections`. Não adicione isso a nenhum existente `sectionGroups`.

   Para EC2Config versões 3.17 ou anteriores

   ```
   <configSections>
      <section name="aws" type="Amazon.AWSSection, AWSSDK"/>
   </configSections>
   ```

Para EC2Config versões 3.18 ou posteriores

```
<configSections>
     <section name="aws" type="Amazon.AWSSection, AWSSDK.Core"/>
</configSections>
```

3. Adicione o elemento `aws` a seguir ao arquivo `Ec2Config.exe.config`.

```
<aws>
   <proxy
     host="string value"
     port="string value"
     username="string value"
     password="string value" />
</aws>
```

4. Salve as alterações.

Definir as configurações de proxy usando o elemento system.net

É possível especificar as configurações de proxy em um elemento `system.net` no arquivo `Ec2Config.exe.config`. Para obter mais informações, consulte o elemento defaultProxy (configurações de rede).

Para especificar o elemento system.net em Ec2Config.exe.config

1. Edite o arquivo `Ec2Config.exe.config` em uma instância onde deseja que o serviço EC2Config se comunica através de um proxy. Por padrão, o arquivo está localizado no seguinte diretório: `%ProgramFiles%\Amazon\Ec2ConfigService`.
2. Adicione uma entrada `defaultProxy` a `system.net`. Para obter mais informações, consulte o elemento defaultProxy (configurações de rede).

   Por exemplo, a configuração a seguir roteia todo o tráfego para usar o proxy atualmente configurado para Internet Explorer, com exceção de metadados e tráfego de licenciamento, que contorneará o proxy.

```
<defaultProxy>
    <proxy usesystemdefault="true" />
    <bypasslist>
        <add address="169.254.169.250" />
```

```
        <add address="169.254.169.251" />
        <add address="169.254.169.254" />
        <add address="[fd00:ec2::250]" />
        <add address="[fd00:ec2::254]" />
    </bypasslist>
</defaultProxy>
```

3. Salve as alterações.

Definir as configurações de proxy usando as políticas do grupo Microsoft e o Internet Explorer

O serviço EC2Config é executado sob a conta do usuário do sistema local. É possível especificar configurações de proxy em toda a instância para essa conta no Internet Explorer depois de alterar as configurações de Política do Grupo na instância.

Para definir as configurações de proxy usando as políticas de grupo e o Internet Explorer

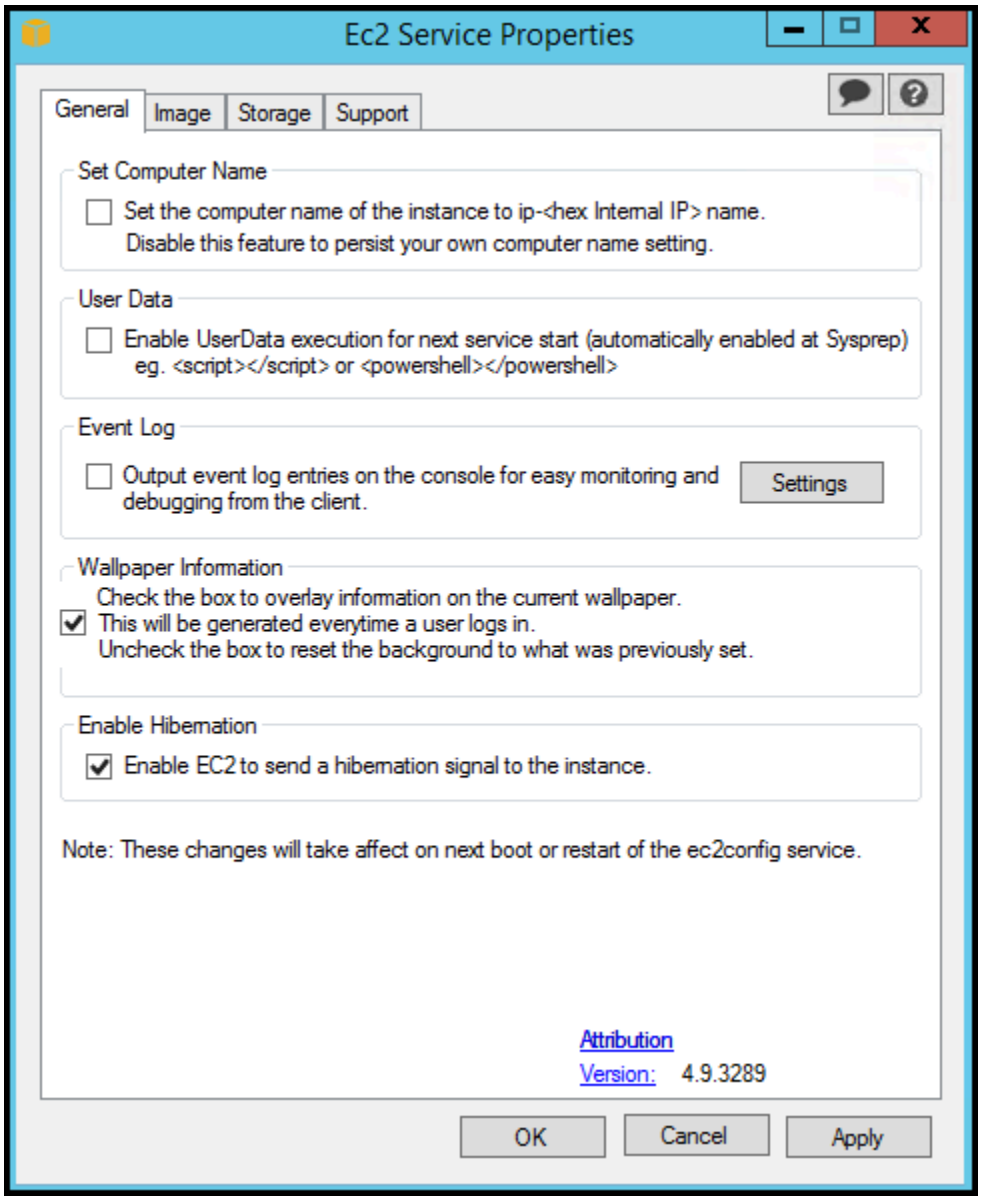
1. Em uma instância na qual você deseja que o serviço EC2Config se comunique por um proxy, abra um prompt de comando como administrador, digite **`gpedit.msc`** e pressione Enter.
2. No editor de políticas do grupo local, em Política do computador local, escolha Configuração do computador, Modelos administrativos, Componentes do Windows, Internet Explorer.
3. No painel à direita, escolha Definir as configurações de proxy por máquina (não por usuário) e, em seguida, Editar configuração da política.
4. Selecione Habilitado e, em seguida, selecione Aplicar.
5. Abra o Internet Explorer e selecione o botão Ferramentas.
6. Escolha Opção de Internet e escolha a guia Conexões.
7. Escolha Configurações da LAN.
8. Em Servidor proxy, escolha a opção Usar um Servidor Proxy para LAN.
9. Especifique as informações de endereço e porta e selecione OK.

Definir as propriedades do serviço EC2Config na caixa de diálogo do sistema na instância EC2 Windows

O procedimento a seguir descreve como usar a caixa de diálogo Propriedades do serviço do EC2 do sistema para habilitar ou desabilitar configurações.

1. Execute e conecte-se à sua instância do Windows.

2. No menu Iniciar, clique em Todos os programas e escolha Configurações do EC2ConfigService.



3. Na guia Geral da caixa de diálogo Propriedades do serviço do EC2 do sistema, você pode habilitar ou desabilitar as configurações a seguir.

   Definir o nome do computador

   Se essa configuração estiver habilitada (está desabilitada por padrão), o nome do host será comparado ao endereço IP interno atual a cada inicialização; se o nome de host e o endereço IP interno não corresponderem, o nome do host será redefinido para conter o endereço IP interno, e o sistema reiniciará para pegar o novo nome de host. Ao configurar seu próprio nome de host ou para impedir a modificação de um nome de host existente, não habilite essa configuração.

Dados do usuário

A execução de dados do usuário permite especificar scripts nos metadados da instância. Por padrão, esses scripts são executados durante a execução inicial. Também é possível configurá-los para que sejam executados na próxima vez que você reiniciar ou iniciar a instância, ou sempre que fizer esse procedimento.

Se você tem um script grande, recomendamos usar dados do usuário para fazer download do script e, em seguida, executá-lo.

Para obter mais informações, consulte Execução de dados do usuário.

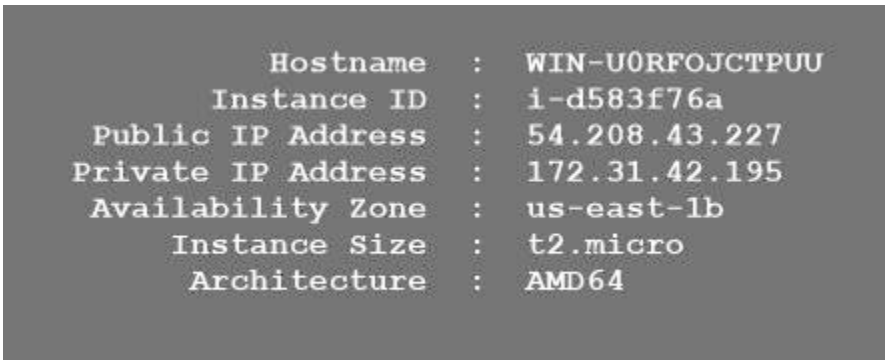
Log de eventos

Use essa configuração para exibir entradas de log de eventos no console durante a inicialização para facilitar o monitoramento e a depuração.

Clique em Configurações para especificar filtros para as entradas do log enviadas ao console. O filtro padrão enviar as três entradas de erros mais recentes do log de eventos do sistema ao console.

Informações sobre o papel de parede

Use essa configuração para exibir informações do sistema no segundo plano do desktop. A seguir está um exemplo das informações exibidas na tela de fundo do desktop.

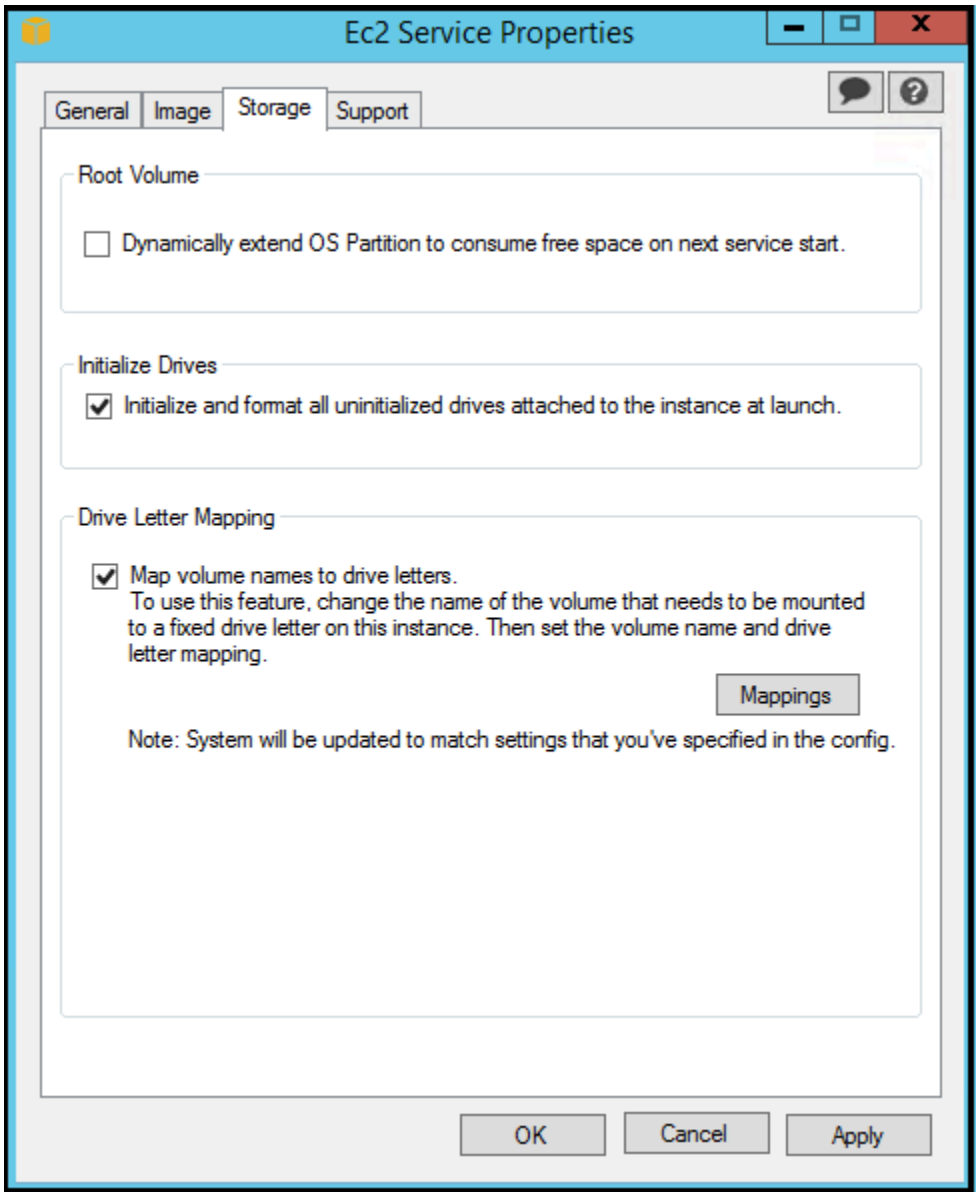


As informações exibidas em segundo plano no desktop são controladas pelo arquivo de configurações `EC2ConfigService\Settings\WallpaperSettings.xml`.

Enable Hibernation (Habilitar a hibernação

Use essa configuração para permitir que o EC2 sinalize ao sistema operacional para executar a hibernação.

4. Clique na guia Armazenamento. É possível habilitar ou desabilitar as configurações a seguir.



Volume do dispositivo raiz

Essa configuração amplia dinamicamente o Disco 0/Volume 0 para incluir qualquer espaço não particionado. Isto pode ser útil quando a instância é inicializada usando um volume raiz com tamanho personalizado.

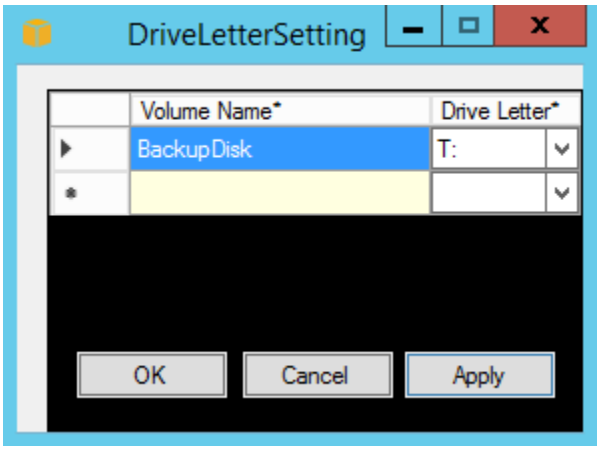
Inicializar unidades

Essa configuração formata e monta todos os volumes associados à instância durante a inicialização.

Mapeamento da letra da unidade

O sistema mapeia os volumes associados a uma instância para as letras de unidade. Para volumes do Amazon EBS, o padrão é atribuir letras de unidade que vão de D: a Z:. Para volumes de armazenamento de instâncias, o padrão depende do driver . AWS Os drivers PV e Citrix PV atribuem aos volumes de armazenamento de instância letras que vão de Z: a A: Os drivers do Red Hat atribuem aos volumes de armazenamento da instância letras de unidades que vão de D: a Z:.

Para selecionar as letras de unidade para seus volumes, clique em Mapeamentos. Na caixa de diálogo DriveLetterSetting, especifique os valores de Volume Name (Nome do volume) e Drive Letter (Letra da unidade) para cada volume e clique em Apply (Aplicar) e, em seguida, OK. Recomendamos que você selecione letras de unidade que evitem conflitos com as letras de unidade que provavelmente estão em uso, como as do meio do alfabeto.



Após especificar um mapeamento de letra de unidade e associar um volume com o mesmo rótulo que um dos nomes de volume especificado, o EC2Config atribui automaticamente sua letra especificada para esse volume. Contudo, o mapeamento da letra de unidade falhará se a letra já estiver em uso. Observe que EC2Config não altera as letras de unidade dos volumes já montados ao especificar o mapeamento da letra de unidade.

5. Para salvar suas configurações e continuar trabalhando nelas depois, clique em OK para fechar a caixa de diálogo Propriedades do serviço do EC2 do sistema. Se você tiver concluído a personalização da sua instância e quiser criar uma AMI com base nessa instância, consulte Criar uma AMI do Amazon EC2 usando o Sysprep do Windows.

Solucionar problemas com o agente de execução do EC2Config

As informações a seguir podem ajudá-lo a resolver problemas com o serviço EC2Config.

Atualizar o EC2Config em uma instância inacessível

Use o procedimento a seguir para atualizar o serviço EC2Config em uma instância do Windows Server inacessível usando o Desktop Remoto.

Para atualizar o EC2Config em um a instância do Windows baseada no Amazon EBS à qual você não pode se conectar

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Localize a instância afetada. Selecione a instância e escolha Instance state (Estado da instância) e, em seguida, escolha Stop instance (Interromper instância).

   > **Warning**
   >
   > Quando você interrompe uma instância, os dados em todos os volumes de armazenamento de instâncias são apagados. Para manter dados longe dos volumes de armazenamento de instância, faça backup no armazenamento persistente.

4. Escolha Launch instances (Executar instância) e crie uma instância `t2.micro` temporária na mesma zona de disponibilidade que a instância afetada. Use uma AMI diferente da que você usou para executar a instância afetada.

   > **Important**
   >
   > Se você não criar a instância na mesma zona de disponibilidade que a instância afetada, não conseguirá associar o volume do dispositivo raiz da instância afetada à nova instância.

5. No console do EC2, selecione Volumes.
6. Localize o volume do dispositivo raiz da instância afetada. Desanexe o volume e anexe o volume à instância temporária criada anteriormente. Associe-a com o nome do padrão do dispositivo (xvdf).
7. Use o Desktop Remoto para se conectar à instância temporária e use em utilitário Gerenciamento de Disco para disponibilizar o volume para uso.
8. Faça download da versão mais recente do serviço EC2Config. Extraia arquivos do arquivo `.zip` para o diretório `Temp` na unidade que você associou.

9. Na instância temporária, abra a caixa de diálogo Run (Executar), digite **`regedit`** e pressione Enter.
10. Escolha `HKEY_LOCAL_MACHINE`. No menu Arquivo, escolha Carregar Hive. Escolha a unidade, vá até ele e abra o seguinte arquivo: `Windows\System32\config\SOFTWARE`. Quando solicitado, especifique o nome da chave.
11. Selecione a chave que você acabou de carregar e vá até `Microsoft\Windows \CurrentVersion`. Escolha a chave `RunOnce`. Se essa chave não existir, escolha `CurrentVersion` no menu contextual (clique com o botão direito do mouse), escolha Novo e selecione Chave. Nomeie a chave `RunOnce`.
12. No menu contextual (clique com o botão direito do mouse), escolha a chave `RunOnce`, escolha Novo e escolha no Valor da string. Insira `Ec2Install` como o nome e `C:\Temp \Ec2Install.exe /quiet` como dados.
13. Escolha a chave `HKEY_LOCAL_MACHINE\`*`specified key name`*`\Microsoft\Windows NT \CurrentVersion\Winlogon`. No menu contextual (clique com o botão direito do mouse), escolha Novo e selecione Valor da string. Insira **`AutoAdminLogon`** como o nome e **`1`** como dados.
14. Escolha a chave `HKEY_LOCAL_MACHINE\`*`specified key name`*`\Microsoft\Windows NT\CurrentVersion\Winlogon`>. No menu contextual (clique com o botão direito do mouse), escolha Novo e selecione Valor da string. Insira **`DefaultUserName`** como o nome e **`Administrator`** como dados.
15. Escolha a chave `HKEY_LOCAL_MACHINE\`*`specified key name`*`\Microsoft\Windows NT \CurrentVersion\Winlogon`. No menu contextual (clique com o botão direito do mouse), escolha Novo e selecione Valor da string. Digite **`DefaultPassword`** como nome e digite uma senha nos dados de valor.
16. No painel de navegação do Editor de Registro, escolha a chave temporária que você criou quando abriu pela primeira vez o Editor de Registro.
17. No menu Arquivo, escolha Descarregar Hive.
18. No utilitário Gerenciamento de Disco, escolha o disco que você anexou anteriormente, abra o menu de contexto (botão direito do mouse) e escolha Offline.
19. No console do Amazon EC2, separe o volume afetado da instância temporária e reanexe-o à instância original com o nome de dispositivo `/dev/sda1`. Especifique o nome desse dispositivo para designar o volume como volume do dispositivo raiz.
20. Início e interrupção de instâncias do Amazon EC2 a instância.

21. Depois que a instância for iniciada, verifique o log do sistema e veja se a mensagem Windows is ready to use aparece.
22. Abra o Editor de Registro e escolha `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon`. Exclua as chaves de valor da string criada anteriormente: AutoAdminLogon, DefaultUserName e DefaultPassword.
23. Exclua ou interrompa a instância temporária que você criou nesse procedimento.

Histórico de versões do EC2Config

A tabela a seguir descreve as versões liberadas do EC2Config. Para obter informações sobre as atualizações do SSM Agent, consulte Notas de release do Systems Manager SSM Agent.

> **Important**
>
> O EC2Config atingiu o fim do suporte. Somente a versão mais recente do agente do EC2Config está disponível para download. As versões anteriores estão marcadas como privadas.

Versão	Detalhes	Data de lançamento
4.9.5777	• Corrigido o problema em que a configuração de RSS era definida incorretamente para alguns tipos de instância. • Nova versão do SSM Agent `3.3.484.0` .	17 de junho de 2024
4.9.5554	• Limitação da devolução de nomes de domínio com base na entrada do registro: `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Dnscache\Parameters\DomainNameDevolutionLevel` . • Nova versão do SSM Agent `3.2.1630.0` .	4 de outubro de 2023
4.9.5467	•	1º de agosto de 2023

Versão	Detalhes	Data de lançamento
	Adicionado o recurso de repetição de tentativas para descobrir a porta do console. • Nova versão do SSM Agent `3.1.2282.0` .	
4.9.5288	• O AWS Core SDK foi atualizado para a versão `3.7.103.23` . • Corrigido problema em que o documento SSM `AWS-UpdateEC2Config` falhava ao atualizar `EC2Config` em instâncias habilitadas somente com o IMDSv2. • Nova versão do SSM Agent `3.1.2144.0` .	8 de março de 2023
4.9.5231	• Nova versão do SSM Agent 3.1.1927.0.	14 de fevereiro de 2023
4.9.5103	• Corrigido um problema em que volumes efêmeros eram identificados incorretamente nas famílias de instâncias r5d e i4i. • Nova versão do SSM Agent 3.1.1856.0.	5 de dezembro de 2022
4.9.5064	• Atualizado para usar de informações do segmento PCI para selecionar a porta do console. • Assinados scripts do PowerShell e adicionados cabeçalhos de direitos autorais. • Corrigida a lógica da seleção do adaptador da rede primária. • Nova versão do SSM Agent 3.1.1732.0.	16 de novembro de 2022

Versão	Detalhes	Data de lançamento
4.9.4588	• Atualizada a lógica de espera IMDS para fazer somente solicitações IMDSv2. • Adicionada a biblioteca compartilhada do agente de inicializ ação libec2launch.dll. • Nova versão do SSM Agent 3.1.1188.0.	31 de maio de 2022
4.9.4556	• Adicionada lógica de espera para garantir a inicialização completa da NIC antes do uso. • A nova versão do Log4Net 2.0.14.0 inclui o patch de segurança. • A nova versão do SSM Agent 3.1.1045.0 inclui o patch de segurança.	1º de março de 2022
4.9.4536	• Corrigido um problema em que os dados do usuário falham quando a pasta Temp está ausente. • Nova versão do SSM Agent 3.1.804.0.	31 de janeiro de 2022
4.9.4508	• Correção do problema para calcular corretamente o caminho do script diskpart. • Nova versão do SSM Agent 3.1.338.0.	6 de outubro de 2021
4.9.4500	• `Install-EgpuManagerConfig` atualizado com suporte a IMDS v2. • Links atualizados para usar https. • Nova versão do SSM Agent 3.1.282.0	7 de setembro de 2021

Versão	Detalhes	Data de lançamento
4.9.4419	• Lógica de fallback de versão 1 IMDS corrigida. • Atualizado todo o uso do diretório temporário do Windows para o diretório temporário do EC2Config • Nova versão do SSM Agent 3.0.1124.0	2 de junho de 2021
4.9.4381	• Adicionado suporte para o esquema de documentos SSM versão 2.2 no EC2ConfigUpdater • Incluída a versão do pacote do AWS Nitro Enclaves no log do console • Nova versão do SSM Agent 3.0.529.0	4 de maio de 2021
4.9.4326	• Todos os links na interface do usuário de configurações foram removidos • Esta é a última versão do EC2Config que oferece suporte ao Windows Server 2008.	3 de março de 2021
4.9.4279	• Corrigido problema de segurança relacionado à tarefa `Ec2ConfigMonitor` agendada • Corrigido problema de mapeamento de letras de unidade fixa e contagem de disco temporário incorreta • Adicionados`OsCurrentBuild` e `OsReleaseId` à saída do console. • Nova versão do SSM Agent 2.3.871.0	11 de dezembro de 2020
4.9.4222	• Lógica de fallback de versão 1 IMDS corrigida. • Nova versão do SSM Agent 2.3.842.0	7 de abril de 2020
4.9.4122	• Suporte adicionado para IMDS v2 • Nova versão do SSM Agent 2.3.814.0	4 de março de 2020

Versão	Detalhes	Data de lançamento
4.9.3865	• Correção de um problema que detecta a porta COM para Windows Server 2008 R2 em instâncias metal • Nova versão do SSM Agent 2.3.722.0	31 de outubro de 2019
4.9.3519	• Nova versão do SSM Agent 2.3.634.0	18 de junho de 2019
4.9.3429	• Nova versão do SSM Agent 2.3.542.0	25 de abril de 2019
4.9.3289	• Nova versão do SSM Agent 2.3.444.0	11 de fevereiro de 2019
4.9.3270	• Plugin adicionado a fim de configurar o monitor para nunca desligar ao corrigir problemas de ACPI • Edição e versão do SQL Server gravadas no console • Nova versão do SSM Agent 2.3.415.0	22 de janeiro de 2019
4.9.3230	• A descrição do Mapeamento da letra da unidade foi atualizad a para se alinhar melhor à funcionalidade. • Nova versão do SSM Agent 2.3.372.0	10 de janeiro de 2019
4.9.3160	• Aumentado o tempo de espera para NIC primário • Adição de configuração padrão para RSS e configurações de fila de recebimento para dispositivos ENA • Hibernação desabilitada durante Sysprep • Nova versão do SSM Agent 2.3.344.0 • AWS SDK atualizado para 3.3.29.13	15 de dezembro de 2018
4.9.3067	• Melhorias feitas na hibernação de instâncias • Nova versão do SSM Agent 2.3.235.0	8 de novembro de 2018

Versão	Detalhes	Data de lançamento
4.9.3034	• Adição da rota 169.254.169.253/32 para servidor DNS • Nova versão do SSM Agent 2.3.193.0	24 de outubro de 2018
4.9.2986	• Adição de assinatura para todos os binários relacionados ao EC2Config • Nova versão do SSM Agent 2.3.136.0	11 de outubro de 2018
4.9.2953	Nova versão do SSM Agent (2.3.117.0)	2 de outubro de 2018
4.9.2926	Nova versão do SSM Agent (2.3.68.0)	18 de setembro de 2018
4.9.2905	• Nova versão do SSM Agent (2.3.50.0) • Rota 169.254.169.123/32 adicionada ao serviço de horário do AMZN • Rota 169.254.169.249/32 adicionada ao serviço de licença do GRID • Corrigido um problema que fazia com que os volumes do EBS NVMe fossem marcados como efêmeros	17 de setembro de 2018
4.9.2854	Nova versão do SSM Agent (2.3.13.0)	17 de agosto de 2018
4.9.2831	Nova versão do SSM Agent (2.2.916.0)	7 de agosto de 2018
4.9.2818	Nova versão do SSM Agent (2.2.902.0)	31 de julho de 2018
4.9.2756	Nova versão do SSM Agent (2.2.800.0)	27 de junho de 2018

Versão	Detalhes	Data de lançamento
4.9.2688	Nova versão do SSM Agent (2.2.607.0)	25 de maio de 2018
4.9.2660	Nova versão do SSM Agent (2.2.546.0)	11 de maio de 2018
4.9.2644	Nova versão do SSM Agent (2.2.493.0)	26 de abril de 2018
4.9.2586	Nova versão do SSM Agent (2.2.392.0)	28 de março de 2018
4.9.2565	• Nova versão do SSM Agent (2.2.355.0) • Foi corrigido um problema nas instâncias M5 e C5 (não conseguem encontrar os drivers PV) • Adicionado o registro em log no console para tipo de instância , drivers PV mais recentes e drivers NVMe	13 de março de 2018
4.9.2549	Nova versão do SSM Agent (2.2.325.0)	8 de março de 2018
4.9.2461	Nova versão do SSM Agent (2.2.257.0)	15 de fevereiro de 2018
4.9.2439	Nova versão do SSM Agent (2.2.191.0)	6 de fevereiro de 2018
4.9.2400	Nova versão do SSM Agent (2.2.160.0)	16 de janeiro de 2018

Versão	Detalhes	Data de lançamento
4.9.2327	• Nova versão do SSM Agent (2.2.120.0) • Descoberta de porta COM adicionada em instâncias bare metal do Amazon EC2 • Registro em log de status Hyper-V adicionado em instâncias bare metal do Amazon EC2	2 de janeiro de 2018
4.9.2294	Nova versão do SSM Agent (2.2.103.0)	4 de dezembro de 2017
4.9.2262	Nova versão do SSM Agent (2.2.93.0)	15 de novembro de 2017
4.9.2246	Nova versão do SSM Agent (2.2.82.0)	11 de novembro de 2017
4.9.2218	Nova versão do SSM Agent (2.2.64.0)	29 de outubro de 2017
4.9.2212	Nova versão do SSM Agent (2.2.58.0)	23 de outubro de 2017
4.9.2203	Nova versão do SSM Agent (2.2.45.0)	19 de outubro de 2017
4.9.2188	Nova versão do SSM Agent (2.2.30.0)	10 de outubro de 2017
4.9.2180	• Nova versão do SSM Agent (2.2.24.0) • Plugin de GPU elástica adicionado a instâncias de GPU	5 de outubro de 2017

Versão	Detalhes	Data de lançamento
4.9.2143	Nova versão do SSM Agent (2.2.16.0)	1º de outubro de 2017
4.9.2140	Nova versão do SSM Agent (2.1.10.0)	
4.9.2130	Nova versão do SSM Agent (2.1.4.0)	
4.9.2106	Nova versão do SSM Agent (2.0.952.0)	
4.9.2061	Nova versão do SSM Agent (2.0.922.0)	
4.9.2047	Nova versão do SSM Agent (2.0.913.0)	
4.9.2031	Nova versão do SSM Agent (2.0.902.0)	
4.9.2016	• Nova versão do SSM Agent (2.0.879.0) • Caminho do diretório do CloudWatch Logs corrigido para o Windows Server 2003	
4.9.1981	• Nova versão do SSM Agent (2.0.847.0) • Corrigido o problema com `important.txt` sendo gerado em volumes do EBS.	
4.9.1964	Nova versão do SSM Agent (2.0.842.0)	
4.9.1951	• Nova versão do SSM Agent (2.0.834.0) • Corrigido o problema com letra de unidade não mapeada de Z: para discos temporários.	

Versão	Detalhes	Data de lançamento
4.9.1925	• Nova versão do SSM Agent (2.0.822.0) • [Bug] Essa versão não é um destino de atualização válido do SSM Agent v4.9.1775.	
4.9.1900	Nova versão do SSM Agent (2.0.805.0)	
4.9.1876	• Nova versão do SSM Agent (2.0.796.0) • Corrigido um problema com redirecionamento de saída/erro para execução de userdata do administrador.	
4.9.1863	• Nova versão do SSM Agent (2.0.790.0) • Corrigidos problemas com a conexão de vários volumes do EBS a uma instância do Amazon EC2. • Melhorado o CloudWatch para pegar um caminho de configuração, mantendo a retrocompatibilidade.	
4.9.1791	Nova versão do SSM Agent (2.0.767.0)	
4.9.1775	Nova versão do SSM Agent (2.0.761.0)	
4.9.1752	Nova versão do SSM Agent (2.0.755.0)	
4.9.1711	Nova versão do SSM Agent (2.0.730.0)	
4.8.1676	Nova versão do SSM Agent (2.0.716.0)	
4.7.1631	Nova versão do SSM Agent (2.0.682.0)	

Versão	Detalhes	Data de lançamento
4.6.1579	• Nova versão do SSM Agent (2.0.672.0) • Corrigido problema de atualização do agente com v4.3, v4.4 e v4.5	
4.5.1534	Nova versão do SSM Agent (2.0.645.1)	
4.4.1503	Nova versão do SSM Agent (2.0.633.0)	
4.3.1472	Nova versão do SSM Agent (2.0.617.1)	
4.2.1442	Nova versão do SSM Agent (2.0.599.0)	
4.1.1378	Nova versão do SSM Agent (2.0.558.0)	

Versão	Detalhes	Data de lançamento
4.0.1343	• O Run Command, o State Manager, o agente do CloudWatch e o suporte à união de domínios foram transferidos para outro agente, chamado SSM Agent. O SSM Agent será instalado como parte do upgrade do EC2Config. Para obter mais informações, consulte EC2Config e AWS Systems Manager. • Se você tiver um proxy configurado no EC2Config, precisará atualizar suas configurações de proxy para o SSM Agent antes de fazer o upgrade. Se você não atualizar as configura ções do proxy, não poderá usar o comando Executar para gerenciar suas instâncias. Para evitar isso, consulte as informações a seguir antes de atualizar para a versão mais recente: Instalação e configuração do SSM Agent em instâncias do Windows no Guia do usuário do AWS Systems Manager. • Se você tiver previamente habilitado a integração com o CloudWatch nas suas instâncias usando um arquivo de configuração local (`AWS.EC2.Windows.CloudWatch.json`), precisará configurar o arquivo para trabalhar com o SSM Agent.	
3.19.1153	• Reativado o plugin de ativação para instâncias com a configuração antiga do AWS KMS. Ignore a ativação para usuários BYOL. • Altere o comportamento padrão do TRIM para estar desabilit ado durante a operação de formatação do disco e adicione FormatWithTRIM para sobrescrever o plugin InitializeDisks com userdata.	

Versão	Detalhes	Data de lançamento
3.18.1118	• Correção para adicionar rotas com confiança ao adaptador de rede primário. • Atualizações para melhorar o suporte aos serviços da AWS.	
3.17.1032	• As correções duplicam os logs do sistema que aparecem quando os filtros são colocados na mesma categoria. • Correções para evitar suspensão durante a inicialização do disco.	
3.16.930	Adicionado suporte ao evento no log "A janela está pronta para usar" ao log do evento no Windows no início.	
3.15.880	Correção para permitir upload da saída do Systems Manager Run Command para nomes do bucket S3 com o caractere ".".	
3.14.786	Adicionado suporte para sobrescrever as configurações de plugin de InitializeDisks. Por exemplo: Para acelerar a inicializ ação do disco SSD, é possível temporariamente desabilitar o TRIM ao especificar o seguinte em userdata: <InitializeDrivesSettings><SettingsGroup>FormatWithoutTRIM</SettingsGroup></InitializeDrivesSettings	
3.13.727	Systems Manager Run Command – Correções dos comandos do processo com confiança após reinicialização do Windows.	

Versão	Detalhes	Data de lançamento
3.12.649	• Correção para lidar tranquilamente com a reinicialização ao executar comandos/scripts. • Correção para cancelar com confiança os comandos de execução. • Adicione suporte para carregar (opcionalmente) logs de MSI no S3 ao instalar aplicações via Systems Manager Run Command.	
3.11.521	• Correções para permitir a geração de thumbprint de RDP para Windows Server 2003. • Correções para incluir o fuso horário e a compensação do UTC nas linhas de log do EC2Config. • Suporte a Systems Manager para executar comandos do Run Command em paralelo. • Retornar à alteração anterior para colocar discos particion ados online.	
3.10.442	• Corrigir falhas de configuração do Systems Manager ao instalar aplicações MSI. • Correção para colocar discos de armazenamento online com confiança. • Atualizações para melhorar o suporte aos serviços da AWS.	

Versão	Detalhes	Data de lançamento
3.9.359	• Correção no script pós-Sysprep para deixar a configuração do Windows atualizar em um estado padrão. • Correção do plugin de geração de senha para melhorar a confiabilidade ao obter as configurações da política de senha do GPO. • Restrição às permissões da pasta do log de EC2Config/SSM ao grupo Administradores local. • Atualizações para melhorar o suporte aos serviços da AWS.	
3.8.294	• Corrigido um problema com o CloudWatch que impedia os logs de serem atualizados quando não estivessem na unidade primária. • Melhorado o processo de inicialização de disco ao adicionar a lógica de repetição. • Adicionada manipulação de erro melhorada quando o plugin SetPassword falhava ocasionalmente durante a criação de AMI. • Atualizações para melhorar o suporte aos serviços da AWS.	

Versão	Detalhes	Data de lançamento
3.7.308	• Melhorias ao utilitário ec2config-cli para testes de config e a solução de problemas na instância. • Evite adicionar rotas estáticas ao serviço de metadados do AWS KMS em um adaptador OpenVPN. • Corrigido um problema no qual a execução de dados do usuário não estava honrando a tag "persist". • A manipulação de erro melhorada ao fazer login no console do EC2 não está disponível. • Atualizações para melhorar o suporte aos serviços da AWS.	
3.6.269	• Correção de confiabilidade da ativação do Windows para usar primeiro o endereço local do link 169.254.0.250/251 para ativar o Windows via AWS KMS • Manuseio do proxy aprimorado para cenários de Systems Manager, Windows Activation e Domain Join • Corrigido um problema em que linhas duplicadas de contas de usuário eram adicionadas ao arquivo de resposta do Sysprep	
3.5.228	• Resolvido um cenário em que o plugin do CloudWatch poderia consumir em excesso CPU e memória ao ler os logs de evento do Windows • Adicionado um link para a documentação de configuração do CloudWatch na UI de configurações do EC2Config	

Versão	Detalhes	Data de lançamento
3.4.212	• Correções do EC2Config quando usadas em combinação com o VM Import. • Corrigido o problema de nomeação do serviço no instalador do WiX.	
3.3.174	• Melhorada a manipulação de exceção para Systems Manager e falhas de junção de domínio. • Alteração para dar suporte ao versionamento do esquema do Systems Manager SSM. • Corrigida a formação de discos temporários em Win2K3. • Alteração para suporte do tamanho do disco de configuração maior que 2TB. • Uso reduzido de memória virtual ao definir o modo GC para padrão. • Suporte para baixar artefatos do caminho UNC nos plugins `aws:psModule` e `aws:application` . • Melhora no registro em log do plugin de ativação do Windows.	

Versão	Detalhes	Data de lançamento
3.2.97	• Melhorias de performance ao atrasar o carregamento de montagens do Systems Manager SSM. • Melhora na manipulação de exceção para sysprep2008.xml malformado. • Suporte à linha de comando para a configuração "Apply (Aplicar)" do Systems Manager. • Alteração para suporte de união do domínio quando houver uma renomeação de computador pendente. • Suporte para parâmetros opcionais no plugin `aws:applications` . • Suporte para o array de comando no plugin `aws:psModule` .	
3.0.54	• Habilitar suporte para Systems Manager. • O domínio integra automaticamente as instâncias do EC2 do Windows a um diretório da AWS via Systems Manager. • Configure e carregue logs/métricas do CloudWatch via Systems Manager. • Instale os módulos do PowerShell via Systems Manager. • Instale as aplicações de MSI via Systems Manager.	

Versão	Detalhes	Data de lançamento
2.4.233	• Adicionada uma tarefa programada para recuperar o EC2Config de falhas no startup do serviço. • Melhorias nas mensagens de erro do log do Console. • Atualizações para melhorar o suporte aos serviços da AWS.	
2.3.313	• Corrigido o problema do grande consumo de memória em alguns casos quando o recurso CloudWatch Logs estiver habilitado. • Corrigido um bug no upgrade, de forma que versões do EC2Config anteriores à 2.1.19 agora podem atualizar para a mais recente. • Atualizada a exceção de abertura de porta COM para ser mais amigável e útil em logs. • A UI do Ec2configServiceSettings desabilitou o redimensi onamento e corrigiu a atribuição e o posicionamento de exibição da versão na UI.	
2.2.12	• NullPointerException processado ao consultar uma chave do registro para determinar o estado do Windows Sysprep que retorna nulo ocasionalmente. • Liberados recursos não gerenciados no bloco final.	
2.2.11	Corrigido um problema no plugin do CloudWatch para lidar com linhas vazias do log.	

Versão	Detalhes	Data de lançamento
2.2.10	• Removidas a configuração dos ajustes dos CloudWatch Logs por meio de UI. • Permitir que os usuários definam configurações do CloudWatch Logs no arquivo `%ProgramFiles%\Amazon\Ec2ConfigService\Settings\AWS.EC2.Windows.CloudWatch.json` para permitir melhorias futuras.	
2.2.9	Corrigida a exceção não gerenciada e adicionado registro em log.	
2.2.8	• Corrige verificação da versão do SO do Windows no instalador do EC2Config para dar suporte ao Windows Server 2003 SP1 e posterior. • Corrige o manuseio do valor nulo ao ler as chaves de registro relacionadas à atualização dos arquivos de config do Sysprep.	
2.2.7	• Adicionado suporte para o EC2Config executar durante a execução do Sysprep para Windows 2008 e posterior. • Manipulação de exceções aperfeiçoada e registro em log para melhores diagnósticos	
2.2.6	• Reduzida a carga na instância e no CloudWatch Logs ao carregar os eventos de log. • Resolvido um problema de upgrade, no qual o plugin do CloudWatch Logs nem sempre ficava habilitado	

Versão	Detalhes	Data de lançamento
2.2.5	• Adicionado suporte ao carregamento de logs para o CloudWatch Log Service. • Corrigido um problema de condição de raça no plugin Ec2OutputRDPCert • Alterada a opção de recuperação do serviço EC2Config para reiniciar a partir de TakeNoAction • Adicionada mais informações de exceção quando o EC2Config dá erro	
2.2.4	• Corrigido um erro em PostSysprep.cmd • Corrigido o bug em que o EC2Config não se fixa no menu Iniciar para OS2012+	

Versão	Detalhes	Data de lançamento
2.2.3	• Adicionada opção de instalar o EC2Config sem que o serviço comece imediatamente após a instalação. Para usar, execute 'Ec2Install.exe start=false' pelo prompt de comando • Adicionado parâmetro no plugin do papel de parede para controlar a adição/remoção do papel de parede. Para usar, execute "Ec2WallpaperInfo.exe set" ou "Ec2WallpaperInfo.exe revert" no prompt de comando • Adicionada verificação da chave RealTimeIsUniversal, configurações incorretas de saída da chave de registro de RealTimeIsUniveral para o console • Removida dependência do EC2Config na pasta de temporári os do Windows • Removida dependência de execução de UserData no .Net 3.5	
2.2.2	• Adicionada a verificação para comportamento de parada de serviço para verificar se os recursos estão sendo liberados • Corrigido o problema com longos períodos de execução ao ingressar no domínio	

Versão	Detalhes	Data de lançamento
2.2.1	• Atualizado o instalador para permitir upgrades de versões mais antigas • Corrigido o bug Ec2WallpaperInfo no ambiente exclusivo do .Net4.5 • Corrigindo o bug de detecção do driver intermitente • Adicionada a opção de instalação silenciosa. Execute Ec2Install.exe com a opção '-q', por exemplo: 'Ec2Install.exe -q'	
2.2.0	• Adicionado suporte para ambientes exclusivos de .Net4 e .Net4.5 • Atualizado o instalador	
2.1.19	• Adicionado suporte à etiqueta do disco efêmera ao usar o driver de rede da Intel (por exemplo, tipo de instância C3). Para obter mais informações, consulte Redes aperfeiçoadas para instâncias do Amazon EC2. • Adicionado suporte à versão de origem da AMI e ao nome de origem da AMI para a saída do console • Alterações feitas à saída do Console para formatação/análise consistente • Arquivo de ajuda atualizado	

Versão	Detalhes	Data de lançamento
2.1.18	• Adicionado objetivo de WMI do EC2Config para notificação de conclusão (-Namespace root\Amazon -Class EC2_ConfigService) • Performance aprimorada da consulta de WMI de startup com grandes logs de evento; pode causar uso elevado prolongado da CPU durante a execução inicial	
2.1.17	• Corrigido problema de execução com enchimento de buffer de saída padrão e erro padrão • O thumbprint de RDP incorreto fixo que às vezes aparece em saída do console para o SO >= w2k8 • A saída do console agora contém "RDPCERTIFICATE-SubjectName:" para Windows 2008+, que contém o valor do nome da máquina • Adicionado D:\ ao menu suspenso de mapeamento da letra de unidade • Movido o botão Ajuda para o canto direito superior e alterada a aparência • Adicionado link de pesquisa de Feedback ao canto direito superior	

Versão	Detalhes	Data de lançamento
2.1.16	• A guia Geral inclui o link da página de download do EC2Config para novas versões • A sobreposição do papel de parede do desktop agora está armazenada na pasta Users Local Appdata, em vez de em Meus Documentos, compatível com o redirecionamento do MyDoc • Nome do MSSQLServer sincronizado com o sistema no script do Post-Sysprep (2008+) • Pasta de aplicação reordenada (arquivos movidos para o diretório Plugin e removidos os arquivos em duplicata) • Alterada saída do log do sistema (Console): • *Movido para o formato data, nome, valor para facilitar a análise (comece a migrar as dependências para um novo formato) • *Adicionado o status do plugin 'Ec2SetPassword' • *Adicionado a hora de início e fim do Sysprep • Corrigido o problema de discos temporários não serem marcados como "Armazenamento Temporário" para sistemas operacionais não em inglês • Corrigida a falha de desinstalação do EC2Config depois de executar Sysprep	

Versão	Detalhes	Data de lançamento
2.1.15	• Solicitações otimizadas do serviço de metadados • Os metadados agora contornam as configurações do proxy • Discos temporários marcados como "Armazenamento temporário" e Important.txt colocados no volume quando encontrados (somente drivers do Citrix PV). Para obter mais informações, consulte Atualizar drivers PV em instâncias do Windows do EC2. • Discos temporários com letras Z a A (somente drivers do Citrix PV) – a atribuição pode ser sobrescrita usando o plugin de mapeamento de letra da unidade com etiquetas de Volume "Armazenamento Temporário X", onde x é um número 0-25 • O UserData agora é executado imediatamente depois de "Windows está pronto"	
2.1.14	Correções do papel de parede do desktop	
2.1.13	• Por padrão, o papel de parede do desktop exibirá o hostname • Dependência removida do serviço de Horário do Windows • Rota adicionada nos casos em que vários IPs são atribuídos a uma única interface	
2.1.11	• Alterações feitas no plugin Ec2Activation • - Verifica o status de Ativação cada 30 dias • - Se o período de carência tiver 90 dias restantes (dos 180), tenta novamente a ativação	

Versão	Detalhes	Data de lançamento
2.1.10	• A sobreposição do papel de parede do desktop não persiste mais com Sysprep ou desativação sem Sysprep • Opção de UserData para executar em cada início de serviço com <persist>true</persist> • Local e nome alterados de /DisableWinUpdate.cmd para /Scripts/PostSysprep.cmd • Senha do administrador definida para não expirar por padrão em /Scripts/PostSysprep.cmd • A desinstalação removerá o script PostSysprep do EC2Config c:\windows\setup\script\CommandComplete.cmd • O Add Route suporta métricas de interface personalizada	
2.1.9	A execução de UserData não é mais limitada a 3851 caracteres	

Versão	Detalhes	Data de lançamento
2.1.7	• Identificador da versão do SO e do idioma gravado no console • Versão do EC2Config gravada no console • Versão do driver PV gravada no console • Detecção de verificação de bugs e saída para o console na inicialização seguinte, quando encontrado • Adicionada opção para o config.xml manter as credenciais de Sysprep • Adicionar lógica de Route Retry nos casos em que o ENI está indisponível no início • PID de execução dos dados do usuário gravados no console • Comprimento mínimo de senha gerado recuperado de GPO • Ajuste o início do serviço para refazer 3 tentativas • Adicionados exemplos S3_DownloadFile.ps1 e S3_Upload file.ps1 à pasta /Scripts	

Versão	Detalhes	Data de lançamento
2.1.6	• Informações da versão adicionadas à guia Geral • Guia Pacote renomeada para Imagem • Simplificado o processo de especificação de senhas e movidas as UIs relacionadas à senha da guia Geral para a guia Imagem • Guia Configurações do disco rebatizada de Armazenamento • Adicionada a guia Suporte com ferramentas comuns para a resolução de problemas • `sysprep.ini` do Windows 2003 configurado para ampliar a partição do SO por padrão • Adicionado o endereço IP privado ao papel de parede • Endereço IP privado exibido no papel de parede • Lógica de tentativas adicionada à saída do Console • Exceção da porta de Com fixa para acessibilidade de metadados – fez com que o EC2Config fosse encerrado, pois a saída do console é exibida • Verifica o status da ativação em cada inicialização – ativa conforme o necessário • Problema corrigido de caminhos relativos – causado ao executar manualmente o atalho do papel de parede pela pasta de startup; apontando para Administrador/logs •	

Versão	Detalhes	Data de lançamento
	Cor de fundo padrão corrigida para usuário do Windows Server 2003 (além do Administrador)	

Versão	Detalhes	Data de lançamento
2.1.2	• Timestamps do console em UTC (Zulu) • Removida a aparência hyperlink na guia Sysprep • Adição de recurso para expandir dinamicamente o volume do dispositivo raiz na primeira inicialização para Windows 2008+ • Quando a opção Set-Password estiver habilitada, permite automaticamente que o EC2Config defina a senha • O EC2Config verifica o status de ativação antes de executar o Sysprep (apresenta uma advertência se não estiver ativado) • O `Sysprep.xml` do Windows Server 2003 agora usa como padrão o fuso horário UTC em vez de hora do Pacífico • Servidores de ativação aleatórios • Guia Mapeamento da unidade rebatizada para Configurações do disco • Itens de UI de Inicializar unidades movidas da guia Geral para a guia Configurações do disco • O botão Ajuda agora aponta para o arquivo de ajuda HTML • Arquivo HTML de ajuda atualizado com alterações • Texto "Observação" atualizado para mapeamentos das letras da unidade • Adicionado InstallUpdates.ps1 à pasta /Scripts para automatizar patches e limpeza antes de Sysprep	

Versão	Detalhes	Data de lançamento
2.1.0	• O papel de parede do desktop exibe informações da instância por padrão no primeiro login (não desconectar/reconectar) • O PowerShell pode ser executado a partir de userdata ao cercar o código com <powershell></powershell>	

Uso do EC2 Fast Launch para as instâncias do Windows

Quando você configura uma AMI do Windows Server para o EC2 Fast Launch, o Amazon EC2 cria um conjunto de snapshots pré-provisionados que serão usados para uma inicialização mais rápida, como se segue.

1. O Amazon EC2 lança um conjunto de instâncias t3 temporárias, com base em suas configurações.
2. À medida que cada instância temporária completa as etapas de lançamento padrão, o Amazon EC2 cria um snapshot pré-provisionado da instância. Ele armazena o snapshot em seu bucket do Amazon S3.
3. Quando o snapshot estiver pronto, o Amazon EC2 encerra a instância t3 associada para manter os custos dos recursos o mais baixos possível.
4. A próxima vez que o Amazon EC2 iniciar uma instância usando uma AMI habilitada para o EC2 Fast Launch, ele usará um dos snapshots para reduzir significativamente o tempo necessário para a inicialização.

O Amazon EC2 reabastece automaticamente os snapshots que você tem disponíveis à medida que os usa para iniciar instâncias usando a AMI habilitada para o EC2 Fast Launch.

Qualquer conta que tenha acesso a uma AMI com o EC2 Fast Launch pode se beneficiar de tempos de inicialização reduzidos. Quando o proprietário da AMI concede acesso para você iniciar instâncias, os snapshots pré-provisionados vêm da conta do proprietário da AMI.

Se uma AMI compatível com o EC2 Fast Launch for compartilhada com você, você mesmo poderá habilitar ou desabilitar a inicialização mais rápida na AMI compartilhada. Se você habilitar uma AMI compartilhada para o EC2 Fast Launch, o Amazon EC2 criará os snapshots pré-provisionados

diretamente na sua conta. Se você esgotar os snapshots da sua conta, ainda poderá usar os snapshots da conta do proprietário da AMI.

> **Note**
>
> O EC2 Fast Launch exclui os snapshots pré-provisionados assim que eles são consumidos por uma inicialização para minimizar os custos de armazenamento e evitar a reutilização. No entanto, se os snapshots excluídos corresponderem a uma regra de retenção, a Lixeira os reterá automaticamente. Recomendamos que você revise o escopo das regras de retenção da Lixeira para que isso não aconteça. Para ter mais informações, consulte Lixeira no Guia do usuário do Amazon EBS.
>
> Esse atributo não é o mesmo que a restauração rápida de snapshots do EBS. É necessário habilitar explicitamente a restauração rápida de snapshots do EBS em cada snapshot, e ela tem seus próprios custos associados.

O vídeo a seguir demonstra como configurar sua AMI do Windows para uma inicialização mais rápida com uma visão geral rápida dos principais termos relacionados e suas definições: Lançamento de instâncias do EC2 Windows até 65% mais rápido na AWS.

Custos com recursos

O serviço de configuração das AMIs do Windows para o EC2 Fast Launch não é cobrado. No entanto, o preço padrão se aplica a qualquer recurso da AWS subjacente que o Amazon EC2 usa. Para saber mais sobre os custos de recursos associados e como gerenciá-los, consulte Gerenciar custos dos recursos subjacentes do EC2 Fast Launch.

Conteúdo

- Principais termos
- Pré-requisitos do EC2 Fast Launch para Windows
- Configurar o EC2 Fast Launch para a AMI do Windows Server do Amazon EC2
- Visualização de AMIs com o EC2 Fast Launch habilitado
- Gerenciar custos dos recursos subjacentes do EC2 Fast Launch
- Monitorar o EC2 Fast Launch
- Perfil vinculado ao serviço para o EC2 Fast Launch
- Solucionar problemas do Windows EC2 Fast Launch

Principais termos

O atributo EC2 Fast Launch usa os seguintes termos básicos:

Snapshot pré-provisionado

Um snapshot de uma instância que foi iniciada de uma AMI do Windows com o EC2 Fast Launch habilitado e que concluiu as etapas de inicialização do Windows a seguir, reinicializando conforme necessário.

- Especialização sysprep
- Experiência Imediata do Windows (OOBE)

Quando essas etapas são concluídas, o EC2 Fast Launch interrompe a instância e cria um snapshot que é usado posteriormente para uma inicialização mais rápida usando a AMI, de acordo com a sua configuração.

Frequência de execução

Controla o número de snapshots pré-provisionados que o Amazon EC2 pode executar durante o período especificado. Quando você habilita o EC2 Fast Launch para a AMI, o Amazon EC2 cria o conjunto inicial de snapshots pré-provisionados em segundo plano. Por exemplo, se a frequência de inicialização for definida como cinco inicializações por hora, que é o padrão, o EC2 Fast Launch criará um conjunto inicial de cinco snapshots pré-provisionados.

Quando o Amazon EC2 inicia uma instância usando uma AMI com o EC2 Fast Launch habilitado, ele usa um dos snapshots pré-provisionados para reduzir o tempo de inicialização. Conforme são usados, os snapshots são automaticamente reabastecidos até o número especificado pela frequência de execução.

Se você espera um pico no número de instâncias que são iniciadas a partir da AMI (durante um evento especial, por exemplo), é possível aumentar a frequência de execução com antecedência para cobrir as instâncias adicionais necessárias. Quando sua taxa de execuções voltar ao normal, é possível reajustar a frequência e diminuí-la.

Se você observar um número de inicializações superior ao previsto, poderá usar todos os snapshots pré-provisionados que estiverem disponíveis. Isso não faz com que nenhuma execução falhe. No entanto, isso pode resultar em algumas instâncias passando pelo processo de início padrão, até que os snapshots possam ser reabastecidos.

Contagem de recursos de destino

O número de snapshots pré-provisionados a ser mantido disponível para uma AMI do Windows Server do Amazon EC2 com o EC2 Fast Launch habilitado.

Número máximo de execuções paralelas

Controla quantas instâncias o Amazon EC2 pode iniciar ao mesmo tempo para criar snapshots pré-provisionados para o EC2 Fast Launch. Se a contagem de recursos de destino for maior que o número máximo de execuções em paralelo, o Amazon EC2 iniciará o número de instâncias especificado por Máximo de execuções em paralelo para começar a criar os snapshots. Quando essas instâncias concluem o processo, o Amazon EC2 tira o snapshot e interrompe a instância. Em seguida, ele continua iniciando mais instâncias até que o número total de instantâneos disponíveis atinja a contagem de recursos desejada. O valor de Número máximo de execuções paralelas deve ser 6 ou maior.

Pré-requisitos do EC2 Fast Launch para Windows

Antes de configurar o EC2 Fast Launch, certifique-se de ter atendido aos seguintes pré-requisitos de criação de snapshots para as AMIs em sua Conta da AWS:

- Se você fornecer um modelo de inicialização personalizado ao configurar o EC2 Fast Launch, o serviço usará a VPC e outras configurações que você definiu no modelo de inicialização. Para obter mais informações, consulte Usar um modelo de inicialização ao configurar o EC2 Fast Launch.
- Se você não usar um modelo de inicialização personalizado para definir as configurações, deverá anexar a política EC2FastLaunchFullAccess ao seu perfil do IAM atual antes de habilitar o EC2 Fast Launch. Então, o serviço cria automaticamente uma pilha do CloudFormation com os seguintes recursos em sua Conta da AWS.
  - Uma nuvem privada virtual (VPC).
  - Sub-redes privadas em várias zonas de disponibilidade
  - Um modelo de inicialização configurado com o Instance Metadata Service versão 2 (IMDSv2)
  - Um grupo de segurança sem regras de entrada e saída
- As AMIs do EC2 Fast Launch devem ser compatíveis com a execução de scripts de dados do usuário.

- Para configurar o EC2 Fast Launch para uma AMI, você deve criar a AMI usando Sysprep com a opção de desligamento. Atualmente, o atributo EC2 Fast Launch não é compatível com AMIs criadas em uma instância em execução.

  Para criar uma AMI usando Sysprep, consulte Criar uma AMI do Amazon EC2 usando o Sysprep do Windows.
- Para habilitar o EC2 Fast Launch para uma AMI criptografada que usa uma chave gerenciada pelo cliente para criptografia, é necessário conceder ao perfil vinculado ao serviço do EC2 Fast Launch permissão para usar a CMK. Para obter mais informações, consulte the section called “Acesso às chaves gerenciadas pelo usuário”.
- A cota padrão para Número máximo de execuções paralelas em todas as AMIs em uma Conta da AWS é de 40 por região. É possível solicitar um aumento do Service Quotas de sua conta, da maneira a seguir.

  1. Abra o console Service Quotas em https://console.aws.amazon.com/servicequotas/.
  2. No painel de navegação, escolha Serviços da AWS.
  3. Na barra de pesquisa, digite **`EC2 Fast Launch`** e selecione o resultado.
  4. Selecione o link para Inicializações paralelas de instâncias para abrir a página de detalhes da cota de serviço.
  5. Escolha Solicitar aumento no nível da conta.

  Para obter mais informações, consulte Solicitando um Aumento de Cota no Guia do Usuário do Service Quotas.

Configurar o EC2 Fast Launch para a AMI do Windows Server do Amazon EC2

É possível configurar o EC2 Fast Launch para as AMIs do Windows de que é proprietário ou para as AMIs compartilhadas com você usando o Console de gerenciamento da AWS, a API, os SDKs, o CloudFormation ou a AWS Command Line Interface (AWS CLI). Antes de configurar o EC2 Fast Launch, certifique-se de que a AMI atenta a todos os pré-requisitos para a criação de snapshots pré-provisionados. Para obter mais informações, consulte Pré-requisitos do EC2 Fast Launch para Windows.

Quando você habilita a inicialização mais rápida de instâncias do Windows, o Amazon EC2 verifica se você tem as permissões necessárias para iniciar instâncias na AMI e no modelo de inicialização especificados (se fornecidos), incluindo permissões para AMIs criptografadas. Para evitar erros

durante o processo de inicialização da instância, o serviço valida suas permissões antes que o EC2 Fast Launch seja habilitado. Caso não haja permissões obrigatórias, o serviço retornará um erro e não habilitará o EC2 Fast Launch.

O EC2 Fast Launch se integra ao EC2 Image Builder para ajudar você a criar imagens personalizadas com o EC2 Fast Launch habilitado. Para obter mais informações, consulte Criar configurações de distribuição para uma AMI Windows com o EC2 Fast Launch habilitado (AWS CLI) no Guia do usuário do EC2 Image Builder.

Habilitar o EC2 Fast Launch

Antes de alterar essas configurações, certifique-se de que sua AMI e região de execução atendam a todos os Pré-requisitos do EC2 Fast Launch para Windows.

Console

Para habilitar o EC2 Fast Launch

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, em Images (Imagens), escolha AMIs.
3. Escolha a AMI a atualizar marcando a caixa de seleção ao lado de Name (Nome).
4. No menu Ações acima da lista de AMIs, escolha Configurar início rápido. Isso abre a página Configurar inicialização rápida na qual você configura o EC2 Fast Launch.
5. Para começar a usar snapshots pré-provisionados para iniciar instâncias da sua AMI do Windows com mais rapidez, marque a caixa de seleção Habilitar a inicialização rápida do Windows.
6. Na lista suspensa Set anticipated launch frequency (Definir a frequência antecipada de execução), escolha um valor para especificar o número de snapshots que são criados e mantidos para cobrir o volume esperado de execuções de instância.
7. Quando terminar de fazer as alterações, escolha Save changes (Salvar alterações).

> **Note**
>
> Se você precisar usar um modelo de inicialização para especificar uma VPC ou definir configurações de metadados para o IMDSv2, consulte Usar um modelo de inicialização ao configurar o EC2 Fast Launch.

AWS CLI

Para habilitar o EC2 Fast Launch

Use o seguinte comando enable-fast-launch para habilitar o EC2 Fast Launch para a AMI especificada, iniciando seis instâncias paralelas para pré-provisionamento.

```
aws ec2 enable-fast-launch \
    --image-id ami-0abcdef1234567890  \
    --max-parallel-launches 6 \
    --resource-type snapshot
```

O seguinte é um exemplo de saída.

```
{
 "ImageId": "ami-0abcdef1234567890",
 "ResourceType": "snapshot",
 "SnapshotConfiguration": {
     "TargetResourceCount": 10
 },
 "LaunchTemplate": {},
 "MaxParallelLaunches": 6,
 "OwnerId": "0123456789123",
 "State": "enabling",
 "StateTransitionReason": "Client.UserInitiated",
 "StateTransitionTime": "2022-01-27T22:16:03.199000+00:00"
}
```

PowerShell

Para habilitar o EC2 Fast Launch

Use o cmdlet Enable-EC2FastLaunch para habilitar o EC2 Fast Launch para a AMI especificada e iniciar seis instâncias paralelas para pré-provisionamento.

```
Enable-EC2FastLaunch `
 -ImageId ami-0abcdef1234567890 `
 -MaxParallelLaunch 6 `
 -Region us-west-2 `
 -ResourceType snapshot
```

O seguinte é um exemplo de saída.

```
ImageId               : ami-0abcdef1234567890
 LaunchTemplate        :
 MaxParallelLaunches   : 6
 OwnerId               : 0123456789123
 ResourceType          : snapshot
 SnapshotConfiguration : Amazon.EC2.Model.FastLaunchSnapshotConfigurationResponse
 State                 : enabling
 StateTransitionReason : Client.UserInitiated
 StateTransitionTime   : 2/25/2022 12:24:11 PM
```

Desabilitar o EC2 Fast Launch

Antes de alterar essas configurações, certifique-se de que sua AMI e região de execução atendam a todos os Pré-requisitos do EC2 Fast Launch para Windows.

Console

Para desabilitar o EC2 Fast Launch

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, em Images (Imagens), escolha AMIs.
3. Escolha a AMI a atualizar marcando a caixa de seleção ao lado de Name (Nome).
4. No menu Ações acima da lista de AMIs, escolha Configurar início rápido. Isso abre a página Configurar inicialização rápida na qual você configura o EC2 Fast Launch.
5. Desmarque a caixa de seleção Habilitar inicialização rápida no Windows para desabilitar a inicialização rápida do EC2 e remover os snapshots pré-provisionados. Isso resulta na AMI usando o processo de início padrão para cada instância, daqui para frente.

   > **Note**
   >
   > Quando você desabilita a otimização de imagens do Windows, todos os snapshots pré-provisionados existentes são excluídos automaticamente. Essa etapa deve ser concluída antes que você possa começar a usar o recurso novamente.

6. Quando terminar de fazer as alterações, escolha Save changes (Salvar alterações).

AWS CLI

Para desabilitar o EC2 Fast Launch

Use o seguinte comando disable-fast-launch para desabilitar o EC2 Fast Launch na AMI especificada e limpar os snapshots pré-provisionados existentes.

```
aws ec2 disable-fast-launch --image-id ami-01234567890abcedf
```

O seguinte é um exemplo de saída.

```
{
    "ImageId": "ami-01234567890abcedf",
    "ResourceType": "snapshot",
    "SnapshotConfiguration": {},
    "LaunchTemplate": {
        "LaunchTemplateId": "lt-01234567890abcedf",
        "LaunchTemplateName": "EC2FastLaunchDefaultResourceCreation-
a8c6215d-94e6-441b-9272-dbd1f87b07e2",
        "Version": "1"
    },
    "MaxParallelLaunches": 6,
    "OwnerId": "0123456789123",
    "State": "disabling",
    "StateTransitionReason": "Client.UserInitiated",
    "StateTransitionTime": "2022-01-27T22:47:29.265000+00:00"
}
```

PowerShell

Para desabilitar o EC2 Fast Launch

Use o cmdlet Disable-EC2FastLaunch para desabilitar o EC2 Fast Launch na AMI especificada e limpar os snapshots pré-provisionados existentes.

```
Disable-EC2FastLaunch -ImageId ami-0abcdef1234567890
```

O seguinte é um exemplo de saída.

```
ImageId               : ami-0abcdef1234567890
 LaunchTemplate        :
 Amazon.EC2.Model.FastLaunchLaunchTemplateSpecificationResponse
 MaxParallelLaunches   : 6
```

```
OwnerId               : 0123456789123
ResourceType          : snapshot
SnapshotConfiguration :
State                 : disabling
StateTransitionReason : Client.UserInitiated
StateTransitionTime   : 2/25/2022 1:10:08 PM
```

Usar um modelo de inicialização ao configurar o EC2 Fast Launch

Com um modelo de inicialização, é possível configurar um conjunto de parâmetros de inicialização que é usado pelo Amazon EC2 toda vez que ele inicializa uma instância com base nesse modelo. É possível especificar opções como uma AMI a ser usada para sua imagem base, tipos de instância, armazenamento, configurações de rede e muito mais.

Os modelos de inicialização são opcionais, exceto nos seguintes casos específicos em que é necessário usar um modelo de inicialização para sua AMI do Windows ao configurar a inicialização mais rápida:

- Você deve usar um modelo de inicialização para especificar uma VPC existente para a AMI do Windows. Isso não se aplicará se você usar a VPC padrão para a sua Conta da AWS.
- Se a conta incluir uma política que imponha o IMDSv2 para instâncias do Amazon EC2, é necessário criar um modelo de execução que especifique a configuração de metadados para aplicar o IMDSv2.

  Use o modelo de inicialização que inclui sua configuração de metadados do console do EC2 console ou execute o comando enable-fast-launch na AWS CLI ou chame a ação da API EnableFastLaunch.

O EC2 Fast Launch do Amazon EC2 não é compatível com a configuração a seguir quando você usa um modelo de inicialização. Se você usar um modelo de inicialização para o EC2 Fast Launch, não deverá especificar nenhum dos seguintes itens:

- Scripts de dados do usuário
- Termination protection
- Metadados desabilitados
- Opção spot
- Comportamento de desligamento que encerra a instância

- Etiquetas de recursos para solicitações de interfaces de rede, de gráficos elásticos ou de instâncias spot

Especificar uma VPC

Etapa 1: Criar um modelo de execução

Crie um modelo de execução que especifique os seguintes detalhes para suas instâncias do Windows:

- A sub-rede da VPC.
- Um tipo de instância de `t3.xlarge`.

Para obter mais informações, consulte Criar um modelo de execução do Amazon EC2.

Etapa 2: especifique o modelo de inicialização para a AMI do EC2 Fast Launch

Console

Para especificar o modelo de inicialização do EC2 Fast Launch

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, em Images (Imagens), escolha AMIs.
3. Escolha a AMI a atualizar marcando a caixa de seleção ao lado de Name (Nome).
4. No menu Ações acima da lista de AMIs, escolha Configurar início rápido. Isso abre a página Configurar inicialização rápida na qual você configura o EC2 Fast Launch.
5. A caixa Launch template (Modelo de inicialização) executa uma pesquisa filtrada que localiza modelos de inicialização em sua conta na região atual que correspondem ao texto digitado. Especifique todo ou parte do nome ou ID do modelo de inicialização na caixa para mostrar uma lista de modelos de inicialização correspondentes. Por exemplo, se você inserir `fast` na caixa, o Amazon EC2 encontrará todos os modelos de inicialização em sua conta na região atual que contêm "fast" no nome.

   Para criar um novo modelo de inicialização, escolha Create launch template (Criar modelo de inicialização).
6. Quando um modelo de inicialização é selecionado, o Amazon EC2 mostra a versão padrão desse modelo na caixa Source template version (Versão do modelo de origem). Para

especificar uma versão diferente, realce a versão padrão para substituí-la e insira o número da versão desejada na caixa.

7. Quando terminar de fazer as alterações, escolha Save changes (Salvar alterações).

AWS CLI

Para especificar o modelo de inicialização do EC2 Fast Launch

Use o comando enable-fast-launch com a opção `--launch-template`, especificando o nome ou o ID do modelo de inicialização.

```
--launch-template LaunchTemplateName=my-launch-template
```

PowerShell

Para especificar o modelo de inicialização do EC2 Fast Launch

Use o cmdlet Enable-EC2FastLaunch com o parâmetro `-LaunchTemplate_LaunchTemplateId` ou `-LaunchTemplate_LaunchTemplateName`.

```
-LaunchTemplate_LaunchTemplateName my-launch-template
```

Para obter mais informações sobre modelos de inicialização do EC2, consulte Armazenar os parâmetros de execução de instâncias nos modelos de execução do Amazon EC2.

Visualização de AMIs com o EC2 Fast Launch habilitado

Você pode usar o comando describe-fast-launch-images na AWS CLI ou o Cmdlet Get-EC2FastLaunchImage do Tools for PowerShell para obter os detalhes das AMIs que têm o EC2 Fast Launch habilitado.

O Amazon EC2 fornece os seguintes detalhes para cada AMI do Windows retornada nos resultados:

- O ID da imagem de uma AMI com o EC2 Fast Launch habilitado.
- O tipo de recurso usado para pré-provisionamento da AMI do Windows associada. Valor compatível: `snapshot`.
- A configuração de snapshot, que é um grupo de parâmetros usados para pré-provisionar a AMI do Windows associada usando snapshots.

- Informações do modelo de execução, incluindo o ID, o nome e a versão do modelo de execução que a AMI associada usa quando executa instâncias do Windows de snapshots pré-provisionados.
- O número máximo de instâncias que podem ser executadas ao mesmo tempo para a criação de recursos.
- O ID do proprietário da AMI associada. Isso não é preenchido para as AMIs que são compartilhadas com você.
- O estado atual do EC2 Fast Launch para a AMI associada. Os valores com suporte incluem: `enabling | enabling-failed | enabled | enabled-failed | disabling | disabling-failed`.

> **Note**
>
> É possível ver também o estado atual exibido na página Manage image optimization (Gerenciar otimização de imagens) no console do EC2 em Image optimization state (Estado da otimização de imagem).

- O motivo pelo qual o EC2 Fast Launch para a AMI associada foi alterado para o estado atual.
- A hora em que o EC2 Fast Launch para a AMI associada foi alterado para o estado atual.

AWS CLI

Para encontrar AMIs configuradas para EC2 Fast Launch

Use o seguinte comando describe-fast-launch-images para descrever os detalhes de cada uma das AMIs na conta que estão configuradas para o EC2 Fast Launch. Neste exemplo, apenas uma AMI da conta está configurada para o EC2 Fast Launch.

```
aws ec2 describe-fast-launch-images
```

O seguinte é um exemplo de saída.

```
{
    "FastLaunchImages": [
        {
            "ImageId": "ami-01234567890abcedf",
            "ResourceType": "snapshot",
            "SnapshotConfiguration": {},
            "LaunchTemplate": {
```

```
                "LaunchTemplateId": "lt-01234567890abcedf",
                "LaunchTemplateName": "EC2FastLaunchDefaultResourceCreation-
a8c6215d-94e6-441b-9272-dbd1f87b07e2",
                "Version": "1"
            },
            "MaxParallelLaunches": 6,
            "OwnerId": "0123456789123",
            "State": "enabled",
            "StateTransitionReason": "Client.UserInitiated",
            "StateTransitionTime": "2022-01-27T22:20:06.552000+00:00"
        }
    ]
}
```

PowerShell

Para encontrar AMIs configuradas para EC2 Fast Launch

Use o seguinte cmdlet Get-EC2FastLaunchImage para descrever os detalhes de cada uma das AMIs da conta que estão configuradas para o EC2 Fast Launch. Neste exemplo, apenas uma AMI da conta está configurada para o EC2 Fast Launch.

```
Get-EC2FastLaunchImage -ImageId ami-0abcdef1234567890
```

O seguinte é um exemplo de saída.

```
ImageId               : ami-0abcdef1234567890
LaunchTemplate        :
 Amazon.EC2.Model.FastLaunchLaunchTemplateSpecificationResponse
MaxParallelLaunches   : 6
OwnerId               : 012345678912
ResourceType          : snapshot
SnapshotConfiguration :
State                 : enabled
StateTransitionReason : Client.UserInitiated
StateTransitionTime   : 2/25/2022 12:54:43 PM
```

Gerenciar custos dos recursos subjacentes do EC2 Fast Launch

O serviço de configuração das AMIs do Windows para o EC2 Fast Launch não é cobrado. Porém, quando você habilita o EC2 Fast Launch. para uma AMI do Windows do Amazon EC2, os preços

padrão se aplicam aos recursos subjacentes da AWS que o Amazon EC2 usa para preparar e armazenar os snapshots pré-provisionados. Você pode configurar tags de alocação de custos para ajudar a rastrear e gerenciar os custos associados aos recursos do EC2 Fast Launch. Para obter mais informações sobre como configurar tags de alocação de custos, consulte Acompanhar os custos do EC2 Fast Launch em sua fatura.

O exemplo a seguir demonstra como os custos associados aos snapshots do EC2 Fast Launch podem ser alocados.

Cenário de exemplo: a empresa de exemplo AtoZ tem uma AMI do Windows com um volume raiz do EBS com 50 GiB. A empresa habilitou o EC2 Fast Launch.para a AMI e definiu o número de recursos de destino como cinco. No decorrer de um mês, o uso do EC2 Fast Launch para a AMI custa aproximadamente USD 5,00. O detalhamento de custos é o seguinte:

1. Quando o exemplo da AtoZ habilita o EC2 Fast Launch, o Amazon EC2 inicia cinco instâncias pequenas. Cada instância é executada pelas etapas de execução Sysprep e OOBE Windows, reinicializando conforme necessário. Isso leva vários minutos para cada instância (o tempo pode variar de acordo com o nível de movimentação da região ou Availability Zone [AZ – Zona de disponibilidade] e com o tamanho da AMI).

   Custos

   - Custos de runtime de instância (ou tempo mínimo de execução, se for o caso): 5 instâncias
   - Custos de volume: 5 volumes raiz do EBS
2. Quando o processo de pré-provisionamento é concluído, o Amazon EC2 obtém um snapshot da instância e armazena no Amazon S3. Normalmente, os snapshots são armazenados por 4 a 8 horas antes de serem consumidos por uma inicialização. Nesse caso, o custo é de aproximadamente USD 0,02 a USD 0,05 por snapshot.

   Custos

   - Armazenamento de snapshots (Amazon S3): 5 snapshots
3. Após obter o snapshot, o Amazon EC2 interrompe a instância. Nesse momento, a instância não está mais acumulando custos. No entanto, os custos por volume do EBS continuam sendo acumulados.

   Custos

   - Volumes do EBS: os custos continuam para os volumes raiz associados do EBS.

> **Note**
>
> Os custos apresentados aqui são apenas para fins de demonstração. Seus custos vão variar de acordo com a configuração da AMI e do plano de preços.

Acompanhar os custos do EC2 Fast Launch em sua fatura

As tags de alocação de custos podem ajudar você a organizar sua fatura da AWS para refletir os custos associados ao EC2 Fast Launch. Você pode usar a seguinte tag que o Amazon EC2 adiciona aos recursos que cria ao preparar e armazenar snapshots pré-provisionados para o EC2 Fast Launch:

Chave de etiqueta: `CreatedBy`, Valor: `EC2 Fast Launch`

Após a etiqueta ser ativada no console do Billing and Cost Management e seu relatório de faturamento detalhado ser configurado, a coluna `user:CreatedBy` aparece no relatório. A coluna inclui valores de todos os serviços. No entanto, se você baixar o arquivo CSV, poderá importar os dados para uma planilha e filtrar por `EC2 Fast Launch` no valor. Essas informações também são exibidas no AWS Cost and Usage Report quando a etiqueta está ativada.

Etapa 1: ativar etiquetas de alocação de custos definidas pelo usuário

Para incluir etiquetas de recursos nos relatórios de custos, é necessário ativá-las primeiro no console do Billing and Cost Management. Para obter mais informações, consulte Ativar tags de alocação de custos definidos pelo usuário no Guia do usuário do AWS Billing and Cost Management.

> **Note**
>
> A ativação pode demorar até 24 horas.

Etapa 2: configurar um relatório de custos

Se você já tiver um relatório de custos configurado, uma coluna para sua etiqueta será exibida na próxima vez que o relatório for executado após a conclusão da ativação. Para configurar os relatórios de custos pela primeira vez, escolha uma das opções a seguir.

- Consulte Setting up a monthly cost allocation report (Configurar um relatório de alocação de custos mensal) no Guia do usuário do AWS Billing and Cost Management.

- Consulte Creating cost and usage reports (Criar relatórios de custos e uso) no Guia do usuário do AWS Cost and Usage Report.

> **Note**
>
> Pode demorar até 24 horas para que a AWS comece a entregar relatórios em seu bucket do S3.

Você pode configurar o EC2 Fast Launch para as AMIs do Windows das quais é o proprietário ou das AMIs compartilhadas com você usando o console, a API e os SDKs do Amazon EC2, o CloudFormation ou os comandos ec2 da AWS CLI. As seções a seguir abrangem as etapas de configuração para o console do Amazon EC2 e a AWS CLI.

Você também pode criar AMIs do Windows personalizadas que são configuradas para o EC2 Fast Launch com o EC2 Image Builder. Para obter mais informações, consulte Create distribution settings for a Windows AMI with EC2 Fast Launch enabled (AWS CLI).

Monitorar o EC2 Fast Launch

Esta seção aborda como monitorar as AMIs do Windows Server do Amazon EC2 da sua conta que têm o EC2 Fast Launch habilitado.

Monitorar as alterações de estado do EC2 Fast Launch com o EventBridge

Quando o estado de uma AMI do Windows com o EC2 Fast Launch habilitado é alterado, o Amazon EC2 gera um evento de `EC2 Fast Launch State-change Notification`. Em seguida, o Amazon EC2 envia o evento de mudança de estado ao Amazon EventBridge (anteriormente conhecido como Amazon CloudWatch Events).

É possível criar regras do EventBridge que acionem uma ou mais ações em resposta ao evento de mudança de estado. Por exemplo, você pode criar uma regra do EventBridge que detecta quando o EC2 Fast Launch está habilitado e executa as seguintes ações:

- Envia uma mensagem para um tópico do Amazon SNS que notifica seus assinantes.
- Invoca uma função do Lambda que executa alguma ação.
- Envia os dados de alteração de estado ao Amazon Data Firehose para analytics.

Para obter mais informações, consulte Criar regras do Amazon EventBridge que reajam a eventos no Guia do usuário do Amazon EventBridge.

Eventos de alteração de estado

O atributo EC2 Fast Launch faz todos os esforços para emitir eventos de alteração de estado no formato JSON. O Amazon EC2 envia os eventos ao EventBridge praticamente em tempo real. Esta seção descreve os campos do evento e mostra um exemplo do formato do evento.

`EC2 Fast Launch State-change Notification`

imageId

Identifica a AMI com a alteração de estado do EC2 Fast Launch.

resourceType

O tipo de recurso a ser usado para pré-provisionamento. Valor compatível: `snapshot`. O valor padrão é `snapshot`.

estado

O estado atual do atributo EC2 Fast Launch para a AMI especificada. Entre os valores válidos estão os seguintes:

- enabling: você habilitou o atributo EC2 Fast Launch para a AMI, e o Amazon EC2 iniciou a criação de snapshots para o processo de pré-provisionamento.
- enabling-failed: houve algum tipo de problema que causou falha no processo de pré-provisionamento a primeira vez que você habilitou o EC2 Fast Launch para uma AMI. Isso pode acontecer a qualquer momento durante o processo de pré-provisionamento.
- enabled: o atributo EC2 Fast Launch está habilitado. O estado é alterado para `enabled` assim que o Amazon EC2 cria o primeiro snapshot pré-provisionado para uma AMI do EC2 Fast Launch recém-habilitada. Se a AMI já estiver habilitada e passar pelo pré-provisionamento novamente, a mudança de estado ocorrerá imediatamente.
- enabled-failed: esse estado só se aplicará se não for a primeira vez que a AMI do EC2 Fast Launch passa pelo processo de pré-provisionamento. Isso poderá acontecer se o atributo EC2 Fast Launch for desabilitado e depois habilitado novamente, se houver uma alteração na configuração ou outro erro após o pré-provisionamento ser concluído pela primeira vez.
- disabling: o proprietário da AMI desativou o atributo EC2 Fast Launch para a AMI e o Amazon EC2 iniciou o processo de limpeza.

- disabled: o atributo EC2 Fast Launch está desabilitado. O estado muda para `disabled` assim que o Amazon EC2 conclui o processo de limpeza.
- disabling-failed (falha de desabilitando): algo deu errado e causou a falha no processo de limpeza. Isso significa que alguns snapshots pré-provisionados ainda podem permanecer na conta.

stateTransitionReason

O motivo pelo qual o estado da AMI do EC2 Fast Launch foi alterado.

> **Note**
>
> Todos os campos desta mensagem de evento são obrigatórios.

O exemplo a seguir mostra uma AMI do EC2 Fast Launch recém-habilitada que iniciou a primeira instância para começar o processo de pré-provisionamento. Neste ponto, o estado é `enabling`. Depois que o Amazon EC2 cria o primeiro snapshot pré-provisionado, o estado muda para `enabled`.

```
{
 "version": "0",
 "id": "01234567-0123-0123-0123-012345678901",
 "detail-type": "EC2 Fast Launch State-change Notification",
 "source": "aws.ec2",
 "account": "123456789012",
 "time": "2022-08-31T20:30:12Z",
 "region": "us-east-1",
 "resources": [
  "arn:aws:ec2:us-east-1:123456789012:image/ami-123456789012"
 ],
 "detail": {
  "imageId": "ami-123456789012",
  "resourceType": "snapshot",
  "state": "enabling",
  "stateTransitionReason": "Client.UserInitiated"
 }
}
```

Monitorar as métricas do EC2 Fast Launch com o CloudWatch

As AMIs do Amazon EC2 com o EC2 Fast Launch habilitado enviam 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 EC2 Fast Launch envia para o CloudWatch. O namespace `AWS/EC2` inclui as seguintes métricas do EC2 Fast Launch:

Métrica	Descrição
NumberOfAvailableFastLaunchSnapshots	O número de snapshots pré-provisionados disponível por AMI habilitada para o EC2 Fast Launch.
NumberOfInstancesFastLaunched	O número de instâncias por AMI habilitada para o EC2 Fast Launch que foram iniciadas em snapshots pré-provisionados.
NumberOfInstancesNotFastLaunched	O número de instâncias por AMI habilitada para o EC2 Fast Launch que resultaram em uma inicialização a frio devido à falta de instantân eos pré-provisionados disponíveis na hora da inicialização.
FastLaunchSnapshotUsedToRefillStartTime	A data e hora em que o Amazon EC2 iniciou uma nova imagem usando uma AMI habilitad a para o EC2 Fast Launch para criar outro snapshot após um snapshot existente ser usado.
FastLaunchSnapshotCreationTime	Mede o tempo que o Amazon EC2 leva para iniciar uma instância e criar um snapshot para uma AMI habilitada para o EC2 Fast Launch.

Perfil vinculado ao serviço para o EC2 Fast Launch

O Amazon EC2 usa funções vinculadas ao serviço para as permissões necessárias para chamar outros Serviços da AWS em seu nome. O perfil vinculado ao serviço é um tipo exclusivo de perfil do IAM vinculado diretamente ao AWS service (Serviço da AWS). Os perfis vinculados a serviços

oferecem uma maneira segura de delegar permissões a outros Serviços da AWS, pois somente o serviço vinculado pode assumir uma função vinculada ao serviço. Para obter mais informações sobre o Amazon EC2 usa as funções do IAM, incluindo funções vinculadas ao serviço, consulte Funções do IAM para Amazon EC2.

O Amazon EC2 usa a função vinculada ao serviço de nome AWSServiceRoleForEC2FastLaunch para criar e gerenciar um conjunto de snapshots pré-provisionados que reduzem o tempo necessário para iniciar instâncias a partir da sua AMI do Windows.

Permissões concedidas pelo AWSServiceRoleForEC2FastLaunch

A função vinculada ao serviço AWSServiceRoleForEC2FastLaunch confia no seguinte serviço para assumir a função:

- `ec2fastlaunch.amazonaws.com`

O Amazon EC2 usa a política gerenciada EC2FastLaunchServiceRolePolicy para concluir as ações a seguir:

- AWS CloudFormation: permitir que o EC2 Fast Launch obtenha uma descrição das pilhas do CloudFormation associadas.
- Amazon CloudWatch: publicar os dados das métricas associadas ao EC2 Fast Launch para o namespace do Amazon EC2.
- Amazon EC2: acesso concedido ao EC2 Fast Launch para realizar as seguintes ações:
  - Iniciar instâncias em uma AMI do Windows Server do Amazon EC2 com o EC2 Fast Launch habilitado para realizar as etapas de provisionamento. Além disso, especifique o padrão de recursos que permite `ec2:RunInstances` para uma AMI associada ao License Manager.
  - Parar e encerar uma instância que foi iniciada pelo EC2 Fast Launch depois que ela criar snapshot pré-provisionado.
  - Descrever os recursos do tipo imagem e instância usados para iniciar instâncias e criar snapshots de uma AMI do Amazon EC2 para Windows Server com o EC2 Fast Launch habilitado.
  - Descrever os recursos do modelo de inicialização e iniciar instâncias a partir de um modelo de inicialização.
  - Descrever instâncias, atributos de instâncias e status de instâncias, volumes e atributos de volumes.
  - Descrever interfaces de rede.

  - Excluir os recursos que o EC2 Fast Launch criou, incluindo snapshots, modelos de execução, volumes e interfaces de rede.
  - Marcar os recursos que o EC2 Fast Launch cria para iniciar e pré-provisionar instâncias do Windows e criar snapshots para o processo final de inicialização consumir.
- Amazon EventBridge: inclui acesso para criar regras de eventos do EventBridge e recuperar detalhes sobre elas ou excluir as regras que ele criou. O EC2 Fast Launch também pode obter uma lista dos serviços que recebem eventos do EC2 Fast Launch que são encaminhados com base nas regras de eventos e adicionar serviços de destino ou removê-los das regras de eventos que ele criou.
- IAM: permite que o EC2 Fast Launch crie o perfil vinculado ao serviço `EC2FastLaunchServiceRolePolicy`, obtenha e use perfis de instância cujo nome contenha `ec2fastlaunch` e inicie instâncias em seu nome usando o perfil de instância do modelo de inicialização.
- AWS KMS: inclui acesso para criar concessões e listar as concessões que foram criadas pelo EC2 Fast Launch que podem ser retiradas. Também para descrever ou usar chaves com a finalidade de criptografar ou descriptografar volumes anexados às instâncias que o EC2 Fast Launch criar, e para gerar chaves de dados que não estejam em texto simples.

Para visualizar as permissões para esta política, consulte EC2FastLaunchServiceRolePolicy na Referência de políticas gerenciadas pela AWS.

Para obter mais informações sobre o uso de políticas gerenciadas no Amazon EC2, consulte Políticas gerenciadas pela AWS para o Amazon EC2.

Criar um perfil vinculado ao serviço

Você não precisa criar manualmente essa função vinculada ao serviço. Quando você começa a usar o EC2 Fast Launch para a AMI, o Amazon EC2 cria o perfil vinculado ao serviço, caso ele ainda não exista.

Se o perfil vinculado ao serviço for excluído de sua conta, você poderá habilitar o EC2 Fast Launch para outra AMI do Windows a fim de recriar o perfil em sua conta. Ou então, você pode desabilitar o EC2 Fast Launch para a AMI atual e, em seguida, habilitá-lo novamente. No entanto, desabilitar o atributo resulta em sua AMI usando o processo de início padrão para todas as novas instâncias, enquanto o Amazon EC2 remove todos os snapshots pré-provisionados. Depois que todos os snapshots pré-provisionados são excluídos, você pode habilitar novamente o uso do EC2 Fast Launch para a AMI.

Acesso às chaves gerenciadas pelo usuário

Para habilitar o EC2 Fast Launch em uma AMI criptografada que usa uma chave gerenciada pelo cliente para criptografia, é necessário conceder ao perfil AWSServiceRoleForEC2FastLaunch permissão para usar a CMK. Para fazer isso, chame o comando create-grant. Para `--grantee-principal`, especifique o ARN para o perfil AWSServiceRoleForEC2FastLaunch em sua conta. Em `--operations`, especifique `CreateGrant`.

```
aws kms create-grant \
    --key-id arn:aws:kms:us-
east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab \
    --grantee-principal arn:aws:iam::111122223333:role/AWSServiceRoleForEC2FastLaunch \
    --operations CreateGrant
```

Editar um perfil vinculado ao serviço

O Amazon EC2 não permite que você edite a função vinculada ao serviço do AWSServiceRoleForEC2FastLaunch. Depois que você criar uma função vinculada a serviço, não poderá alterar o nome da função, pois várias entidades podem fazer referência à função. No entanto, será possível editar a descrição da função usando o IAM. Para obter mais informações, consulte Editar um perfil vinculado ao serviço no Guia do usuário do IAM.

Excluir um perfil vinculado ao serviço

É possível excluir uma função vinculada ao serviço somente depois de excluir todos os recursos relacionados. Isso protege os recursos do Amazon EC2 que estão associados à AMI do Windows Server do Amazon EC2 com o EC2 Fast Launch habilitado, pois não será possível remover acidentalmente a permissão para acessar os recursos.

Use o console do IAM, a AWS CLI ou a API da AWS para excluir o perfil vinculado ao serviço AWSServiceRoleForEC2FastLaunch. Para obter mais informações, consulte Excluir uma função vinculada ao serviço no Guia do usuário do IAM.

Regiões do compatíveis

O Amazon EC2 é compatível com o perfil vinculado ao serviço do EC2 Fast Launch em todas as regiões em que o serviço do Amazon EC2 está disponível.

Solucionar problemas do Windows EC2 Fast Launch

Cenários de solução de problemas

Os seguintes cenários podem ajudar a diagnosticar e corrigir problemas comuns que você pode encontrar ao tentar habilitar o EC2 Fast Launch.

Não é possível parar a instância para a criação de snapshots

Descrição

Quando você habilita o EC2 Fast Launch, o serviço inicia um conjunto de instâncias que são usadas para criar os snapshots pré-provisionados. Cada instância tem 30 minutos para concluir o processo. Se alguma instância for concluída com êxito, o serviço definirá o status de Fast Launch da AMI como `Enabled`. Porém, se alguma instância não concluir o processo no tempo estipulado e nenhuma das outras instâncias tiver concluído o processo, o serviço encerrará todas as instâncias e definirá o status do Fast Launch da AMI como `enabling_failed` e o motivo do status do Fast Launch como o seguinte:

```
Unable to stop instance ID=i-1234567890abcdef0 for snapshot creation.
```

Causa

A maioria das vezes, isso é causado pela tentativa de habilitar o EC2 Fast Launch para uma AMI do Windows criada em uma instância em execução ou em uma AMI que não atende a todos os Pré-requisitos do EC2 Fast Launch.

Solução

Certifique-se de que a AMI que você usa atenda a todos os Pré-requisitos do EC2 Fast Launch.

Para configurar o EC2 Fast Launch para uma AMI, você deve criar a AMI usando Sysprep com a opção de desligamento. Para obter mais informações, consulte Criar uma AMI do Amazon EC2 usando o Sysprep do Windows.

Você atingiu o limite de VPCs

Descrição

Se você não usar um modelo de inicialização para especificar uma VPC existente e não tiver uma VPC padrão definida para a conta, o serviço criará automaticamente uma pilha da CloudFormation que inclui uma VPC e outros recursos, conforme descrito em Pré-requisitos do EC2 Fast Launch.

Causa

Você atingiu o número máximo de VPCs permitidas em sua Conta da AWS para a região e não especificou uma VPC existente para o EC2 Fast Launch usar. Isso causa a falha do processo.

Solução

Você pode resolver o problema com uma das seguintes opções:

- Você pode solicitar um aumento da cota
- Você pode fornecer um modelo de inicialização que especifique uma VPC existente

Para solicitar um aumento no número de VPCs que a conta pode definir por região, siga estas etapas:

1. Abra o console Service Quotas em https://console.aws.amazon.com/servicequotas/.
2. No Painel do console do serviço, escolha Amazon Virtual Private Cloud (Amazon VPC). Isso abre as cotas de serviço da VPC.
3. Filtre por `VPCs per Region` para ir diretamente para a cota.
4. Selecione VPCs por região e escolha Solicitar aumento no nível da conta.

Se você tiver uma solicitação de cota urgente ou se sua solicitação de aumento de cota for negada, entre em contato com o Suporte para obter ajuda. Para obter mais informações, consulte Solicitando um Aumento de Cota no Guia do Usuário do Service Quotas.

Permissões insuficientes para habilitar o EC2 Fast Launch

Descrição

Quando você ativa o EC2 Fast Launch a primeira vez sem especificar um modelo de inicialização, o EC2 Fast Launch cria uma pilha do CloudFormation de propriedade do serviço com os recursos padrão do serviço. Porém, os modelos do CloudFormation não serão implantados com sucesso se a entidade principal do IAM (perfil ou usuário) não tiver as permissões necessárias.

A mensagem do log pode algo ser assim:

```
Can't enable EC2 Fast Launch. The IAM credentials that you are using do not have
 sufficient permissions. Attach EC2FastLaunchFullAccess in the IAM console.
```

Causa

O usuário ou o perfil do IAM não têm as permissões necessárias para habilitar o EC2 Fast Launch.

Solução

Verifique se a entidade principal do IAM (usuário ou perfil) que habilita o EC2 Fast Launch tem a política de `EC2FastLaunchFullAccess` anexada. Essa política gerenciada pela AWS concede acesso total a todos os recursos do EC2 Fast Launch. Para visualizar as permissões dessa política, consulte a política EC2FastLaunchFullAccess na AWS Managed Policy Reference.

Alterar a senha de administrador do Windows da instância do Amazon EC2

Se você executar a instância de uma AMI do Windows da AWS, os agentes de execução pré-instalados definirão a senha padrão da seguinte forma:

- Para o Windows Server 2022 e versões posteriores, o EC2Launch v2 gera a senha padrão.
- Para o Windows Server 2016 e 2019, o agente EC2Launch gera a senha padrão.
- Para o Windows Server 2012 R2 e versões anteriores, o Serviço EC2Config gera a senha padrão.

> **Note**
>
> Para o Windows Server 2016 e AMIs posteriores, a opção `Password never expires` está desabilitada para o administrador local. Para as versões da AMI anteriores ao Windows Server 2016, a opção `Password never expires` está habilitada para o administrador local.

Alterar a senha de administrador após a conexão

Quando você se conectar a uma instância pela primeira vez, recomendamos alterar a senha de administrador de seu valor padrão. Use o procedimento a seguir para alterar a senha de administrador para uma instância do Windows.

> **Important**
>
> Armazene a nova senha em um lugar seguro. Você não poderá recuperar a nova senha usando o console do Amazon EC2. O console só pode recuperar a senha padrão. Se você

tentar se conectar à instância usando a senha padrão depois de alterá-la, será exibido o erro "Suas credenciais não funcionaram".

Para alterar a senha de administrador local

1. Conecte-se à instância e abra o prompt de comando.
2. Execute o seguinte comando. Se sua nova senha incluir caracteres especiais, coloque a senha entre aspas duplas.

```
net user Administrator "new_password"
```

3. Armazene a nova senha em um lugar seguro.

Alterar uma senha perdida ou expirada

Se a senha for perdida ou expirar, será possível gerar uma nova senha. Para obter os procedimentos de redefinição de senha, consulte Redefinir a senha de administrador do Windows para uma instância do Windows do Amazon EC2.

Adicionar componentes opcionais do Windows Server a instâncias do Windows do Amazon EC2

Para acessar e instalar os componentes adicionais, é necessário encontrar o snapshot do EBS correto para sua versão do Windows Server, criar um novo volume do snapshot e anexar o volume à sua instância.

Antes de começar

Use o Console de gerenciamento da AWS ou a ferramenta da linha de comando para obter o ID da instância e a zona de disponibilidade de sua instância. É necessário criar seu volume do EBS na mesma zona de disponibilidade de sua instância.

Use um dos procedimentos a seguir para adicionar componentes do Windows à instância.

Console

Para adicionar componentes do Windows à sua instância

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

2. No painel de navegação, selecione Snapshots.
3. Na barra Filter (Filtro), escolha Public Snapshots (Snapshots públicos).
4. Adicione o filtro Owner Alias (Alias de proprietário) e escolha amazon.
5. Adicione o filtro Description (Descrição) e insira **`Windows`**.
6. Pressione Enter
7. Selecione o snapshot que corresponde à arquitetura do sistema e seu idioma de preferência. Por exemplo, selecione Windows 2019 English Installation Media se sua instância estiver executando o Windows Server 2019.
8. Escolha Actions (Ações), Create volume from snapshot (Criar volume a partir do snapshot).
9. Para Availability Zone (Zona de disponibilidade), selecione a zona de disponibilidade que corresponde à instância do Windows. Escolha Add Tag (Adicionar tag) e insira **`Name`** para a chave de tag e um nome descritivo para o valor da tag. Escolha Create volume (Criar volume).
10. Na mensagem Volume Successfully Created (Volume criado com êxito, banner verde), escolha o volume que você acabou de criar.
11. Escolha Actions (Ações), Attach volume (Anexar volume).
12. Em Instance (Instância) selecione o ID da instância.
13. Em Device name (Nome do dispositivo), insira o nome do dispositivo para o anexo. Se precisar de ajuda com o nome do dispositivo, consulte Nomes de dispositivos para volumes em instâncias do Amazon EC2.
14. Selecione Attach volume (Anexar volume).
15. Conecte-se à sua instância e disponibilize o volume. Para obter mais informações, consulte Disponibilizar um volume do Amazon EBS para uso no Guia do usuário do Amazon EBS.

    > **Important**
    >
    > Não inicialize o volume.

16. Abra o Painel de Controle, Programas e Recursos. Escolha Ativar ou desativar recursos do Windows. Se for solicitado pela mídia de instalação, especifique o volume do EBS com a mídia instalação.
17. (Opcional) Ao terminar de usar a mídia de instalação, será possível desanexar o volume. Depois de desanexar o volume, será possível excluí-lo.

AWS CLI

Para adicionar componentes do Windows à sua instância

1. Use o comando describe-snapshots com o parâmetro `owner-ids` e o filtro `description` para obter uma lista dos snapshots de mídia de instalação disponíveis.

```
aws ec2 describe-snapshots \
    --owner-ids amazon \
    --filters Name=description,Values=Windows*
```

2. Na saída, observe o ID do snapshot que corresponde à arquitetura do sistema e seu idioma de preferência. Por exemplo:

```
{
    "Snapshots": [
    ...
        {
            "OwnerAlias": "amazon",
            "Description": "Windows 2019 English Installation Media",
            "Encrypted": false,
            "VolumeId": "vol-be5eafcb",
            "State": "completed",
            "VolumeSize": 6,
            "Progress": "100%",
            "StartTime": "2019-10-25T20:00:47.000Z",
            "SnapshotId": "snap-22da283e",
            "OwnerId": "123456789012"
        },
    ...
   ]
}
```

3. Use o comando create-volume para criar um volume do snapshot. Especifique a mesma zona de disponibilidade de sua instância.

```
aws ec2 create-volume \
    --snapshot-id snap-0abcdef1234567890 \
    --volume-type gp2 \
    --availability-zone us-east-1a
```

4. Na saída, observe o ID do volume.

```
{
    "AvailabilityZone": "us-east-1a",
    "Encrypted": false,
    "VolumeType": "gp2",
    "VolumeId": "vol-01234567890abcdef",
    "State": "creating",
    "Iops": 100,
    "SnapshotId": "snap-0abcdef1234567890",
    "CreateTime": "2017-04-18T10:33:10.940Z",
    "Size": 6
}
```

5. Use o comando attach-volume para associar o volume à sua instância.

```
aws ec2 attach-volume \
    --volume-id vol-0c98b37f30bcbc290 \
    --instance-id i-01474ef662b89480 \
    --device xvdg
```

6. Conecte-se à sua instância e disponibilize o volume. Para obter mais informações, consulte Disponibilizar um volume do Amazon EBS para uso no Guia do usuário do Amazon EBS.

> **Important**
>
> Não inicialize o volume.

7. Abra o Painel de Controle, Programas e Recursos. Escolha Ativar ou desativar recursos do Windows. Se for solicitado pela mídia de instalação, especifique o volume do EBS com a mídia instalação.
8. (Opcional) Ao terminar de usar a mídia de instalação, use o comando detach-volume para desanexar o volume da instância. Depois de desanexar o volume, é possível usar o comando delete-volume para excluir o volume.

PowerShell

Para adicionar componentes do Windows à sua instância

1. Use o cmdlet Get-EC2Snapshot com os filtros `Owner` e `description` para obter uma lista dos snapshots de mídia de instalação disponíveis.

```
Get-EC2Snapshot `
    -Owner amazon `
    -Filter @{ Name="description"; Values="Windows*" }
```

2. Na saída, observe o ID do snapshot que corresponde à arquitetura do sistema e seu idioma de preferência. Por exemplo:

```
...
DataEncryptionKeyId :
Description         : Windows 2019 English Installation Media
Encrypted           : False
KmsKeyId            :
OwnerAlias          : amazon
OwnerId             : 123456789012
Progress            : 100%
SnapshotId          : snap-0abcdef1234567890
StartTime           : 10/25/2019 8:00:47 PM
State               : completed
StateMessage        :
Tags                : {}
VolumeId            : vol-01234567890abcdef
VolumeSize          : 6
...
```

3. Use o cmdlet New-EC2Volume para criar um volume do snapshot. Especifique a mesma zona de disponibilidade de sua instância.

```
New-EC2Volume `
    -AvailabilityZone us-east-1a `
    -VolumeType gp2 `
    -SnapshotId snap-0abcdef1234567890
```

4. Na saída, observe o ID do volume.

```
Attachments      : {}
AvailabilityZone : us-east-1a
CreateTime       : 4/18/2017 10:50:25 AM
Encrypted        : False
Iops             : 100
KmsKeyId         :
Size             : 6
SnapshotId       : snap-0abcdef1234567890
```

```
State            : creating
Tags             : {}
VolumeId         : vol-01234567890abcdef
VolumeType       : gp2
```

5. Use o cmdlet Add-EC2Volume para associar o volume à sua instância.

```
Add-EC2Volume `
    -InstanceId i-1234567890abcdef0 `
    -VolumeId vol-01234567890abcdef `
    -Device xvdh
```

6. Conecte-se à sua instância e disponibilize o volume. Para obter mais informações, consulte Disponibilizar um volume do Amazon EBS para uso no Guia do usuário do Amazon EBS.

> **Important**
>
> Não inicialize o volume.

7. Abra o Painel de Controle, Programas e Recursos. Escolha Ativar ou desativar recursos do Windows. Se for solicitado pela mídia de instalação, especifique o volume do EBS com a mídia instalação.
8. (Opcional) Ao terminar de usar a mídia de instalação, use o cmdlet Dismount-EC2Volume para desanexar o volume da instância. Depois de desanexar o volume, é possível usar o cmdlet Remove-EC2Volume para excluir o volume.

Instalar o Windows Subsystem para Linux na instância do Windows do EC2

O Subsistema do Windows para Linux (WSL) é um recurso do Microsoft Windows. Ao instalar o WSL na instância do Windows do EC2, você pode executar ferramentas nativas do Linux diretamente na instância do Windows.

Há duas versões do Subsistema do Windows para Linux (WSL): WSL 1 e WSL 2. Para obter mais informações, consulte Documentação do Subsistema do Windows para Linux no site da Microsoft.

Requisitos

- O sistema operacional deve ser o Windows Server 2019 ou posterior.
- Você só pode instalar o WSL 1 em instâncias virtualizadas do Windows (o tamanho da instância não é `.metal` ou não é compatível com a virtualização aninhada).

- Você pode instalar o WSL 1 ou o WSL 2 em instâncias que oferecem suporte à virtualização aninhada e têm a opção de `NestedVirtualization` da CPU habilitada.
- Você pode instalar o WSL 1 ou o WSL 2 em instâncias bare metal (o tamanho da instância é `.metal`). As instâncias bare metal fornecem o suporte necessário para a virtualização aninhada por padrão.

Para obter mais informações sobre virtualização aninhada para EC2, consulte Use a virtualização aninhada para executar hipervisores em instâncias do Amazon EC2.

Instale o WSL em sua instância do Windows

Para instalar o WSL 1

1. Instale o WSL. O processo usado depende da versão do Windows Server que sua instância estiver executando.
   - Windows Server 2022 e posterior: execute o comando de instalação padrão a seguir na instância do EC2.

     ```
     wsl --install --enable-wsl1 --no-launch
     ```

   - Windows Server 2019: habilite o WSL e depois instale-o conforme descrito em Instalar o WSL em versões anteriores do Windows Server no site da Microsoft.
2. Reinicie sua instância do EC2.

   ```
   shutdown -r -t 20
   ```

3. Para configurar o WSL a usar o WSL 1, execute o comando a seguir na sua instância. Esta etapa é necessária para instâncias virtualizadas (o tamanho da instância não é `.metal` ou não está configurada para virtualização aninhada).

   ```
   wsl --set-default-version 1
   ```

4. Instale a distribuição padrão.

   ```
   wsl --install
   ```

Para instalar o WSL 2 (.metal ou instâncias com virtualização aninhada habilitada)

Execute o comando de instalação padrão a seguir na instância do EC2. O WSL 2 é instalado por padrão.

```
wsl --install
```

Utilitários de solução de problemas de problemas do EC2

O driver `EC2WinUtil` fornece os seguintes tipos de suporte à solução de problemas para sua instância do Windows.

Pilhas de chamadas interrompidas

`EC2WinUtil` coleta informações básicas sobre falhas da sua instância e as grava no console serial. A lista a seguir inclui alguns dos principais detalhes que o utilitário grava no console.

- Identificação do módulo que gerou a falha.
- O código de erro do Windows associada ao evento.
- Um rastreamento da pilha das chamadas mais recentes.

Com esses detalhes, você pode realizar uma análise inicial da causa raiz e determinar se é necessária uma análise adicional. A saída para o console serial também permite que o AWS rastreie tendências de interrupção para drivers do Amazon EC2 e diagnostique eventos de interrupção em grande escala.

> **Note**
>
> O `EC2WinUtil` não coleta nenhum dado do cliente em suas pilhas de chamadas interrompidas.

Hibernar/retomar a estabilidade

O `EC2WinUtil` rastreia as configurações de virtualização da instância em todos os ciclos de hibernação/retomada. Isso ajuda a melhorar a estabilidade de longo prazo das instâncias que permitiram a hibernação.

Para obter as notas de release do driver, consulte Histórico de versões do EC2 Windows Utility Driver.

Histórico de versões do EC2 Windows Utility Driver

A tabela a seguir mostra quais drivers `EC2WinUtil` são executados em cada versão do Windows Server no Amazon EC2. As versões anteriores do sistema operacional usam o driver pré-instalado nas AWS AMIs do Windows Server das quais a instância foi executada. As AMIs que são compartilhadas com você ou que você assina pelo AWS Marketplace não têm o driver pré-instalado.

Versão Windows Server	Versão do driver EC2WinUtil
Windows Server 2025	versão mais recente
Windows Server 2022	versão mais recente
Windows Server 2019	versão mais recente
Windows Server 2016	versão mais recente

> **Note**
>
> Antes da versão 3.0.0, o driver `EC2WinUtil` não estava disponível para download para instalação manual. As versões anteriores estavam disponíveis apenas como drivers pré-instalados para AWS AMIs do Windows.

A tabela a seguir descreve as versões lançadas do driver `EC2WinUtil`.

Versão do pacote	Versão do driver	Detalhes	Data de lançamento
3.1.0	3.1.0	Tratamento aprimorado de eventos de gerenciamento de energia.	4 de fevereiro de 2026
3.0.0	3.0.0	O driver para o Windows 10 foi modernizado e agora há suporte para instalação como um driver primitivo.	13 de junho de 2024

Versão do pacote	Versão do driver	Detalhes	Data de lançamento
2.0.0	2.0.0	Foi adicionado suporte para saída em portas seriais MMIO para tipos de instâncias metálicas. A análise de falhas também foi aprimorada e o formato de saída atualizado.	23 de agosto de 2018
1.0.1	1.0.1	O nome do driver foi alterado para `EC2WinUtil` devido a um conflito de namespace com o Amazon Inspector. Várias correções de bugs estão incluídas.	1º de março de 2018
1.0.0	1.0.0	Versão inicial. O driver era inicialmente chamado de `AwsAgent`.	28 de novembro de 2017

Atualizar uma instância do Windows do EC2 para uma versão mais recente do Windows Server

Se estiver na hora de atualizar o sistema operacional Windows Server na instância do Windows do EC2 de uma versão anterior, você pode usar um dos métodos a seguir.

Atualização no local

Uma atualização local opera em uma instância existente. Somente os arquivos do sistema operacional são afetados durante esse processo, enquanto suas configurações, perfis de servidor e dados permanecem intactos.

Migração (também conhecida como atualização lado a lado)

A migração envolve a captura de configurações, as configurações, os dados e a portabilidade dos mesmos para um sistema operacional mais recente em uma nova instância do Windows do EC2. É possível inicializar a instância em uma AMI pública ou privada do Windows que você assina no AWS Marketplace ou em uma AMI compartilhada com você. Você também pode criar uma AMI personalizada com o EC2 Image Builder. Para obter mais informações, consulte o Guia do usuário do Image Builder.

> **Note**
>
> A AWS fornece um conjunto de Imagens de máquina da Amazon (AMI) disponíveis publicamente para versões do Windows Server que são executadas em instâncias do EC2. Essas AMIs são atualizadas mensalmente. Para obter informações sobre as AMIs mais recentes do Windows, consulte a AWS Windows AMI Reference.

A Microsoft recomenda tradicionalmente a migração para uma versão mais recente do Windows Server em vez de atualizá-la no local. A migração pode resultar em menos erros ou problemas de atualização, mas pode demorar mais do que uma atualização no local devido à necessidade de provisionar uma nova instância, planejar e fazer a portabilidade de aplicações e ajustar as configurações na nova instância. Uma atualização local pode ser mais rápida, mas incompatibilidades de software podem produzir erros.

Conteúdo

- Executar uma atualização no local na instância do Windows do EC2
- Usar runbooks de automação para atualizar uma instância do Windows do EC2
- Migrar uma instância do EC2 Windows para um tipo de instância baseada em Nitro
- Solucionar problemas de atualização de um sistema operacional em uma instância do Windows do EC2

Executar uma atualização no local na instância do Windows do EC2

Para executar uma atualização local, é necessário determinar quais drivers de rede a instância está executando. Os drivers de rede PV permitem que você acesse sua instância usando o Desktop Remoto. As instâncias usam drivers PV da AWS, do adaptador de rede Intel ou da rede avançada. Para obter mais informações, consulte Drivers paravirtuais para as instâncias do Windows.

Antes de iniciar uma atualização no local

Execute as seguintes tarefas e observe os seguintes detalhes importantes antes de começar a atualização local.

- Leia a documentação da Microsoft para compreender os requisitos de atualização, os problemas conhecidos e as restrições. Além disso, leia as instruções oficiais de atualização.
  - Opções de atualização para Windows Server 2012

  - Opções de atualização para Windows Server 2012 R2
  - Opções de atualização e conversão para Windows Server 2016 e superior
  - Atualizações do Windows Server
- Recomendamos a execução de uma atualização do sistema operacional em instâncias com pelo menos 2 vCPUs e 4 GB de RAM. Se necessário, é possível alterar a instância para um tamanho maior do mesmo tipo (t2.small para t2.large, por exemplo), executar a atualização e redimensioná-la de volta para o tamanho original. Se você precisar manter o tamanho da instância, poderá monitorar o progresso usando o instance console screenshot. Para obter mais informações, consulte Alterações no tipo de instância do Amazon EC2.
- Verifique se o volume raiz de sua instância do Windows tem espaço em disco suficiente. O processo de configuração do Windows poderá não avisá-lo sobre espaço em disco insuficiente. Para obter informações sobre a quantidade de espaço em disco que é necessária para atualizar um sistema operacional específico, consulte a documentação da Microsoft. Se o volume não tiver espaço suficiente, é possível expandi-lo. Para obter mais informações, consulte Volumes Elásticos do Amazon EBS no Guia do usuário do Amazon EBS.
- Determine seu caminho de atualização. É necessário atualizar o sistema operacional para a mesma arquitetura. Por exemplo, atualize um sistema de 32 bits para um sistema de 32 bits. O Windows Server 2008 R2 e posterior são apenas 64 bits.
- Desabilite o software antivírus e antispyware e os firewalls. Esses tipos de software podem entrar em conflito com o processo de atualização. Habilite novamente o software antivírus e antispyware e os firewalls quando a atualização for concluída.
- Atualize para os drivers mais recentes, conforme descrito em Migrar uma instância do EC2 Windows para um tipo de instância baseada em Nitro.
- O Upgrade Helper Service só oferece suporte a instâncias que estejam executando drivers Citrix PV. Se a instância estiver executando drivers Red Hat, atualize manualmente esses drivers primeiro.

Atualizar uma instância no local com AWS PV, adaptador de rede Intel ou drivers de rede avançada

Use o seguinte procedimento para atualizar uma instância do Windows Server usando AWS PV, adaptador de rede Intel ou drivers de rede avançada.

Para executar a atualização local

1. Crie uma AMI do sistema que você planeja atualizar para fins de backup ou teste. Em seguida, é possível fazer a atualização na cópia a fim de simular um ambiente de teste. Se a atualização for concluída, será possível alternar o tráfego para essa instância com um período de inatividade curto. Se ocorrer falha na atualização, será possível reverter para o backup. Para obter mais informações, consulte Criação de uma AMI baseada no Amazon EBS.
2. Verifique se a instância do Windows Server está usando os drivers de rede mais recentes.
   a. Para atualizar seu driver do AWS PV, consulte Atualizar drivers PV em instâncias do Windows do EC2.
   b. Para atualizar seu driver do ENA, consulte Instalar o driver do ENA em instâncias do Windows do EC2.
   c. Para atualizar seus drivers da Intel, consulte Habilitar redes aperfeiçoadas com a interface Intel 82599 VF.
3. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
4. No painel de navegação, escolha Instances (Instâncias). Localize a instância. Anote o ID da instância e o ID da zona de disponibilidade da instância. Você precisará dessas informações mais tarde neste procedimento.
5. Se você estiver atualizando do Windows Server 2012 ou 2012 R2 para o Windows Server 2016 ou posterior, siga os procedimentos a seguir na instância antes de continuar.
   a. Desinstale o serviço EC2Config. Para obter mais informações, consulte Administração do Serviço do Windows para agentes do EC2Launch v2 e EC2Config.
   b. Instale o EC2Launch v1 ou o agente EC2Launch v2. Para mais informações, consulte Usar o agente do EC2Launch v1 para realizar tarefas durante a execução da instância EC2 Windows e Usar o agente do EC2Launch v2 para realizar tarefas durante a execução da instância EC2 Windows.
   c. Instalar o SSM Agent do AWS Systems Manager. Para obter mais informações, consulte Instalar manualmente o SSM Agent no Amazon EC2 para Windows Server, no Guia do usuário do AWS Systems Manager.
6. Crie um o novo volume de um snapshot de mídia de instalação do Windows Server.
   a. No painel de navegação à esquerda, em Elastic Block Store, escolha Snapshots.
   b. Na barra do filtro, escolha Snapshots públicos.
   c. Na barra de pesquisa, especifique os seguintes filtros:

- Escolha Alias do proprietário, depois = e depois amazon.
- Escolha Descrição e comece a digitar **`Windows`**. Selecione o filtro do Windows que corresponde à arquitetura do sistema e à preferência de idioma para as quais você está fazendo a atualização. Por exemplo, escolha Windows 2019 English Installation Media para fazer a atualização para o Windows Server 2019.

d. Marque a caixa de seleção ao lado do snapshot que corresponde à arquitetura do sistema e à preferência de idioma para a qual você está fazendo a atualização e, em seguida, escolha Ações, Criar volume com base no snapshot.

e. Na página Criar volume, escolha a zona de disponibilidade que corresponde à instância do Windows e escolha Criar volume.

7. No banner Volume vol-***`1234567890example`*** criado com êxito na parte superior da página, escolha o ID do volume que você acabou de criar.
8. Escolha Actions (Ações), Attach volume (Anexar volume).
9. Na página Anexar volume, em Instância, selecione o ID da instância do Windows e, em seguida, escolha Anexar volume.
10. Disponibilize o novo volume para uso ao seguir as etapas apresentadas em Make an Amazon EBS volume available for use.

> **Important**
>
> Não inicialize o disco porque isso excluirá os dados existentes.

11. No Windows PowerShell, mude para a nova unidade de volume. Comece a atualização abrindo o volume de mídia de instalação que você anexou à instância.

a. Se você estiver fazendo a atualização para o Windows Server 2016 ou posterior, execute o seguinte:

```
.\setup.exe /auto upgrade /dynamicupdate disable
```

> **Note**
>
> Executar setup.exe com a opção `/dynamicupdate` definida como desabilitada impede que o Windows instale atualizações durante o processo de upgrade do Windows Server, pois a instalação de atualizações durante o upgrade pode causar

falhas. É possívelrá instalar atualizações com o Windows Update após a conclusão do upgrade.

Se você estiver fazendo a atualização para uma versão anterior do Windows Server, execute o seguinte:

```
Sources\setup.exe
```

b. Em Selecionar o sistema operacional que deseja instalar, selecione a opção de instalação completa da instância do Windows Server e escolha Avançar.

c. Em Which type of installation do you want? (Qual tipo de instalação deseja?), escolha Upgrade (Atualizar).

d. Assista todo o assistente.

A configuração do Windows Server copia e processa os arquivos. Após alguns minutos, sua sessão do Remote Desktop será encerrada. O tempo necessário para concluir a atualização depende do número de aplicações e das funções de servidor em execução na instância do Windows Server. O processo de atualização pode levar 40 minutos ou várias horas. A instância poderá falhar em uma ou mais verificações de status durante o processo de atualização. Quando a atualização for concluída, todas as verificações de status serão concluídas com êxito. É possível verificar no log do sistema a saída do console ou usar as métricas do Amazon CloudWatch para a atividade do disco e da CPU a fim de determinar se a atualização está em andamento.

> **Note**
>
> Se você estiver fazendo a atualização para o Windows Server 2019, depois que a atualização for concluída, será possível alterar a tela de fundo do desktop manualmente para remover o nome do sistema operacional anterior, se desejado.

Se a instância não passou em todas as verificações de status após várias horas, consulte Solucionar problemas de atualização de um sistema operacional em uma instância do Windows do EC2.

Tarefas de pós-atualização

1. Inicie a sessão na instância para iniciar uma atualização do .NET Framework e reinicializar o sistema quando solicitado.
2. Se ainda não tiver feito isso em uma etapa anterior, instale o agente do EC2Launch v1 ou do EC2Launch v2. Para mais informações, consulte Usar o agente do EC2Launch v1 para realizar tarefas durante a execução da instância EC2 Windows e Usar o agente do EC2Launch v2 para realizar tarefas durante a execução da instância EC2 Windows.
3. Se você fez a atualização para o Windows Server 2012 R2, recomendamos atualizar os drivers PV para drivers AWS PV. Caso tenha atualizado em uma instância baseada em Nitro, recomendamos a instalação ou atualização dos drivers NVME e ENA. Para ter mais informações, consulte AWSDrivers NVMe ou Habilitar redes avançadas no Windows.
4. Habilite novamente o software antivírus e antispyware e os firewalls.

Usar runbooks de automação para atualizar uma instância do Windows do EC2

É possível executar uma atualização automatizada de suas instâncias do Windows e do SQL Server na AWS com runbooks do AWS Systems Manager Automation.

Conteúdo

- Serviços relacionados
- Opções de execução
- Atualizar o Windows Server
- Atualizar o SQL Server

Serviços relacionados

Os seguintes serviços da AWS são usados no processo de atualização automatizada:

- AWS Systems Manager. O AWS Systems Manager é uma interface poderosa e unificada para gerenciar centralmente seus recursos da AWS. Para obter mais informações, consulte o Guia do usuário do AWS Systems Manager.
- O AWS Systems Manager Agent (SSM Agent) é um software da Amazon que pode ser instalado e configurado em uma instância do Amazon EC2, em um servidor on-premises ou em uma máquina

virtual (VM). O SSM Agent permite que o Systems Manager atualize, gerencie e configure esses recursos. O agente processa as solicitações do serviço do Systems Manager na Nuvem AWS e as executa conforme especificado na solicitação. Para obter mais informações, consulte Trabalho com o SSM Agent no Guia do usuário do AWS Systems Manager.

- Runbooks do AWS Systems Manager SSM. Um runbook do SSM define as ações que o Systems Manager realiza nas suas instâncias gerenciadas. Os runbooks do SSM usam JavaScript Object Notation (JSON) ou YAML e incluem etapas e parâmetros especificados por você. Esse tópico usa dois runbooks do SSM do Systems Manager para automação. Para obter mais informações, consulte Referência de runbook do AWS Systems Manager Automation no Guia do usuário do AWS Systems Manager.

Opções de execução

Ao selecionar Automation (Automação) no console do Systems Manager, selecione Execute (Executar). Depois de selecionar um documento de automação, você será solicitado a escolher uma opção de execução da automação. É possível escolher entre as opções a seguir. Nas etapas dos caminhos fornecidos neste tópico, usamos a opção Simple execution (Execução simples).

Execução simples

Escolha esta opção se deseja atualizar uma única instância, mas não deseja passar por cada etapa de automação para auditar os resultados. Tal opção é explicada com mais detalhes nas etapas de atualização a seguir.

Rate control (Controle de taxa)

Escolha esta opção se você deseja aplicar a atualização a mais de uma instância. Defina as configurações a seguir.

- Parâmetro

  Essa configuração, que também é definida nas configurações Multi-Account and Region (Várias contas e região), define como sua automação se expande.

- Destinos

  Selecione o destino ao qual você deseja aplicar a automação. Essa configuração também é definida nas configurações Multi-Account and Region (Várias contas e região).

- Valores de parâmetros

Use os valores definidos nos parâmetros do documento de automação.

- Grupo de recursos

  Na AWS , um recurso é uma entidade com a qual é possível trabalhar. Os exemplos incluem instâncias do Amazon EC2, pilhas do AWS CloudFormation ou buckets do Amazon S3. Se você trabalha com vários recursos, pode ser útil gerenciá-los como um grupo, em vez de migrar de um serviço da AWS para outro em todas as tarefas. Em alguns casos, é possível querer gerenciar um grande número de recursos relacionados, como instâncias do EC2 que compõem uma camada de aplicação. Nesse caso, você provavelmente precisará realizar ações em massa nesses recursos ao mesmo tempo.

- Tags

  As tags ajudam a categorizar os recursos da AWS de diferentes maneiras, como por finalidade, por proprietário ou por ambiente. Essa categorização é útil quando você tem muitos recursos do mesmo tipo. É possível identificar rapidamente um recurso específico usando as tags atribuídas.

- Rate Control (Controle de taxa)

  A opção Rate Control (Controle de taxa) também é definida nas configurações Multi-Account and Region (Várias contas e região). Ao definir os parâmetros de controle de taxa, você define a quanto da sua frota a automação será aplicada, seja por contagem de alvos ou por porcentagem da frota.

Multi-Account and Region (Várias contas e região)

Além dos parâmetros especificados em Rate Control (Controle de taxa), que também são usados nas configurações Multi-Account and Region (Várias contas e região), há duas configurações adicionais:

- Contas e unidades organizacionais (UOs)

  Especifique várias contas nas quais você deseja executar a automação.

- Regiões da AWS

  Especifique várias Regiões da AWS nas quais você deseja executar a automação.

Execução manual

Esta opção é semelhante a Simple execution (Execução simples), mas permite percorrer cada etapa de automação e auditar os resultados.

Atualizar o Windows Server

O runbook `AWSEC2-CloneInstanceAndUpgradeWindows` cria uma imagem de máquina da Amazon (AMI) usando uma instância do Windows Server na sua conta e atualiza essa AMI para uma versão com suporte de sua escolha. Esse processo com diversas etapas pode levar até duas horas para ser concluído.

Existem duas AMIs incluídas no processo de atualização automatizada:

- Instância atual em execução. A primeira AMI é a instância em execução atual, que não é atualizada. Essa AMI é usada para iniciar outra instância para executar a atualização no local. Quando o processo é concluído, essa AMI é excluída da sua conta, a menos que você solicite especificamente que a instância original seja mantida. Essa configuração é tratada pelo parâmetro `KeepPreUpgradeImageBackUp` (o valor padrão é `false`, o que significa que a AMI é excluída por padrão).
- AMI atualizada. Esta AMI é o resultado do processo de automação.

O resultado final é uma AMI, que é a instância atualizada da AMI.

Quando a atualização estiver concluída, será possível testar a funcionalidade da sua aplicação iniciando a nova AMI na sua Amazon VPC. Depois de concluir o teste e antes de executar outra atualização, programe o tempo de inatividade da aplicação antes de mudar completamente para a instância atualizada.

Pré-requisitos

Para automatizar a atualização do seu Windows Server com o documento do AWS Systems Manager Automation, é necessário executar as seguintes tarefas:

- Criar uma função do IAM com as políticas do IAM especificadas para permitir que o Systems Manager execute tarefas de automação nas suas instâncias do Amazon EC2 e verifique se você atende aos pré-requisitos para usar o Systems Manager. Para obter mais informações, consulte Criação de uma função para delegar permissões a um serviço da AWS no Guia do usuário do AWS Identity and Access Management.
- Selecione a opção de como você deseja que a automação seja executada. As opções para execução são Simple execution (Execução simples), Rate control (Controle de taxa), Multi-account

and Region (Várias contas e região) e Manual execution (Execução manual). Para obter mais informações sobre essas opções, consulte Opções de execução.

- Verifique se o SSM Agent está instalado na sua instância. Para obter mais informações, consulte Instalação e configuração do SSM Agent em instâncias do Amazon EC2 no Windows Server.
- O Windows PowerShell 3.0 ou posterior deve ser instalado em sua instância.
- Para instâncias ingressadas em um domínio do Microsoft Active Directory, é recomendável especificar um `SubnetId` que não tenha conectividade com seus controladores de domínio para ajudar a evitar conflitos de nome de host.
- A sub-rede da instância deve ter conectividade de saída com a Internet, o que fornece acesso a Serviços da AWS, como o Amazon S3, e acesso para baixar correções da Microsoft. Esse requisito será atendido se a sub-rede for pública e a instância tiver um endereço IP público ou se a sub-rede for uma sub-rede privada com uma rota que envie o tráfego da Internet para um dispositivo NAT público.
- Essa automação funciona com instâncias que executam o Windows Server 2008 R2, o Windows Server 2012 R2, o Windows Server 2016 e o Windows Server 2019.
- Verifique se a instância tem 20 GB de espaço livre em disco no disco de inicialização.
- Se a instância não usar uma licença do Windows fornecida pela AWS, especifique um ID de snapshot do Amazon EBS que inclua a mídia de instalação do Windows Server 2012 R2. Para fazer isso:
  1. Verifique se a instância do Amazon EC2 está executando o Windows Server 2012 ou posterior.
  2. Crie um volume do Amazon EBS de 6 GB na mesma zona de disponibilidade em que a instância está sendo executada. Associe o volume à instância. Instale-a, por exemplo, como unidade D.
  3. Clique com o botão direito do mouse no ISO e instale-o a uma instância como, por exemplo, unidade E.
  4. Copie o conteúdo do ISO da unidade E:\ para a unidade D:\
  5. Crie um snapshot do Amazon EBS do volume de 6 GB criado na etapa 2 acima.

Limitações de atualização do Windows Server

Essa automação não oferece suporte para a atualização de controladores de domínio do Windows, clusters ou sistemas operacionais de desktop do Windows. Além disso, essa automação não oferece suporte a instâncias do Amazon EC2 para Windows Server com as seguintes funções instaladas:

- Host de sessão de área de trabalho remota (RDSH)

- Agente de conexão de área de trabalho remota (RDCB)
- Host de virtualização de área de trabalho remota (RDVH)
- Acesso via Web à Área de Trabalho Remota (RDWA)

Etapas para executar uma atualização automatizada do Windows Server

Siga estas etapas para atualizar sua instância do Windows Server usando o runbook de automação AWSEC2-CloneInstanceAndUpgradeWindows.

1. Abra o Systems Manager no Console de Gerenciamento da AWS.
2. No painel de navegação à esquerda, em Change Management (Gerenciamento de alterações), escolha Automation (Automação).
3. Escolha Execute automation.
4. Procure o documento de automação chamado `AWSEC2-CloneInstanceAndUpgradeWindows`.
5. Quando o nome do documento aparecer, selecione-o. Ao selecioná-lo, os detalhes do documento aparecerão.
6. Selecione Execute automation (executar automação) para introduzir os parâmetros desse documento. Deixe Simple execution (Execução simples) selecionada na parte superior da página.
7. Insira os parâmetros solicitados com base na orientação a seguir.

   - `InstanceID`

     Tipo: string

     (Obrigatório) A instância que executa o Windows Server 2008 R2, 2012 R2, 2016 or 2019 w com o SSM Agent instalado.

   - `InstanceProfile`.

     Tipo: string

     (Obrigatório) O perfil da instância do IAM. Essa é a função do IAM usada para executar a automação do Systems Manager em relação à instância do Amazon EC2 e às AMIs da AWS. Para obter mais informações, consulte Configurar permissões de instância do EC2 no Guia do usuário do AWS Systems Manager.

- `TargetWindowsVersion`

  Tipo: string

  (Obrigatório) Selecione a versão de destino do Windows.

- `SubnetId`

  Tipo: string

  (Obrigatório) Esta é a sub-rede do processo de atualização e onde reside sua instância de origem do EC2. Verifique se a sub-rede tem conectividade de saída para serviços da AWS, incluindo o Amazon S3 e também para a Microsoft (para fazer download de patches).

- `KeepPreUpgradedBackUp`

  Tipo: string

  (Opcional) Se esse parâmetro estiver definido como `true`, a automação retém a imagem criada a partir da instância. A configuração padrão é `false`.

- `RebootInstanceBeforeTakingImage`

  Tipo: string

  (Opcional) O padrão é `false` (sem reinicialização). Se esse parâmetro estiver configurado como `true`, o Systems Manager reinicializará a instância antes de criar uma AMI para a atualização.

8. Depois de inserir os parâmetros, selecione Execute (Executar). Quando a automação começar, será possível monitorar o progresso da execução.
9. Quando a automação for concluída, você verá o ID da AMI. É possível iniciar a AMI para verificar se o sistema operacional Windows está atualizado.

> **Note**
>
> Não é necessário que a automação execute todas as etapas. As etapas são condicionais com base no comportamento da automação e da instância. O Systems Manager pode pular algumas etapas que não são obrigatórias.
> Além disso, algumas etapas podem expirar. O Systems Manager tenta atualizar e instalar todos os patches mais recentes. Às vezes, porém, os patches expiram com base em uma configuração de tempo limite definida para a etapa especificada. Quando isso

acontece, a automação do Systems Manager segue para a próxima etapa para garantir que o sistema operacional interno seja atualizado para a versão do Windows Server de destino.

10. Após a conclusão da automação, é possível iniciar uma instância do Amazon EC2 usando o ID da AMI para revisar sua atualização. Para obter mais informações sobre como criar uma instância do Amazon EC2 usando uma AMI da AWS, consulte Como iniciar uma instância do EC2 a partir de uma AMI personalizada?

Atualizar o SQL Server

O script AWSEC2-CloneInstanceAndUpgradeSQLServer cria uma AMI de uma instância do Amazon EC2 executando o SQL Server em sua conta e atualiza a AMI para uma versão posterior do SQL Server. Esse processo com diversas etapas pode levar até duas horas para ser concluído.

Nesse fluxo de trabalho, a automação cria uma AMI da instância e inicia a nova AMI na sub-rede que você fornecer. A automação, então, executa uma atualização local do SQL Server. Após a conclusão da atualização, a automação cria uma nova AMI antes de encerrar a instância atualizada.

Existem duas AMIs incluídas no processo de atualização automatizada:

- Instância atual em execução. A primeira AMI é a instância em execução atual, que não é atualizada. Essa AMI é usada para iniciar outra instância para executar a atualização no local. Quando o processo é concluído, essa AMI é excluída da sua conta, a menos que você solicite especificamente que a instância original seja mantida. Essa configuração é tratada pelo parâmetro `KeepPreUpgradeImageBackUp` (o valor padrão é `false`, o que significa que a AMI é excluída por padrão).
- AMI atualizada. Esta AMI é o resultado do processo de automação.

O resultado final é uma AMI, que é a instância atualizada da AMI.

Quando a atualização estiver concluída, será possível testar a funcionalidade da sua aplicação iniciando a nova AMI na sua Amazon VPC. Depois de concluir o teste e antes de executar outra atualização, programe o tempo de inatividade da aplicação antes de mudar completamente para a instância atualizada.

Pré-requisitos

Para automatizar a atualização do seu SQL Server com o documento do AWS Systems Manager Automation, é necessário executar as seguintes tarefas:

- Criar uma função do IAM com as políticas do IAM especificadas para permitir que o Systems Manager execute tarefas de automação nas suas instâncias do Amazon EC2 e verifique se você atende aos pré-requisitos para usar o Systems Manager. Para obter mais informações, consulte Criar um perfil para delegar permissões a um AWS service (Serviço da AWS) no Guia do usuário do AWS Identity and Access Management.
- Selecione a opção de como você deseja que a automação seja executada. As opções para execução são Simple execution (Execução simples), Rate control (Controle de taxa), Multi-account and Region (Várias contas e região) e Manual execution (Execução manual). Para obter mais informações sobre essas opções, consulte Opções de execução.
- A instância do Amazon EC2 deve usar o Windows Server 2008 R2 ou posterior and o SQL Server 2008 ou posterior.
- Verifique se o SSM Agent está instalado na sua instância. Para obter mais informações, consulte Trabalho com o SSM Agent em instâncias do Amazon EC2 para Windows Server.
- Verifique se a instância tem espaço em disco suficiente:
  - Se estiver atualizando do Windows Server 2008 R2 para o 2012 R2 ou do Windows Server 2012 R2 para um sistema operacional posterior, verifique se você tem 20 GB de espaço livre no disco de inicialização da instância.
  - Se estiver atualizando do Windows Server 2008 R2 para o 2016 ou posterior, verifique se a instância tem 40 GB de espaço livre no disco de inicialização da instância.
- Para instâncias que usam uma versão Traga sua própria licença (BYOL) do SQL Server, os seguintes pré-requisitos adicionais se aplicam:
  - Forneça um ID de snapshot do Amazon EBS que inclua a mídia de instalação do SQL Server desejado. Para fazer isso:
    1. Verifique se a instância do Amazon EC2 está executando o Windows Server 2008 R2 ou posterior.
    2. Crie um volume do Amazon EBS de 6 GB na mesma zona de disponibilidade em que a instância está sendo executada. Associe o volume à instância. Instale-a, por exemplo, como unidade D.
    3. Clique com o botão direito do mouse no ISO e instale-o a uma instância como, por exemplo, unidade E.

4. Copie o conteúdo do ISO da unidade E:\ para a unidade D:\
5. Crie um snapshot do Amazon EBS do volume de 6 GB criado na etapa 2.

Limitações da atualização automatizada do SQL Server

As seguintes limitações se aplicam ao usar o runbook AWSEC2-CloneInstanceAndUpgradeSQLServer para realizar uma atualização automatizada:

- A atualização só pode ser realizada em um SQL Server usando a autenticação do Windows.
- Verifique se há atualizações de patch de segurança pendentes nas instâncias. Abra Control Panel (Painel de controle) e, em seguida, escolha Check for updates (Verificar atualizações).
- Implantações do SQL Server no modo HA e espelhamento não são compatíveis.

Etapas para executar uma atualização automatizada do SQL Server

Siga estas etapas para atualizar sua instância do SQL Server usando o runbook de automação AWSEC2-CloneInstanceAndUpgradeSQLServer.

1. Se isso ainda não foi feito, faça download do arquivo .iso do SQL Server 2016 e monte-o no servidor de origem.
2. Após a montagem do arquivo .iso, copie todos os arquivos do componente e coloque-os em qualquer volume de sua escolha.
3. Faça um snapshot do volume do Amazon EBS e copie o ID do snapshot em uma área de transferência para uso posterior. Para obter mais informações, consulte Create Amazon EBS snapshots no Guia do usuário do Amazon EBS.
4. Anexe o perfil da instância à instância de origem do Amazon EC2. Isso permite que o Systems Manager se comunique com a instância do EC2 e execute comandos nele depois que ele é adicionado ao serviço do AWS Systems Manager. Para esse exemplo, nomeamos a função `SSM-EC2-Profile-Role` com a política `AmazonSSMManagedInstanceCore` anexada à função.
5. No console do AWS Systems Manager, no painel de navegação à esquerda, selecione Managed Instances (Instâncias gerenciadas). Verifique se sua instância do EC2 está na lista de instâncias gerenciadas. Se você não vir a instância depois de alguns minutos, leia Onde estão minhas instâncias? no Guia do usuário do AWS Systems Manager.
6. No painel de navegação à esquerda, em Change Management (Gerenciamento de alterações), escolha Automation (Automação).

7. Escolha Execute automation.
8. Procure o documento de automação chamado `AWSEC2-CloneInstanceAndUpgradeSQLServer`.
9. Escolha documento do SSM `AWSEC2-CloneInstanceAndUpgradeSQLServer` e selecione Next (Avançar).
10. Verifique se a opção Simple execution (Execução simples) está selecionada.
11. Insira os parâmetros solicitados com base na orientação a seguir.

    - `InstanceId`

      Tipo: string

      (Obrigatório) A instância executando o SQL Server 2008 R2 (ou posterior).

    - `IamInstanceProfile`

      Tipo: string

      (Obrigatório) O perfil da instância do IAM.

    - `SQLServerSnapshotId`

      Tipo: string

      (Obrigatório) O ID do snapshot para a mídia de instalação do SQL Server de destino. Esse parâmetro não é necessário para instâncias incluídas na licença do SQL Server.

    - `SubnetId`

      Tipo: string

      (Obrigatório) Esta é a sub-rede do processo de atualização e onde reside sua instância de origem do EC2. Verifique se a sub-rede tem conectividade de saída para serviços da AWS, incluindo o Amazon S3 e também para a Microsoft (para fazer download de patches).

    - `KeepPreUpgradedBackUp`

      Tipo: string

      (Opcional) Se esse parâmetro estiver definido como `true`, a automação retém a imagem criada a partir da instância. A configuração padrão é `false`.

    - `RebootInstanceBeforeTakingImage`

Tipo: string

(Opcional) O padrão é `false` (sem reinicialização). Se esse parâmetro estiver configurado como `true`, o Systems Manager reinicializará a instância antes de criar uma AMI para a atualização.

- `TargetSQLVersion`

  Tipo: string

  (Opcional) A versão do SQL Server de destino. O padrão é `2016`.

12. Depois de inserir os parâmetros, selecione Execute (Executar). Quando a automação começar, será possível monitorar o progresso da execução.
13. Quando Execution status (Status de execução) mostrar Success (Sucesso), expanda Outputs (Saídas) para visualizar as informações da AMI. É possível usar o ID da AMI para iniciar sua instância do SQL Server para a VPC de sua escolha.
14. Abra o console do Amazon EC2. No painel de navegação à esquerda, selecione AMIs. É necessário ver a nova AMI.
15. Para verificar se a nova versão do SQL Server foi instalada com êxito, selecione a nova AMI e escolha Launch (Iniciar).
16. Escolha o tipo de instância que você deseja para a AMI, a VPC e a sub-rede que você deseja implantar e o armazenamento que deseja usar. Como você está lançando a nova instância de uma AMI, os volumes são apresentados como uma opção para incluir na nova instância do EC2 que você está executando. É possível remover qualquer um desses volumes ou adicionar volumes.
17. Adicione uma tag para ajudar você a identificar sua instância.
18. Adicione o grupo de segurança ou grupos à instância.
19. Escolha Launch Instance (Executar instância).
20. Escolha o nome da tag para a instância e selecione Connect (Conectar) no menu suspenso Actions (Ações).
21. Verifique se a nova versão do SQL Server é mecanismo de banco de dados na nova instância.

Migrar uma instância do EC2 Windows para um tipo de instância baseada em Nitro

As AMIs do Windows da AWS são configuradas com as definições padrão usadas pela mídia de instalação da Microsoft com algumas personalizações. As personalizações incluem drivers e configurações compatíveis com instâncias baseadas em Nitro, como M5 e C5.

Ao migrar de instâncias baseadas em Xen para instâncias baseadas em Nitro, inclusive instâncias bare metal, recomendamos seguir as etapas deste tópico nos seguintes casos:

- Se você estiver iniciando instâncias a partir de AMIs personalizadas do Windows
- Se você estiver iniciando instâncias a partir de AMIs do Windows fornecidas pela Amazon que foram criadas antes de agosto de 2018

Como alternativa, é possível usar o documento de automação do `AWSSupport-UpgradeWindowsAWSDrivers` para automatizar os procedimentos descritos em Parte 1, Parte 2 e Parte 3. Se você optar por usar o procedimento automatizado, consulte (Alternativa) Atualizar os drivers PV, ENA e NVMe da AWS usando o AWS Systems Manager e continue com a Parte 4 e a Parte 5.

Para obter mais informações, consulte Atualização do Amazon EC2 – tipos de instância adicionais, Sistema Nitro e opções de CPU.

> **Note**
>
> Os procedimentos de migração a seguir podem ser executados no Windows Server versão 2016 e posterior. As versões anteriores do sistema operacional que chegaram ao fim da vida útil não foram testadas e podem não ser compatíveis com os tipos de instância mais recentes.
> Para migrar instâncias Linux, consulte the section called “Alterações no tipo de instância”.

Sumário

- Parte 1: Instalar e atualizar drivers da AWS PV
- Parte 2: Instalar e atualizar ENA
- Parte 3: Atualizar drivers AWS NVMe

- Parte 4: Atualizar o EC2Config e o EC2Launch
- Parte 5: Instalar o driver de porta serial para instâncias bare metal
- Parte 6: Atualizar as configurações de gerenciamento de energia
- Parte 7: Atualizar drivers do chipset Intel para novos tipos de instância
- (Alternativa) Atualizar os drivers PV, ENA e NVMe da AWS usando o AWS Systems Manager

Antes de começar

Este procedimento pressupõe que você tenha uma instância baseada em Xen, como uma M4 ou C4, e esteja migrando para uma instância baseada em Nitro.

Use a versão 3.0 do PowerShell, ou posterior, para fazer a atualização com êxito.

> **Note**
>
> Ao migrar, as configurações de IP estático ou de DNS personalizado no cartão de interface de rede existente poderão ser perdidas uma vez que a instância será padronizada para um novo dispositivo de adaptador de redes aperfeiçoadas.

Antes de seguir as etapas neste procedimento, recomendamos que você crie um backup de instância. No Console EC2, escolha a instância que requer a migração, abra o menu de contexto (botão direito do mouse), escolha Estado da instância e Parar.

> **Warning**
>
> Quando você interrompe uma instância, os dados em todos os volumes de armazenamento de instâncias são apagados. Para preservar dados em volumes de armazenamento de instâncias, faça backup dos dados no armazenamento persistente.

Abra o menu de contexto (clique com o botão direito do mouse) da instância, no Console EC2, escolha Imagem, e depois escolha Criar imagem.

> **Note**
>
> As partes 4 e 5 destas instruções podem ser concluídas após a migração ou alteração do tipo de instância. No entanto, recomendamos que você as conclua antes da migração, especialmente se estiver migrando para um tipo de instância bare metal.

Parte 1: Instalar e atualizar drivers da AWS PV

Embora os drivers AWS PV não sejam utilizados no sistema Nitro, você ainda deve atualizá-los se você estiver em versões anteriores do Citrix PV ou AWS PV. Os drivers AWS PV mais recentes resolvem erros em versões anteriores dos drivers que podem aparecer enquanto você estiver no sistema Nitro, ou se você precisar migrar de volta a uma instância baseada em Xen. Como prática recomendada, recomendamos sempre atualizar os drivers mais recentes de instâncias do Windows na AWS.

Use o seguinte procedimento para executar uma atualização no local dos drivers AWS PV ou fazer uma atualização de drivers Citrix PV para drivers AWS PV no Windows Server 2008 R2, no Windows Server 2012, no Windows Server 2012 R2, no Windows Server 2016 ou no Windows Server 2019. Para obter mais informações, consulte Atualizar drivers PV em instâncias do Windows do EC2.

Para atualizar um controlador de domínio, consulte Atualizar um controlador de domínio (atualização do AWS PV).

Para executar uma atualização de drivers AWS PV

1. Conecte-se à instância usando o Remote Desktop e prepare a instância a ser atualizada. Deixe offline todos os discos que não sejam do sistema antes de executar a atualização. Essa etapa não será necessária se você executar uma atualização no local dos drivers AWS PV. Defina serviços não essenciais como inicialização Manual no console de Services.
2. Faça download do pacote de drivers mais recente na instância.
3. Extraia o conteúdo da pasta e execute `AWSPVDriverSetup.msi`.

Depois de executar o MSI, a instância é reinicializada automaticamente e, em seguida, atualiza o driver. A instância pode ficar indisponível por até 15 minutos.

Após o término da atualização e a instância passar nas duas verificações de integridade no console do Amazon EC2, conecte-se à instância usando o Remote Desktop e verifique se o novo driver foi

instalado. Em Device Manager (Gerenciador de dispositivos), em Storage Controllers (Controladores de armazenamento), localize AWS PV Storage Host Adapter (Adaptador host de armazenamento do PV). Verifique se a versão do driver é a mesma que a versão mais recente listada na tabela Histórico de versões do driver. Para obter mais informações, consulte Histórico do pacote de drivers AWS PV.

Parte 2: Instalar e atualizar ENA

Atualize para o driver Elastic Network Adapter mais recente para garantir todos os recursos de rede sejam aceitos. Se você executou a instância e ela não tiver a rede avançada habilitada, faça download e instale o driver do adaptador de rede obrigatório na instância. Depois, defina o atributo da instância enaSupport para ativar a rede avançada. Você somente poderá ativar esse atributo em tipos de instância suportados e somente se o driver ENA estiver instalado. Para obter mais informações, consulte Habilitar redes aperfeiçoadas com o ENA em instâncias do EC2.

1. Faça download do driver mais recente para a instância. Se você precisar de uma versão anterior do driver, consulte Histórico da versão do driver do ENA do Windows.
2. Extraia o arquivo zip.
3. Instale o driver executando o script de PowerShell `install.ps1` da pasta extraída.

   > **Note**
   >
   > Para evitar erros de instalação, execute o script `install.ps1` como um administrador.

4. Verifique se AMI tem enaSupport ativado. Em caso negativo, continue seguindo a documentação em Habilitar redes aperfeiçoadas com o ENA em instâncias do EC2.

Parte 3: Atualizar drivers AWS NVMe

Os drivers AWS NVMe são usados para interagir com volumes de armazenamento de instâncias de Amazon EBS e de SSD que são expostos como dispositivos de bloco de NVMe no sistema Nitro para melhor performance.

> **Important**
>
> As instruções a seguir são modificadas especificamente para quando você instala ou atualiza o AWS NVMe em uma instância baseada em Xen com a intenção de migrar a instância para um tipo de instância baseada em Nitro.

1. Faça download do pacote de drivers mais recente na instância.

   Se você precisar de uma versão anterior do driver, consulte Versões do driver NVMe para Windows para verificar as versões compatíveis.
2. Extraia o arquivo zip.
3. Instale o driver conforme descrito em `Readme.txt`.
4. Abra uma sessão do PowerShell e execute este comando:

   ```
   PS C:\> start rundll32.exe sppnp.dll,Sysprep_Generalize_Pnp -wait
   ```

   > **Note**
   >
   > Para aplicar o comando, é necessário executar a sessão do PowerShell como administrador. As versões do PowerShell (x86) resultarão em um erro.
   > Esse comando executa somente um sysprep em dispositivos do driver. Não executa uma preparação de sysprep completa.
5. Para o Windows Server 2008 R2 e o Windows Server 2012, encerre a instância, altere o tipo da instância e a inicie. Depois, prossiga para a Parte 4. Se você iniciar a instância novamente em um tipo de instância baseada em Xen antes de migrar para um tipo de instância baseada em Nitro, ela não será reiniciada. Para outras AMIs do Windows compatíveis, é possível alterar o tipo de instância a qualquer momento após o sysprep do dispositivo.

Parte 4: Atualizar o EC2Config e o EC2Launch

Para instâncias do Windows, os utilitários EC2Config e EC2Launch mais recentes fornecem funcionalidade e informações adicionais na execução em sistema Nitro, incluindo o Bare Metal EC2. Por padrão, o serviço EC2Config está incluído em AMIs anteriores ao Windows Server 2016. O EC2Launch substitui o EC2Config nas AMIs do Windows Server 2016 e posterior.

Quando os serviços EC2Config e EC2Launch forem atualizados, as novas AMIs do Windows da AWS incluirão a versão mais recente do serviço. Contudo, você precisa atualizar suas próprias instâncias e AMIs do Windows com a versão mais recente do EC2Config e EC2Launch.

Para instalar ou atualizar EC2Config

1. Faça download e descompacte o instalador do EC2Config.

2. Execute `EC2Install.exe`. Para uma lista completa de opções, execute `EC2Install` com a opção `/?`. Por padrão, a configuração exibe os prompts. Para executar o comando sem prompts, use a opção `/quiet`.

Para obter mais informações, consulte Instalar a versão mais recente do EC2Config.

Para instalar ou atualizar EC2Launch

1. Se você já tiver instalado e configurado o EC2Launch em uma instância, faça um backup do arquivo de configuração do EC2Launch. O processo de instalação não preserva as alterações feitas nesse arquivo. Por padrão, o arquivo está localizado no diretório `C:\ProgramData\Amazon\EC2-Windows\Launch\Config`.
2. Faça download do EC2-Windows-Launch.zip em um diretório na instância.
3. Faça download do install.ps1 no mesmo diretório onde você baixou o `EC2-Windows-Launch.zip`.
4. Execute `install.ps1`.

   > **Note**
   >
   > Para evitar erros de instalação, execute o script `install.ps1` como um administrador.

5. Se você fez um backup do arquivo de configuração do EC2Launch, copie-o no diretório `C:\ProgramData\Amazon\EC2-Windows\Launch\Config`.

Para obter mais informações, consulte Usar o agente do EC2Launch v1 para realizar tarefas durante a execução da instância EC2 Windows.

Parte 5: Instalar o driver de porta serial para instâncias bare metal

O tipo de instância `i3.metal` usa um dispositivo serial baseado em PCI em vez de um dispositivo serial baseado em porta de E/S. Os AMIs do Windows mais recentes automaticamente usam dispositivo de série baseado em PCI e tem o driver de porta serial instalados. Se você não estiver usando uma instância lançada de um AMI do Windows fornecido pela Amazon, datado de 11.04.2018 ou posterior, deverá instalar o Driver de porta serial para habilitar o dispositivo serial para recursos de EC2 como Geração de senha e Saída de console. Os utilitários EC2Config e EC2Launch mais recentes também suportam o i3.metal e fornecem funcionalidade adicional. Caso ainda não tenha feito, siga as etapas da Parte 4.

Para instalar o driver de porta serial

1. Faça download do pacote de drivers de série mais recente na instância.
2. Extraia o conteúdo da pasta, abra o menu de contexto (clique com o botão direito) em `aws_ser.INF` e selecione install (instalar).
3. Escolha OK.

Parte 6: Atualizar as configurações de gerenciamento de energia

A seguinte atualização das configurações de gerenciamento de energia definirá os vídeos para nunca desligarem, o que permite desligamentos normais do sistema operacional no sistema Nitro. Todas as AMIs do Windows fornecidas pela Amazon a partir de 2018.11.28 já têm essa configuração padrão.

1. Abra um prompt de comando ou uma sessão do PowerShell.
2. Execute os seguintes comandos:

```
powercfg /setacvalueindex 381b4222-f694-41f0-9685-ff5bb260df2e 7516b95f-
f776-4464-8c53-06167f40cc99 3c0bc021-c8a8-4e07-a973-6b14cbcb2b7e 0
powercfg /setacvalueindex 8c5e7fda-e8bf-4a96-9a85-a6e23a8c635c 7516b95f-
f776-4464-8c53-06167f40cc99 3c0bc021-c8a8-4e07-a973-6b14cbcb2b7e 0
powercfg /setacvalueindex a1841308-3541-4fab-bc81-f71556f20b4a 7516b95f-
f776-4464-8c53-06167f40cc99 3c0bc021-c8a8-4e07-a973-6b14cbcb2b7e 0
```

Parte 7: Atualizar drivers do chipset Intel para novos tipos de instância

Os tipos de instância `u-6tb1.metal`, `u-9tb1.metal` e `u-12tb1.metal` usam hardware que exige drivers de chipset que não foram instalados anteriormente nas AMIs do Windows. Se você não estiver usando uma instância executada de uma AMI do Windows fornecida pela Amazon, datada de 19/11/2018 ou posterior, deverá instalar os drivers usando o utilitário INF do Chipset Intel.

Para instalar os drivers de chipset

1. Utilitário Chipset INF na instância.
2. Extraia os arquivos.
3. Execute `SetupChipset.exe`.
4. Aceite o contrato de licença do software Intel e instale os drivers do chipset.

5. Reinicialize a instância.

(Alternativa) Atualizar os drivers PV, ENA e NVMe da AWS usando o AWS Systems Manager

O documento de automação do `AWSSupport-UpgradeWindowsAWSDrivers` automatiza as etapas descritas em Parte 1, Parte 2 e Parte 3. Esse método também pode reparar uma instância onde houve falha nas atualizações de driver.

O documento de automação do `AWSSupport-UpgradeWindowsAWSDrivers` atualiza ou repara os drivers AWS de armazenamento e rede na instância do EC2 especificada. O documento tenta instalar as versões mais recentes dos drivers da AWS online chamando o AWS Systems Manager Agent (SSM Agent). Se o SSM Agent não puder ser conectado, o documento poderá executar uma instalação offline dos drivers da AWS caso solicitado explicitamente.

> **Note**
>
> Esse procedimento falhará em um controlador de domínio. Para atualizar drivers em um controlador de domínio, consulte Atualizar um controlador de domínio (atualização do AWS PV).

Como atualizar automaticamente os drivers AWS PV, ENA e NVMe usando AWS Systems Manager

1. Abra o console do Systems Manager em https://console.aws.amazon.com/systems-manager.
2. Escolha Automation (Automação), Execute Automation (Executar automação).
3. Pesquise e selecione o documento de automação AWSSupport-UpgradeWindowsAWSDrivers e escolha Executar automação.
4. Na seção Parâmetros de entrada, configure as seguintes opções:

   ID da instância

   Insira o ID exclusivo da instância a ser atualizada.

   AllowOffline

   (Opcional) Escolha uma das seguintes opções:

   - `True`: escolha essa opção para executar uma instalação offline. A instância é interrompida e reiniciada durante o processo de atualização.

> **Warning**
>
> Quando você interrompe uma instância, os dados em todos os volumes de armazenamento de instâncias são apagados. Para preservar dados em volumes de armazenamento de instâncias, faça backup dos dados no armazenamento persistente.

- `False`: (Padrão) para executar uma instalação online, deixe essa opção selecionada. A instância é reiniciada durante o processo de atualização.

> **Important**
>
> As atualizações online e offline criam uma AMI antes de tentar as operações de atualização. A AMI persiste depois da conclusão da automação. Garanta seu acesso à AMI ou exclua-o se não for mais necessário.

SubnetId

(Opcional) Insira um dos seguintes valores:

- `SelectedInstanceSubnet` — (Padrão) O processo de atualização executa a instância helper na mesma sub-rede da instância que deve ser atualizada. A sub-rede deve permitir a comunicação com os endpoints Systems Manager (`ssm.*`).
- `CreateNewVPC` — O processo de atualização executa a instância helper em uma nova VPC. Use essa opção se não souber ao certo se a sub-rede da instância de destino permite a comunicação com os endpoints `ssm.*`. O usuário deve ter permissão para criar uma VPC.
- Um ID de sub-rede específico — Especifique o ID de uma sub-rede específica na qual executar a instância helper. A sub-rede na mesma zona de disponibilidade da instância que deve ser atualizada, e deve permitir a comunicação com os endpoints `ssm.*`.

5. Clique em Executar.
6. Deixe a atualização terminar. Pode levar até 10 minutos para concluir uma atualização online e até 25 minutos para concluir uma atualização offline.

Solucionar problemas de atualização de um sistema operacional em uma instância do Windows do EC2

A AWS oferece suporte à atualização para problemas com o Upgrade Helper Service, um utilitário da AWS que ajuda você a executar atualizações no local que envolvem drivers Citrix PV.

Após a atualização, a instância pode apresentar temporariamente uma utilização de CPU maior do que a média enquanto o serviço .NET Runtime Optimization otimiza o .NET Framework. Esse comportamento é esperado.

Se a instância não foi aprovada em todas verificações de status após várias horas, verifique os aspectos a seguir.

- Se você fez a atualização para o Windows Server 2008 e ambas as verificações de status falharem após várias horas, a atualização pode ter falhado e estar apresentando um prompt para Clicar em OK a fim de confirmar a reversão. Como o console não está acessível nesse estado, não há como clicar no botão. Para contornar isso, execute uma reinicialização através da API ou do console do Amazon EC2. A reinicialização levará 10 minutos ou mais para ser iniciada. A instância pode se tornar disponível após 25 minutos.
- Remova as aplicações ou as funções do servidor e tente novamente.

Se a instância não for aprovada em todas as verificações de status após a remoção das aplicações ou funções do servidor, faça o seguinte.

- Interrompa a instância e anexe o volume raiz a outra instância. Para obter mais informações, consulte a descrição de como parar e anexar o volume raiz a outra instância em "Esperando o serviço de metadados".
- Analise os arquivos de log de configuração e os logs de eventos do Windows para ver se há falhas.

Para outros problemas com uma atualização ou uma migração do sistema operacional, recomendamos analisar os artigos indicados em Antes de iniciar uma atualização no local.

Tutorial: conectar uma instância do Amazon EC2 a um banco de dados do Amazon RDS

Objetivo do tutorial

O objetivo deste tutorial é aprender a configurar a conexão entre uma instância do Amazon EC2 e um banco de dados do Amazon RDS usando o Console de gerenciamento da AWS.

Há diferentes opções para configurar a conexão. Neste tutorial, vamos explorar estas três opções:

- Opção 1: conectar automaticamente uma instância ao banco de dados do RDS usando o console do EC2

  Use o recurso de conexão automática do console do EC2 para configurar automaticamente a conexão entre a instância do EC2 e o banco de dados do RDS para permitir o tráfego entre a instância do EC2 e o banco de dados do RDS.
- Opção 2: conectar automaticamente uma instância a um banco de dados do RDS usando o console do RDS

  Use o recurso de conexão automática do console do RDS para configurar automaticamente a conexão entre a instância do EC2 e o banco de dados do RDS para permitir o tráfego entre a instância do EC2 e o banco de dados do RDS.
- Opção 3: conectar manualmente uma instância a um banco de dados do RDS criando grupos de segurança

  Configure a conexão entre a instância do EC2 e o banco de dados do RDS configurando e atribuindo manualmente os grupos de segurança para reproduzir a configuração criada automaticamente pelo recurso de conexão automática na opção 1 e na opção 2.

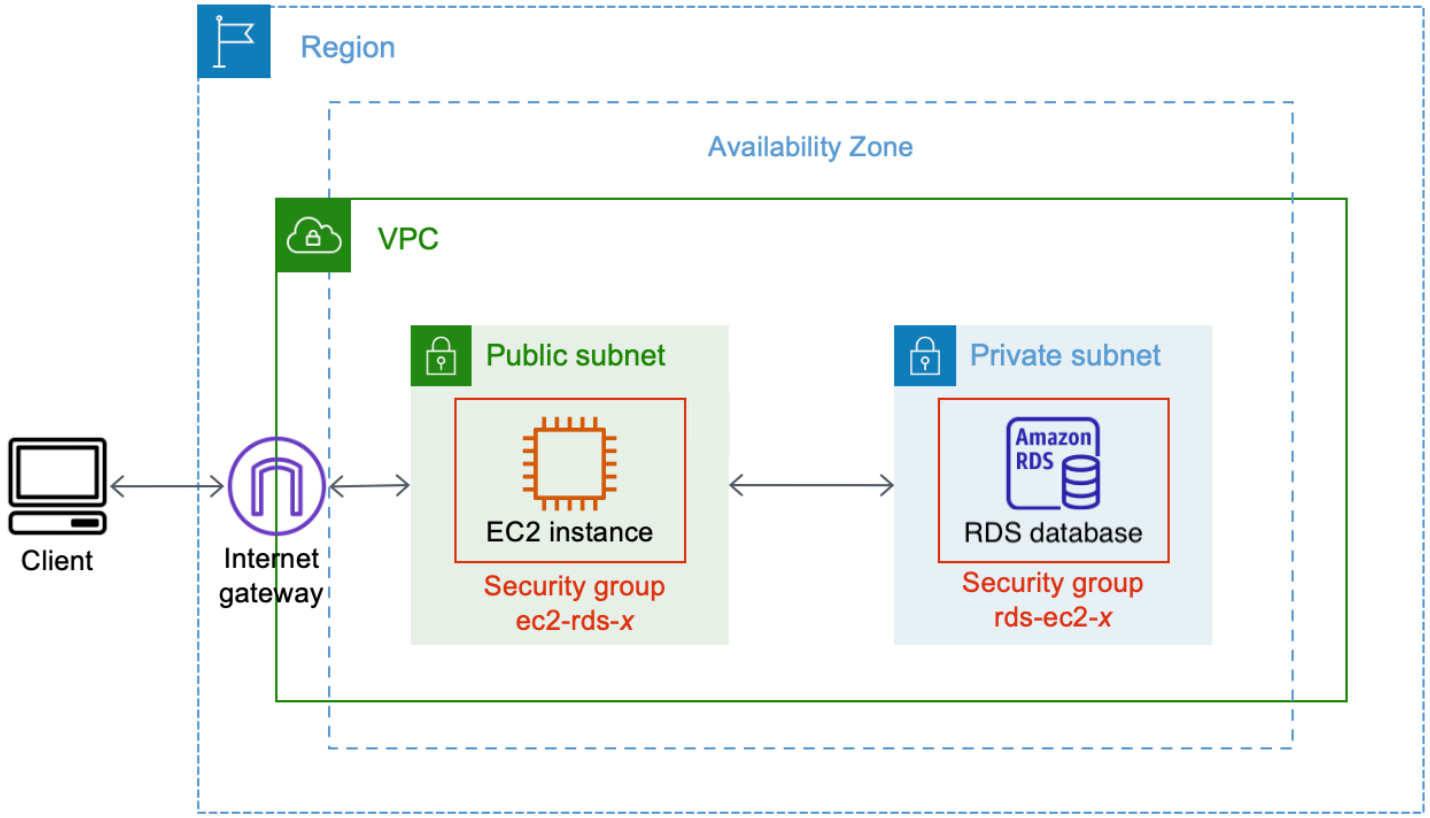
Contexto

Como contexto do motivo para configurar uma conexão entre a instância do EC2 e um banco de dados do RDS, vamos considerar o seguinte cenário: seu site apresenta um formulário para os usuários preencherem. É necessário captar os dados do formulário em um banco de dados. É possível hospedar o site em uma instância do EC2 que foi configurada como servidor Web e captar os dados do formulário em um banco de dados do RDS. A instância do EC2 e o banco de dados do RDS precisam estar conectados entre si para que os dados do formulário possam sair da instância

do EC2 para o banco de dados do RDS. Este tutorial explica como configurar a conexão. Este é apenas um exemplo de um caso de uso para conectar uma instância do EC2 e um banco de dados do RDS.

Arquitetura

O diagrama a seguir mostra os recursos criados e a configuração arquitetônica resultante da conclusão de todas as etapas deste tutorial.



O diagrama ilustra os seguintes recursos que você criará:

- Você criará uma instância do EC2 e um banco de dados do RDS na mesma Região da AWS, VPC e zona de disponibilidade.
- Você criará a instância do EC2 em uma sub-rede pública.
- Você criará o banco de dados do RDS em uma sub-rede privada.

  Ao usar o console do RDS para criar o banco de dados do RDS e conectar automaticamente a instância do EC2, a VPC, o grupo de sub-redes de banco de dados e as configurações de acesso público para o banco de dados são selecionados automaticamente. O banco de dados do RDS é criado automaticamente em uma sub-rede privada na mesma VPC da instância do EC2.

- Os usuários da Internet podem se conectar à instância do EC2 usando SSH ou HTTP/HTTPS por um gateway da Internet.
- Os usuários da Internet não podem se conectar diretamente ao banco de dados do RDS, apenas a instância do EC2 está conectada ao banco de dados do RDS.
- Quando você usa o recurso de conexão automática para permitir o tráfego entre a instância do EC2 e o banco de dados do RDS, estes grupos de segurança são automaticamente criados e adicionados:
  - O grupo de segurança ec2-rds-***x*** é criado e adicionado à instância do EC2. Ele tem uma regra de saída que referencia o grupo de segurança rds-ec2-***x*** como destino. Isso permite que o tráfego da instância do EC2 atinja o banco de dados do RDS com o grupo de segurança rds-ec2-***x***.
  - O grupo de segurança rds-ec2-***x*** é criado e adicionado ao banco de dados do RDS. Ele tem uma regra de entrada que referencia o grupo de segurança ec2-rds-***x*** como origem. Isso permite que o tráfego da instância do EC2 com o grupo de segurança ec2-rds-***x*** atinja o banco de dados do RDS.

  Ao usar grupos de segurança separados (um para a instância do EC2 e outro para o banco de dados do RDS), você tem mais controle sobre a segurança da instância e do banco de dados. Se você usasse o mesmo grupo de segurança na instância e no banco de dados e depois modificasse o grupo de segurança para se adequar, digamos, somente ao banco de dados, a modificação afetaria tanto a instância como o banco de dados. Em outras palavras, se usasse um grupo de segurança, você poderia modificar involuntariamente a segurança de um recurso (instância ou banco de dados) porque esqueceu que o grupo de segurança estava anexado a ele.

  Os grupos de segurança criados automaticamente também respeitam o privilégio mínimo, pois permitem somente a conexão mútua para essa workload na porta do banco de dados, criando um par de grupos de segurança específico da workload.

Considerações

Considere o seguinte ao concluir as tarefas deste tutorial:

- Dois consoles: você usará estes dois consoles neste tutorial:
  - Console do Amazon EC2: você usará o console do EC2 para iniciar instâncias, conectar automaticamente uma instância do EC2 a um banco de dados do RDS e para a opção manual de configurar a conexão criando os grupos de segurança.

  - Console do Amazon RDS: você usará o console do RDS para criar um banco de dados do RDS e conectar automaticamente uma instância do EC2 a um banco de dados do RDS.
- Uma VPC: para usar o recurso de conexão automática, a instância do EC2 e o banco de dados do RDS devem estar na mesma VPC.

  Se você configurasse manualmente a conexão entre a instância do EC2 e o banco de dados do RDS, poderia iniciar a instância do EC2 em uma VPC e o banco de dados do RDS em outra VPC, mas precisaria definir uma configuração adicional de encaminhamento e VPC. Este cenário não é abordado neste tutorial.
- Uma Região da AWS: a instância do EC2 e o banco de dados do RDS devem estar localizados na mesma região.
- Dois grupos de segurança: a conectividade entre a instância do EC2 e o banco de dados do RDS é configurada por dois grupos de segurança, um grupo de segurança para a instância do EC2 e um grupo de segurança para o banco de dados do RDS.

  Quando você usa o recurso de conexão automática no console do EC2 ou no console do RDS para configurar a conectividade (opção 1 e opção 2 deste tutorial), os grupos de segurança são criados automaticamente e atribuídos à instância do EC2 e ao banco de dados do RDS.

  Se você não usar o recurso de conexão automática, será necessário criar e atribuir os grupos de segurança manualmente. Faça isso na opção 3 deste tutorial.

É hora de concluir o tutorial

30 minutos

É possível concluir o tutorial inteiro de uma só vez ou pode realizar uma tarefa por vez.

Custos

Ao concluir este tutorial, será possível incorrer em custos para os recursos da AWS criados.

É possível usar o Amazon EC2 no nível gratuito, desde que a conta da AWS se qualifique para isso e seus recursos estejam configurados de acordo com os requisitos do nível gratuito. Para obter mais informações, Benefícios do nível gratuito antes e depois de 15 de julho de 2025.

Se sua instância do EC2 e o banco de dados do RDS estiverem em zonas de disponibilidade diferentes, serão aplicadas taxas de transferências de dados. Para evitar que essas taxas estejam

aplicadas, a instância do EC2 e o banco de dados do RDS devem estar na mesma zona de disponibilidade. Para obter informações, consulte a seção Transferência de dados na página Preço sob demanda do Amazon EC2.

Para evitar custos após a conclusão do tutorial, exclua os recursos, caso eles não sejam mais necessários. Para saber as etapas para excluir os recursos, consulte Tarefa 4 (opcional): limpar.

Opção 1: conectar automaticamente uma instância ao banco de dados do RDS usando o console do EC2

O objetivo da opção 1 é explorar o recurso de conexão automática do console do EC2 que configura automaticamente a conexão entre a instância do EC2 e o banco de dados do RDS para permitir o tráfego da instância do EC2 para o banco de dados do RDS. Na opção 3, você aprenderá a configurar a conexão manualmente.

Tarefas

- Antes de começar
- Tarefa 1 (opcional): criar um banco de dados do RDS
- Tarefa 2 (opcional): executar uma instância do EC2
- Tarefa 3: conectar automaticamente a instância do EC2 ao banco de dados do RDS
- Tarefa 4: verificar a configuração da conexão
- Tarefa 5 (opcional): limpar

Antes de começar

Você precisará do seguinte para concluir este tutorial:

- Um banco de dados do RDS que está na mesma VPC da instância do EC2. É possível usar um banco de dados RDS existente ou seguir as etapas na tarefa 1 para criar um novo banco de dados do RDS.
- Uma instância do EC2 que está na mesma VPC do banco de dados do RDS. É possível usar uma instância do EC2 existente ou seguir as etapas na tarefa 2 para criar uma nova instância do EC2.
- Permissões para chamar estas operações:
  - `ec2:AssociateRouteTable`
  - `ec2:AuthorizeSecurityGroupEgress`
  - `ec2:CreateRouteTable`

- `ec2:CreateSecurityGroup`
- `ec2:CreateSubnet`
- `ec2:DescribeInstances`
- `ec2:DescribeNetworkInterfaces`
- `ec2:DescribeRouteTables`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeSubnets`
- `ec2:ModifyNetworkInterfaceAttribute`
- `ec2:RevokeSecurityGroupEgress`

Tarefa 1 (opcional): criar um banco de dados do RDS

> **Note**
>
> O foco deste tutorial não é criar um banco de dados do Amazon RDS. Se você já tiver um banco de dados do RDS e quiser usá-lo neste tutorial, poderá ignorar esta tarefa.
> Se usar um banco de dados do RDS existente, certifique-se de que ele esteja na mesma VPC da instância do EC2 para poder usar o recurso de conexão automática.

O objetivo desta tarefa é criar um banco de dados do RDS para que você possa concluir a tarefa 3, na qual configura a conexão entre a instância do EC2 e o banco de dados do RDS. As etapas desta tarefa configuram o banco de dados do RDS da seguinte forma:

- Tipo de mecanismo: MySQL
- Modelo: nível gratuito
- Identificador da instância de banco de dados: **`tutorial-database-1`**
- Classe da instância de banco de dados: `db.t3.micro`

> **Important**
>
> Para um ambiente de produção, é necessário configurar o banco de dados para atender às suas necessidades específicas.

Para criar um banco de dados MySQL RDS

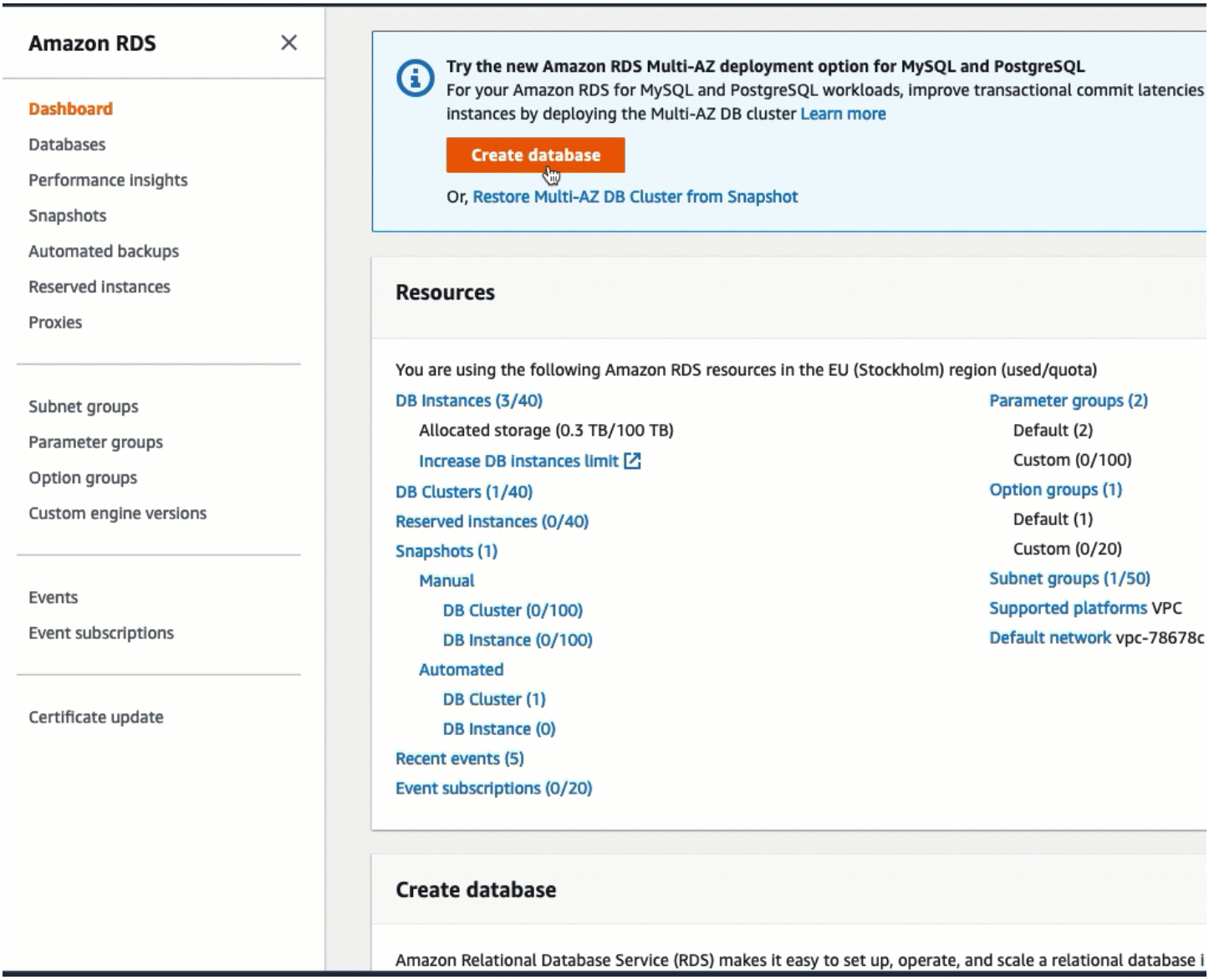
1. Abra o console do Amazon RDS em https://console.aws.amazon.com/rds/.
2. No seletor Region (Região), no canto superior direito, escolha uma Região da AWS. O banco de dados e a instância do EC2 devem estar na mesma região para usar o recurso de conexão automática no console do EC2.
3. No painel, escolha Create database (Criar banco de dados).
4. Em Choose a database creation method (Escolher um método de criação de banco de dados), verifique se a opção Standard Create (Criação padrão) está selecionada. Se você escolher Easy create (Criação fácil), o seletor VPC não estará disponível. Verifique se o banco de dados está na mesma VPC da sua instância do EC2 para usar o recurso de conexão automática no console do EC2.
5. Em Engine options (Opções de mecanismo), em Engine type (Tipo de mecanismo), escolha MySQL.
6. Em Templates (Modelos), escolha um modelo de exemplo que atenda às suas necessidades. Neste tutorial, escolha o Free tier (Nível gratuito) para criar um banco de dados do RDS sem nenhum custo. No entanto, observe que o nível gratuito só está disponível para contas que são elegíveis. É possível ler mais escolhendo o link Info (Informações) na caixa Free tier (Nível gratuito).
7. Em Configurações, faça o seguinte:
   a. Em DB instance identifier (Identificador da instância de banco de dados), insira um nome para o banco de dados. Para este tutorial, insira **`tutorial-database-1`**.
   b. Em Master username (Nome de usuário principal), deixe o nome padrão, que é **`admin`**.
   c. Em Master password (Senha principal), digite uma senha da qual você consiga se lembrar para este tutorial e, em Confirm password (Confirmar senha), insira a senha novamente.
8. Em Configuração da instância, para a Classe de instância de banco de dados, deixe o padrão, que é db.t3.micro. Se a conta for elegível para o nível gratuito, será possível usar essa classe de banco de dados gratuitamente. Para obter mais informações, consulte Nível gratuito da AWS.
9. Em Connectivity (Conectividade), em Compute resource (Recurso de computação), escolha Don't connect to an EC2 compute resource (Não se conectar a um recurso computacional do EC2), pois você conectará a instância do EC2 e o banco de dados do RDS posteriormente na tarefa 3.

(Posteriormente, na opção 2 deste tutorial, você experimentará o recurso de conexão automática no console do RDS escolhendo Connect to an EC2 compute resource [Conectar a um recurso computacional do EC2].)

10. Em Virtual private cloud (VPC) (Nuvem privada virtual [VPC]), selecione uma VPC. A VPC deve ter um grupo de sub-redes de banco de dados. Para usar o recurso de conexão automática, a instância do EC2 e o banco de dados do RDS devem estar na mesma VPC.
11. Mantenha os valores padrão para os outros campos desta página.
12. Selecione Criar banco de dados.

    Na tela Databases (Bancos de dados), o Status do novo banco de dados é Creating (Criando) até que o banco de dados esteja pronto para uso. Quando o status mudar para Available (Disponível), será possível conectar-se ao banco de dados. Dependendo da classe de banco de dados e da quantidade de armazenamento, pode levar até 20 minutos para que o novo banco de dados esteja disponível.

Visualizar uma animação: criar um banco de dados do RDS



Tarefa 2 (opcional): executar uma instância do EC2

> **Note**
>
> O foco deste tutorial não é iniciar uma instância. Se você já tiver uma instância do Amazon EC2 e quiser usá-la neste tutorial, pode ignorar esta tarefa.
>
> Se usar uma instância do EC2 existente, certifique-se de que ela esteja na mesma VPC do banco de dados do RDS para poder usar o recurso de conexão automática.

O objetivo desta tarefa é iniciar uma instância do EC2 para que você possa concluir a tarefa 3, na qual configura a conexão entre a instância do EC2 e o banco de dados do Amazon RDS. As etapas desta tarefa configuram a instância do EC2 da seguinte forma:

- Nome da instância: **`tutorial-instance-1`**
- AMI: Amazon Linux 2
- Tipo de instância: `t2.micro`
- Atribuir automaticamente IP público: habilitado
- Grupo de segurança com estas três regras:
  - Permitir SSH de seu endereço IP
  - Permitir tráfego HTTPS de qualquer lugar
  - Permitir tráfego HTTP de qualquer lugar

> **Important**
>
> Para um ambiente de produção, é necessário configurar a instância para atender às suas necessidades específicas.

Para iniciar uma instância do EC2

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No seletor Region (Região), no canto superior direito, escolha uma Região da AWS. A instância e o banco de dados do RDS devem estar na mesma região para usar o recurso de conexão automática no console do EC2.
3. No painel do EC2, escolha Launch Instance (Iniciar instância).
4. Em Name and tags (Nome e etiquetas), para Name (Nome), insira um nome para identificar a instância. Para este tutorial, insira o nome da instância **`tutorial-instance-1`**. Embora o nome da instância não seja obrigatório, ao selecionar a instância no console do EC2, o nome ajudará você a identificá-la facilmente.
5. Em Application and OS Images (Imagens da aplicação e do sistema operacional), escolha uma AMI que atenda às necessidades de seu servidor Web. Este tutorial usa o Amazon Linux 2.
6. Em Instance type (Tipo de instância), para Instance type (Tipo de instância), selecione um tipo de instância que atenda às necessidades de seu servidor Web. Este tutorial usa `t2.micro`.

> **Note**
>
> Dependendo de quando sua conta foi criada, ela pode ser elegível para usar o Amazon EC2 no nível gratuito.
> Caso tenha criado sua Conta da AWS antes de 15 de julho de 2025 e ela tenha menos de 12 meses, será possível usar o Amazon EC2 no nível gratuito selecionando o tipo de instância t2.micro ou o tipo de instância t3.micro em regiões onde o tipo t2.micro estiver indisponível. Lembre-se de que, quando você executa uma instância t3.micro, o padrão é o modo Ilimitado, o que pode gerar cobranças adicionais com base no uso da CPU. Se um tipo de instância puder ser usada no nível gratuito, ela terá o rótulo Elegível para o nível gratuito.
> Se você tiver criado sua Conta da AWS a partir de 15 de julho de 2025, poderá usar os tipos de instância t3.micro, t3.small, t4g.micro, t4g.small, c7i-flex.large e m7i-flex.large durante seis meses ou até seus créditos acabarem.
> Para obter mais informações, consulte Benefícios do nível gratuito antes e depois de 15 de julho de 2025.

7. Em Key pair (login) (Par de chaves [login]), para Key pair name (Nome do par de chaves), escolha o par de chaves.
8. Em Network settings (Configurações de rede), faça o seguinte:

   a. Em Network (Rede) e Subnet (Sub-rede), se você não fez alterações na VPC ou nas sub-redes padrão, pode manter as configurações padrão.

      Se você fez alterações na VPC ou nas sub-redes padrão, verifique o seguinte:

      i. A instância do EC2 e o banco de dados do RDS devem estar na mesma VPC para usar o recurso de conexão automática. Por padrão, você tem apenas uma VPC.

      ii. A VPC na qual você está iniciando a instância deve ter um gateway da Internet conectado a ela para que você possa acessar seu servidor Web pela Internet. Sua VPC padrão é configurada automaticamente com um gateway da Internet.

      iii. Para garantir que a instância receba um endereço IP público, em Auto-assign public IP (Atribuir IP público automaticamente), verifique se a opção Enable (Habilitar) está selecionada. Se a opção Disable (Desabilitar) estiver selecionada, escolha Edit (Editar) à direita de Network Settings (Configurações de rede) e, para Auto-assign public IP (Atribuir IP público automaticamente), escolha Enable (Habilitar).

b. Para se conectar à instância usando SSH, é necessário ter uma regra de grupo de segurança que autorize o tráfego SSH (Linux) ou RDP (Windows) do endereço IPv4 público do computador. Por padrão, quando você executa uma instância, cria-se um novo grupo de segurança com uma regra que permite tráfego SSH de entrada de qualquer lugar.

   Para garantir que somente seu endereço IP possa se conectar à instância, em Firewall (grupos de segurança), na lista suspensa ao lado da caixa de seleção Permitir tráfego SSH de, escolha Meu IP.

c. Para permitir o tráfego da Internet para a instância, marque as seguintes caixas de seleção:

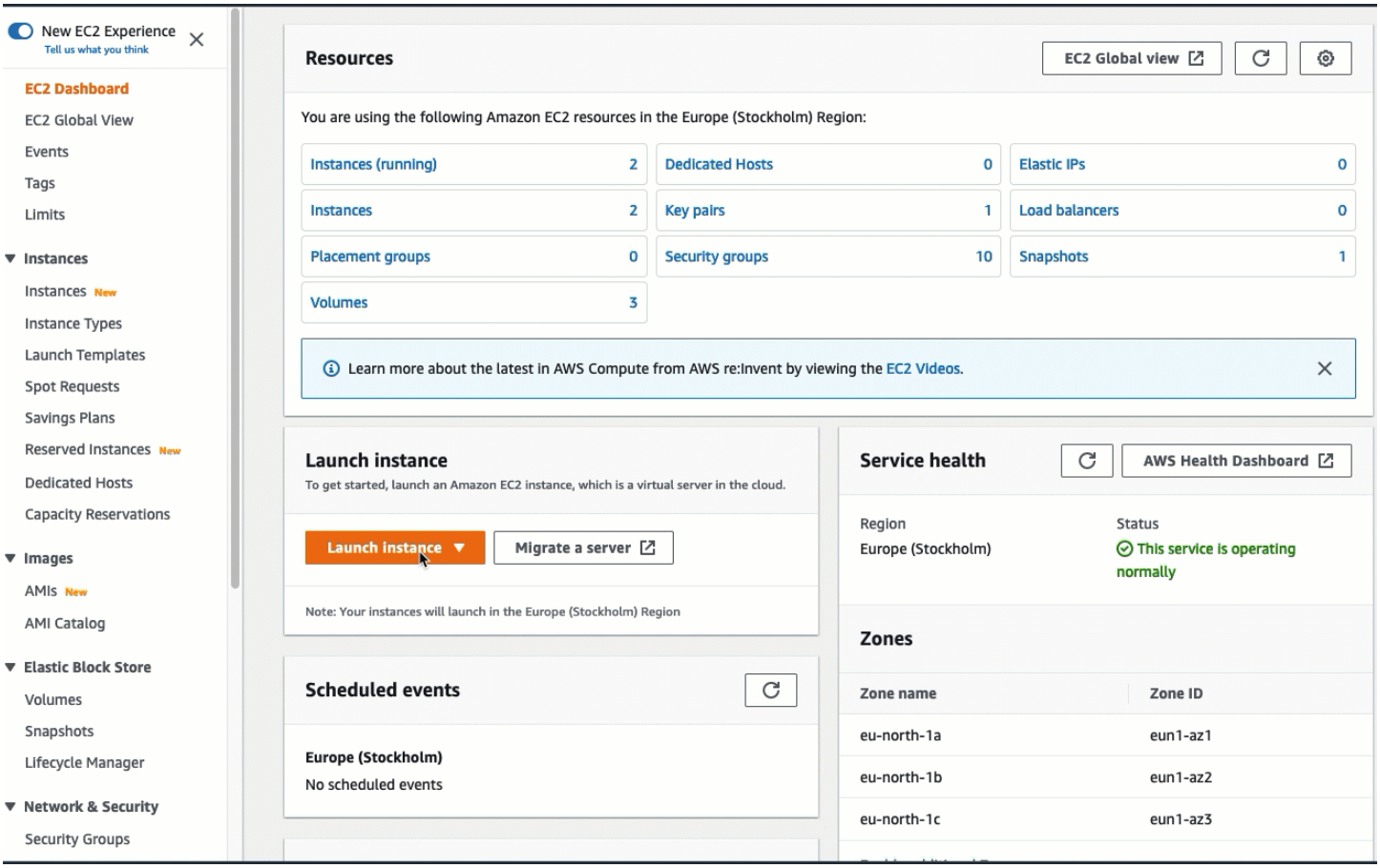
   - Permitir tráfego HTTPs da Internet
   - Permitir tráfego HTTP da Internet

9. No painel Summary (Resumo), analise a configuração da instância e selecione Launch instance (Iniciar instância).
10. Deixe a página de confirmação aberta. Você precisará dela na próxima tarefa ao conectar automaticamente a instância ao banco de dados.

    Se a instância não executar ou o estado passar imediatamente para `terminated`, em vez de `running`, consulte Solucionar problemas de inicialização de instâncias do Amazon EC2.

Para obter mais informações sobre como iniciar uma instância MySQL, consulte Executar uma instância do EC2 usando o assistente de inicialização de instâncias no console.

Visualizar uma animação: iniciar uma instância do EC2



Tarefa 3: conectar automaticamente a instância do EC2 ao banco de dados do RDS

O objetivo desta tarefa é usar o recurso de conexão automática no console do EC2 para configurar automaticamente a conexão entre a instância do EC2 e o banco de dados do RDS.

Para conectar automaticamente uma instância do EC2 a um banco de dados do RDS usando o console do EC2

1. Na página de confirmação de inicialização da instância (ela deve ser aberta na tarefa anterior), escolha Connect an RDS database (Conectar um banco de dados do RDS).

   Se você fechou a página de confirmação, siga estas etapas:

   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 do EC2 que você acabou de criar e escolha Actions (Ações), Networking (Redes), Connect RDS database (Conectar banco de dados do RDS).

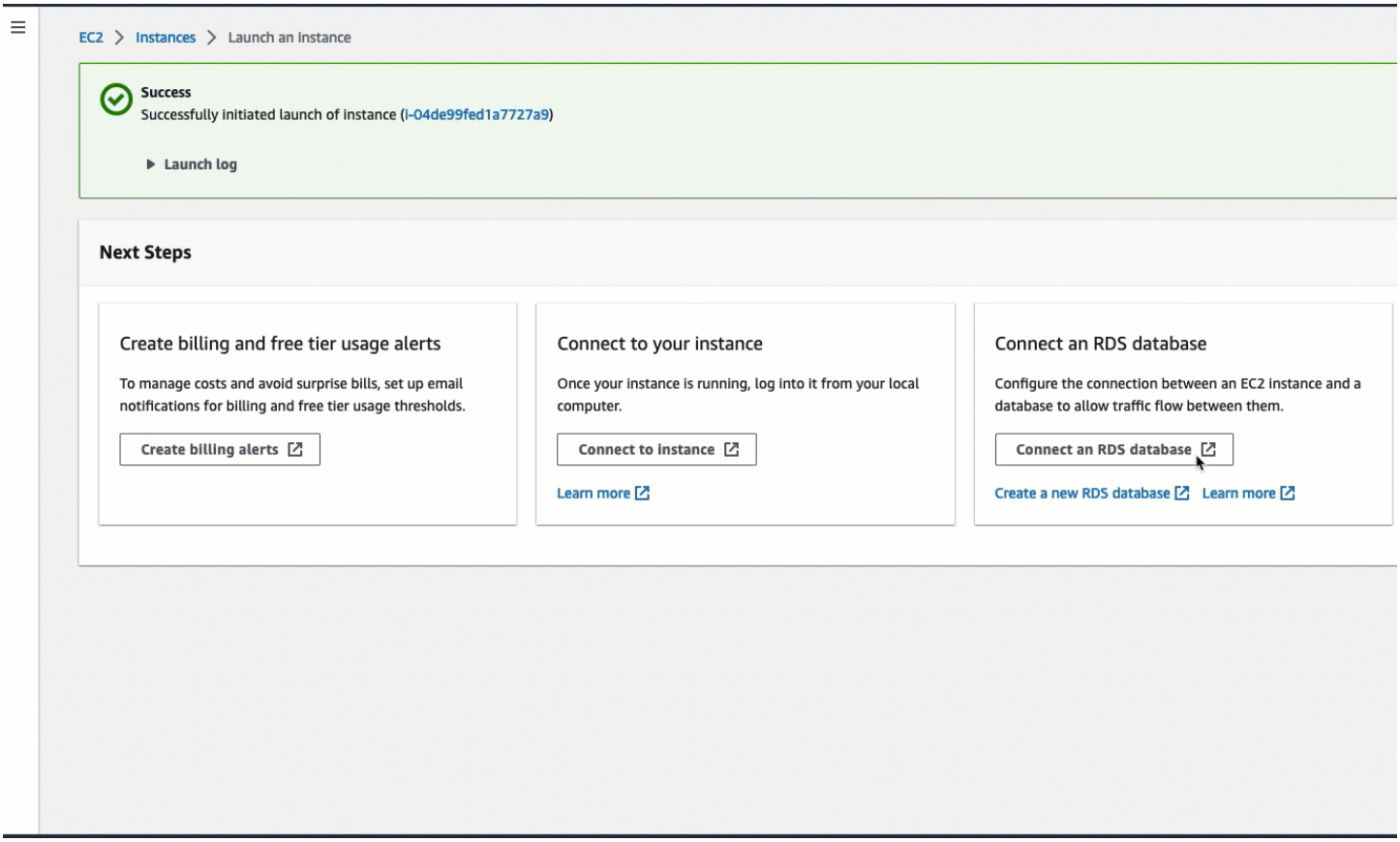
Se Connect RDS database (Conectar banco de dados do RDS) não estiver disponível, verifique se a instância do EC2 está no estado Running (Em execução).

2. Em Database role (Perfil de banco de dados), escolha Instance (Instância). Nesse caso, Instance (Instância) refere-se à instância do banco de dados.
3. Em RDS database (Banco de dados do RDS), escolha o banco de dados do RDS que você criou na tarefa 1.

> **Note**
>
> A instância do EC2 e o banco de dados do RDS devem estar na mesma VPC para se conectarem um ao outro.

4. Selecione Conectar.

Visualizar uma animação: conectar automaticamente uma instância do EC2 recém-iniciada a um banco de dados do RDS



Tarefa 4: verificar a configuração da conexão

O objetivo desta tarefa é verificar se os dois grupos de segurança foram criados e atribuídos à instância e ao banco de dados.

Quando você usa o recurso de conexão automática no console para configurar a conectividade, os grupos de segurança são criados automaticamente e atribuídos à instância e ao banco de dados da seguinte forma:

- O grupo de segurança rds-ec2-***x*** é criado e adicionado ao banco de dados do RDS. Ele tem uma regra de entrada que referencia o grupo de segurança ec2-rds-***x*** como origem. Isso permite que o tráfego da instância do EC2 com o grupo de segurança ec2-rds-***x*** atinja o banco de dados do RDS.
- O grupo de segurança ec2-rds-***x*** é criado e adicionado à instância do EC2. Ele tem uma regra de saída que referencia o grupo de segurança rds-ec2-***x*** como destino. Isso permite que o tráfego da instância do EC2 atinja o banco de dados do RDS com o grupo de segurança rds-ec2-***x***.

Para verificar a configuração da conexão usando o console

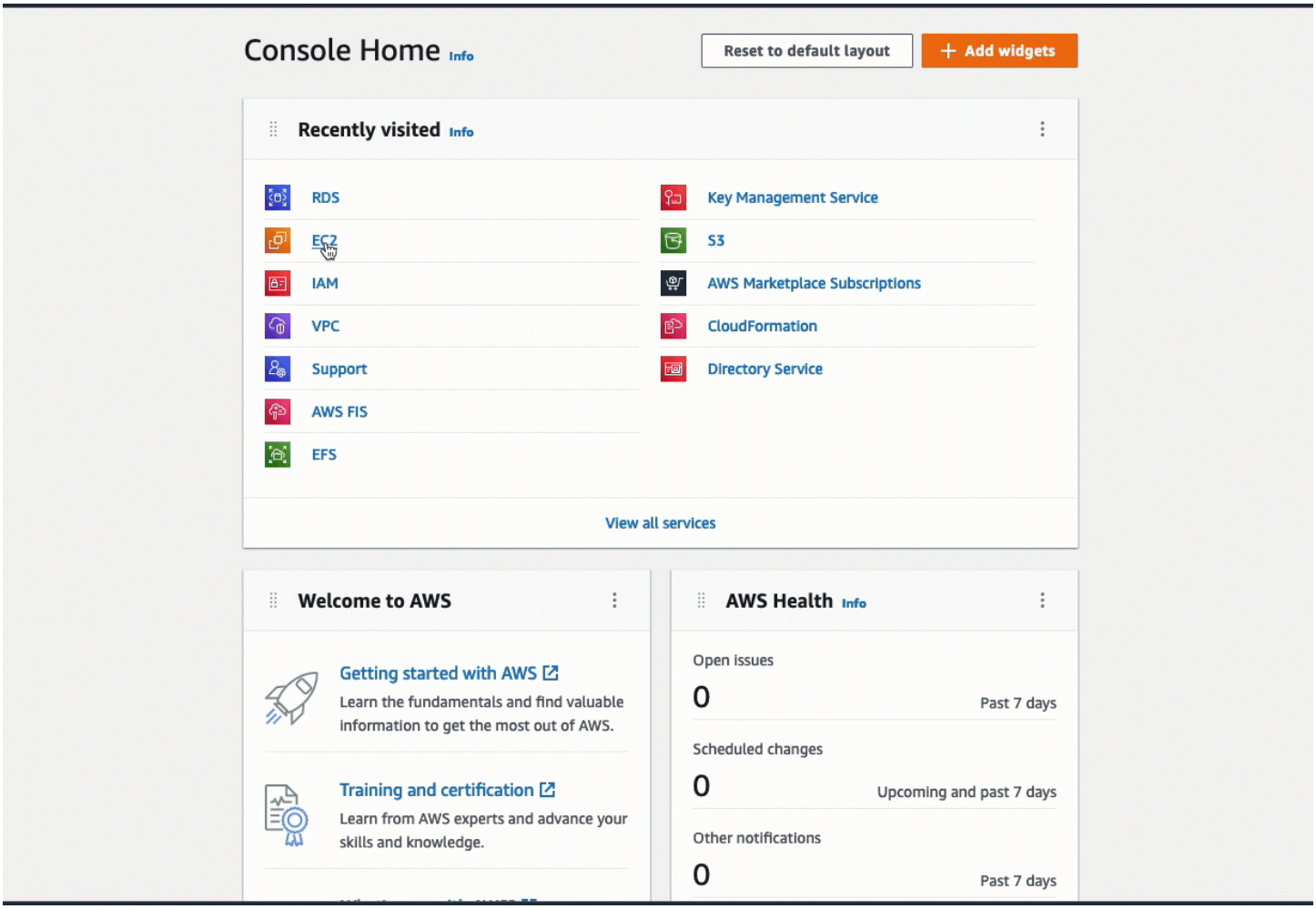
1. Abra o console do Amazon RDS em https://console.aws.amazon.com/rds/.
2. Na página de navegação, escolha Databases (Bancos de dados).
3. Escolha o banco de dados do RDS que você criou para este tutorial.
4. Na guia Conectividade e segurança, em Segurança, Grupos de segurança da VPC, verifique se um grupo de segurança chamado rds-ec2-***x*** está sendo exibido.
5. Escolha o grupo de segurança rds-ec2-***x***. A tela Security Groups (Grupos de segurança) no console do EC2 é aberta.
6. Escolha o grupo de segurança rds-ec2-***x*** para abrir.
7. Escolha a guia Regras de entrada.
8. Verifique se a seguinte regra de grupo de segurança existe, da seguinte forma:
    - Digite: MySQL/Aurora
    - Intervalo de porta: 3306
    - Origem: ***sg-0987654321example*** / ec2-rds-***x***: este é o grupo de segurança atribuído à instância do EC2 que você verificou nas etapas anteriores.
    - Descrição: regra para permitir conexões de instâncias do EC2 com ***sg-1234567890example*** anexado

9. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
10. No painel de navegação, escolha Instances (Instâncias).
11. Escolha a instância do EC2 que você selecionou para se conectar ao banco de dados do RDS na tarefa anterior e escolha a guia Security (Segurança).
12. Em Detalhes de segurança, Grupos de segurança, verifique se um grupo de segurança chamado ec2-rds-*x* está na lista. *x* é um número.
13. Escolha o grupo de segurança ec2-rds-*x* para abrir.
14. Escolha a guia Outbound rules (Regras de saída).
15. Verifique se a seguinte regra de grupo de segurança existe, da seguinte forma:

    - Digite: MySQL/Aurora
    - Intervalo de porta: 3306
    - Destino: ***sg-1234567890example*** / rds-ec2-***x***
    - Descrição: regra para permitir conexões a **`database-tutorial`** de qualquer instância à qual esse grupo de segurança esteja vinculado

Ao verificar se esses grupos de segurança e regras de grupos de segurança existem e se estão atribuídos ao banco de dados do RDS e à instância do EC2, conforme descrito neste procedimento, você pode verificar se a conexão foi configurada automaticamente usando o recurso de conexão automática.

Visualizar uma animação: verificar a configuração da conexão



Você concluiu a opção 1 deste tutorial. Agora você pode concluir a opção 2, que ensina a usar o console do RDS para conectar automaticamente uma instância do EC2 a um banco de dados do RDS, ou pode concluir a opção 3, que ensina a configurar manualmente os grupos de segurança que foram criados automaticamente na opção 1.

Tarefa 5 (opcional): limpar

> **Warning**
>
> O encerramento de uma instância é permanente e irreversível.
> Depois de encerrar uma instância, não será mais possível se conectar a ela e ela não poderá ser recuperada. Todos os volumes anexados do Amazon EBS configurados para serem excluídos no encerramento também serão excluídos permanentemente e não poderão ser recuperados. Todos os dados armazenados em volumes de armazenamento de instância

serão perdidos permanentemente. Para obter mais informações, consulte Como funciona o encerramento de uma instância.
Antes de encerrar uma instância, certifique-se de ter feito backup de todos os dados que você precise reter após o encerramento no armazenamento persistente.

Agora que você concluiu o tutorial, é uma prática recomendada limpar (excluir) os recursos que não queira mais usar. Limpar os recursos da AWS evita que sua conta incorra em cobranças adicionais.

Se você iniciou uma instância do EC2 especificamente para este tutorial, pode encerrá-la para parar de incorrer em quaisquer cobranças associadas a ela.

Para encerrar 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 criada para este tutorial e escolha Instance state (Estado da instância), Terminate instance (Terminar instância).
4. Quando a confirmação for solicitada, escolha Encerrar.

Se você criou um banco de dados do RDS especificamente para este tutorial, pode excluí-lo para parar de incorrer em quaisquer cobranças associadas a ele.

Para excluir um banco de dados do RDS usando o console

1. Abra o console do Amazon RDS em https://console.aws.amazon.com/rds/.
2. No painel de navegação, escolha Databases (Bancos de dados).
3. Selecione o banco de dados do RDS criado para este tutorial e escolha Actions (Ações), Delete (Excluir).
4. Insira **`delete me`** na caixa e escolha Delete (Excluir).

Opção 2: conectar automaticamente uma instância a um banco de dados do RDS usando o console do RDS

O objetivo da opção 2 é explorar o recurso de conexão automática do console do RDS que configura automaticamente a conexão entre a instância do EC2 e o banco de dados do RDS para permitir

o tráfego da instância do EC2 para o banco de dados do RDS. Na opção 3, você aprenderá a configurar a conexão manualmente.

Tarefas

- Antes de começar
- Tarefa 1 (opcional): executar uma instância do EC2
- Tarefa 2: criar um banco de dados do RDS e conectá-lo automaticamente à instância do EC2
- Tarefa 3: verificar a configuração da conexão
- Tarefa 4 (opcional): limpar

Antes de começar

Você precisará do seguinte para concluir este tutorial:

- Uma instância do EC2 que está na mesma VPC do banco de dados do RDS. É possível usar uma instância do EC2 existente ou seguir as etapas na tarefa 1 para criar uma nova instância.
- Permissões para chamar estas operações:
  - `ec2:AssociateRouteTable`
  - `ec2:AuthorizeSecurityGroupEgress`
  - `ec2:CreateRouteTable`
  - `ec2:CreateSecurityGroup`
  - `ec2:CreateSubnet`
  - `ec2:DescribeInstances`
  - `ec2:DescribeNetworkInterfaces`
  - `ec2:DescribeRouteTables`
  - `ec2:DescribeSecurityGroups`
  - `ec2:DescribeSubnets`
  - `ec2:ModifyNetworkInterfaceAttribute`
  - `ec2:RevokeSecurityGroupEgress`

Tarefa 1 (opcional): executar uma instância do EC2

> **Note**
>
> O foco deste tutorial não é iniciar uma instância. Se você já tiver uma instância do Amazon EC2 e quiser usá-la neste tutorial, pode ignorar esta tarefa.

O objetivo desta tarefa é iniciar uma instância do EC2 para que você possa concluir a tarefa 2, na qual configura a conexão entre a instância do EC2 e o banco de dados do Amazon RDS. As etapas desta tarefa configuram a instância do EC2 da seguinte forma:

- Nome da instância: **`tutorial-instance-2`**
- AMI: Amazon Linux 2
- Tipo de instância: `t2.micro`
- Atribuir automaticamente IP público: habilitado
- Grupo de segurança com estas três regras:
  - Permitir SSH de seu endereço IP
  - Permitir tráfego HTTPS de qualquer lugar
  - Permitir tráfego HTTP de qualquer lugar

> **Important**
>
> Para um ambiente de produção, é necessário configurar a instância para atender às suas necessidades específicas.

Para iniciar uma instância do EC2

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel do EC2, escolha Launch Instance (Iniciar instância).
3. Em Name and tags (Nome e etiquetas), para Name (Nome), insira um nome para identificar a instância. Para este tutorial, insira o nome da instância **`tutorial-instance-2`**. Embora o nome da instância não seja obrigatório, quando você selecionar a instância no console do RDS, o nome o ajudará a identificá-la facilmente.

4. Em Application and OS Images (Imagens da aplicação e do sistema operacional), escolha uma AMI que atenda às necessidades de seu servidor Web. Este tutorial usa o Amazon Linux.
5. Em Instance type (Tipo de instância), para Instance type (Tipo de instância), selecione um tipo de instância que atenda às necessidades de seu servidor Web. Este tutorial usa `t2.micro`.

> **Note**
>
> Dependendo de quando sua conta foi criada, ela pode ser elegível para usar o Amazon EC2 no nível gratuito.
> Caso tenha criado sua Conta da AWS antes de 15 de julho de 2025 e ela tenha menos de 12 meses, será possível usar o Amazon EC2 no nível gratuito selecionando o tipo de instância t2.micro ou o tipo de instância t3.micro em regiões onde o tipo t2.micro estiver indisponível. Lembre-se de que, quando você executa uma instância t3.micro, o padrão é o modo Ilimitado, o que pode gerar cobranças adicionais com base no uso da CPU. Se um tipo de instância puder ser usada no nível gratuito, ela terá o rótulo Elegível para o nível gratuito.
> Se você tiver criado sua Conta da AWS a partir de 15 de julho de 2025, poderá usar os tipos de instância t3.micro, t3.small, t4g.micro, t4g.small, c7i-flex.large e m7i-flex.large durante seis meses ou até seus créditos acabarem.
> Para obter mais informações, consulte Benefícios do nível gratuito antes e depois de 15 de julho de 2025.

6. Em Key pair (login) (Par de chaves [login]), para Key pair name (Nome do par de chaves), escolha o par de chaves.
7. Em Network settings (Configurações de rede), faça o seguinte:

    a. Em Network (Rede) e Subnet (Sub-rede), se você não fez alterações na VPC ou nas sub-redes padrão, pode manter as configurações padrão.

    Se você fez alterações na VPC ou nas sub-redes padrão, verifique o seguinte:

    i. A instância e o banco de dados do RDS devem estar na mesma VPC para usar a configuração de conexão automática. Por padrão, você tem apenas uma VPC.

    ii. A VPC na qual você está iniciando a instância deve ter um gateway da Internet conectado a ela para que você possa acessar seu servidor Web pela Internet. Sua VPC padrão é configurada automaticamente com um gateway da Internet.

iii. Para garantir que a instância receba um endereço IP público, em Auto-assign public IP (Atribuir IP público automaticamente), verifique se a opção Enable (Habilitar) está selecionada. Se a opção Disable (Desabilitar) estiver selecionada, escolha Edit (Editar) à direita de Network Settings (Configurações de rede) e, para Auto-assign public IP (Atribuir IP público automaticamente), escolha Enable (Habilitar).

b. Para se conectar à instância usando SSH, é necessário ter uma regra de grupo de segurança que autorize o tráfego SSH (Linux) ou RDP (Windows) do endereço IPv4 público do computador. Por padrão, quando você executa uma instância, cria-se um novo grupo de segurança com uma regra que permite tráfego SSH de entrada de qualquer lugar.

   Para garantir que somente seu endereço IP possa se conectar à instância, em Firewall (grupos de segurança), na lista suspensa ao lado da caixa de seleção Permitir tráfego SSH de, escolha Meu IP.

c. Para permitir o tráfego da Internet para a instância, marque as seguintes caixas de seleção:

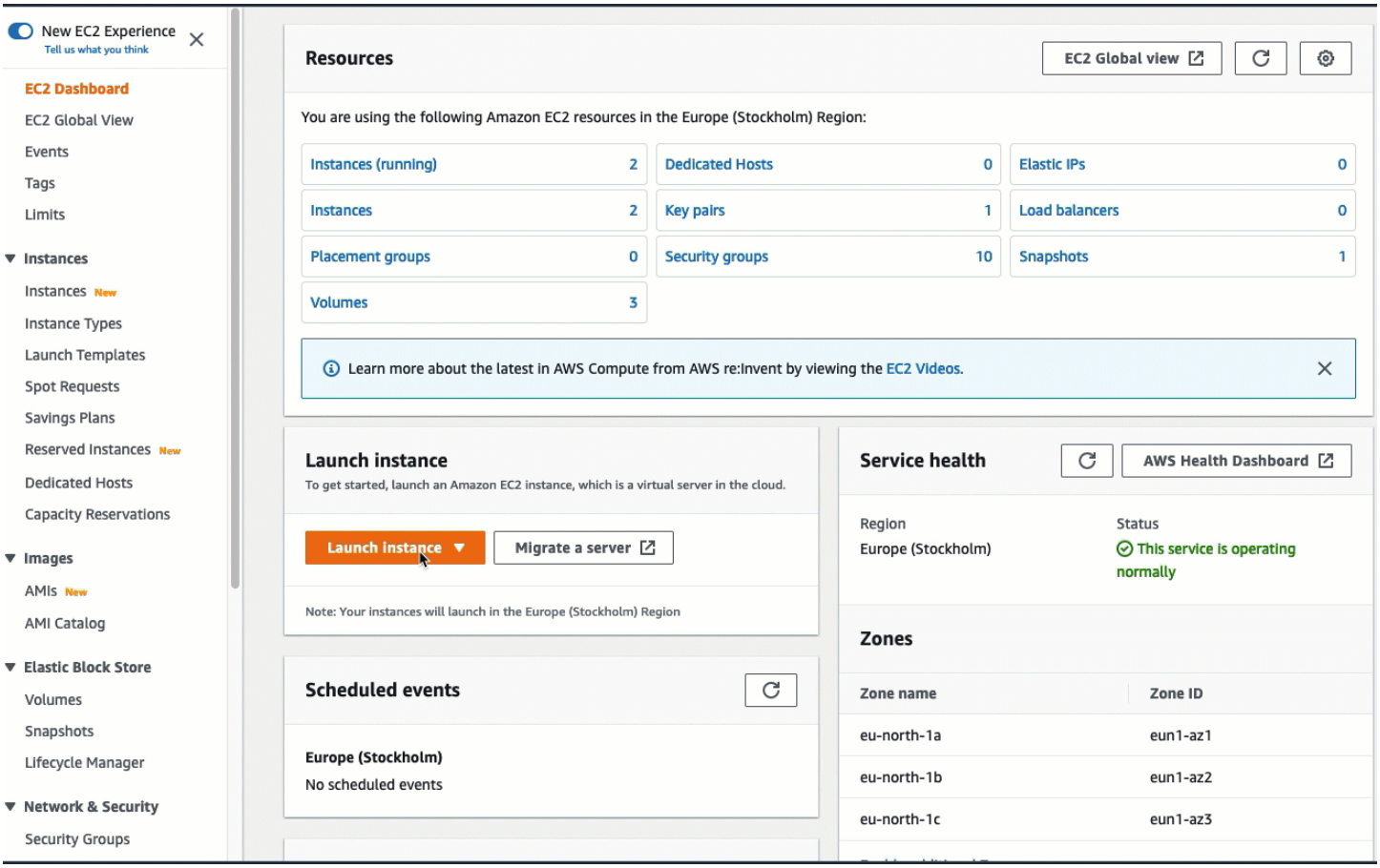
   - Permitir tráfego HTTPs da Internet
   - Permitir tráfego HTTP da Internet

8. No painel Summary (Resumo), analise a configuração da instância e selecione Launch instance (Iniciar instância).
9. Escolha View all instances (Visualizar todas as instâncias) para fechar a página de confirmação e voltar ao console. Sua instância estará primeiro em um estado `pending` e depois entrará no estado `running`.

   Se a instância não executar ou o estado passar imediatamente para `terminated`, em vez de `running`, consulte Solucionar problemas de inicialização de instâncias do Amazon EC2.

Para obter mais informações sobre como iniciar uma instância MySQL, consulte Executar uma instância do EC2 usando o assistente de inicialização de instâncias no console.

Visualizar uma animação: iniciar uma instância do EC2



Tarefa 2: criar um banco de dados do RDS e conectá-lo automaticamente à instância do EC2

O objetivo desta tarefa é criar um banco de dados do RDS e usar o recurso de conexão automática no console do RDS para configurar automaticamente a conexão entre a instância do EC2 e o banco de dados do RDS. As etapas desta tarefa configuram a instância do banco de dados da seguinte forma:

- Tipo de mecanismo: MySQL
- Modelo: nível gratuito
- Identificador da instância de banco de dados: **`tutorial-database`**
- Classe da instância de banco de dados: `db.t3.micro`

> **Important**
>
> Para um ambiente de produção, é necessário configurar a instância para atender às suas necessidades específicas.

Para criar um banco de dados do RDS e conectá-lo automaticamente a uma instância do EC2

1. Abra o console do Amazon RDS em https://console.aws.amazon.com/rds/.
2. No seletor Region (Região), no canto superior direito, escolha a Região da AWS na qual você criou a instância do EC2. A instância do EC2 e o banco de dados do RDS devem estar na mesma região.
3. No painel, escolha Create database (Criar banco de dados).
4. Em Choose a database creation method (Escolher um método de criação de banco de dados), verifique se a opção Standard Create (Criação padrão) está selecionada. Se você escolher Easy create (Criação fácil), o recurso de conexão automática não estará disponível.
5. Em Engine options (Opções de mecanismo), em Engine type (Tipo de mecanismo), escolha MySQL.
6. Em Templates (Modelos), escolha um modelo de exemplo que atenda às suas necessidades. Neste tutorial, escolha o Free tier (Nível gratuito) para criar um banco de dados do RDS sem nenhum custo. No entanto, observe que o nível gratuito só estará disponível se a conta for elegível. É possível ler mais escolhendo o link Info (Informações) na caixa Free tier (Nível gratuito).
7. Em Configurações, faça o seguinte:
   a. Em DB instance identifier (Identificador da instância de banco de dados), insira um nome para o banco de dados. Para este tutorial, insira **`tutorial-database`**.
   b. Em Master username (Nome de usuário principal), deixe o nome padrão, que é **`admin`**.
   c. Em Master password (Senha principal), digite uma senha da qual você consiga se lembrar para este tutorial e, em Confirm password (Confirmar senha), insira a senha novamente.
8. Em Configuração da instância, em Classe de instância de banco de dados, deixe o padrão, que é db.t3.micro. Se a conta for elegível para o nível gratuito, será possível usar essa instância gratuitamente. Para obter mais informações, consulte Nível gratuito da AWS.

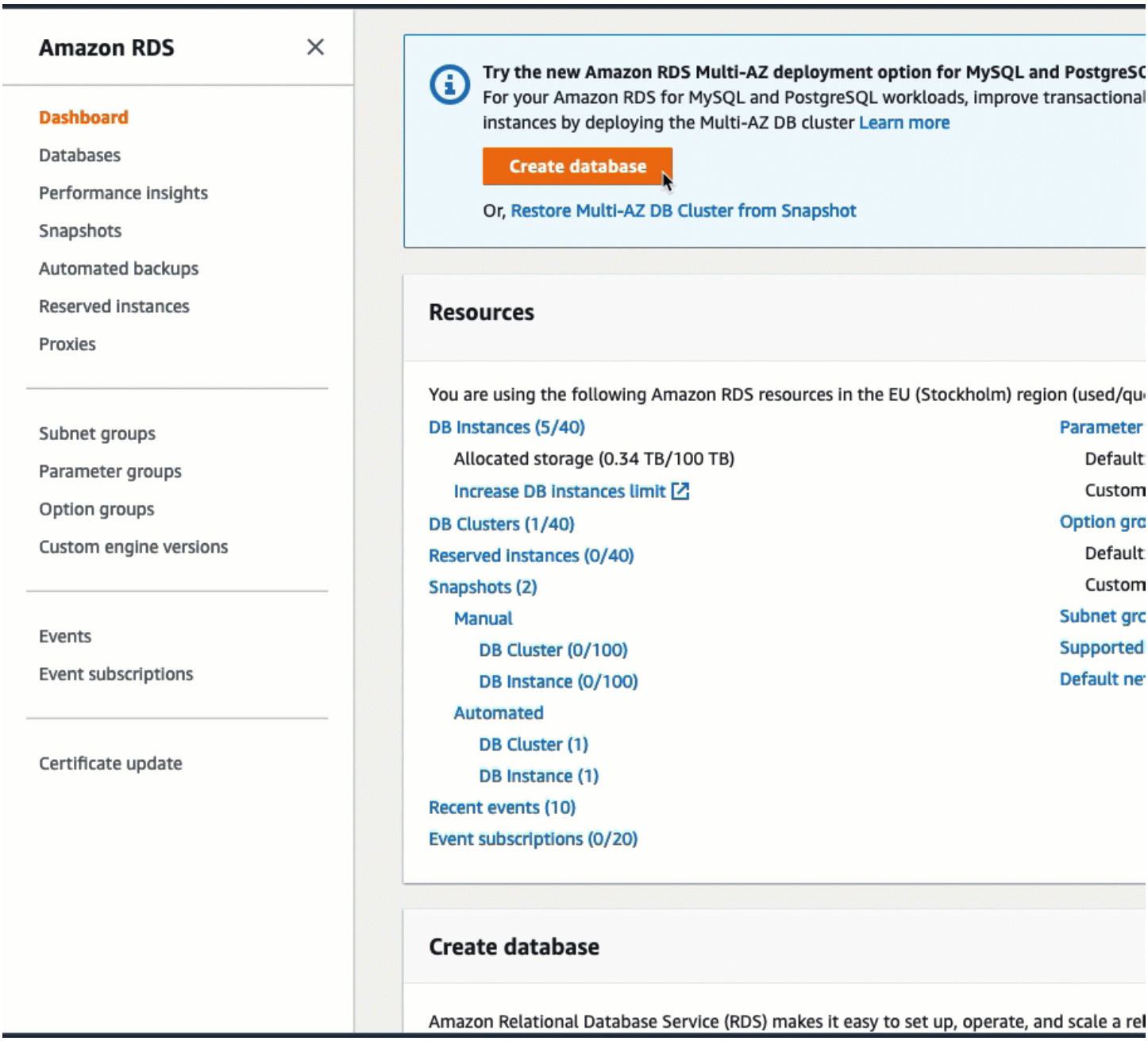
9. Em Connectivity (Conectividade), para Compute resource (Recurso de computação), escolha Connect to an EC2 compute resource (Conectar-se a um recurso de computação do EC2). Esse é o recurso de conexão automática no console do RDS.
10. Em EC2 instance (Instância do EC2), selecione o nome da instância à qual você deseja se conectar. Para os fins deste tutorial, você pode escolher a instância criada na tarefa anterior, chamada **`tutorial-instance`**, ou escolher outra instância existente. Caso não veja sua instância na lista, escolha o ícone de atualização à direita de Connectivity (Conectividade).

    Quando você usa o recurso de conexão automática, um grupo de segurança é adicionado a essa instância do EC2, e outro grupo de segurança é adicionado ao banco de dados do RDS. Os grupos de segurança são configurados automaticamente para permitir o tráfego entre a instância do EC2 e o banco de dados do RDS. Na próxima tarefa, você verificará se os grupos de segurança foram criados e atribuídos à instância do EC2 e ao banco de dados do RDS.
11. Selecione Criar banco de dados.

    Na tela Databases (Bancos de dados), o Status do novo banco de dados é Creating (Criando) até que o banco de dados esteja pronto para uso. Quando o status mudar para Available (Disponível), será possível conectar-se ao banco de dados. Dependendo da classe de banco de dados e da quantidade de armazenamento, pode levar até 20 minutos para que o novo banco de dados esteja disponível.

Para saber mais, consulte Configurar a conectividade automática de rede com uma instância do EC2 no Guia do usuário do Amazon RDS.

Visualizar uma animação: criar um banco de dados do RDS e conectar automaticamente a uma instância do EC2



Tarefa 3: verificar a configuração da conexão

O objetivo desta tarefa é verificar se os dois grupos de segurança foram criados e atribuídos à instância e ao banco de dados.

Quando você usa o recurso de conexão automática no console para configurar a conectividade, os grupos de segurança são criados automaticamente e atribuídos à instância e ao banco de dados da seguinte forma:

- O grupo de segurança rds-ec2-***x*** é criado e adicionado ao banco de dados do RDS. Ele tem uma regra de entrada que referencia o grupo de segurança ec2-rds-***x*** como origem. Isso permite que o tráfego da instância do EC2 com o grupo de segurança ec2-rds-***x*** atinja o banco de dados do RDS.
- O grupo de segurança ec2-rds-***x*** é criado e adicionado à instância do EC2. Ele tem uma regra de saída que referencia o grupo de segurança rds-ec2-***x*** como destino. Isso permite que o tráfego da instância do EC2 atinja o banco de dados do RDS com o grupo de segurança rds-ec2-***x***.

Para verificar a configuração da conexão usando o console

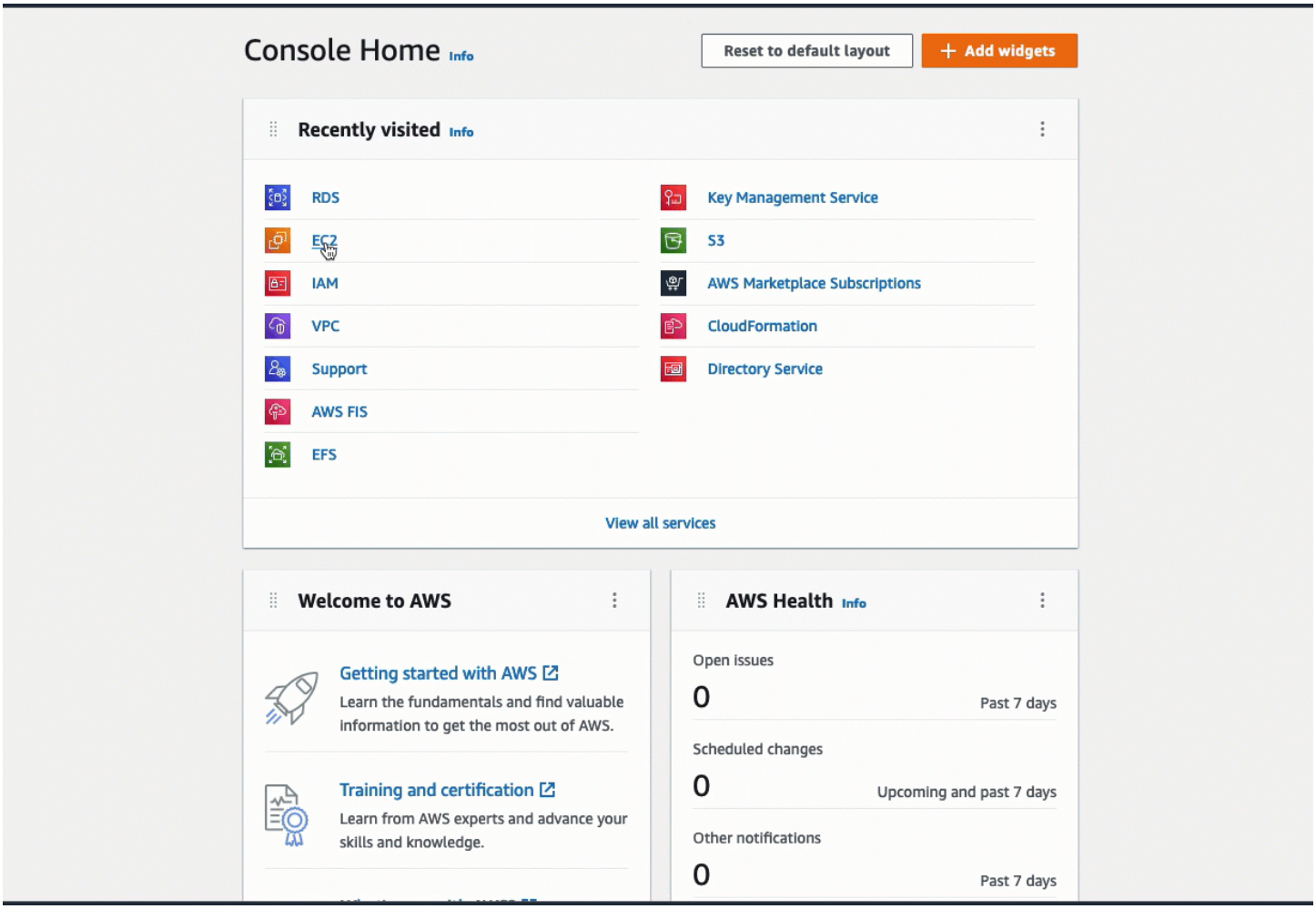
1. Abra o console do Amazon RDS em https://console.aws.amazon.com/rds/.
2. Na página de navegação, escolha Databases (Bancos de dados).
3. Escolha o banco de dados do RDS que você criou para este tutorial.
4. Na guia Conectividade e segurança, em Segurança, Grupos de segurança da VPC, verifique se um grupo de segurança chamado rds-ec2-***x*** está sendo exibido.
5. Escolha o grupo de segurança rds-ec2-***x***. A tela Security Groups (Grupos de segurança) no console do EC2 é aberta.
6. Escolha o grupo de segurança rds-ec2-***x*** para abrir.
7. Escolha a guia Regras de entrada.
8. Verifique se a seguinte regra de grupo de segurança existe, da seguinte forma:
   - Digite: MySQL/Aurora
   - Intervalo de porta: 3306
   - Origem: ***sg-0987654321example*** / ec2-rds-***x***: este é o grupo de segurança atribuído à instância do EC2 que você verificou nas etapas anteriores.
   - Descrição: regra para permitir conexões de instâncias do EC2 com ***sg-1234567890example*** anexado
9. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
10. No painel de navegação, escolha Instances (Instâncias).
11. Escolha a instância do EC2 que você selecionou para se conectar ao banco de dados do RDS na tarefa anterior e escolha a guia Security (Segurança).

12. Em Detalhes de segurança, Grupos de segurança, verifique se um grupo de segurança chamado ec2-rds-*x* está na lista. *x* é um número.
13. Escolha o grupo de segurança ec2-rds-*x* para abrir.
14. Escolha a guia Outbound rules (Regras de saída).
15. Verifique se a seguinte regra de grupo de segurança existe, da seguinte forma:

    - Digite: MySQL/Aurora
    - Intervalo de porta: 3306
    - Destino: ***sg-1234567890example*** / rds-ec2-*x*
    - Descrição: regra para permitir conexões a **`database-tutorial`** de qualquer instância à qual esse grupo de segurança esteja vinculado

Ao verificar se esses grupos de segurança e regras de grupos de segurança existem e se estão atribuídos ao banco de dados do RDS e à instância do EC2, conforme descrito neste procedimento, você pode verificar se a conexão foi configurada automaticamente usando o recurso de conexão automática.

Visualizar uma animação: verificar a configuração da conexão



Você concluiu a opção 2 deste tutorial. Agora você pode concluir a opção 3, que ensina a configurar manualmente os grupos de segurança que foram criados automaticamente na opção 2.

Tarefa 4 (opcional): limpar

> **Warning**
>
> O encerramento de uma instância é permanente e irreversível.
> Depois de encerrar uma instância, não será mais possível se conectar a ela e ela não poderá ser recuperada. Todos os volumes anexados do Amazon EBS configurados para serem excluídos no encerramento também serão excluídos permanentemente e não poderão ser recuperados. Todos os dados armazenados em volumes de armazenamento de instância serão perdidos permanentemente. Para obter mais informações, consulte Como funciona o encerramento de uma instância.

Antes de encerrar uma instância, certifique-se de ter feito backup de todos os dados que você precise reter após o encerramento no armazenamento persistente.

Agora que você concluiu o tutorial, é uma prática recomendada limpar (excluir) os recursos que não queira mais usar. Limpar os recursos da AWS evita que sua conta incorra em cobranças adicionais.

Se você iniciou uma instância do EC2 especificamente para este tutorial, pode encerrá-la para parar de incorrer em quaisquer cobranças associadas a ela.

Para encerrar 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 criada para este tutorial e escolha Instance state (Estado da instância), Terminate instance (Terminar instância).
4. Quando a confirmação for solicitada, escolha Encerrar.

Se você criou um banco de dados do RDS especificamente para este tutorial, pode excluí-lo para parar de incorrer em quaisquer cobranças associadas a ele.

Para excluir um banco de dados do RDS usando o console

1. Abra o console do Amazon RDS em https://console.aws.amazon.com/rds/.
2. No painel de navegação, escolha Databases (Bancos de dados).
3. Selecione o banco de dados do RDS criado para este tutorial e escolha Actions (Ações), Delete (Excluir).
4. Insira **`delete me`** na caixa e escolha Delete (Excluir).

Opção 3: conectar manualmente uma instância a um banco de dados do RDS criando grupos de segurança

O objetivo da opção 3 é aprender a configurar manualmente a conexão entre uma instância do EC2 e um banco de dados do RDS reproduzindo manualmente a configuração do recurso de conexão automática.

Tarefas

- Antes de começar
- Tarefa 1 (opcional): executar uma instância do EC2
- Tarefa 2 (opcional): criar um banco de dados do RDS
- Tarefa 3: conectar manualmente sua instância do EC2 ao banco de dados do RDS criando grupos de segurança e atribuindo-os às instâncias
- Tarefa 4 (opcional): limpar

Antes de começar

Você precisará do seguinte para concluir este tutorial:

- Uma instância do EC2 que está na mesma VPC do banco de dados do RDS. É possível usar uma instância do EC2 existente ou seguir as etapas na tarefa 1 para criar uma nova instância.
- Um banco de dados do RDS que está na mesma VPC da instância do EC2. É possível usar um banco de dados do RDS existente ou seguir as etapas na tarefa 2 para criar um novo banco de dados.
- Permissões para chamar estas operações:
  - `ec2:AssociateRouteTable`
  - `ec2:AuthorizeSecurityGroupEgress`
  - `ec2:CreateRouteTable`
  - `ec2:CreateSecurityGroup`
  - `ec2:CreateSubnet`
  - `ec2:DescribeInstances`
  - `ec2:DescribeNetworkInterfaces`
  - `ec2:DescribeRouteTables`
  - `ec2:DescribeSecurityGroups`
  - `ec2:DescribeSubnets`
  - `ec2:ModifyNetworkInterfaceAttribute`
  - `ec2:RevokeSecurityGroupEgress`

Tarefa 1 (opcional): executar uma instância do EC2

> **Note**
>
> O foco deste tutorial não é iniciar uma instância. Se você já tiver uma instância do Amazon EC2 e quiser usá-la neste tutorial, pode ignorar esta tarefa.

O objetivo desta tarefa é iniciar uma instância do EC2 para que você possa concluir a tarefa 3, na qual configura a conexão entre a instância do EC2 e o banco de dados do Amazon RDS. As etapas desta tarefa configuram a instância do EC2 da seguinte forma:

- Nome da instância: **`tutorial-instance`**
- AMI: Amazon Linux 2
- Tipo de instância: `t2.micro`
- Atribuir automaticamente IP público: habilitado
- Grupo de segurança com estas três regras:
  - Permitir SSH de seu endereço IP
  - Permitir tráfego HTTPS de qualquer lugar
  - Permitir tráfego HTTP de qualquer lugar

> **Important**
>
> Para um ambiente de produção, é necessário configurar a instância para atender às suas necessidades específicas.

Para iniciar uma instância do EC2

1. Faça login no Console de gerenciamento da AWS e abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel do EC2, escolha Launch Instance (Iniciar instância).
3. Em Name and tags (Nome e etiquetas), para Name (Nome), insira um nome para identificar a instância. Para este tutorial, insira o nome da instância **`tutorial-instance-manual-1`**. Embora o nome da instância não seja obrigatório, o nome o ajudará a identificá-la facilmente.

4. Em Application and OS Images (Imagens da aplicação e do sistema operacional), escolha uma AMI que atenda às necessidades de seu servidor Web. Este tutorial usa o Amazon Linux.
5. Em Instance type (Tipo de instância), para Instance type (Tipo de instância), selecione um tipo de instância que atenda às necessidades de seu servidor Web. Este tutorial usa `t2.micro`.

> **Note**
>
> Dependendo de quando sua conta foi criada, ela pode ser elegível para usar o Amazon EC2 no nível gratuito.
> Caso tenha criado sua Conta da AWS antes de 15 de julho de 2025 e ela tenha menos de 12 meses, será possível usar o Amazon EC2 no nível gratuito selecionando o tipo de instância t2.micro ou o tipo de instância t3.micro em regiões onde o tipo t2.micro estiver indisponível. Lembre-se de que, quando você executa uma instância t3.micro, o padrão é o modo Ilimitado, o que pode gerar cobranças adicionais com base no uso da CPU. Se um tipo de instância puder ser usada no nível gratuito, ela terá o rótulo Elegível para o nível gratuito.
> Se você tiver criado sua Conta da AWS a partir de 15 de julho de 2025, poderá usar os tipos de instância t3.micro, t3.small, t4g.micro, t4g.small, c7i-flex.large e m7i-flex.large durante seis meses ou até seus créditos acabarem.
> Para obter mais informações, consulte Benefícios do nível gratuito antes e depois de 15 de julho de 2025.

6. Em Key pair (login) (Par de chaves [login]), para Key pair name (Nome do par de chaves), escolha o par de chaves.
7. Em Network settings (Configurações de rede), faça o seguinte:

   a. Em Network (Rede) e Subnet (Sub-rede), se você não fez alterações na VPC ou nas sub-redes padrão, pode manter as configurações padrão.

      Se você fez alterações na VPC ou nas sub-redes padrão, verifique o seguinte:

      i. A instância deve estar na mesma VPC do banco de dados do RDS. Por padrão, você tem apenas uma VPC.

      ii. A VPC na qual você está iniciando a instância deve ter um gateway da Internet conectado a ela para que você possa acessar seu servidor Web pela Internet. Sua VPC padrão é configurada automaticamente com um gateway da Internet.

iii. Para garantir que a instância receba um endereço IP público, em Auto-assign public IP (Atribuir IP público automaticamente), verifique se a opção Enable (Habilitar) está selecionada. Se a opção Disable (Desabilitar) estiver selecionada, escolha Edit (Editar) à direita de Network Settings (Configurações de rede) e, para Auto-assign public IP (Atribuir IP público automaticamente), escolha Enable (Habilitar).

b. Para se conectar à instância usando SSH, é necessário ter uma regra de grupo de segurança que autorize o tráfego SSH (Linux) ou RDP (Windows) do endereço IPv4 público do computador. Por padrão, quando você executa uma instância, cria-se um novo grupo de segurança com uma regra que permite tráfego SSH de entrada de qualquer lugar.

   Para garantir que somente seu endereço IP possa se conectar à instância, em Firewall (grupos de segurança), na lista suspensa ao lado da caixa de seleção Permitir tráfego SSH de, escolha Meu IP.

c. Para permitir o tráfego da Internet para a instância, marque as seguintes caixas de seleção:

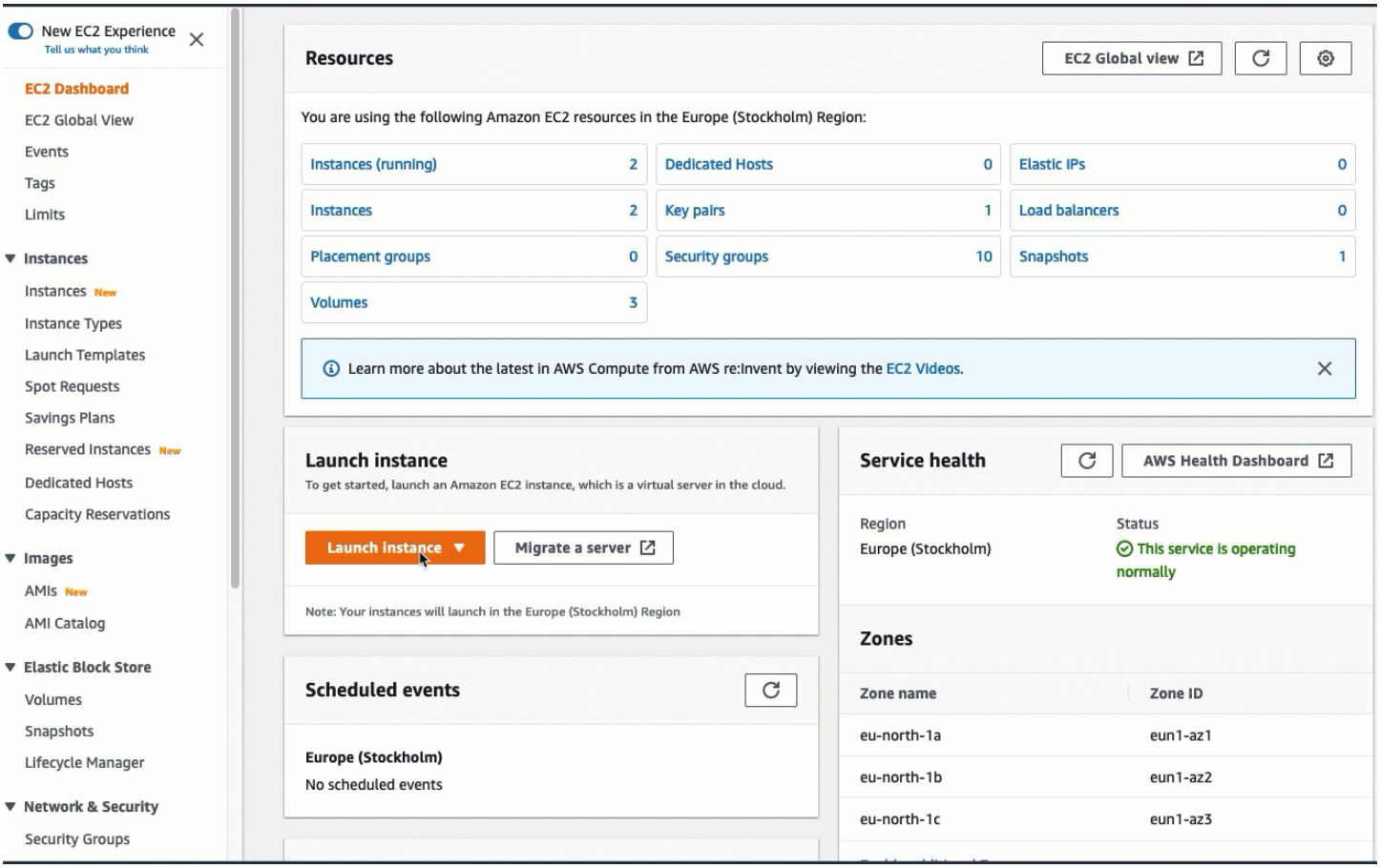
   - Permitir tráfego HTTPs da Internet
   - Permitir tráfego HTTP da Internet

8. No painel Summary (Resumo), analise a configuração da instância e selecione Launch instance (Iniciar instância).
9. Escolha View all instances (Visualizar todas as instâncias) para fechar a página de confirmação e voltar ao console. Sua instância estará primeiro em um estado `pending` e depois entrará no estado `running`.

   Se a instância não executar ou o estado passar imediatamente para `terminated`, em vez de `running`, consulte Solucionar problemas de inicialização de instâncias do Amazon EC2.

Para obter mais informações sobre como iniciar uma instância MySQL, consulte Executar uma instância do EC2 usando o assistente de inicialização de instâncias no console.

Visualizar uma animação: iniciar uma instância do EC2



Tarefa 2 (opcional): criar um banco de dados do RDS

> **Note**
>
> O foco desta parte do tutorial não é criar um banco de dados do RDS. Se você já tiver um banco de dados do RDS e quiser usá-lo para este tutorial, pode ignorar esta tarefa.

O objetivo desta tarefa é criar um banco de dados do RDS. Você usará essa instância na tarefa 3 ao conectá-la à instância do EC2. As etapas desta tarefa configuram o banco de dados do RDS da seguinte forma:

- Tipo de mecanismo: MySQL
- Modelo: nível gratuito
- Identificador da instância de banco de dados: **`tutorial-database-manual`**

- Classe da instância de banco de dados: `db.t3.micro`

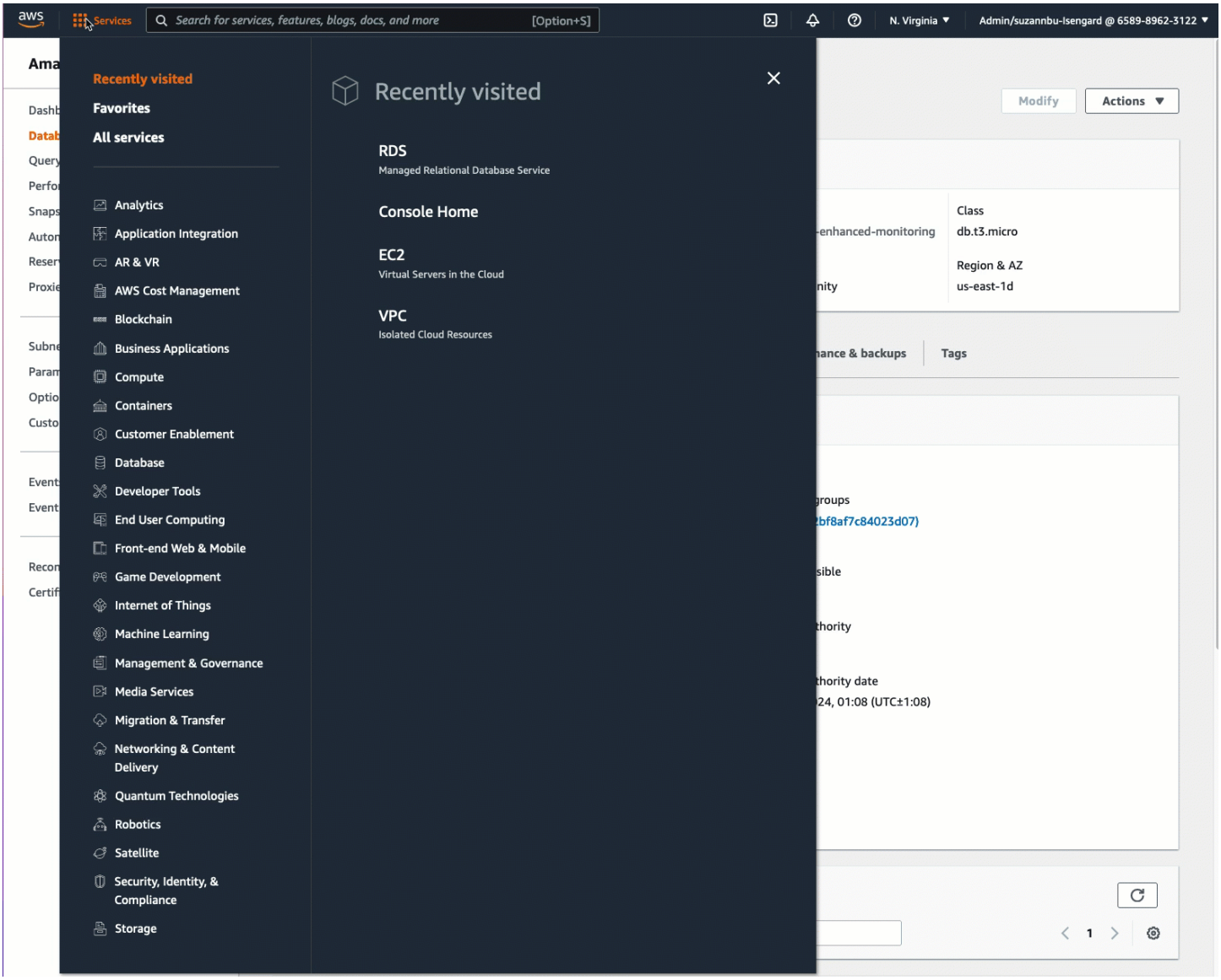
> **Important**
>
> Para um ambiente de produção, é necessário configurar a instância para atender às suas necessidades específicas.

Para criar uma instância de banco de dados MySQL

1. Abra o console do Amazon RDS em https://console.aws.amazon.com/rds/.
2. No seletor Region (Região), no canto superior direito, escolha a Região da AWS na qual você criou a instância do EC2. A instância do EC2 e a instância de banco de dados devem estar na mesma região.
3. No painel, escolha Create database (Criar banco de dados).
4. Em Choose a database creation method (Escolher um método de criação de banco de dados), escolha Easy create (Criação fácil). Quando você escolhe essa opção, o recurso de conexão automática para configurar automaticamente a conexão não está disponível.
5. Em Engine options (Opções de mecanismo), em Engine type (Tipo de mecanismo), escolha MySQL.
6. Em DB instance size (Tamanho da instância de banco de dados), escolha Free tier (Nível gratuito).
7. Em DB instance identifier (Identificador da instância de banco de dados), insira um nome para o banco de dados do RDS. Para este tutorial, insira **`tutorial-database-manual`**.
8. Em Master username (Nome de usuário principal), deixe o nome padrão, que é **`admin`**.
9. Em Master password (Senha principal), digite uma senha da qual você consiga se lembrar para este tutorial e, em Confirm password (Confirmar senha), insira a senha novamente.
10. Selecione Criar banco de dados.

    Na tela Databases (Bancos de dados), o Status da nova instância de banco de dados será Creating (Criando) até que a instância de banco de dados esteja pronta para uso. Quando o status muda para Available (Disponível), você pode se conectar à instância de banco de dados. Dependendo da classe da instância de banco de dados e da quantidade de armazenamento, pode levar até 20 minutos para que a nova instância esteja disponível.

Visualizar uma animação: criar uma instância de banco de dados



Tarefa 3: conectar manualmente sua instância do EC2 ao banco de dados do RDS criando grupos de segurança e atribuindo-os às instâncias

O objetivo desta tarefa é reproduzir a configuração de conexão do recurso de conexão automática executando o seguinte manualmente: você cria dois novos grupos de segurança e adiciona um grupo de segurança à instância do EC2 e ao banco de dados do RDS.

Para criar dois novos grupos de segurança e atribuir à instância do EC2 e outro ao banco de dados do RDS

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

2. Primeiro, crie o grupo de segurança para adicionar à instância do EC2, da seguinte forma:

   a. No painel de navegação, escolha Grupos de segurança.

   b. Escolha Create grupo de segurança (Criar grupo de segurança).

   c. Em Security group name (Nome do grupo de segurança), insira um nome descritivo para o grupo de segurança. Para este tutorial, insira **`ec2-rds-manual-configuration`**.

   d. Em Description (Descrição), insira uma breve descrição. Para este tutorial, insira **`EC2 instance security group to allow EC2 instance to securely connect to RDS database`**.

   e. Escolha Criar grupo de segurança. Você voltará a esse grupo de segurança para adicionar uma regra de saída depois de criar o grupo de segurança de banco de dados do RDS.

3. Agora, crie o grupo de segurança a ser adicionado ao banco de dados do RDS, da seguinte forma:

   a. No painel de navegação, escolha Grupos de segurança.

   b. Escolha Create grupo de segurança (Criar grupo de segurança).

   c. Em Security group name (Nome do grupo de segurança), insira um nome descritivo para o grupo de segurança. Para este tutorial, insira **`rds-ec2-manual-configuration`**.

   d. Em Description (Descrição), insira uma breve descrição. Para este tutorial, insira **`RDS database security group to allow EC2 instance to securely connect to RDS database`**.

   e. Em Inbound rules (Regras de entrada), selecione Add rule (Adicionar regra) e siga estas etapas:

      i. Em Type (Tipo), escolha MySQL/Aurora.

      ii. Em Source (Origem), escolha o grupo de segurança de instâncias ec2-rds-manual-configuration do EC2 que você criou na etapa 2 deste procedimento.

   f. Escolha Criar grupo de segurança.

4. Edite o grupo de segurança da instância do EC2 para adicionar uma regra de saída, da seguinte forma:

   a. No painel de navegação, escolha Security Groups (Grupos de segurança).

   b. Selecione o grupo de segurança da instância do EC2 (chamado **`ec2-rds-manual-configuration`**) e escolha a guia Outbound rules (Regras de saída).

   c. Escolha Edit outbound rules (Editar regras de saída).

d. Selecione Add rule (Adicionar regra) e faça o seguinte:

   i. Em Type (Tipo), escolha MySQL/Aurora.

   ii. Em Destino, escolha o grupo de segurança do banco de dados do RDS rds-ec2-manual-configuration criado na Etapa 3 deste procedimento.

   iii. Selecione Salvar rules.

5. Adicione o grupo de segurança da instância do EC2 à instância do EC2 da seguinte forma:

   a. No painel de navegação, escolha Instâncias.

   b. Selecione a instância do EC2 e escolha Actions (Ações), Security (Segurança), Change security groups (Alterar grupos de segurança).

   c. Em Associated security groups (Grupos de segurança associados), escolha o campo Select security groups (Selecionar grupos de segurança), escolha ec2-rds-manual-configuration criado anteriormente e escolha Add security group (Adicionar grupo de segurança).

   d. Escolha Salvar.

6. Adicione o grupo de segurança do banco de dados do RDS ao banco de dados do RDS, da seguinte forma:

   a. Abra o console do Amazon RDS em https://console.aws.amazon.com/rds/.

   b. No painel de navegação, escolha Databases (Bancos de dados) e selecione o banco de dados.

   c. Escolha Modificar.

   d. Em Connectivity (Conectividade), para Security group (Grupo de segurança), escolha rds-ec2-manual-configuration criado anteriormente e escolha Continue (Continuar).

   e. Em Scheduling of modifications (Programação de modificações), escolha Apply immediately (Aplicar imediatamente).

   f. Selecione Modify DB instance (Modificar instância de banco de dados).

   Agora você concluiu as etapas manuais que imitam as etapas automáticas que ocorrem ao usar o recurso de conexão automática.

Você concluiu a opção 3 deste tutorial. Se você concluiu as opções 1, 2 e 3 e não precisa mais dos recursos criados neste tutorial, exclua-os para evitar custos desnecessários. Para obter mais informações, consulte Tarefa 4 (opcional): limpar.

Tarefa 4 (opcional): limpar

> **Warning**
>
> O encerramento de uma instância é permanente e irreversível.
> Depois de encerrar uma instância, não será mais possível se conectar a ela e ela não poderá ser recuperada. Todos os volumes anexados do Amazon EBS configurados para serem excluídos no encerramento também serão excluídos permanentemente e não poderão ser recuperados. Todos os dados armazenados em volumes de armazenamento de instância serão perdidos permanentemente. Para obter mais informações, consulte Como funciona o encerramento de uma instância.
> Antes de encerrar uma instância, certifique-se de ter feito backup de todos os dados que você precise reter após o encerramento no armazenamento persistente.

Agora que você concluiu o tutorial, é uma prática recomendada limpar (excluir) os recursos que não queira mais usar. Limpar os recursos da AWS evita que sua conta incorra em cobranças adicionais.

Se você iniciou uma instância do EC2 especificamente para este tutorial, pode encerrá-la para parar de incorrer em quaisquer cobranças associadas a ela.

Para encerrar 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 criada para este tutorial e escolha Instance state (Estado da instância), Terminate instance (Terminar instância).
4. Quando a confirmação for solicitada, escolha Encerrar.

Se você criou um banco de dados do RDS especificamente para este tutorial, pode excluí-lo para parar de incorrer em quaisquer cobranças associadas a ele.

Para excluir um banco de dados do RDS usando o console

1. Abra o console do Amazon RDS em https://console.aws.amazon.com/rds/.
2. No painel de navegação, escolha Databases (Bancos de dados).

3. Selecione o banco de dados do RDS criado para este tutorial e escolha Actions (Ações), Delete (Excluir).
4. Insira **`delete me`** na caixa e escolha Delete (Excluir).

Frota do EC2 e frota spot

A frota do EC2 e a frota spot se destinam a constituírem uma forma útil de inicializar uma frota de dezenas, centenas ou milhares de instâncias do Amazon EC2 em uma única operação. Cada instância em uma frota é configurada por um modelo de inicialização ou por um conjunto de parâmetros de inicialização que você configura manualmente na inicialização.

Tópicos

- Recursos e benefícios
- Qual é o melhor método de frota a ser usado?
- Opções de configuração para frota do EC2 ou frota spot
- Trabalhar com uma frota do EC2
- Trabalhar com frotas spot
- Monitorar o EC2 Fleet ou a frota spot
- Tutoriais para o EC2 Fleet
- Exemplo de configurações da CLI para frotas do EC2
- Exemplo de configurações da CLI para frotas spot
- Cotas para frotas do EC2 e frotas spot

Recursos e benefícios

As frotas proporcionam os recursos e benefícios a seguir, permitindo que você maximize a economia de custos e otimize a disponibilidade e a performance quando executar aplicações em várias instâncias do EC2.

Vários tipos de instâncias

Uma frota pode inicializar vários tipos de instâncias, garantindo que não dependa da disponibilidade de um único tipo de instância. Isso aumenta a disponibilidade geral das instâncias na frota.

Distribuição de instâncias entre zonas de disponibilidade

Uma frota pode ser inicializada em várias zonas de disponibilidade, permitindo que você reduza custos e melhore a disponibilidade. Se sua frota incluir instâncias spot, ela selecionará

automaticamente as zonas de disponibilidade com base em suas preferências em relação a preços e interrupções.

Várias opções de compra

Uma frota pode inicializar várias opções de compra (instâncias spot e instâncias sob demanda), permitindo que você otimize os custos por meio do uso da instância spot. Você também pode aproveitar os descontos da instância reservada e dos Savings Plans usando-os com as instâncias sob demanda na frota.

Substituição automatizada de instâncias spot

Se a frota incluir instâncias spot, ela poderá solicitar automaticamente a reposição da capacidade spot se as instâncias spot forem interrompidas. Por meio do Rebalanceamento de capacidade, uma frota também pode monitorar e substituir proativamente as instâncias spot que apresentem risco elevado de interrupção.

Reservar capacidade sob demanda

Uma frota pode usar uma Reserva de capacidade sob demanda para reservar capacidade sob demanda. Uma frota também pode incluir Blocos de capacidade para ML, permitindo que você reserve instâncias de GPU para uma data futura a fim de viabilizar workloads de machine learning (ML) de curta duração.

Qual é o melhor método de frota a ser usado?

Como prática recomendada geral, recomendamos executar as frotas de instâncias spot e sob demanda com o Amazon EC2 Auto Scaling, pois ele fornece recursos adicionais que você pode usar para gerenciar sua frota. A lista de recursos adicionais inclui substituições automáticas da verificação de integridade para instâncias spot e sob demanda, verificações de integridade baseadas em aplicações e uma integração com o Elastic Load Balancing para garantir uma distribuição uniforme do tráfego de aplicações para as suas instâncias íntegras. Você também pode usar os grupos do Auto Scaling ao utilizar serviços da AWS, como o Amazon ECS, o Amazon EKS (grupos de nós autogerenciados) e o Amazon VPC Lattice. Para mais informações, consulte o Guia do usuário do Amazon EC2 Auto Scaling.

Caso não possa usar o Amazon EC2 Auto Scaling, considere usar o EC2 Fleet ou a frota spot. A frota do EC2 e a frota spot oferecem a mesma funcionalidade principal. No entanto, a frota do EC2 só está disponível por meio de uma linha de comando e não fornece suporte a console. A frota spot fornece suporte a console, mas ela se baseia em uma API herdada e sem investimento planejado.

Use a tabela a seguir para determinar o método de frota que será usado.

Método de frota	Quando usar?	Caso de uso
Amazon EC2 Auto Scaling	• Você precisa de várias instâncias com uma só configuração ou uma configuração mista. • Você deseja automatizar o gerenciamento do ciclo de vida das instâncias.	Crie um grupo do Auto Scaling que gerencie o ciclo de vida de suas instâncias enquanto mantém o número desejado de instâncias. Compatível com dimensionamento horizontal da escala (adição de mais instâncias) entre os limites mínimo e máximo especificados.
Frota do EC	• Você precisa de várias instâncias com uma só configuração ou uma configuração mista. • Você deseja gerenciar por conta própria o ciclo de vida da instância. • Se não precisar de ajuste de escala automático, recomendamos que use um tipo `instant` de frota do EC2.	Crie uma frota `instant` de instâncias sob demanda e instâncias spot em uma única operação, com várias especificações de inicialização, que variem de acordo com o tipo de instância, com a AMI, com a zona de disponibilidade ou com a sub-rede. Por padrão, a estratégia de alocação da instância spot usa `lowest-price` por unidade, mas recomendamos alterá-la para `price-capacity-optimized`.
Frota spot	• Desencorajamos firmemente o uso da frota spot, pois ela se baseia em uma API herdada e sem investimento planejado.	Use a frota spot somente se precisar de suporte ao console para um caso de uso em que você usaria a frota do EC2.

Método de frota	Quando usar?	Caso de uso
	• Se você quiser gerenciar o ciclo de vida da instância, use a frota do EC2. • Se não quiser gerenciar o ciclo de vida da instância , use um grupo do Auto Scaling.	

Opções de configuração para frota do EC2 ou frota spot

Quando você planejar uma frota do EC2 ou frota spot, recomendamos que você considere as opções a seguir quando decidir como configurar a frota.

Opção de configuração	Pergunta	Documentação
Tipo de solicitação de frota	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?	Tipos de solicitação de frota do EC2 e de frota spot
Instâncias spot	Você planeja incluir instâncias spot na frota? Analise as práticas recomendadas de spot e use-as ao planejar a frota para poder provisionar as instâncias com o menor preço possível.	Práticas recomendadas para instâncias spot do Amazon EC2
Limite de gastos da frota	Você quer limitar o valor a ser pago pela frota por hora?	Definir um limite de gastos para a frota do EC2 ou a frota spot
Tipos de instância e seleção de tipo de	Você quer especificar os tipos de instância na frota ou permitir que o Amazon EC2 selecione os tipos de instância que atendam aos requisitos da sua aplicação?	Especificar atributos para seleção de tipo de instância para frota do EC2 ou frota spot

Opção de configuração	Pergunta	Documentação
instância baseada em atributos		
Ponderação de instâncias	Você quer atribuir pesos a cada tipo de instância para representar sua capacidade computacional e sua performance para que o Amazon EC2 possa selecionar qualquer combinação de tipos de instância disponíveis para atender à capacidade de destino?	Usar ponderação de instâncias para gerenciar o custo e a performance da frota do EC2 ou da frota spot
Estratégias de alocação	Você quer decidir se deseja otimizar a capacidade disponível, o preço ou os tipos de instância para usar nas instâncias spot e nas instâncias sob demanda da frota?	Usar estratégias de alocação para determinar como a frota do EC2 ou a frota spot atende à capacidade spot e sob demanda
Rebalanceamento de capacidade	Você quer que a frota substitua automaticamente as instâncias spot em risco?	Use o rebalanceamento de capacidade na frota do EC2 e na frota spot para substituir instâncias spot em risco
Reserva de capacidade sob demanda	Você quer reservar capacidade para as instâncias sob demanda da frota?	Use reservas de capacidade para reservar capacidade sob demanda na frota do EC2

Tipos de solicitação de frota do EC2 e de frota spot

O tipo de solicitação de uma frota do EC2 ou de frota spot determina se a solicitação é síncrona ou assíncrona e se é uma solicitação única da capacidade de destino desejada ou um esforço contínuo

para manter a capacidade ao longo do tempo. Ao configurar a frota, você deve especificar o tipo de solicitação.

Tanto a frota do EC2 quanto a frota spot oferecem dois tipos de solicitação: `request` e `maintain`. Além disso, a frota do EC2 oferece um terceiro tipo de solicitação, denominado `instant`.

Tipos de solicitação de frota

`instant` (Somente para frota do EC2)

Se você configurar o tipo de solicitação como `instant`, a Frota do EC2 incluirá uma solicitação síncrona única da capacidade desejada. A resposta da API retorna as instâncias que foram iniciadas e fornece os erros das instâncias que não puderam ser iniciadas. Para obter mais informações, consulte Configurar um EC2 Fleet do tipo instant.

`request`

Se você configurar o tipo de solicitação como `request`, a frota fará uma solicitação assíncrona única da capacidade desejada. Se a capacidade diminuir devido a interrupções de spot, a frota não tentará reabastecer as instâncias spot nem enviará solicitações em grupos de capacidade spot alternativos se a capacidade estiver indisponível. Quando você criar uma frota spot do tipo `request` usando o console, desmarque a caixa de seleção Manter a capacidade de destino.

`maintain` (padrão)

Se você configurar o tipo de solicitação como `maintain`, a frota fará uma solicitação assíncrona única da capacidade desejada e manterá a capacidade ao reabastecer automaticamente as instâncias spot interrompidas. Quando você criar uma frota spot do tipo `maintain` usando o console, marque a caixa de seleção Manter a capacidade de destino

Configurar um EC2 Fleet do tipo instant

A EC2 Fleet do tipo instantâneo é uma solicitação síncrona única que faz apenas uma tentativa de iniciar a capacidade desejada. A resposta da API lista as instâncias que foram iniciadas juntamente com os erros das instâncias que não puderam ser iniciadas. Há vários benefícios de se usar uma EC2 Fleet do tipo Instantâneo, e eles são descritos neste artigo. Exemplos de configurações são fornecidos no fim do artigo.

Para workloads que precisam de uma API somente de inicialização para iniciar instâncias do EC2, você pode usar a API RunInstances. No entanto, com RunInstances, você só pode iniciar Instâncias

sob demanda ou instâncias spot, mas não ambas na mesma solicitação. Além disso, quando você usa RunInstances para iniciar Instâncias spot, sua solicitação de Instância spot é limitada a um tipo de instância e a uma zona de disponibilidade. Isso visa um único grupo de capacidade spot (um conjunto de instâncias com o mesmo tipo de instância e zona de disponibilidade). Se o grupo de capacidade spot não tiver capacidade de instância spot suficiente para sua solicitação, a chamada RunInstances não tem sucesso.

Em vez de usar RunInstances para iniciar Instâncias spot, é recomendável usar a API CreateFleet com o parâmetro `type` definido como `instant` para obter os seguintes benefícios:

- Iniciar Instâncias sob demanda e instâncias spot em uma única solicitação. Uma EC2 Fleet pode iniciar Instâncias sob demanda, instâncias spot ou ambas. A solicitação das Instâncias spot é atendida se houver capacidade disponível e o preço máximo por hora para sua solicitação excede o preço Spot.
- Aumente a disponibilidade das instâncias spot. Usando uma EC2 Fleet do tipo `instant`, você pode iniciar instâncias spot seguindo as Práticas recomendadas para spot com os benefícios decorrentes disso:
  - Prática recomendada para spot: seja flexível sobre tipos de instância e zonas de disponibilidade.

    Benefício: especificando vários tipos de instância e zonas de disponibilidade, você aumenta o número de grupos de capacidade spot. Isso dá ao serviço de spot uma chance maior de encontrar e alocar sua capacidade computacional spot desejada. Uma boa regra geral é ser flexível em pelo menos 10 tipos de instância para cada workload e garantir que todas as zonas de disponibilidade estejam configuradas para uso na sua VPC.
  - Prática recomendada para spot: use a estratégia de alocação de price-capacity-optimized.

    Benefício: a estratégia de alocação de `price-capacity-optimized` identifica instâncias nos grupos de capacidade spot com maior disponibilidade e provisiona as instâncias de menor preço desses grupos. Como a capacidade de instâncias spot é proveniente de grupos com capacidade ideal, isso diminui a possibilidade de que as instâncias spot sejam interrompidas quando o Amazon EC2 precisar recuperar capacidade.
- Tenha acesso a um conjunto mais amplo de recursos. Para workloads que precisam de uma API somente de lançamento e em que você prefere gerenciar o ciclo de vida de sua instância em vez de deixar a frota EC2 gerenciá-lo para você, use a EC2 Fleet do tipo `instant` em vez da API RunInstances. A EC2 Fleet fornece um conjunto mais amplo de recursos do que o RunInstances, conforme demonstrado nos exemplos a seguir. Para todas as outras workloads, você deve usar o Amazon EC2 Auto Scaling, porque ele fornece um conjunto de recursos mais abrangente

para uma grande variedade de workloads, como aplicativos apoiados pelo ELB, workloads em contêineres e trabalhos de processamento de fila.

Você pode usar a Frota do EC2 do tipo instantânea para iniciar instâncias em blocos de capacidade. Para obter mais informações, consulte Tutorial: configurar o EC2 Fleet para executar instâncias em blocos de capacidade.

Os serviços da AWS, como o Amazon EC2 Auto Scaling e o Amazon EMR, usam o tipo de EC2 Fleet instantâneo para iniciar instâncias do EC2.

Pré-requisitos para a EC2 Fleet do tipo instantâneo

Para obter os pré-requisitos para criar uma EC2 Fleet, consulte Pré-requisitos da Frota do EC2.

Como uma EC2 Fleet instantânea funciona

Ao trabalhar com uma EC2 Fleet do tipo `instant`, a sequência de eventos é a seguinte:

1. Configuração: configure o tipo de solicitação CreateFleet como `instant`. Para obter mais informações, consulte Criar uma Frota do EC2.. Observe que, após fazer a chamada de API, você não pode modificá-la.
2. Solicitação: ao efetuar a chamada de API, o Amazon EC2 realizará uma solicitação síncrona única para a capacidade desejada.
3. Resposta: a resposta da API lista as instâncias que foram iniciadas, juntamente com os erros das instâncias que não puderam ser iniciadas.
4. Descrição: é possível descrever a frota do EC2, listar as instâncias associadas à sua frota do EC2 e visualizar o histórico da frota do EC2.
5. Encerramento de instâncias: é possível encerrar as instâncias a qualquer momento.
6. Solicitação de exclusão de frota: a solicitação de frota pode ser excluída manual ou automaticamente:
   - Manual: é possível excluir a solicitação de frota após a inicialização das instâncias.

     Observe que não há suporte para a exclusão de uma frota `instant` com instâncias em execução. Ao excluir uma frota `instant`, o Amazon EC2 encerra automaticamente todas as suas instâncias. Para frotas com mais de mil instâncias, a solicitação de exclusão pode não ser bem-sucedida. Caso sua frota contenha mais de mil instâncias, encerre manualmente a maioria delas, deixando mil ou menos. Em seguida, exclua a frota, e as instâncias restantes serão encerradas automaticamente.

- Automático: o Amazon EC2 exclui a solicitação de frota após algum tempo, caso ocorra um dos seguintes eventos:
  - Todas as instâncias estão encerradas.
  - A frota não consegue iniciar nenhuma instância.

Exemplos

Os exemplos a seguir mostram como usar a EC2 Fleet do tipo `instant` para diferentes casos de uso. Para obter mais informações sobre como usar os parâmetros da APICreateFleet do EC2, consulte Criar frota na Referência de API do Amazon EC2.

Exemplos

- Exemplo 1: Iniciar instâncias spot com a estratégia de alocação otimizada para capacidade
- Exemplo 2: iniciar uma única instância spot com a estratégia de alocação otimizada para capacidade
- Exemplo 3: iniciar uma frota spot usando pesos de instâncias
- Exemplo 4: executar instâncias spot dentro de uma única zona de disponibilidade
- Exemplo 5: iniciar instâncias spot de um tipo de instância único dentro de uma única zona de disponibilidade
- Exemplo 6: iniciar instâncias spot somente se a capacidade mínima pretendida puder ser iniciada
- Exemplo 7: iniciar instâncias spot apenas se a capacidade mínima pretendida puder ser iniciada do mesmo tipo de instância em uma única zona de disponibilidade
- Exemplo 8: iniciar instâncias com vários modelos de lançamento
- Exemplo 9: iniciar instância spot com uma base de Instâncias sob demanda
- Exemplo 10: iniciar Instâncias spot usando uma estratégia de alocação otimizada para capacidade com uma base de Instâncias sob demanda usando Reservas de Capacidade e a estratégia de alocação priorizada
- Exemplo 11: iniciar Instâncias spot usando a estratégia de alocação capacity-optimized-prioritized
- Exemplo 12: especifique um parâmetro do Systems Manager em vez de um ID de AMI

Exemplo 1: Iniciar instâncias spot com a estratégia de alocação otimizada para capacidade

O exemplo a seguir especifica os parâmetros mínimos necessários em uma EC2 Fleet do tipo `instant`: um modelo de lançamento, a capacidade pretendida, a opção de compra padrão e as substituições do modelo de lançamento.

- O modelo de lançamento é identificado por nome e número de versão do modelo de lançamento.
- As 12 substituições do modelo de lançamento especificam 4 tipos de instância diferentes e 3 sub-redes diferentes, cada uma em uma zona de disponibilidade separada. Cada combinação de tipo de instância e sub-rede define um grupo de capacidade spot, resultando em 12 pools de capacidade spot.
- A capacidade mínima pretendida para a frota é de 20 instâncias.
- A opção de compra padrão é `spot`, o que resulta na tentativa da frota de iniciar 20 instâncias spot no grupo de capacidade spot com a capacidade ideal para o número de instâncias que estão sendo iniciadas.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized"
    },
    "LaunchTemplateConfigs": [
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt1",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-49e41922"
            },
            {
```

```
            "InstanceType":"c5d.large",
            "SubnetId":"subnet-fae8c380"
         },
         {
            "InstanceType":"c5d.large",
            "SubnetId":"subnet-e7188bab"
         },
         {
            "InstanceType":"c5d.large",
            "SubnetId":"subnet-49e41922"
         },
         {
            "InstanceType":"m5.large",
            "SubnetId":"subnet-fae8c380"
         },
         {
            "InstanceType":"m5.large",
            "SubnetId":"subnet-e7188bab"
         },
         {
            "InstanceType":"m5.large",
            "SubnetId":"subnet-49e41922"
         },
         {
            "InstanceType":"m5d.large",
            "SubnetId":"subnet-fae8c380"
         },
         {
            "InstanceType":"m5d.large",
            "SubnetId":"subnet-e7188bab"
         },
         {
            "InstanceType":"m5d.large",
            "SubnetId":"subnet-49e41922"
         }
      ]
   }
],
"TargetCapacitySpecification": {
    "TotalTargetCapacity": 20,
    "DefaultTargetCapacityType": "spot"
},
"Type": "instant"
```

```
}
```

Exemplo 2: iniciar uma única instância spot com a estratégia de alocação otimizada para capacidade

Você pode iniciar de forma ideal uma instância spot de cada vez fazendo várias chamadas de API da EC2 Fleet do tipo `instant`, definindo o TotalTargetCapacity como 1.

O exemplo a seguir especifica os parâmetros mínimos necessários em uma EC2 Fleet do tipo instantâneo: um modelo de lançamento, a capacidade pretendida, a opção de compra padrão e as substituições do modelo de lançamento. O modelo de lançamento é identificado por nome e número de versão do modelo de lançamento. As 12 substituições do modelo de lançamento têm 4 tipos de instância diferentes e 3 sub-redes diferentes, cada uma em uma zona de disponibilidade separada. A capacidade pretendida da frota é 1 instância, e a opção de compra padrão é spot, o que resulta na tentativa da frota de iniciar uma instância spot a partir de um dos 12 grupos de capacidade spot com base na estratégia de alocação otimizada para capacidade, para iniciar uma instância spot a partir do grupo de capacidade mais disponível.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized"
    },
    "LaunchTemplateConfigs": [
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt1",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"c5d.large",
```

```
                "SubnetId":"subnet-fae8c380"
            },
            {
                "InstanceType":"c5d.large",
                "SubnetId":"subnet-e7188bab"
            },
            {
                "InstanceType":"c5d.large",
                "SubnetId":"subnet-49e41922"
            },
            {
                "InstanceType":"m5.large",
                "SubnetId":"subnet-fae8c380"
            },
            {
                "InstanceType":"m5.large",
                "SubnetId":"subnet-e7188bab"
            },
            {
                "InstanceType":"m5.large",
                "SubnetId":"subnet-49e41922"
            },
            {
                "InstanceType":"m5d.large",
                "SubnetId":"subnet-fae8c380"
            },
            {
                "InstanceType":"m5d.large",
                "SubnetId":"subnet-e7188bab"
            },
            {
                "InstanceType":"m5d.large",
                "SubnetId":"subnet-49e41922"
            }
         ]
      }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 1,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

Exemplo 3: iniciar uma frota spot usando pesos de instâncias

Os exemplos a seguir usam o peso da instância, o que significa que o preço é por hora em vez de ser por hora de instância. Cada configuração de execução lista um tipo de instância diferente e um peso diferente com base em quantas unidades da workload podem ser executadas na instância, pressupondo que uma unidade da workload requeira 15 GB de memória e 4 vCPUs. Por exemplo, m5.xlarge (4 vCPUs e 16 GB de memória) pode executar uma unidade e tem peso 1, m5.2xlarge (8 vCPUs e 32 GB de memória) pode executar 2 unidades e tem peso 2, e assim por diante. A capacidade total pretendida é definida como 40 unidades. A opção de compra padrão é spot, e a estratégia de alocação é otimizada para capacidade, o que resulta em 40 m5.xlarge (40 dividido por 1), 20 m5.2xlarge (40 dividido por 2), 10 m5.4xlarge (40 dividido por 4), 5 m5.8xlarge (40 dividido por 8) ou uma combinação de tipos de instância com pesos que somam a capacidade desejada com base na estratégia de alocação otimizada para capacidade.

Para obter mais informações, consulte Usar ponderação de instâncias para gerenciar o custo e a performance da frota do EC2 ou da frota spot.

```
{
   "SpotOptions":{
      "AllocationStrategy":"capacity-optimized"
   },
   "LaunchTemplateConfigs":[
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt1",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"m5.xlarge",
               "SubnetId":"subnet-fae8c380",
               "WeightedCapacity":1
            },
            {
               "InstanceType":"m5.xlarge",
               "SubnetId":"subnet-e7188bab",
               "WeightedCapacity":1
            },
            {
               "InstanceType":"m5.xlarge",
               "SubnetId":"subnet-49e41922",
               "WeightedCapacity":1
```

```
            },
            {
               "InstanceType":"m5.2xlarge",
               "SubnetId":"subnet-fae8c380",
               "WeightedCapacity":2
            },
            {
               "InstanceType":"m5.2xlarge",
               "SubnetId":"subnet-e7188bab",
               "WeightedCapacity":2
            },
            {
               "InstanceType":"m5.2xlarge",
               "SubnetId":"subnet-49e41922",
               "WeightedCapacity":2
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-fae8c380",
               "WeightedCapacity":4
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-e7188bab",
               "WeightedCapacity":4
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-49e41922",
               "WeightedCapacity":4
            },
            {
               "InstanceType":"m5.8xlarge",
               "SubnetId":"subnet-fae8c380",
               "WeightedCapacity":8
            },
            {
               "InstanceType":"m5.8xlarge",
               "SubnetId":"subnet-e7188bab",
               "WeightedCapacity":8
            },
            {
               "InstanceType":"m5.8xlarge",
               "SubnetId":"subnet-49e41922",
```

```
               "WeightedCapacity":8
            }
         ]
      }
   ],
   "TargetCapacitySpecification":{
      "TotalTargetCapacity":40,
      "DefaultTargetCapacityType":"spot"
   },
   "Type":"instant"
}
```

Exemplo 4: executar instâncias spot dentro de uma única zona de disponibilidade

Você pode configurar uma frota para iniciar todas as instâncias em uma única zona de disponibilidade definindo as opções de spot SingleAvailabilityZone como true.

As 12 substituições do modelo de lançamento têm tipos de instância e sub-redes diferentes (cada uma em uma zona de disponibilidade separada), mas a mesma capacidade ponderada. A capacidade total pretendida é de 20 instâncias, a opção de compra padrão é spot e a estratégia de alocação spot é otimizada para capacidade. A EC2 Fleet inicia 20 instâncias spot, todas em uma única AZ, a partir dos grupos de capacidade spot com capacidade ideal usando as especificações de lançamento.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized",
        "SingleAvailabilityZone": true
    },
    "LaunchTemplateConfigs": [
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt1",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-e7188bab"
```

```
            },
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"c5d.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5d.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"c5d.4xlarge",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"m5d.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"m5d.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"m5d.4xlarge",
               "SubnetId":"subnet-49e41922"
            }
         ]
      }
   ],
```

```
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

Exemplo 5: iniciar instâncias spot de um tipo de instância único dentro de uma única zona de disponibilidade

Você pode configurar uma frota para iniciar todas as instâncias do mesmo tipo de instância em uma única zona de disponibilidade definindo SpotOptions SingleInstanceType como true e SingleAvailabilityZone como true.

As 12 substituições do modelo de lançamento têm tipos de instância e sub-redes diferentes (cada uma em uma zona de disponibilidade separada), mas a mesma capacidade ponderada. A capacidade total pretendida é de 20 instâncias, a opção de compra padrão é spot e a estratégia de alocação spot é otimizada para capacidade. A EC2 Fleet inicia 20 instâncias spot do mesmo tipo de instância, todas em uma única AZ, a partir do grupo de capacidade spot com capacidade ideal usando as especificações de lançamento.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized",
        "SingleInstanceType": true,
        "SingleAvailabilityZone": true
    },
    "LaunchTemplateConfigs": [
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt1",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
```

```
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"c5d.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5d.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"c5d.4xlarge",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"m5d.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"m5d.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"m5d.4xlarge",
               "SubnetId":"subnet-49e41922"
            }
         ]
      }
   ],
   "TargetCapacitySpecification": {
```

```
        "TotalTargetCapacity": 20,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

Exemplo 6: iniciar instâncias spot somente se a capacidade mínima pretendida puder ser iniciada

Você pode configurar uma frota para iniciar as instâncias somente se a capacidade mínima pretendida puder ser iniciada, definindo as opções de spot MinTargetCapacity como a capacidade pretendida que você deseja iniciar em conjunto.

Ao especificar a MinTargetCapacity, você deve especificar, pelo menos, um destes parâmetros: SingleInstanceType ou SingleAvailabilityZone. Nesse exemplo, SingleInstanceType é especificado para que todas as 20 instâncias devam usar o mesmo tipo de instância.

As 12 substituições do modelo de lançamento têm tipos de instância e sub-redes diferentes (cada uma em uma zona de disponibilidade separada), mas a mesma capacidade ponderada. A capacidade total pretendida e a capacidade mínima pretendida são ambas definidas como 20 instâncias, a opção de compra padrão é spot e a estratégia de alocação de spot é otimizada para capacidade. A Frota do EC2 inicia 20 instâncias spot a partir do grupo de capacidade spot com capacidade ideal usando as substituições do modelo de lançamento, apenas se puder iniciar todas as 20 instâncias ao mesmo tempo.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized",
        "SingleInstanceType": true,
        "MinTargetCapacity": 20
    },
    "LaunchTemplateConfigs": [
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt1",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
```

```
            "InstanceType":"c5.4xlarge",
            "SubnetId":"subnet-e7188bab"
         },
         {
            "InstanceType":"c5.4xlarge",
            "SubnetId":"subnet-49e41922"
         },
         {
            "InstanceType":"c5d.4xlarge",
            "SubnetId":"subnet-fae8c380"
         },
         {
            "InstanceType":"c5d.4xlarge",
            "SubnetId":"subnet-e7188bab"
         },
         {
            "InstanceType":"c5d.4xlarge",
            "SubnetId":"subnet-49e41922"
         },
         {
            "InstanceType":"m5.4xlarge",
            "SubnetId":"subnet-fae8c380"
         },
         {
            "InstanceType":"m5.4xlarge",
            "SubnetId":"subnet-e7188bab"
         },
         {
            "InstanceType":"m5.4xlarge",
            "SubnetId":"subnet-49e41922"
         },
         {
            "InstanceType":"m5d.4xlarge",
            "SubnetId":"subnet-fae8c380"
         },
         {
            "InstanceType":"m5d.4xlarge",
            "SubnetId":"subnet-e7188bab"
         },
         {
            "InstanceType":"m5d.4xlarge",
            "SubnetId":"subnet-49e41922"
         }
      ]
```

```
      }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

Exemplo 7: iniciar instâncias spot apenas se a capacidade mínima pretendida puder ser iniciada do mesmo tipo de instância em uma única zona de disponibilidade

Você pode configurar uma frota para iniciar as instâncias apenas se a capacidade mínima pretendida puder ser iniciada com um único tipo de instância em uma única zona de disponibilidade, definindo as opções de spot MinTargetCapacity como a capacidade mínima pretendida que você deseja iniciar ao mesmo tempo, juntamente com as opções SingleInstanceType e SingleAvailabilityZone.

As 12 especificações que substituem o modelo de lançamento têm diferentes tipos de instância e sub-redes (cada uma em uma zona de disponibilidade separada), mas a mesma capacidade ponderada. A capacidade total pretendida e a capacidade mínima pretendida são ambas definidas como 20 instâncias, a opção de compra padrão é spot, a estratégia de alocação spot é otimizada para capacidade, SingleInstanceType é true e SingleAvailabilityZone é true. A EC2 Fleet inicia 20 instâncias spot, todas do mesmo tipo de instância e todas em uma única AZ, a partir do grupo de capacidade spot com capacidade ideal usando as especificações de lançamento, apenas se puder iniciar todas as 20 instâncias ao mesmo tempo.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized",
        "SingleInstanceType": true,
        "SingleAvailabilityZone": true,
        "MinTargetCapacity": 20
    },
    "LaunchTemplateConfigs": [
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt1",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5.4xlarge",
```

```
            "SubnetId":"subnet-fae8c380"
         },
         {
            "InstanceType":"c5.4xlarge",
            "SubnetId":"subnet-e7188bab"
         },
         {
            "InstanceType":"c5.4xlarge",
            "SubnetId":"subnet-49e41922"
         },
         {
            "InstanceType":"c5d.4xlarge",
            "SubnetId":"subnet-fae8c380"
         },
         {
            "InstanceType":"c5d.4xlarge",
            "SubnetId":"subnet-e7188bab"
         },
         {
            "InstanceType":"c5d.4xlarge",
            "SubnetId":"subnet-49e41922"
         },
         {
            "InstanceType":"m5.4xlarge",
            "SubnetId":"subnet-fae8c380"
         },
         {
            "InstanceType":"m5.4xlarge",
            "SubnetId":"subnet-e7188bab"
         },
         {
            "InstanceType":"m5.4xlarge",
            "SubnetId":"subnet-49e41922"
         },
         {
            "InstanceType":"m5d.4xlarge",
            "SubnetId":"subnet-fae8c380"
         },
         {
            "InstanceType":"m5d.4xlarge",
            "SubnetId":"subnet-e7188bab"
         },
         {
            "InstanceType":"m5d.4xlarge",
```

```
                "SubnetId":"subnet-49e41922"
            }
         ]
      }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

Exemplo 8: iniciar instâncias com vários modelos de lançamento

Você pode configurar uma frota para iniciar instâncias com diferentes especificações de lançamento para diferentes tipos de instância ou um grupo de tipos de instância, especificando vários modelos de lançamento. Neste exemplo, queremos ter diferentes tamanhos de volume do EBS para diferentes tipos de instância e temos isso configurado nos modelos de lançamento ec2-fleet-lt-4xl, ec2-fleet-lt-9xl e ec2-fleet-lt-18xl.

Neste exemplo, usaremos 3 modelos de lançamento diferentes para os 3 tipos de instância, com base em seu tamanho. As especificação de lançamento faz a substituição em todos os modelos de lançamento que usam pesos de instância com base nas vCPUs no tipo de instância. A capacidade total pretendida é de 144 instâncias, a opção de compra padrão é spot e a estratégia de alocação de spot é otimizada para capacidade. A EC2 Fleet pode iniciar 9 c5n.4xlarge (144 dividido por 16) usando o modelo de lançamento ec2-fleet-4xl, ou 4 c5n.9xlarge (144 dividido por 36), usando o modelo de lançamento ec2-fleet-9xl, ou 2 c5n.18xlarge (144 dividido por 72), usando o modelo de lançamento ec2-fleet-18xl, ou uma combinação dos tipos de instância com pesos que somam a capacidade desejada com base na estratégia de alocação otimizada para capacidade.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized"
    },
    "LaunchTemplateConfigs": [
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt-18xl",
            "Version":"$Latest"
         },
         "Overrides":[
```

```
            {
               "InstanceType":"c5n.18xlarge",
               "SubnetId":"subnet-fae8c380",
               "WeightedCapacity":72
            },
            {
               "InstanceType":"c5n.18xlarge",
               "SubnetId":"subnet-e7188bab",
               "WeightedCapacity":72
            },
            {
               "InstanceType":"c5n.18xlarge",
               "SubnetId":"subnet-49e41922",
               "WeightedCapacity":72
            }
         ]
      },
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt-9xl",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5n.9xlarge",
               "SubnetId":"subnet-fae8c380",
               "WeightedCapacity":36
            },
            {
               "InstanceType":"c5n.9xlarge",
               "SubnetId":"subnet-e7188bab",
               "WeightedCapacity":36
            },
            {
               "InstanceType":"c5n.9xlarge",
               "SubnetId":"subnet-49e41922",
               "WeightedCapacity":36
            }
         ]
      },
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt-4xl",
            "Version":"$Latest"
```

```
         },
         "Overrides":[
            {
               "InstanceType":"c5n.4xlarge",
               "SubnetId":"subnet-fae8c380",
               "WeightedCapacity":16
            },
            {
               "InstanceType":"c5n.4xlarge",
               "SubnetId":"subnet-e7188bab",
               "WeightedCapacity":16
            },
            {
               "InstanceType":"c5n.4xlarge",
               "SubnetId":"subnet-49e41922",
               "WeightedCapacity":16
            }
         ]
      }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 144,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

Exemplo 9: iniciar instância spot com uma base de Instâncias sob demanda

O exemplo a seguir especifica a capacidade total pretendida de 20 instâncias para a frota e uma capacidade pretendida de 5 Instâncias sob demanda. A opção de compra padrão é spot. A frota inicia 5 Instâncias sob demanda, conforme especificado, mas precisa iniciar mais 15 instâncias para atender à capacidade total pretendida. A opção de compra para a diferença é calculada como TotalTargetCapacity – OnDemandTargetCapacity = DefaultTargetCapacityType, que resulta no lançamento pela frota de 15 Instâncias spot a partir de um dos 12 grupos de capacidade de spot com base na estratégia de alocação otimizada para capacidade.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized"
    },
    "LaunchTemplateConfigs": [
```

```
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt1",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"c5d.large",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5d.large",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"c5d.large",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"m5.large",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"m5.large",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"m5.large",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"m5d.large",
```

```
                "SubnetId":"subnet-fae8c380"
            },
            {
                "InstanceType":"m5d.large",
                "SubnetId":"subnet-e7188bab"
            },
            {
                "InstanceType":"m5d.large",
                "SubnetId":"subnet-49e41922"
            }
         ]
      }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "OnDemandTargetCapacity": 5,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

Exemplo 10: iniciar Instâncias spot usando uma estratégia de alocação otimizada para capacidade com uma base de Instâncias sob demanda usando Reservas de Capacidade e a estratégia de alocação priorizada

É possível configurar uma frota para usar Reservas de Capacidade sob demanda primeiro ao iniciar Instâncias sob demanda com o tipo de capacidade pretendida padrão como spot, definindo a estratégia de uso para Reservas de Capacidade como use-capacity-reservations-first. E se vários grupos de instâncias tiverem Reservas de Capacidade não utilizadas, a estratégia de alocação sob demanda escolhida será aplicada. Neste exemplo, a estratégia de alocação sob demanda é priorizada.

Neste exemplo, há 6 Reservas de Capacidade não utilizadas disponíveis. Isso é menos que a capacidade sob demanda pretendida da frota de 10 Instâncias sob demanda.

A conta tem as seguintes 6 Reservas de Capacidade não utilizadas em 2 grupos diferentes. O número de Reservas de Capacidade em cada grupo é indicado por AvailableInstanceCount.

```
{
    "CapacityReservationId": "cr-111",
    "InstanceType": "m5.large",
    "InstancePlatform": "Linux/UNIX",
```

```
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount": 3,
    "InstanceMatchCriteria": "open",
    "State": "active"
}

{
    "CapacityReservationId": "cr-222",
    "InstanceType": "c5.large",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount": 3,
    "InstanceMatchCriteria": "open",
    "State": "active"
}
```

A configuração de frota a seguir mostra somente as configurações pertinentes a este exemplo. A estratégia de alocação sob demanda é priorizada, e a estratégia de uso para Reservas de Capacidade é use-capacity-reservations-first. A estratégia de alocação spot é otimizada para capacidade. A capacidade total pretendida é de 20, a capacidade sob demanda pretendida é de 10 e o tipo de capacidade pretendida padrão é spot.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized"
    },
    "OnDemandOptions":{
       "CapacityReservationOptions": {
         "UsageStrategy": "use-capacity-reservations-first"
       },
       "AllocationStrategy":"prioritized"
    },
    "LaunchTemplateConfigs": [
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt1",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-fae8c380",
               "Priority": 1.0
```

```
            },
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-e7188bab",
               "Priority": 2.0
            },
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-49e41922",
               "Priority": 3.0
            },
            {
               "InstanceType":"c5d.large",
               "SubnetId":"subnet-fae8c380",
               "Priority": 4.0
            },
            {
               "InstanceType":"c5d.large",
               "SubnetId":"subnet-e7188bab",
               "Priority": 5.0
            },
            {
               "InstanceType":"c5d.large",
               "SubnetId":"subnet-49e41922",
               "Priority": 6.0
            },
            {
               "InstanceType":"m5.large",
               "SubnetId":"subnet-fae8c380",
               "Priority": 7.0
            },
            {
               "InstanceType":"m5.large",
               "SubnetId":"subnet-e7188bab",
               "Priority": 8.0
            },
            {
               "InstanceType":"m5.large",
               "SubnetId":"subnet-49e41922",
               "Priority": 9.0
            },
            {
               "InstanceType":"m5d.large",
               "SubnetId":"subnet-fae8c380",
```

```
                "Priority": 10.0
            },
            {
                "InstanceType":"m5d.large",
                "SubnetId":"subnet-e7188bab",
                "Priority": 11.0
            },
            {
                "InstanceType":"m5d.large",
                "SubnetId":"subnet-49e41922",
                "Priority": 12.0
            }
         ]
      }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "OnDemandTargetCapacity": 10,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

Depois de criar a frota instantânea usando a configuração anterior, as 20 instâncias a seguir serão iniciadas para atender à capacidade pretendida:

- 7 Instâncias sob demanda c5.large em us-east-1a – c5.large em us-east-1a é priorizada, e há 3 Reservas de Capacidade c5.large não utilizadas disponíveis. As Reservas de Capacidade são usadas primeiro para iniciar 3 Instâncias sob demanda, e 4 Instâncias sob demanda adicionais são iniciadas de acordo com a estratégia de alocação sob demanda, que é priorizada neste exemplo.
- 3 Instâncias sob demanda m5.large em us-east-1a – m5.large em us-east-1a é priorizada em segundo lugar, e há 3 Reservas de Capacidade c3.large não utilizadas disponíveis
- 10 instâncias spot a partir de um dos 12 grupos de capacidade spot que tem a capacidade ideal, de acordo com a estratégia de alocação otimizada para capacidade.

Depois que a frota for lançada, será possível executar describe-capacity-reservations para ver quantas Reservas de capacidade não utilizadas restam. Neste exemplo, você deve ver a resposta a seguir, que mostra que todas as Reservas de Capacidade de c5.large e m5.large foram usadas.

```
{
```

```
    "CapacityReservationId": "cr-111",
    "InstanceType": "m5.large",
    "AvailableInstanceCount": 0
}

{
    "CapacityReservationId": "cr-222",
    "InstanceType": "c5.large",
    "AvailableInstanceCount": 0
}
```

Exemplo 11: iniciar Instâncias spot usando a estratégia de alocação capacity-optimized-prioritized

O exemplo a seguir especifica os parâmetros mínimos necessários em uma EC2 Fleet do tipo instantâneo: um modelo de lançamento, a capacidade pretendida, a opção de compra padrão e as substituições do modelo de lançamento. O modelo de lançamento é identificado por nome e número de versão do modelo de lançamento. As 12 especificações que substituem o modelo de lançamento têm 4 tipos de instância diferentes com uma prioridade atribuída e 3 sub-redes diferentes, cada uma em uma zona de disponibilidade separada. A capacidade pretendida para a frota é de 20 instâncias, e a opção de compra padrão é spot, o que resulta na tentativa da frota de iniciar 20 instâncias spot a partir de um dos 12 grupos de capacidade spot com base na estratégia de alocação capacity-optimized-prioritized, que tenta ao máximo implementar as prioridades, mas otimiza a capacidade em primeiro lugar.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized-prioritized"
    },
    "LaunchTemplateConfigs": [
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt1",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-fae8c380",
               "Priority": 1.0
            },
            {
               "InstanceType":"c5.large",
```

```
            "SubnetId":"subnet-e7188bab",
            "Priority": 1.0
         },
         {
            "InstanceType":"c5.large",
            "SubnetId":"subnet-49e41922",
            "Priority": 1.0
         },
         {
            "InstanceType":"c5d.large",
            "SubnetId":"subnet-fae8c380",
            "Priority": 2.0
         },
         {
            "InstanceType":"c5d.large",
            "SubnetId":"subnet-e7188bab",
            "Priority": 2.0
         },
         {
            "InstanceType":"c5d.large",
            "SubnetId":"subnet-49e41922",
            "Priority": 2.0
         },
         {
            "InstanceType":"m5.large",
            "SubnetId":"subnet-fae8c380",
            "Priority": 3.0
         },
         {
            "InstanceType":"m5.large",
            "SubnetId":"subnet-e7188bab",
            "Priority": 3.0
         },
         {
            "InstanceType":"m5.large",
            "SubnetId":"subnet-49e41922",
            "Priority": 3.0
         },
         {
            "InstanceType":"m5d.large",
            "SubnetId":"subnet-fae8c380",
            "Priority": 4.0
         },
         {
```

```
                "InstanceType":"m5d.large",
                "SubnetId":"subnet-e7188bab",
                "Priority": 4.0
            },
            {
                "InstanceType":"m5d.large",
                "SubnetId":"subnet-49e41922",
                "Priority": 4.0
            }
         ]
      }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

Exemplo 12: especifique um parâmetro do Systems Manager em vez de um ID de AMI

O exemplo a seguir usa um modelo de inicialização que especifica a configuração das instâncias na frota. Neste exemplo, em `ImageId`, em vez de especificar um ID da AMI, a AMI é referenciada com um parâmetro do System Manager. Na inicialização da instância, o parâmetro do Systems Manager resolverá para um ID da AMI.

Neste exemplo, o parâmetro do Systems Manager é especificado em um formato válido: `resolve:ssm:golden-ami`. Há outros formatos válidos para o parâmetro do Systems Manager. Para obter mais informações, consulte Use um parâmetro de Systems Manager em vez de um ID de AMI.

> **Note**
>
> O tipo da frota deve ser do tipo `instant`. Outros tipos de frota não são compatíveis com a especificação de um parâmetro do System Manager em vez de um ID da AMI.

```
{
    "LaunchTemplateData": {
        "ImageId": "resolve:ssm:golden-ami",
        "InstanceType": "m5.4xlarge",
```

```
        "TagSpecifications": [{
            "ResourceType": "instance",
            "Tags": [{
                "Key": "Name",
                "Value": "webserver"
            }]
        }]
    }
}
```

Definir um limite de gastos para a frota do EC2 ou a frota spot

É possível definir um limite de quanto quer gastar por hora na frota do EC2 ou na frota spot. Quando seu limite de gastos for atingido, a frota interromperá a inicialização de instâncias, mesmo que a capacidade de destino não tenha sido atingida.

Existem limites separados de gastos para instâncias sob demanda e instâncias spot.

Configurar um limite de gastos para instâncias sob demanda e instâncias spot na frota do EC2

Use o comando create-fleet e os parâmetros a seguir:

- Em instâncias sob demanda: na estrutura `OnDemandOptions`, especifique seu limite de gastos no campo `MaxTotalPrice`.
- Em instâncias spot: na estrutura `SpotOptions`, especifique seu limite de gastos no campo `MaxTotalPrice`.

Configurar um limite de gastos para instâncias sob demanda e instâncias spot na frota spot

É possível usar o console do Amazon EC2 ou a AWS CLI para configurar seu limite de gastos.

(Console) Quando criar a frota spot, marque a caixa de seleção Definir custo máximo para instâncias spot e, em seguida, insira um valor para Definir seu custo máximo (por hora). Para obter mais informações, consulte a etapa 6.e. em Criar uma solicitação de frota spot usando parâmetros definidos.

(AWS CLI) Use o comando request-spot-fleet e os seguintes parâmetros:

- Em instâncias sob demanda: especifique seu limite de gastos no campo `OnDemandMaxTotalPrice`.
- Em instâncias spot: especifique seu limite de gastos no campo `SpotMaxTotalPrice`.

Exemplos

Os exemplos a seguir mostram duas situações diferentes. No primeiro exemplo, a frota para de inicializar instâncias sob demanda quando atinge a capacidade de destino definida para instâncias sob demanda (`OnDemandTargetCapacity`). No segundo exemplo, a frota para de inicializar instâncias sob demanda ao atingir o valor máximo que você está disposto a pagar por hora pelas instâncias sob demanda (`MaxTotalPrice`).

Exemplo: parar de inicializar instâncias sob demanda quando a capacidade de destino é atingida

Dada uma solicitação de `m4.large` Instâncias on-demand, na qual:

- Preço sob demanda: 0,10 USD por hora
- `OnDemandTargetCapacity`: 10
- `MaxTotalPrice`: 1,50 USD

A frota inicializa dez instâncias sob demanda, porque o total de USD 1,00 (10 instâncias x USD 0,10) não excede o `MaxTotalPrice` de USD 1,50 para instâncias sob demanda.

Exemplo: parar de executar instâncias sob demanda quando o preço máximo total é atingido

Dada uma solicitação de `m4.large` Instâncias on-demand, na qual:

- Preço sob demanda: 0,10 USD por hora
- `OnDemandTargetCapacity`: 10
- `MaxTotalPrice`: 0,80 USD

Se a frota inicializar a capacidade de destino sob demanda (dez instâncias sob demanda), o custo total por hora será de USD 1,00. Isso é mais que a quantidade (0,80 USD) especificada para `MaxTotalPrice` para Instâncias on-demand. Para evitar gastar mais do que você pretende, a frota inicializará somente oito instâncias sob demanda (abaixo da capacidade de destino sob demanda), porque se inicializar mais, o `MaxTotalPrice` de instâncias sob demanda será excedido.

Instâncias expansíveis

Se você executar as Instâncias spot usando um tipo de instância expansível e planeja usar as instâncias spot expansíveis imediatamente e por um breve período, sem tempo ocioso para

acumular créditos de CPU, recomendamos executá-las no modo padrão para evitar pagar custos mais elevados. Se executar as Instâncias spot expansíveis no modo ilimitado e esgotar a CPU imediatamente, você gastará os créditos excedentes por isso. Se a instância for usada por um curto período, não haverá tempo para acumular créditos de CPU para pagamento dos créditos excedentes, e você precisará pagar os créditos excedentes ao encerrar a instância.

O modo ilimitado será adequado para instâncias spot expansíveis somente se a instância for executada por tempo suficiente para acumular créditos de CPU para expansão. Caso contrário, pagar por créditos excedentes torna a as instâncias spot expansíveis mais caras do que o uso de outras instâncias. Para obter mais informações, consulte Quando usar o modo ilimitado versus CPU fixa.

Os créditos de lançamento são feitos para fornecer uma experiência de lançamento inicial produtiva para instâncias T2 fornecendo recursos computacionais suficientes para configurar a instância. Lançamentos repetidos de instâncias T2 para acessar novos créditos de lançamento não são permitidos. Se você precisar de uma CPU sustentada, poderá obter créditos (ficando inativo durante um período), usar o modo Ilimitado para T2 Instâncias spot ou usar um tipo de instância com CPU dedicada.

Especificar atributos para seleção de tipo de instância para frota do EC2 ou frota spot

Ao criar uma frota do EC2 ou frota spot, você deve especificar um ou mais tipos de instância para configurar as instâncias sob-demanda e as instâncias spot na frota. Como alternativa à especificação manual dos tipos de instância, você pode especificar os atributos que uma instância deve ter, e o Amazon EC2 identificará todos os tipos de instância com esses atributos. Isso é conhecido como seleção de tipo de instância baseada em atributos. Por exemplo, você pode especificar o número mínimo e máximo de vCPUs necessárias para suas instâncias, e a frota inicializará as instâncias usando todos os tipos de instância disponíveis que atendam a esses requisitos de vCPU.

A seleção de tipo de instância baseada em atributos é ideal para workloads e frameworks que possam ser flexíveis em relação a que tipos de instância elas usam, como ao executar contêineres ou frotas da Web, processar big data e implementar ferramentas de integração e implantação contínuas (CI/CD).

Benefícios

A seleção de tipo de instância baseada em atributos oferece os seguintes benefícios:

- Use facilmente os tipos de instâncias certos: com tantos tipos de instância disponíveis, encontrar os tipos de instância corretos para a workload pode ser demorado. Se você especificar os atributos de instância, os tipos de instância terão automaticamente os atributos necessários para sua workload.
- Configuração simplificada: para especificar manualmente vários tipos de instância para uma frota, crie uma substituição de modelo de inicialização separada para cada tipo de instância. Mas, com a seleção de tipo de instância baseada em atributos, para fornecer vários tipos de instância, você só precisa especificar os atributos das instâncias no modelo de lançamento ou em uma substituição de modelo de lançamento.
- Uso automático de novos tipos de instâncias: quando atributos de instância são especificados em vez de tipos de instância, sua frota pode usar tipos de instância de gerações mais novas à medida que são lançados, tornando a configuração da frota "à prova de obsolescência".
- Flexibilidade de tipo de instância: quando você especifica atributos de instância em vez de tipos de instância, a frota pode selecionar em uma ampla variedade de tipos de instância para inicializar instâncias spot, o que atende às Práticas recomendadas para instâncias spot da flexibilidade de tipo de instância.

Tópicos

- Como funciona a seleção de tipo de instância baseada em atributos
- Proteção de preço
- Proteção de performance
- Considerações
- Criar uma Frota do EC2 com seleção de tipo de instância baseada em atributos
- Criar uma frota spot com seleção de tipo de instância baseada em atributos
- Exemplos de configurações de frota do EC2 que são válidas e não válidas
- Exemplos de configurações de frota spot que são válidas e não válidas
- Previsualizar os tipos de instância com os atributos especificados

Como funciona a seleção de tipo de instância baseada em atributos

Para usar a seleção de tipo de instância baseada em atributos na configuração de frota, substitua a lista dos tipos de instância por uma lista dos atributos de instância que suas instâncias requerem. A frota do EC2 ou a frota spot inicializará instâncias em todos os tipos de instância disponíveis que tenham os atributos de instância especificados.

Tópicos

- Tipos de atributos de instância
- Onde configurar a seleção de tipo de instância baseada em atributos
- Como a frota do EC2 ou a frota spot usa a seleção de tipo de instância baseada em atributos ao provisionar uma frota

Tipos de atributos de instância

Há vários atributos de instância que você pode especificar para expressar seus requisitos de computação, p. ex.:

- Contagem de vCPUs: o número mínimo e máximo de vCPUs por instância.
- Memória: o mínimo e o máximo de GiBs de memória por instância.
- Armazenamento local: se o sistema deve usar o EBS ou volumes de armazenamento de instâncias para armazenamento local.
- Performance intermitente: se o sistema deve usar a família de instâncias T, incluindo os tipos T4g, T3a, T3 e T2.

Para obter uma descrição de cada atributo e os valores padrão, consulte InstanceRequirements na Referência de API do Amazon EC2.

Onde configurar a seleção de tipo de instância baseada em atributos

Dependendo de você usar o console ou a AWS CLI, é possível especificar os atributos de instância para a seleção de tipo de instância baseada em atributos da seguinte forma:

No console, você pode especificar os atributos de instância nos seguintes componentes de configuração de frota:

- Em um modelo de inicialização, referencie o modelo de inicialização na solicitação da frota
- (Somente frota spot) Na solicitação de frota

Na AWS CLI, você pode especificar os atributos de instância em um ou ambos os componentes de configuração de frota a seguir:

- Em um modelo de inicialização, referencie o modelo de inicialização na solicitação da frota
- Em uma substituição de modelo de lançamento

Se desejar uma combinação de instâncias que usam AMIs diferentes, você pode especificar atributos de instância em várias substituições de modelo de lançamento. Por exemplo, diferentes tipos de instância podem usar processadores baseados em x86 e Arm.

- (Somente frota spot) Em uma especificação de inicialização

Como a frota do EC2 ou a frota spot usa a seleção de tipo de instância baseada em atributos ao provisionar uma frota

A frota do EC2 ou a frota spot provisiona uma frota da seguinte maneira:

- Ela identifica os tipos de instância que têm os atributos especificados.
- Ela usa proteção de preço para determinar quais tipos de instância excluir.
- Ela determina os grupos de capacidade dos quais considerará inicializar as instâncias com base nas regiões ou zonas de disponibilidade da AWS que possuem os tipos de instância correspondentes.
- Ela aplica a estratégia de alocação especificada para determinar os grupos de capacidade dos quais as instâncias serão inicializadas.

  Observe que a seleção de tipo de instância baseada em atributos não escolhe os grupos de capacidade dos quais provisionará a frota; isso cabe às estratégias de alocação.

  Se você especificar uma estratégia de alocação, a frota inicializará as instâncias de acordo com a estratégia de alocação especificada.

  - Nas instâncias spot, a seleção do tipo de instância baseada em atributos oferece suporte às estratégias de alocação otimizada para capacidade de preço, capacidade otimizada e menor preço. Não recomendamos a estratégia de alocação de spot menor preço porque ela representa o risco mais alto de interrupção para as instâncias spot.
  - Para instâncias sob demanda, a seleção de tipo de instância baseada em atributos oferece suporte à estratégia de alocação menor preço.
- Se não houver capacidade para os tipos de instância com os atributos de instância especificados, nenhuma instância poderá ser iniciada e a frota retornará um erro.

Proteção de preço

A proteção de preços é um recurso que impede que a frota do EC2 ou a frota spot use tipos de instância que você consideraria muito caros, mesmo que atendessem aos atributos especificados.

Para usar a proteção de preço, você define um limite de preço. Em seguida, quando o Amazon EC2 selecionar tipos de instância com seus atributos, ele excluirá os tipos de instância que tenham preços acima do limite.

A forma como o Amazon EC2 calcula o limite de preço é a seguinte:

- Primeiro, o Amazon EC2 identifica o tipo de instância com o menor preço dentre aqueles que correspondem aos seus atributos.
- Em seguida, o Amazon EC2 pegará o valor (expresso como uma porcentagem) que você especificou para o parâmetro de proteção de preço e o multiplicará pelo preço do tipo de instância identificado. O resultado é o preço usado como o limite de preço.

Há limites distintos de preço para instâncias sob demanda e instâncias spot.

Quando você cria uma frota com seleção de tipo de instância baseada em atributos, a proteção de preço é habilitada por padrão. É possível manter os valores padrão ou especificar seus próprios valores.

Você também pode desativar a proteção de preços. Para indicar que não há limite de proteção de preço, especifique um valor percentual alto, como 999999.

Tópicos

- Identificação do tipo de instância com o menor preço
- Proteção de preço de instância sob demanda
- Proteção de preço de instância spot
- Especificar o limite de proteção de preço

Identificação do tipo de instância com o menor preço

O Amazon EC2 determina o preço básico do limite de preço ao identificar o tipo de instância com o menor preço dentre aquelas que correspondem aos atributos especificados. Ele faz isso da seguinte maneira:

- Primeiro, ele analisa os tipos de instância C, M ou R da geração atual que correspondem aos seus atributos. Se houver alguma correspondência, ele identificará o tipo de instância com o menor preço.

- Se não houver uma correspondência, ele analisará os tipos de instância da geração atual que correspondem aos seus atributos. Se houver alguma correspondência, ele identificará o tipo de instância com o menor preço.
- Se não houver correspondência, ele examinará todos os tipos de instância da geração anterior que correspondam aos seus atributos e identificará o tipo de instância com o menor preço.

Proteção de preço de instância sob demanda

O limite de proteção de preço para tipos de instância sob demanda é calculado como uma porcentagem maior do que o tipo de instância sob demanda de menor preço identificado (`OnDemandMaxPricePercentageOverLowestPrice`). Você especifica maior a porcentagem que está disposto a pagar. Se você não especificar esse parâmetro, um valor padrão de `20` será usado para calcular um limite de proteção de preço 20% superior ao preço identificado.

Por exemplo, se o preço da instância sob demanda identificada for `0.4271`, e você especificar `25`, o limite de preço será 25% maior que `0.4271`. Isso é calculado da seguinte forma: `0.4271 * 1.25 = 0.533875`. O preço calculado é o máximo que você está disposto a pagar por instâncias sob demanda e, neste exemplo, o Amazon EC2 excluirá qualquer tipo de instância sob demanda com preço superior a `0.533875`.

Proteção de preço de instância spot

Por padrão, o Amazon EC2 aplicará automaticamente a proteção de preço de instância spot ideal para selecionar de forma consistente entre uma ampla variedade de tipos de instância. Você também pode definir manualmente a proteção de preço. No entanto, deixar que o Amazon EC2 faça isso por você pode aumentar a probabilidade de que sua capacidade de spot seja atendida.

É possível especificar manualmente a proteção de preço usando uma das opções a seguir. Se você definir manualmente a proteção de preço, recomendamos usar a primeira opção.

- Um percentual do tipo de instância sob demanda com o menor preço identificado [`MaxSpotPriceAsPercentageOfOptimalOnDemandPrice`]

  Por exemplo, se o preço do tipo de instância sob demanda identificada for `0.4271`, e você especificar `60`, o limite de preço será 60% de `0.4271`. Isso é calculado da seguinte forma: `0.4271 * 0.60 = 0.25626`. O preço calculado é o máximo que você está disposto a pagar por instâncias spot e, neste exemplo, o Amazon EC2 excluirá qualquer tipo de instância spot com preço superior a `0.25626`.

- Um percentual maior do que o tipo de instância spot com o menor preço identificado [`SpotMaxPricePercentageOverLowestPrice`]

  Por exemplo, se o preço do tipo de instância spot identificada for `0.1808`, e você especificar `25`, o limite de preço será 25% maior que `0.1808`. Isso é calculado da seguinte forma: `0.1808 * 1.25 = 0.226`. O preço calculado é o máximo que você está disposto a pagar por instâncias spot e, neste exemplo, o Amazon EC2 excluirá qualquer tipo de instância spot com preço superior a `0.266`. Não é recomendável usar esse parâmetro, pois os preço spot podem flutuar e, portanto, seu limite de proteção de preço também poderá flutuar.

Especificar o limite de proteção de preço

Especificar o limite de proteção de preço usando a AWS CLI

Quando estiver criando uma frota do EC2 ou uma frota spot usando a AWS CLI, configure a frota para seleção de tipo de instância baseada em atributos e, em seguida, faça o seguinte:

- Para especificar o limite de proteção de preço da instância sob demanda, no arquivo de configuração JSON, em estrutura `InstanceRequirements`, para `OnDemandMaxPricePercentageOverLowestPrice`, insira o limite de proteção de preço como uma porcentagem.
- Para especificar o limite de proteção de preço da instância spot, no arquivo de configuração JSON, na estrutura `InstanceRequirements`, especifique um destes parâmetros:
  - Para `MaxSpotPriceAsPercentageOfOptimalOnDemandPrice`, insira o limite de proteção de preço como uma porcentagem.
  - Para `SpotMaxPricePercentageOverLowestPrice`, insira o limite de proteção de preço como uma porcentagem.

Para ter mais informações, consulte Criar uma Frota do EC2 com seleção de tipo de instância baseada em atributos ou Criar uma frota spot com seleção de tipo de instância baseada em atributos.

(Somente frota spot) Para especificar o limite de proteção de preço usando o console

Quando estiver criando uma frota spot, configure a frota para seleção de tipo de instância baseada em atributos e, em seguida, faça o seguinte:

- Para especificar o limite de proteção de preço da instância sob demanda, em Atributo de instância adicional, escolha Proteção de preços sob demanda e Adicionar atributo e insira o limite de proteção de preço como uma porcentagem.
- Para especificar o limite de proteção de preço da instância sob demanda, em Atributo de instância adicional, escolha Proteção de preço spot, Adicionar atributo, escolha um valor básico no qual basear o preço e, em seguida, insira o limite de proteção de preço como uma porcentagem.

> **Note**
>
> Ao criar a frota, se você definir `TargetCapacityUnitType` para `vcpu` ou `memory-mib`, o limite de proteção de preço será aplicado com base no preço por VCPU ou no preço por memória, em vez de no preço por instância.

Proteção de performance

A proteção de performance é um recurso para garantir que a frota do EC2 ou frota spot use tipos de instância que sejam semelhantes ou excedam uma linha de base de performance especificada. Para usar a proteção de performance, especifique uma família de instâncias como referência de linha de base. Os recursos da família de instâncias especificada estabelecem o nível de performance mais baixo aceitável. Quando o Amazon EC2 seleciona tipos de instância para sua frota, ele considera os atributos e a linha de base de performance especificados. Os tipos de instância que estão abaixo da linha de base de performance são automaticamente excluídos da seleção, mesmo que correspondam aos outros atributos especificados. Isso garante que todos os tipos de instância selecionados ofereçam performance semelhante ou melhor do que a linha de base estabelecida pela família de instâncias especificada. O Amazon EC2 usa essa linha de base para orientar a seleção do tipo de instância, mas não há garantia de que os tipos de instância selecionados sempre excederão a linha de base de cada aplicação.

No momento, esse recurso oferece suporte apenas à performance da CPU como fator de performance da linha de base. A performance da CPU do processador de CPU da família de instâncias especificada serve como linha de base de performance, garantindo que os tipos de instância selecionados sejam semelhantes ou excedam essa linha de base. Famílias de instâncias com os mesmos processadores de CPU levam aos mesmos resultados de filtragem, mesmo que a performance da rede ou do disco seja diferente. Por exemplo, especificar `c6in` ou `c6i` como referência de linha de base produziria resultados de filtragem idênticos com base na performance porque as duas famílias de instâncias usam o mesmo processador de CPU.

Famílias de instâncias não compatíveis

As famílias de instâncias a seguir não oferecem suporte à proteção de performance:

- Uso geral: Mac1 | Mac2 | Mac2-m1ultra | Mac2-m2 | Mac2-m2pro | M1 | M2 | T1
- Otimizada para computação: C1
- Otimizadas para memória: U-3tb1 | U-6tb1 | U-9tb1 | U-12tb1 | U-18tb1 | U-24tb1 | U7i-12tb | U7in-16tb | U7in-24tb | U7in-32tb
- Computação acelerada: G3 | G3s | P3dn | P4d | P5
- Computação de alta performance: Hpc7g

Se você habilitar a proteção de performance especificando uma família de instâncias compatível, os tipos de instância retornados excluirão as famílias de instâncias incompatíveis acima.

Se você especificar uma família de instâncias não compatível como um valor para a performance da linha de base, a API retornará uma resposta vazia para GetInstanceTypesFromInstanceRequirements e uma exceção para CreateFleet, RequestSpotFleet, ModifyFleet e ModifySpotFleetRequest.

Exemplo: definir uma linha de base de performance da CPU

No exemplo a seguir, o requisito da instância é ser iniciada com tipos de instância que tenham núcleos de CPU com a mesma performance da família de instâncias `c6i`. Isso filtrará os tipos de instância com processadores de CPU de performance inferior, mesmo que atendam aos outros requisitos de instância especificados, como o número de vCPUs. Por exemplo, se os atributos de instância especificados incluírem 4 vCPUs e 16 GB de memória, um tipo de instância com esses atributos, mas com performance de CPU inferior ao `c6i`, será excluído da seleção.

```
"BaselinePerformanceFactors": {
        "Cpu": {
            "References": [
                {
                    "InstanceFamily": "c6i"
                }
            ]
        }
```

Considerações

- É possível especificar tipos de instância ou atributos de instância em uma frota do EC2 ou frota spot, mas não ambos ao mesmo tempo.

  Ao usar a CLI, as substituições do modelo de lançamento prevalecerão sobre o modelo de lançamento. Por exemplo, se o modelo de lançamento contiver um tipo de instância e a substituição do modelo de lançamento contiver atributos de instância, as instâncias identificadas pelos atributos da instância prevalecerão sobre o tipo de instância no modelo de lançamento.
- Ao usar a CLI, quando você especifica atributos de instância como substituições, não pode especificar também pesos ou prioridades.
- É possível especificar, no máximo, quatro estruturas de `InstanceRequirements` em uma configuração de solicitação.

Criar uma Frota do EC2 com seleção de tipo de instância baseada em atributos

É possível configurar uma frota do EC2 para usar a seleção de tipo de instância baseada em atributos. Não é possível criar uma frota do EC2 usando o console do Amazon EC2.

Os parâmetros para a seleção de tipo de instância baseada nos atributos são especificados na estrutura `InstanceRequirements`. Quando `InstanceRequirements` for incluído na configuração da frota, `InstanceType` e `WeightedCapacity` deverão ser excluídos; eles não podem determinar a configuração da frota ao mesmo tempo que os atributos da instância.

Nos exemplos da AWS CLI e do PowerShell, os seguintes atributos são especificados:

- `VCpuCount`: no mínimo 2 vCPUs e no máximo 4 vCPUs. Se você não precisar de um limite máximo, poderá omitir o valor máximo.
- `MemoryMiB`: mínimo de 8 GiB de memória e máximo de 16 GiB. Se você não precisar de um limite máximo, poderá omitir o valor máximo.

Essa configuração identifica quaisquer tipos de instância com 2 a 4 vCPUs e 8 a 16 GiB de memória. Porém, a estratégia proteção de preços e de alocação pode excluir alguns tipos de instância quando a Frota do EC2 provisiona a frota.

AWS CLI

Para criar uma frota do EC2 com a seleção de tipo de instância baseada em atributos

Use o comando create-fleet para criar uma frota do EC2. Especifique a configuração da frota em um arquivo JSON.

```
aws ec2 create-fleet \
    --region us-east-1 \
    --cli-input-json file://file_name.json
```

O arquivo de exemplo *file_name*.json a seguir contém os parâmetros que configuram uma frota do EC2 para usar a seleção de tipo de instância baseada em atributos.

```
{
    "SpotOptions": {
        "AllocationStrategy": "price-capacity-optimized"
    },
    "LaunchTemplateConfigs": [{
        "LaunchTemplateSpecification": {
            "LaunchTemplateName": "my-launch-template",
            "Version": "1"
        },
        "Overrides": [{
            "InstanceRequirements": {
                "VCpuCount": {
                    "Min": 2,
                    "Max": 4
                },
                "MemoryMiB": {
                    "Min": 8192,
                    "Max": 16384
                }
            }
        }]
    }],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

PowerShell

Para criar uma frota do EC2 com a seleção de tipo de instância baseada em atributos

Use o cmdlet New-EC2Fleet.

```
$vcpuCount = New-Object Amazon.EC2.Model.VCpuCountRangeRequest
$vcpuCount.Min = 2
$vcpuCount.Max = 4
$memoryMiB = New-Object Amazon.EC2.Model.MemoryMiBRequest
$memoryMiB.Min = 8192
$memoryMiB.Max = 16384
$instanceRequirements = New-Object Amazon.EC2.Model.InstanceRequirementsRequest
$instanceRequirements.VCpuCount = $vcpuCount
$instanceRequirements.MemoryMiB = $memoryMiB

$launchTemplateSpec = New-Object
 Amazon.EC2.Model.FleetLaunchTemplateSpecificationRequest
$launchTemplateSpec.LaunchTemplateName = "my-launch-template"
$launchTemplateSpec.Version = "1"
$override = New-Object Amazon.EC2.Model.FleetLaunchTemplateOverridesRequest
$override.InstanceRequirements = $instanceRequirements
$launchTemplateConfig = New-Object Amazon.EC2.Model.FleetLaunchTemplateConfigRequest
$launchTemplateConfig.LaunchTemplateSpecification = $launchTemplateSpec
$launchTemplateConfig.Overrides = @($override)

New-EC2Fleet `
    -SpotOptions_AllocationStrategy "price-capacity-optimized" `
    -LaunchTemplateConfig @($launchTemplateConfig) `
    -TargetCapacitySpecification_DefaultTargetCapacityType "spot" `
    -TargetCapacitySpecification_TotalTargetCapacity 20 `
    -Type "instant"
```

Criar uma frota spot com seleção de tipo de instância baseada em atributos

É possível configurar uma frota para usar a seleção de tipo de instância baseada em atributos.

Os parâmetros para a seleção de tipo de instância baseada nos atributos são especificados na estrutura `InstanceRequirements`. Quando `InstanceRequirements` for incluído na configuração da frota, `InstanceType` e `WeightedCapacity` deverão ser excluídos; eles não podem determinar a configuração da frota ao mesmo tempo que os atributos da instância.

Nos exemplos da AWS CLI e do PowerShell, os seguintes atributos são especificados:

- `VCpuCount`: no mínimo 2 vCPUs e no máximo 4 vCPUs. Se você não precisar de um limite máximo, poderá omitir o valor máximo.

- `MemoryMiB`: mínimo de 8 GiB de memória e máximo de 16 GiB. Se você não precisar de um limite máximo, poderá omitir o valor máximo.

Essa configuração identifica quaisquer tipos de instância com 2 a 4 vCPUs e 8 a 16 GiB de memória. Porém, a estratégia proteção de preços e de alocação pode excluir alguns tipos de instância quando a frota spot provisiona a frota.

Console

Para configurar uma frota spot para seleção de tipo de instância baseada em atributos

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Spot Requests (Solicitações de spot) e escolha Request Spot Instances (Solicitar instâncias spot).
3. Siga as etapas para criar um frota spot. Para obter mais informações, consulte Criar uma solicitação de frota spot usando parâmetros definidos.

   Ao criar a frota spot, configure a frota para seleção de tipo de instância baseada em atributos da seguinte forma:

   a. Em Instance type requirements (Requisitos de tipo de instância), escolha Specify instance attributes that match your compute requirements (Especificar atributos de instância que correspondam aos requisitos de computação).

   b. Em vCPUs, insira o número mínimo e máximo desejado de vCPUs. Para não especificar nenhum limite, selecione No minimum (Sem mínimo), No maximum (Sem máximo) ou ambos.

   c. Em Memory (GiB) (Memória), insira a quantidade mínima e máxima de memória desejada. Para não especificar nenhum limite, selecione No minimum (Sem mínimo), No maximum (Sem máximo) ou ambos.

   d. (Opcional) Em Additional instance attributes (Atributos de instância adicionais), você pode, opcionalmente, especificar um ou mais atributos para expressar seus requisitos de computação com mais detalhes. Cada atributo adicional inclui mais restrições à solicitação.

   e. (Opcional) Expanda Preview matching instance types (Previsualizar os tipos de instância correspondentes) para visualizar os tipos de instância que têm os atributos especificados.

AWS CLI

Para configurar uma frota spot para seleção de tipo de instância baseada em atributos

Use o comando request-spot-fleet para criar uma solicitação de frota spot. Especifique a configuração da frota em um arquivo JSON.

```
aws ec2 request-spot-fleet \
    --region us-east-1 \
    --spot-fleet-request-config file://file_name.json
```

O arquivo de exemplo *file_name*.json a seguir contém os parâmetros que configuram uma frota spot para usar a seleção de tipo de instância baseada em atributos.

```
{
    "AllocationStrategy": "priceCapacityOptimized",
    "TargetCapacity": 20,
    "Type": "request",
    "LaunchTemplateConfigs": [{
        "LaunchTemplateSpecification": {
            "LaunchTemplateName": "my-launch-template",
            "Version": "1"
        },
        "Overrides": [{
            "InstanceRequirements": {
                "VCpuCount": {
                    "Min": 2,
                    "Max": 4
                },
                "MemoryMiB": {
                    "Min": 8192,
                    "Max": 16384
                }
            }
        }]
    }]
}
```

PowerShell

Para configurar uma frota spot para seleção de tipo de instância baseada em atributos

Use o cmdlet Request-EC2SpotFleet.

```
$vcpuCount = New-Object Amazon.EC2.Model.VCpuCountRange
$vcpuCount.Min = 2
$vcpuCount.Max = 4
$memoryMiB = New-Object Amazon.EC2.Model.MemoryMiB
$memoryMiB.Min = 8192
$memoryMiB.Max = 16384
$instanceRequirements = New-Object Amazon.EC2.Model.InstanceRequirements
$instanceRequirements.VCpuCount = $vcpuCount
$instanceRequirements.MemoryMiB = $memoryMiB

$launchTemplateSpec = New-Object Amazon.EC2.Model.FleetLaunchTemplateSpecification
$launchTemplateSpec.LaunchTemplateName = "my-launch-template"
$launchTemplateSpec.Version = "1"
$override = New-Object Amazon.EC2.Model.LaunchTemplateOverrides
$override.InstanceRequirements = $instanceRequirements
$launchTemplateConfig = New-Object Amazon.EC2.Model.LaunchTemplateConfig
$launchTemplateConfig.LaunchTemplateSpecification = $launchTemplateSpec
$launchTemplateConfig.Overrides = @($override)

Request-EC2SpotFleet `
    -SpotFleetRequestConfig_AllocationStrategy "PriceCapacityOptimized" `
    -SpotFleetRequestConfig_TargetCapacity 20 `
    -SpotFleetRequestConfig_Type "Request" `
    -SpotFleetRequestConfig_LaunchTemplateConfig $launchTemplateConfig
```

Exemplos de configurações de frota do EC2 que são válidas e não válidas

Se você usar a AWS CLI para criar uma Frota do EC2, deve garantir que a configuração de frota seja válida. Exemplos de configurações que são válidas e não válidas.

As configurações são consideradas não válidas quando contiverem o seguinte:

- Uma única estrutura de `Overrides` com `InstanceRequirements` e `InstanceType`
- Duas estruturas de `Overrides`, uma com `InstanceRequirements` e outra com `InstanceType`
- Duas estruturas de `InstanceRequirements` com valores de atributo sobrepostos na mesma `LaunchTemplateSpecification`

Exemplos de configuração

- Configuração válida: modelo de lançamento único com substituições
- Configuração válida: modelo de lançamento único com vários InstanceRequirements
- Configuração válida: dois modelos de lançamento com substituições em cada
- Configuração válida: somente InstanceRequirements especificados, sem valores de atributo sobrepostos
- Configuração não válida: Overrides contémInstanceRequirements e InstanceType
- Configuração não válida: duas Overrides contêm InstanceRequirements e InstanceType
- Configuração não válida: valores de atributo sobrepostos

Configuração válida: modelo de lançamento único com substituições

A configuração a seguir é válida. Ela contém um modelo de lançamento e uma estrutura de `Overrides` contendo uma estrutura de `InstanceRequirements`. A seguir está um texto explicativo do exemplo de configuração.

```
{
        "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "My-launch-template",
                "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 2,
                            "Max": 8
                        },
                        "MemoryMib": {
                            "Min": 0,
                            "Max": 10240
                        },
                        "MemoryGiBPerVCpu": {
                            "Max": 10000
                        },
                        "RequireHibernateSupport": true
                    }
                }
            ]
```

```
        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 5000,
        "DefaultTargetCapacityType": "spot",
        "TargetCapacityUnitType": "vcpu"
        }
    }
}
```

`InstanceRequirements`

Para usar a seleção de instância baseada em atributos, você deve incluir a estrutura de `InstanceRequirements` na configuração de frota e especificar os atributos desejados para as instâncias da frota.

No exemplo anterior, os seguintes atributos de instância foram especificados:

- `VCpuCount`: os tipos de instância devem ter no mínimo 2 e no máximo 8 vCPUs.
- `MemoryMiB`: os tipos de instância devem ter no máximo 10.240 MiB de memória. Um mínimo de 0 indica que não há limite mínimo.
- `MemoryGiBPerVCpu`: os tipos de instância devem ter no máximo 10.000 GiB de memória. O parâmetro `Min` é opcional. Ao omiti-lo, você indica que não há limite mínimo.

`TargetCapacityUnitType`

O parâmetro `TargetCapacityUnitType` especifica a unidade da capacidade-alvo. No exemplo, a capacidade-alvo é `5000` e o tipo de unidade de capacidade-alvo é `vcpu`, que juntos especificam uma capacidade-alvo desejada de 5000 vCPUs. A Frota do EC2 iniciará instâncias suficientes para que o número total de vCPUs na frota seja 5.000 vCPUs.

Configuração válida: modelo de lançamento único com vários InstanceRequirements

A configuração a seguir é válida. Ela contém um modelo de lançamento e uma estrutura de `Overrides` contendo duas estruturas de `InstanceRequirements`. Os atributos especificados em `InstanceRequirements` são válidos porque os valores não se sobrepõem: a primeira estrutura de `InstanceRequirements` especifica um `VCpuCount` de 0 a 2 vCPUs, enquanto a segunda estrutura de `InstanceRequirements` especifica de 4 a 8 vCPUs.

```
{
```

```
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                },
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 4,
                            "Max": 8
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                }
              ]
            }
        ],
        "TargetCapacitySpecification": {
            "TotalTargetCapacity": 1,
            "DefaultTargetCapacityType": "spot"
        }
    }
}
```

Configuração válida: dois modelos de lançamento com substituições em cada

A configuração a seguir é válida. Ela contém dois modelos de lançamento, cada um deles com uma estrutura de `Overrides` contendo uma estrutura de `InstanceRequirements`. Essa configuração é útil para oferecer suporte às arquiteturas `arm` e `x86` na mesma frota.

```
{
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "armLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                },
                {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "x86LaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                }
              ]
```

```
            }
        ],
         "TargetCapacitySpecification": {
            "TotalTargetCapacity": 1,
            "DefaultTargetCapacityType": "spot"
        }
    }
}
```

Configuração válida: somente **`InstanceRequirements`** especificados, sem valores de atributo sobrepostos

A configuração a seguir é válida. Ela contém duas estruturas de `LaunchTemplateSpecification`, cada uma com um modelo de lançamento e uma estrutura `Overrides` contendo uma estrutura de `InstanceRequirements`. Os atributos especificados em `InstanceRequirements` são válidos porque os valores não se sobrepõem: a primeira estrutura de `InstanceRequirements` especifica um `VCpuCount` de 0 a 2 vCPUs, enquanto a segunda estrutura de `InstanceRequirements` especifica de 4 a 8 vCPUs.

```
{
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                }
              ]
            },
            {
                "LaunchTemplateSpecification": {
```

```
                    "LaunchTemplateName": "MyOtherLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 4,
                            "Max": 8
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                }
              ]
            }
        ],
        "TargetCapacitySpecification": {
            "TotalTargetCapacity": 1,
            "DefaultTargetCapacityType": "spot"
        }
    }
}
```

Configuração não válida: **`Overrides`** contém**`InstanceRequirements`** e **`InstanceType`**

A configuração a seguir não é válida. A estrutura de `Overrides` contém `InstanceRequirements` e `InstanceType`. Em `Overrides`, você pode especificar `InstanceRequirements` ou `InstanceType`, mas não ambos.

```
{
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
```

```
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                },
                {
                    "InstanceType": "m5.large"
                }
              ]
            }
        ],
        "TargetCapacitySpecification": {
            "TotalTargetCapacity": 1,
            "DefaultTargetCapacityType": "spot"
        }
    }
}
```

Configuração não válida: duas **`Overrides`** contêm **`InstanceRequirements`** e **`InstanceType`**

A configuração a seguir não é válida. As estruturas `Overrides` contêm `InstanceRequirements` e `InstanceType`. É possível especificar `InstanceRequirements` ou `InstanceType`, mas não ambos, mesmo que estejam em estruturas de `Overrides` diferentes.

```
{
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
```

```
                    }
                }
              ]
            },
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyOtherLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceType": "m5.large"
                }
              ]
            }
        ],
         "TargetCapacitySpecification": {
            "TotalTargetCapacity": 1,
            "DefaultTargetCapacityType": "spot"
        }
    }
}
```

Configuração não válida: valores de atributo sobrepostos

A configuração a seguir não é válida. As duas estruturas de `InstanceRequirements` contêm `"VCpuCount": {"Min": 0, "Max": 2}`. Os valores desses atributos se sobrepõem, o que resultará em grupos de capacidade duplicados.

```
{
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
```

```
                        "MemoryMiB": {
                            "Min": 0
                        }
                    },
                    {
                      "InstanceRequirements": {
                          "VCpuCount": {
                              "Min": 0,
                              "Max": 2
                          },
                          "MemoryMiB": {
                              "Min": 0
                          }
                      }
                  }
                }
              ]
            }
        ],
         "TargetCapacitySpecification": {
            "TotalTargetCapacity": 1,
            "DefaultTargetCapacityType": "spot"
        }
    }
}
```

Exemplos de configurações de frota spot que são válidas e não válidas

Se você usar a AWS CLI para criar uma frota spot, deverá se certificar de que a configuração da frota seja válida. Exemplos de configurações que são válidas e não válidas.

As configurações são consideradas não válidas quando contiverem o seguinte:

- Uma única estrutura de `Overrides` com `InstanceRequirements` e `InstanceType`
- Duas estruturas de `Overrides`, uma com `InstanceRequirements` e outra com `InstanceType`
- Duas estruturas de `InstanceRequirements` com valores de atributo sobrepostos na mesma `LaunchTemplateSpecification`

Exemplos de configuração

- Configuração válida: modelo de lançamento único com substituições

- Configuração válida: modelo de lançamento único com vários InstanceRequirements
- Configuração válida: dois modelos de lançamento com substituições em cada
- Configuração válida: somente InstanceRequirements especificados, sem valores de atributo sobrepostos
- Configuração não válida: Overrides contémInstanceRequirements e InstanceType
- Configuração não válida: duas Overrides contêm InstanceRequirements e InstanceType
- Configuração não válida: valores de atributo sobrepostos

Configuração válida: modelo de lançamento único com substituições

A configuração a seguir é válida. Ela contém um modelo de lançamento e uma estrutura de `Overrides` contendo uma estrutura de `InstanceRequirements`. A seguir está um texto explicativo do exemplo de configuração.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "priceCapacityOptimized",
        "ExcessCapacityTerminationPolicy": "default",
        "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "My-launch-template",
                "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 2,
                            "Max": 8
                        },
                        "MemoryMib": {
                            "Min": 0,
                            "Max": 10240
                        },
                        "MemoryGiBPerVCpu": {
                            "Max": 10000
                        },
```

```
                        "RequireHibernateSupport": true
                    }
                }
            ]
        }
    ],
        "TargetCapacity": 5000,
            "OnDemandTargetCapacity": 0,
            "TargetCapacityUnitType": "vcpu"
    }
}
```

`InstanceRequirements`

Para usar a seleção de instância baseada em atributos, você deve incluir a estrutura de `InstanceRequirements` na configuração de frota e especificar os atributos desejados para as instâncias da frota.

No exemplo anterior, os seguintes atributos de instância foram especificados:

- `VCpuCount`: os tipos de instância devem ter no mínimo 2 e no máximo 8 vCPUs.
- `MemoryMiB`: os tipos de instância devem ter no máximo 10.240 MiB de memória. Um mínimo de 0 indica que não há limite mínimo.
- `MemoryGiBPerVCpu`: os tipos de instância devem ter no máximo 10.000 GiB de memória. O parâmetro `Min` é opcional. Ao omiti-lo, você indica que não há limite mínimo.

`TargetCapacityUnitType`

O parâmetro `TargetCapacityUnitType` especifica a unidade da capacidade-alvo. No exemplo, a capacidade-alvo é `5000` e o tipo de unidade de capacidade-alvo é `vcpu`, que juntos especificam uma capacidade-alvo desejada de 5000 vCPUs. A frota spot executará instâncias suficientes para que o número total de vCPUs na frota seja de 5.000 vCPUs.

Configuração válida: modelo de lançamento único com vários InstanceRequirements

A configuração a seguir é válida. Ela contém um modelo de lançamento e uma estrutura de `Overrides` contendo duas estruturas de `InstanceRequirements`. Os atributos especificados em `InstanceRequirements` são válidos porque os valores não se sobrepõem: a primeira estrutura de `InstanceRequirements` especifica um `VCpuCount` de 0 a 2 vCPUs, enquanto a segunda estrutura de `InstanceRequirements` especifica de 4 a 8 vCPUs.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "priceCapacityOptimized",
        "ExcessCapacityTerminationPolicy": "default",
        "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                },
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 4,
                            "Max": 8
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                }
              ]
            }
        ],
        "TargetCapacity": 1,
        "OnDemandTargetCapacity": 0,
        "Type": "maintain"
    }
}
```

Configuração válida: dois modelos de lançamento com substituições em cada

A configuração a seguir é válida. Ela contém dois modelos de lançamento, cada um deles com uma estrutura de `Overrides` contendo uma estrutura de `InstanceRequirements`. Essa configuração é útil para oferecer suporte às arquiteturas `arm` e `x86` na mesma frota.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "priceCapacityOptimized",
        "ExcessCapacityTerminationPolicy": "default",
        "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "armLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                },
                {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "x86LaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
```

```
                            "Min": 0
                        }
                    }
                }
              ]
            }
        ],
        "TargetCapacity": 1,
        "OnDemandTargetCapacity": 0,
        "Type": "maintain"
    }
}
```

Configuração válida: somente **`InstanceRequirements`** especificados, sem valores de atributo sobrepostos

A configuração a seguir é válida. Ela contém duas estruturas de `LaunchTemplateSpecification`, cada uma com um modelo de lançamento e uma estrutura `Overrides` contendo uma estrutura de `InstanceRequirements`. Os atributos especificados em `InstanceRequirements` são válidos porque os valores não se sobrepõem: a primeira estrutura de `InstanceRequirements` especifica um `VCpuCount` de 0 a 2 vCPUs, enquanto a segunda estrutura de `InstanceRequirements` especifica de 4 a 8 vCPUs.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "priceCapacityOptimized",
        "ExcessCapacityTerminationPolicy": "default",
        "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
```

```
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                }
              ]
            },
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyOtherLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 4,
                            "Max": 8
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                }
              ]
            }
        ],
        "TargetCapacity": 1,
        "OnDemandTargetCapacity": 0,
        "Type": "maintain"
    }
}
```

Configuração não válida: **`Overrides`** contém **`InstanceRequirements`** e **`InstanceType`**

A configuração a seguir não é válida. A estrutura de `Overrides` contém `InstanceRequirements` e `InstanceType`. Em `Overrides`, você pode especificar `InstanceRequirements` ou `InstanceType`, mas não ambos.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "priceCapacityOptimized",
        "ExcessCapacityTerminationPolicy": "default",
```

```
        "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                },
                {
                    "InstanceType": "m5.large"
                }
              ]
            }
        ],
        "TargetCapacity": 1,
        "OnDemandTargetCapacity": 0,
        "Type": "maintain"
    }
}
```

Configuração não válida: duas **`Overrides`** contêm **`InstanceRequirements`** e **`InstanceType`**

A configuração a seguir não é válida. As estruturas `Overrides` contêm `InstanceRequirements` e `InstanceType`. É possível especificar `InstanceRequirements` ou `InstanceType`, mas não ambos, mesmo que estejam em estruturas de `Overrides` diferentes.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "priceCapacityOptimized",
        "ExcessCapacityTerminationPolicy": "default",
```

```
        "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                }
              ]
            },
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyOtherLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceType": "m5.large"
                }
              ]
            }
        ],
        "TargetCapacity": 1,
        "OnDemandTargetCapacity": 0,
        "Type": "maintain"
    }
}
```

Configuração não válida: valores de atributo sobrepostos

A configuração a seguir não é válida. As duas estruturas de `InstanceRequirements` contêm `"VCpuCount": {"Min": 0, "Max": 2}`. Os valores desses atributos se sobrepõem, o que resultará em grupos de capacidade duplicados.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "priceCapacityOptimized",
        "ExcessCapacityTerminationPolicy": "default",
        "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    },
                    {
                      "InstanceRequirements": {
                          "VCpuCount": {
                              "Min": 0,
                              "Max": 2
                          },
                          "MemoryMiB": {
                              "Min": 0
                          }
                      }
                  }
                }
              ]
            }
```

```
        ],
        "TargetCapacity": 1,
        "OnDemandTargetCapacity": 0,
        "Type": "maintain"
    }
}
```

Previsualizar os tipos de instância com os atributos especificados

É possível usar o comando get-instance-types-de-instance-requirements para previsualizar os tipos de instância que correspondem aos atributos especificados por você. Isso é especialmente útil para determinar quais atributos especificar na configuração da solicitação sem iniciar nenhuma instância. Observe que o comando não considera a capacidade disponível.

Para previsualizar uma lista de tipos de instância especificando atributos usando a AWS CLI

1. (Opcional) Para gerar todos os atributos possíveis que podem ser especificados, use o comando get-instance-types-de-instance-requirements e o parâmetro `--generate-cli-skeleton`. Opcionalmente, você pode direcionar a saída para um arquivo e salvá-lo usando `input > attributes.json`.

   ```
   aws ec2 get-instance-types-from-instance-requirements \
       --region us-east-1 \
       --generate-cli-skeleton input > attributes.json
   ```

   Saída esperada

   ```
   {
       "DryRun": true,
       "ArchitectureTypes": [
           "i386"
       ],
       "VirtualizationTypes": [
           "hvm"
       ],
       "InstanceRequirements": {
           "VCpuCount": {
               "Min": 0,
               "Max": 0
           },
           "MemoryMiB": {
   ```

```
            "Min": 0,
            "Max": 0
        },
        "CpuManufacturers": [
            "intel"
        ],
        "MemoryGiBPerVCpu": {
            "Min": 0.0,
            "Max": 0.0
        },
        "ExcludedInstanceTypes": [
            ""
        ],
        "InstanceGenerations": [
            "current"
        ],
        "SpotMaxPricePercentageOverLowestPrice": 0,
        "OnDemandMaxPricePercentageOverLowestPrice": 0,
        "BareMetal": "included",
        "BurstablePerformance": "included",
        "RequireHibernateSupport": true,
        "NetworkInterfaceCount": {
            "Min": 0,
            "Max": 0
        },
        "LocalStorage": "included",
        "LocalStorageTypes": [
            "hdd"
        ],
        "TotalLocalStorageGB": {
            "Min": 0.0,
            "Max": 0.0
        },
        "BaselineEbsBandwidthMbps": {
            "Min": 0,
            "Max": 0
        },
        "AcceleratorTypes": [
            "gpu"
        ],
        "AcceleratorCount": {
            "Min": 0,
            "Max": 0
        },
```

```
        "AcceleratorManufacturers": [
            "nvidia"
        ],
        "AcceleratorNames": [
            "a100"
        ],
        "AcceleratorTotalMemoryMiB": {
            "Min": 0,
            "Max": 0
        },
        "NetworkBandwidthGbps": {
            "Min": 0.0,
            "Max": 0.0
        },
        "AllowedInstanceTypes": [
            ""
        ]
    },
    "MaxResults": 0,
    "NextToken": ""
}
```

2. Crie um arquivo de configuração JSON usando a saída da etapa anterior e configure-o da seguinte forma:

> **Note**
>
> Você deve fornecer valores para `ArchitectureTypes`, `VirtualizationTypes`, `VCpuCount` e `MemoryMiB`. É possível omitir os outros atributos; quando omitidos, os valores padrão são usados.
> Para obter uma descrição de cada atributo e seus valores padrão, consulte get-instance-types-from-instance-requirements.

a. Em `ArchitectureTypes`, especifique um ou mais tipos de arquitetura de processador.

b. Em `VirtualizationTypes`, especifique um ou mais tipos de virtualização.

c. Em `VCpuCount`, especifique o número mínimo e máximo de vCPUs. Para não especificar nenhum limite mínimo, em `Min`, especifique `0`. Para não especificar nenhum limite máximo, omita o parâmetro `Max`.

d. Em `MemoryMiB`, especifique a quantidade mínima e máxima de memória em MiB. Para não especificar nenhum limite mínimo, em `Min`, especifique `0`. Para não especificar nenhum limite máximo, omita o parâmetro `Max`.

e. Opcionalmente, você pode especificar um ou mais dos outros atributos para restringir ainda mais a lista de tipos de instância retornados.

3. Para previsualizar os tipos de instância que têm os atributos que você especificou no arquivo JSON, use o comando get-instance-types-from-instance-requirements e especifique o nome e o caminho para seu arquivo JSON usando o parâmetro `--cli-input-json`. Opcionalmente, você pode formatar a saída para ser exibida em formato de tabela.

```
aws ec2 get-instance-types-from-instance-requirements \
    --cli-input-json file://attributes.json \
    --output table
```

Exemplo de arquivo *attributes.json*

Neste exemplo, os atributos necessários estão incluídos no arquivo JSON. Eles são `ArchitectureTypes`, `VirtualizationTypes`, `VCpuCount` e `MemoryMiB`. Além disso, o atributo opcional `InstanceGenerations` também está incluído. Observe que para `MemoryMiB`, o valor `Max` pode ser omitido para indicar que não há limite.

```
{

    "ArchitectureTypes": [
        "x86_64"
    ],
    "VirtualizationTypes": [
        "hvm"
    ],
    "InstanceRequirements": {
        "VCpuCount": {
            "Min": 4,
            "Max": 6
        },
        "MemoryMiB": {
            "Min": 2048
        },
        "InstanceGenerations": [
            "current"
        ]
```

```
    }
}
```

Exemplo de saída

```
-----------------------------------------
|GetInstanceTypesFromInstanceRequirements|
+---------------------------------------+
||             InstanceTypes             ||
|+-------------------------------------+|
||             InstanceType              ||
|+-------------------------------------+|
||  c4.xlarge                          ||
||  c5.xlarge                          ||
||  c5a.xlarge                         ||
||  c5ad.xlarge                        ||
||  c5d.xlarge                         ||
||  c5n.xlarge                         ||
||  d2.xlarge                          ||
...
```

4. Após identificar os tipos de instância que atendem às suas necessidades, anote os atributos de instância usados para que poder usá-los ao configurar a solicitação de frota.

Usar ponderação de instâncias para gerenciar o custo e a performance da frota do EC2 ou da frota spot

Com a ponderação de instâncias, você atribui um peso a cada tipo de instância na frota do EC2 ou na frota spot para representar sua capacidade computacional e a performance na comparação de uma com a outra. Com base nos pesos, a frota pode usar qualquer combinação dos tipos de instância especificados, desde que possa atender à capacidade de destino desejada. Isso pode ajudar você a gerenciar o custo e a performance da frota.

O peso representa as unidades de capacidade que um tipo de instância contribui para a capacidade total de destino.

Exemplo: usar ponderação de instâncias para o gerenciamento de performance

Suponha que a frota tenha dois tipos de instância e você atribua um peso diferente a cada tipo de instância para refletir a quantidade necessária de cada uma para atingir a mesma performance da seguinte forma:

- `m5.large` - peso: 1
- `m5.2xlarge` - peso: 4

Ao atribuir esses pesos, você está afirmando que precisa de quatro instâncias `m5.large` para obter a mesma performance de uma `m5.2xlarge`.

Para calcular quantas instâncias de cada tipo de instância são necessárias para uma determinada capacidade de destino, use a seguinte fórmula:

```
target capacity / weight = number of instances
```

Se sua capacidade de destino for de oito unidades, a frota poderá atingir a capacidade de destino com `m5.large` ou `m5.2xlarge`, ou com uma combinação de ambas, da seguinte forma:

- 8 instâncias `m5.large` (capacidade de 8/peso de 1 = 8 instâncias)
- 2 instâncias `m5.2xlarge` (capacidade de 8/peso de 4 = 2 instâncias)
- 4 `m5.large` e 1 `m5.2xlarge`

Exemplo: usar ponderação de instâncias para gerenciamento de custo

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. É possível calcular o preço por hora dividindo seu preço para um tipo de instância pelo número de unidades que ele representa. A frota calcula o número de instâncias a serem inicializadas 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 de uma frota com capacidade de destino igual a 10.

Tipo de instância	Peso da instância	Capacidade de destino	Número de instâncias executadas	Preço por hora de instância	Preço por hora
`r3.xlarge`	2	10	5 (10 dividido por 2)	0,05 USD	0,025 USD (0,05 dividido por 2)
`r3.8xlarge`	8	10	2 (10 dividido por 8, resultado arredondado para cima)	0,10 USD	0,0125 USD (0,10 dividido por 8)

Use a ponderação da instância da frota como abaixo 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 nas instâncias (o padrão) ou nas unidades de sua preferência, como vCPUs, 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 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 inicialização fornecer o menor preço por unidade (preço por `r3.2xlarge` por hora de instância dividido por 6), a frota inicializará quatro dessas instâncias (24 dividido por 6).

Se a segunda especificação de inicialização fornecer o menor preço por unidade (preço por `c3.xlarge` por hora de instância dividido por 5), a frota inicializará cinco dessas instâncias (24 dividido por 5, resultado arredondado para cima).

Peso da instância e estratégia de alocação

Considere uma solicitação de frota 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 executaria quatro instâncias (30 dividido por 8, resultado arredondado para cima). 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.

Usar estratégias de alocação para determinar como a frota do EC2 ou a frota spot atende à capacidade spot e sob demanda

Quando você usa vários grupos de capacidade (cada um abrangendo um tipo de instância e uma zona de disponibilidade) em uma frota do EC2 ou uma frota spot, você pode usar uma estratégia de alocação para gerenciar como o Amazon EC2 atende às capacidades spot e sob demanda desses grupos. As estratégias de alocação podem otimizar a capacidade disponível, o preço e os tipos de instância a serem usados. Existem diferentes estratégias de alocação para instâncias spot e instâncias sob demanda.

Tópicos

- Estratégias de alocação para Instâncias spot
- Estratégias de alocação para instâncias sob demanda
- Escolher a estratégia de alocação spot apropriada
- Manter a capacidade de destino para instâncias spot

- Priorizar tipos de instâncias para capacidade sob demanda

Estratégias de alocação para Instâncias spot

Sua configuração de inicialização determina todos os possíveis grupos de capacidade spot (tipos de instância e zonas de disponibilidade) nos quais a frota do EC2 ou a frota spot pode inicializar instâncias spot. No entanto, ao inicializar instâncias, a frota usa a estratégia de alocação que você especifica para escolher os grupos específicos de todos os seus grupos possíveis.

> **Note**
>
> (Somente para instâncias do Linux) Se você configurar a instância spot para iniciar com o AMD SEV-SNP ativado, será cobrada uma taxa de utilização por hora adicional equivalente a 10% da taxa horária sob demanda para o tipo de instância selecionado. Se a estratégia de alocação usar o preço como entrada, a frota não incluirá essa taxa adicional; somente o preço spot será usado.

É possível especificar uma destas estratégias de alocação para instâncias spot:

Capacidade de preço otimizada (recomendado)

A frota identifica os grupos com a maior disponibilidade de capacidade para o número de instâncias que estão sendo inicializadas. Isso significa que solicitaremos instâncias spot dos grupos que acreditamos terem a menor probabilidade de interrupção a curto prazo. Em seguida, a frota solicita instâncias spot do grupo com o menor preço desses grupos.

A estratégia de alocação capacidade de preço otimizada é a melhor opção para a maioria das workloads spot, como aplicações em contêiner sem estado, microsserviços, aplicações Web, trabalhos de dados e analytics e processamento em lote.

Se você estiver usando a AWS CLI, o nome do parâmetro será `price-capacity-optimized` para frotas do EC2 e `priceCapacityOptimized` para frotas spot.

Otimizada para capacidade

A frota identifica os grupos com a maior disponibilidade de capacidade para o número de instâncias que estão sendo inicializadas. Isso significa que solicitaremos instâncias spot dos grupos que acreditamos terem a menor probabilidade de interrupção a curto prazo.

Opcionalmente, você pode definir uma prioridade para cada tipo de instância na frota. A frota otimiza primeiro a capacidade, mas se esforça em honrar as prioridades de tipo de instância.

Com as Instâncias spot, a definição de preço muda lentamente ao longo do tempo com base em tendências de longo prazo na oferta e na demanda, mas a capacidade oscila em tempo real. A estratégia capacidade otimizada inicializa instâncias spot automaticamente nos grupos mais disponíveis observando dados de capacidade em tempo real e prevendo quais são os mais disponíveis. Isso funciona bem para workloads que podem ter um custo de interrupção maior associado ao reinício do trabalho, como workloads de integração contínua (CI) longa, de renderização de imagens e mídia, de aprendizado profundo e de computação de alta performance (HPC). Ao oferecer a possibilidade de menos interrupções, a estratégia capacidade otimizada pode reduzir o custo geral da workload.

Como alternativa, você pode usar a estratégia de alocação capacidade otimizada priorizada com um parâmetro de prioridade para ordenar os tipos de instância, da prioridade mais alta para a mais baixa. É possível definir a mesma prioridade para diferentes tipos de instância. A frota otimizará primeiro a capacidade, mas se esforçará em honrar as prioridades de tipo de instância (por exemplo, honrar as prioridades não afetará significativamente a capacidade da frota de provisionar a capacidade ideal). Essa é uma boa opção para workloads em que a possibilidade de interrupção deve ser minimizada e a preferência por determinados tipos de instância for importante. Quando você definir a prioridade para tipos de instância para capacidade spot, a mesma prioridade também será aplicada às instâncias sob demanda se a estratégia de alocação sob demanda estiver definida como priorizada. Para frotas spot, o uso de prioridades só será compatível se a frota usar um modelo de inicialização.

Se você estiver usando a AWS CLI, os nomes dos parâmetros serão `capacity-optimized` e `capacity-optimized-prioritized` para frotas do EC2 e `capacityOptimized` e `capacityOptimizedPrioritized` para frotas spot.

Diversificada

Os Instâncias spot são distribuídos em todos os grupos de capacidade spot. Se você estiver usando a AWS CLI, o nome do parâmetro será `diversified` para frotas do EC2 e frotas spot.

Preço mais baixo (não recomendado)

> **Warning**
>
> Não recomendamos a estratégia de alocação preço mais baixo porque ela representa o risco mais alto de interrupção para as instâncias spot.

As instâncias spot vêm do grupo com o menor preço que tem capacidade disponível. Ao ser usada a AWS CLI, essa é a estratégia padrão. Porém, recomendamos que você substitua o padrão ao especificar a estratégia de alocação otimizada para capacidade de preço.

Com a estratégia de preço mais baixo, se o grupo com preço mais baixo não tiver capacidade disponível, as instâncias spot virão do próximo grupo com preço mais baixo que tiver capacidade disponível. Se um grupo esgotar a capacidade spot antes de atender à capacidade desejada, a frota continuará a atender à solicitação recorrendo ao próximo grupo de preço mais baixo. Para garantir que a capacidade desejada seja atendida, é possível receber instâncias spot de vários grupos.

Como essa estratégia considera apenas o preço da instância e não a disponibilidade de capacidade, ela pode resultar em altas taxas de interrupção.

A estratégia de alocação de preço mais baixo só está disponível quando é usada a AWS CLI. O nome do parâmetro é `lowest-price` para frotas do EC2 e `lowestPrice` para frotas spot.

Número de grupos a serem usados

O número de grupos spot para os quais alocar sua capacidade spot de destino. Válido apenas quando a estratégia de alocação está definida como preço mais baixo. A frota seleciona os grupos spot de preço mais baixo e aloca uniformemente a capacidade spot de destino pelo número de grupos spot que você especifica.

A frota tenta extrair instâncias spot do número de grupos que você especifica com base no melhor esforço. Se um grupo esgotar a capacidade spot antes de atender à capacidade de destino, a frota continuará a atender à solicitação recorrendo ao próximo grupo de preço mais baixo. Para garantir que sua capacidade de destino seja atendida, você pode receber Instâncias Spot de mais do que o número de pools especificado. Da mesma forma, se a maioria dos pools não tiver capacidade spot, será possível receber sua capacidade de destino total de menos do que o número de pools que você especificou.

Esse parâmetro só está disponível quando é especificada a estratégia de alocação preço mais baixo e somente quando é usada a AWS CLI. O nome do parâmetro é `InstancePoolsToUseCount` para frotas do EC2 e para frotas spot.

Estratégias de alocação para instâncias sob demanda

A configuração de inicialização determina todos os possíveis grupos de capacidade (tipos de instância e zonas de disponibilidade) nos quais a frota do EC2 ou a frota spot pode inicializar

instâncias sob demanda. No entanto, ao inicializar instâncias, a frota usa a estratégia de alocação que você especifica para escolher os grupos específicos de todos os seus grupos possíveis.

É possível especificar uma destas estratégias de alocação para instâncias sob demanda:

Preço mais baixo

As instâncias sob demanda vêm do grupo com o preço mais baixo que tem capacidade disponível. Essa é a estratégia padrão.

Se o grupo com preço mas baixo não tiver capacidade disponível, as instâncias sob demanda virão do próximo grupo com preço mais baixo que tiver capacidade disponível.

Se um grupo esgotar a capacidade spot antes de atender à capacidade desejada, a frota continuará a atender à solicitação recorrendo ao próximo grupo de preço mais baixo. Para garantir que a capacidade desejada seja atendida, é possível receber instâncias sob demanda de vários grupos.

Priorizada

A frota usa a prioridade que você atribuiu para cada substituição do modelo de inicialização ao inicializar tipos de instância começando pela prioridade mais alta. Essa estratégia não pode ser usada com a seleção de tipo de instância baseada em atributos. Para obter um exemplo de como usar essa estratégia de alocação, consulte Priorizar tipos de instâncias para capacidade sob demanda.

Escolher a estratégia de alocação spot apropriada

É possível otimizar a frota para seu caso de uso escolhendo a estratégia apropriada de alocação spot.

Equilibrar menor preço e disponibilidade de capacidade

Para obter o equilíbrio entre os grupos de capacidade spot com preço mais baixo e os grupos de capacidade spot com a maior disponibilidade de capacidade, recomendamos que você use a estratégia de alocação otimizada para capacidade de preço. Essa estratégia toma decisões sobre quais grupos devem solicitar instâncias spot com base no preço dos grupos e na disponibilidade de capacidade de instâncias spot nesses grupos. Isso significa que solicitaremos instâncias spot dos grupos que acreditamos terem a menor probabilidade de interrupção em curto prazo, ao mesmo tempo que ainda levaremos o preço em consideração.

Se a frota executar workloads resilientes e sem estado, incluindo aplicações em contêiner, microsserviços, aplicações Web, trabalhos de dados e analytics e processamento em lote, use a estratégia de alocação otimizada para capacidade de preço para otimizar a economia de custos e a disponibilidade de capacidade.

Se a frota executar workloads que possam ter um custo de interrupção maior associado ao reinício do trabalho, você deverá implementar verificações para que as aplicações possam ser reiniciadas no ponto em que foram interrompidas. Ao usar pontos de verificação, você torna a estratégia de alocação otimizada para capacidade de preço uma boa opção para essas workloads, pois ela aloca a capacidade dos grupos com preço mais baixo que também oferecem uma baixa taxa de interrupção de instâncias spot.

Por exemplo, em configurações JSON que usam a estratégia de alocação otimizada para capacidade de preço, veja o seguinte:

- Frota do EC2: Exemplo 10: iniciar instâncias spot em uma frota otimizada para preço-capacidade
- Frota spot: Exemplo 11: executar instâncias spot em uma frota priceCapacityOptimized

Quando as workloads têm um alto custo de interrupção

Opcionalmente, você pode usar a estratégia otimizada para capacidade se executar workloads que usem tipos de instância com preços semelhantes ou em que o custo da interrupção seja tão significativo que qualquer economia de custos será inadequada em comparação com um aumento marginal nas interrupções. Essa estratégia aloca capacidade dos grupos com capacidade spot mais disponível que oferecem a possibilidade de menos interrupções, o que pode reduzir o custo geral da workload.

Quando a possibilidade de interrupções precisa ser minimizada mas a preferência por determinados tipos de instância é importante, é possível expressar as prioridades do grupo usando a estratégia de alocação capacidade otimizada priorizada e definindo a ordem dos tipos de instância a serem usados da prioridade mais alta para a mais baixa.

Observe que, quando você define as prioridades para capacidade otimizada priorizada, as mesmas prioridades também são aplicadas às instâncias sob demanda se a estratégia de alocação sob demanda está definida como priorizada. Observe também que, para frotas spot, o uso de prioridades só será compatível se a frota usar um modelo de inicialização.

Por exemplo, em configurações JSON que usam a estratégia de alocação otimizada para capacidade, observe o seguinte:

- Frota do EC2: Exemplo 8: iniciar instâncias spot em uma frota otimizada para capacidade
- Frota spot: Exemplo 9: iniciar instâncias spot em uma frota otimizada para capacidade

Por exemplo, em configurações JSON que usam a estratégia de alocação capacidade otimizada priorizada, observe o seguinte:

- Frota do EC2: Exemplo 9: iniciar instâncias spot em uma frota otimizada para capacidade com prioridades
- Frota spot: Exemplo 10: iniciar instâncias spot em uma frota otimizada para capacidade com prioridades

Quando a workload é flexível em termos de tempo e a disponibilidade de capacidade não é um fator

Se a frota é pequena ou é executada por um período curto, você pode usar otimizada para capacidade de preço para maximizar a economia de custos, ainda considerando a disponibilidade de capacidade.

Quando sua frota é grande ou é executada por muito tempo

Se sua frota é grande ou é executada há muito tempo, será possível aprimorar a disponibilidade dela distribuindo as instâncias spot por vários grupos, usando a estratégia diversificada. Por exemplo, se a frota especificar dez grupos e uma capacidade de destino de cem instâncias, a frota inicializará dez 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 diversificada, a frota não inicializará instâncias spot em nenhum grupo com um preço spot igual ou maior que o preço sob demanda.

Manter a capacidade de destino para instâncias spot

Depois que as instâncias spot são encerradas devido a uma alteração no preço spot ou na capacidade disponível de um grupo de capacidade spot, uma frota do tipo `maintain` inicializa instâncias spot de substituição. A estratégia de alocação determina os grupos dos quais as instâncias de substituição são iniciadas, da seguinte forma:

- Se a estratégia de alocação for capacidade de preço otimizada, a frota inicializará instâncias de substituição nos grupos com maior disponibilidade de capacidade de instâncias spot, ao mesmo

tempo que também levará em consideração o preço e identificará os grupos de preço mais baixo com alta disponibilidade de capacidade.

- Se a estratégia de alocação for capacidade otimizada, a frota inicializará instâncias de substituição nos grupos com a maior disponibilidade de capacidade de instâncias spot.
- Se a estratégia de alocação for diversificada, a frota distribuirá as instâncias spot de substituição entre os grupos restantes.

Priorizar tipos de instâncias para capacidade sob demanda

Quando uma frota do EC2 ou uma frota spot tenta atender à capacidade sob demanda, o padrão é inicializar primeiro o tipo de instância de preço mais baixo. Se a estratégia de alocação estiver definida como priorizada, a frota usará a prioridade para determinar que tipo de instância será usada primeiro para atender à capacidade sob demanda. A prioridade é atribuída à substituição do modelo de ativação, e a prioridade mais alta é lançada primeiro.

Exemplo: priorizar tipos de instância

Neste exemplo, você configura três substituições de modelo de execução, cada uma com um tipo de instância diferente.

O preço sob demanda para os tipos de instância varia no preço. Estes são os tipos de instância usados neste exemplo, listados em ordem de preço, a partir do tipo de instância mais barato:

- `m4.large`: menor custo
- `m5.large`
- `m5a.large`

Se você não usar prioridade para determinar a ordem, a frota atenderá à capacidade sob demanda começando pelo tipo mais barato de instância.

No entanto, digamos que você tenha instâncias reservadas `m5.large` não utilizadas que deseja usar primeiro. É possível definir a prioridade de substituição do modelo de execução para que os tipos de instância sejam usados na ordem de prioridade, da seguinte forma:

- `m5.large`: prioridade 1
- `m4.large`: prioridade 2
- `m5a.large`: prioridade 3

Use o rebalanceamento de capacidade na frota do EC2 e na frota spot para substituir instâncias spot em risco

Com o rebalanceamento de capacidade, a frota do EC2 ou a frota spot pode manter a capacidade spot desejada ao substituir proativamente as instâncias spot com risco de interrupção. Quando uma instância spot apresenta risco elevado de interrupção, o Amazon EC2 envia uma recomendação de rebalanceamento. Se o rebalanceamento de capacidade estiver habilitado, a recomendação de rebalanceamento acionará a inicialização de uma nova instância spot antes que a instância em risco seja interrompida.

O rebalanceamento de capacidade ajuda a manter a disponibilidade da workload ao aumentar proativamente a frota com uma nova instância spot antes que instâncias em execução sejam interrompidas pelo Amazon EC2.

Configurar a frota do EC2 para usar rebalanceamento de capacidade para inicializar uma Instância spot de substituição

Use o comando create-fleet e os parâmetros relevantes na estrutura `MaintenanceStrategies`. Para ver um exemplo de configuração JSON, consulte Exemplo 7: Configurar o rebalanceamento de capacidade para executar a Instâncias spot de substituição.

Configurar a frota spot para usar rebalanceamento de capacidade para inicializar uma instância spot de substituição

É possível usar o console do Amazon EC2 ou a AWS CLI para configurar o rebalanceamento de capacidade.

(Console) Quando criar a frota spot, marque a caixa de seleção Rebalanceamento de capacidade. Para obter mais informações, consulte a etapa 6.d em Criar uma solicitação de frota spot usando parâmetros definidos.

(AWS CLI) Use o comando request-spot-fleet e os parâmetros relevantes na estrutura `SpotMaintenanceStrategies`. Para ver um exemplo de configuração JSON, consulte Exemplo 8: Configurar o rebalanceamento de capacidade para executar a Instâncias spot de substituição.

Tópicos

- Limitações
- Opções de configuração

- Considerações

Limitações

- O rebalanceamento de capacidade só está disponível para frotas do tipo `maintain`.
- Quando a frota estiver em execução, não é possível modificar a configuração de rebalanceamento de capacidade. Para alterar a configuração de rebalanceamento de capacidade, você deve excluir a frota e criar uma nova.

Opções de configuração

A `ReplacementStrategy` para a frota do EC2 e a frota spot oferece suporte a estes dois valores:

`launch-before-terminate`

O Amazon EC2 termina as Instâncias spot que recebem uma notificação de rebalanceamento após o lançamento de novas Instâncias spot de substituição. Se você especificar `launch-before-terminate`, também deverá especificar um valor para `termination-delay`. Depois que as novas instâncias de substituição são iniciadas, o Amazon EC2 aguarda o período de `termination-delay` e, em seguida, encerra as instâncias antigas. Em `termination-delay`, o mínimo é de 120 segundos (2 minutos) e o máximo é de 7.200 segundos (2 horas).

Recomendamos o uso de `launch-before-terminate` apenas se você puder prever quanto tempo os procedimentos de desligamento da instância levarão. Isso garantirá que as instâncias antigas só sejam terminadas após a conclusão dos procedimentos de desligamento. Observe que o Amazon EC2 pode interromper as instâncias antigas com um aviso dois minutos antes do período de `termination-delay`.

Recomendamos firmemente não usar a estratégia de alocação `lowest-price` (frota do EC2) ou `lowestPrice` (frota spot) em combinação com `launch-before-terminate` para evitar a ocorrência de instâncias spot de substituição que também apresentem risco elevado de interrupção.

`launch`

O Amazon EC2 inicia instâncias spot de substituição quando uma notificação de rebalanceamento é emitida para as instâncias spot existentes. O Amazon EC2 não termina automaticamente as instâncias que recebem uma notificação de rebalanceamento. É possível

terminar as instâncias antigas ou deixá-las em execução. Você é cobrado por todas as instâncias enquanto elas estão sendo executadas.

Considerações

Se você configurar uma frota do EC2 ou uma frota spot para rebalanceamento de capacidade, considere o seguinte:

Forneça o maior número possível de grupos de capacidade spot na solicitação

Configure a frota para usar vários tipos de instância e zonas de disponibilidade. Isso oferece a flexibilidade para executar instâncias spot em vários grupos de capacidade spot. Para obter mais informações, consulte Ser flexível sobre tipos de instância e zonas de disponibilidade.

Evitar um risco elevado de interrupção das instâncias spot substitutas

Para evitar um alto risco de interrupção, recomendamos fortemente a estratégia de alocação `capacity-optimized` ou `capacity-optimized-prioritized`. Essas estratégias garantem que as instâncias spot substitutas sejam iniciadas nos grupos de capacidade spot ideais e, portanto, tenham menos probabilidade de serem interrompidas em futuro próximo. Para obter mais informações, consulte Usar a estratégia de alocação otimizada para preço e capacidade.

Se você usar a estratégia de alocação `lowest-price`, as instâncias spot de substituição poderão apresentar risco elevado de interrupção. Isso ocorre porque o Amazon EC2 sempre iniciará instâncias no grupo de preços mais baixos que tenha capacidade disponível naquele momento, mesmo que exista a probabilidade de que as instâncias spot de substituição sejam interrompidas logo após serem iniciadas.

O Amazon EC2 Auto Scaling só iniciará uma nova instância se a disponibilidade for igual ou superior

Um dos objetivos do rebalanceamento de capacidade é melhorar a disponibilidade de uma instância spot. Se uma instância spot existente receber uma recomendação de rebalanceamento, o Amazon EC2 só iniciará uma nova instância caso a nova instância forneça uma disponibilidade igual ou superior a da instância existente. Se o risco de interrupção de uma nova instância for pior do que a instância existente, o Amazon EC2 não iniciará uma nova instância. No entanto, o Amazon EC2 continuará a avaliar os grupos de capacidade spot e iniciará uma nova instância se a disponibilidade melhorar.

Há uma chance de que a instância existente seja interrompida sem que o Amazon EC2 inicie proativamente uma nova instância. Quando isso acontecer, o Amazon EC2 tentará iniciar uma nova instância, independentemente de a nova instância ter um alto risco de interrupção.

O Rebalanceamento da capacidade não aumenta a taxa de interrupção de instâncias Spot

Quando o Rebalanceamento da capacidade é habilitado, ele não aumenta a Taxa de interrupção de instâncias Spot (o número de instâncias Spot que são recuperadas quando o Amazon EC2 precisa novamente de capacidade). Porém, se o rebalanceamento da capacidade detectar que uma instância está em risco de interrupção, o Amazon EC2 tentará iniciar imediatamente uma nova instância. O resultado é que pode haver a substituição de mais instâncias do que se você esperasse que o Amazon EC2 iniciasse uma nova instância depois que a instância em risco fosse interrompida.

Mesmo podendo substituir mais instâncias com o Rebalanceamento da capacidade habilitado, você se beneficia de ser proativo em vez de reativo, tendo mais tempo para agir antes que suas instâncias sejam interrompidas. Com um Aviso de interrupção de instâncias Spot, normalmente você só tem até dois minutos para encerrar sua instância sem problemas. Com o Rebalanceamento da capacidade iniciando uma nova instância com antecedência, os processos existentes têm maiores chances de serem concluídos na instância em risco. Além disso, você pode iniciar os procedimentos de desligamento da instância e impedir que novos trabalhos sejam agendados na instância em risco. Você também pode começar a preparar a instância recém-lançada para assumir o controle da aplicação. Com a substituição proativa do Rebalanceamento da capacidade, você se beneficia com uma continuidade tranquila.

Como exemplo teórico para demonstrar os riscos e benefícios do uso do Rebalanceamento da capacidade, considere o seguinte cenário:

- 14h: uma recomendação de rebalanceamento é recebida para a instância A, e o Amazon EC2 começa imediatamente a tentar iniciar uma instância B de substituição, dando a você tempo para iniciar os procedimentos de desligamento.*
- 14h30: uma recomendação de rebalanceamento é recebida para a instância-B, substituída pela instância-C, dando a você tempo para iniciar os procedimentos de desligamento.*
- 14h32: se o Rebalanceamento da capacidade não estivesse habilitado e um aviso de interrupção de instância Spot tivesse sido recebido às 14h32 para a instância-A, você teria apenas dois minutos para agir, mas a Instância-A estaria em execução até esse momento.

* Se `launch-before-terminate` for especificado, o Amazon EC2 encerrará a instância em risco depois que a instância de substituição ficar online.

O Amazon EC2 pode iniciar a nova Instâncias spot de substituição até que a capacidade atingida seja o dobro da capacidade visada

Quando uma frota é configurada para rebalanceamento de capacidade, ela tenta executar uma nova instância spot de substituição para cada instância spot que recebe uma recomendação de rebalanceamento. Depois que uma instância spot recebe uma recomendação de rebalanceamento, ela deixa de ser contada como parte da capacidade atendida. Dependendo da estratégia de substituição, o Amazon EC2 termina a instância após um período espera para término pré-configurado ou a deixa em execução. Isso dá a você a oportunidade de executar ações de rebalanceamento na instância.

Se sua frota atingir o dobro da capacidade de destino, ela interrompe a execução de novas instâncias de substituição, mesmo que as próprias instâncias de substituição recebam uma recomendação de rebalanceamento.

Por exemplo, você cria uma frota com uma capacidade de destino de cem instâncias spot. Todas as instâncias spot recebem uma recomendação de rebalanceamento, o que faz com que o Amazon EC2 inicie 100 instâncias spot de substituição. Isso eleva o número de instâncias spot atendidas para 200, o que é o dobro da capacidade de destino. Algumas das instâncias de substituição recebem uma recomendação de rebalanceamento. Porém, nenhuma instância de substituição é inicializada porque a frota não pode exceder o dobro da sua capacidade de destino.

Observe que você é cobrado por todas as instâncias durante a execução.

Recomendamos que você configure a frota para encerrar as instâncias spot que receberem uma recomendação de rebalanceamento

Se você configurar a frota para rebalanceamento de capacidade, recomendamos que só escolha `launch-before-terminate` com um período de espera de encerramento apropriado se puder prever quanto tempo a conclusão dos procedimentos de desligamento da instância demorará. Isso garantirá que as instâncias antigas só sejam terminadas após a conclusão dos procedimentos de desligamento.

Se escolher terminar as instâncias recomendadas para rebalanceamento você mesmo, recomendamos que monitore o aviso da recomendação de rebalanceamento recebido pelas instâncias spot na frota. Ao monitorar o sinal, você pode executar rapidamente ações de rebalanceamento nas instâncias afetadas, antes que o Amazon EC2 as interrompa e, em seguida, você pode encerrá-las manualmente. Se você não encerrar as instâncias,

continuará pagando por elas enquanto estiverem em execução. O Amazon EC2 não encerra automaticamente as instâncias que recebem uma recomendação de rebalanceamento.

É possível configurar notificações usando o Amazon EventBridge ou metadados da instância. Para obter mais informações, consulte Monitorar os sinais de recomendação de rebalanceamento.

A frota não conta as instâncias que recebem uma recomendação de rebalanceamento quando calcula a capacidade atendida durante a redução ou o aumento da escala horizontalmente

Se a frota estiver configurada para rebalanceamento de capacidade e você alterar a capacidade de destino para redução ou aumento da escala horizontalmente, a frota não contará as instâncias marcadas para rebalanceamento como parte da capacidade atendida, como mostrado a seguir:

- Reduzir a escala horizontalmente - Se você diminuir a capacidade visada, o Amazon EC2 encerrará instâncias que não estiverem marcadas para rebalanceamento até que a capacidade desejada seja atingida. As instâncias marcadas para rebalanceamento não são contabilizadas para a capacidade atingida.

  Por exemplo, você cria uma frota com uma capacidade de destino de cem instâncias spot, e dez instâncias recebem uma recomendação de rebalanceamento. Portanto, o Amazon EC2 inicializa dez novas instâncias de substituição, resultando em uma capacidade atendida de 110 instâncias. Em seguida, você reduz a capacidade visada para 50 (reduzir a escala horizontalmente), mas a capacidade de atendimento é, na verdade, 60 instâncias porque as 10 instâncias marcadas para rebalanceamento não são encerradas pelo Amazon EC2. Você precisa encerrar manualmente essas instâncias ou deixá-las em execução.

- Aumentar a escala horizontalmente - Se você aumentar a capacidade visada, o Amazon EC2 iniciará novas instâncias até que a capacidade desejada seja atingida. As instâncias marcadas para rebalanceamento não são contabilizadas para a capacidade atingida.

  Por exemplo, você cria uma frota com uma capacidade de destino de cem instâncias spot. Dez instâncias recebem uma recomendação de rebalanceamento. Portanto, a frota inicializa dez novas instâncias de substituição, resultando em uma capacidade atendida de 110 instâncias. Em seguida, você aumenta a capacidade de destino para 200 (aumento), mas a capacidade de atendimento é, na verdade, 210 instâncias porque as 10 instâncias marcadas para rebalanceamento não são contabilizadas pela frota como parte da capacidade de destino. Você precisa encerrar manualmente essas instâncias ou deixá-las em execução.

Use reservas de capacidade para reservar capacidade sob demanda na frota do EC2

Com as Reservas de Capacidade sob demanda, você pode reservar capacidade computacional para suas Instâncias sob demanda em uma determinada zona de disponibilidade por qualquer duração. É possível configurar uma Frota do EC2 para usar as Reservas de Capacidade primeiro ao iniciar Instâncias sob demanda.

As reservas de capacidade sob demanda só estão disponíveis para a frota do EC2 com o tipo de solicitação definido como `instant`.

As Reservas de Capacidade são configuradas como `open` ou `targeted`. A frota EC2 pode iniciar Instâncias sob demanda nas Reservas de Capacidade `open` ou `targeted`, da seguinte forma:

- Se uma Reserva de capacidade é `open`, as Instâncias sob demanda que tiverem atributos correspondentes serão executadas automaticamente na capacidade reservada.
- Se uma Reserva de capacidade for `targeted`, as Instâncias sob demanda deverão usá-la como destino especificamente para executar na capacidade reservada. Isso é útil para usar Reservas de Capacidade específicas ou para controlar quando usar Reservas de Capacidade específicas.

Se você usar Reservas de Capacidade `targeted` em sua frota EC2, deve haver Reservas de Capacidade suficientes para atender à capacidade sob demanda de destino, caso contrário, o lançamento falhará. Para evitar uma falha no lançamento, adicione as Reservas de Capacidade `targeted` a um grupo de recursos e, em seguida, direcione o grupo de recursos. O grupo de recursos não precisa ter Reservas de Capacidade suficientes; se ficar sem Reservas de Capacidade antes que a capacidade sob demanda de destino seja atendida, a frota poderá iniciar a capacidade de destino restante na capacidade sob demanda regular.

Para usar Reservas de Capacidade com a frota EC2

1. Configurar a frota como tipo `instant`. Não é possível usar Reservas de Capacidade para frotas de outros tipos.
2. Configure a estratégia de uso para Reservas de Capacidade como `use-capacity-reservations-first`.
3. No modelo de lançamento, para Reserva de capacidade, escolha Aberto ou Destino por grupo. Se escolher Destino por grupo, especifique o ID do grupo de recursos de Reservas de Capacidade.

Quando a frota tenta atender à capacidade sob demanda, se descobrir que vários grupos de instâncias têm Reservas de Capacidade correspondentes não utilizadas, ela determina os grupos nos quais iniciar as Instâncias sob demanda com base na estratégia de alocação sob demanda (`lowest-price` ou `prioritized`).

Recursos relacionados

- Para obter exemplos da CLI de como configurar uma frota para usar reservas de capacidade para atender à capacidade sob demanda, consulte Exemplo de configurações da CLI para frotas do EC2, especificamente os exemplos de 5 a 7.
- Para ver um tutorial que mostra as etapas para criar reservas de capacidade, usá-las na frota e visualizar quantas reservas de capacidade ainda restam, consulte Tutorial: configurar o EC2 Fleet para executar instâncias sob demanda usando reservas de capacidade direcionadas.
- Para obter informações sobre configuração das Reservas de Capacidade, consulte Reservar capacidade computacional com reservas de capacidade sob demanda do EC2 e as Perguntas frequentes sobre Reservas de Capacidade.

Trabalhar com uma frota do EC2

Para começar a usar uma frota do EC2, crie uma solicitação que inclua a capacidade total de destino, a capacidade sob demanda, a capacidade spot e um modelo de inicialização especificando a configuração das instâncias da frota. Como alternativa, você pode especificar parâmetros adicionais ou permitir que a frota use valores padrão. Você também pode marcar a solicitação da frota e suas instâncias e seus volumes quando criar a frota.

A frota executa instâncias sob demanda quando há capacidade disponível, e executa Instâncias spot quando o preço máximo excede o preço spot e há capacidade disponível.

Depois que a frota for inicializada, será possível descrever a solicitação, as instâncias e os eventos da frota. Você também poderá atribuir tags adicionais conforme necessário.

Caso precise alterar algum parâmetro da frota, como a capacidade total de destino, você pode modificar a frota, desde que ela tenha sido configurada para manter a capacidade. Você não pode modificar a capacidade de uma solicitação única depois que ela for enviada.

Uma solicitação de frota permanece ativa até que expire ou você a exclua. Ao excluir a solicitação da frota, você pode encerrar as instâncias ou deixá-las em execução. Caso escolha deixá-las em

execução, as instâncias sob demanda serão executadas até que você as encerre, e as Instâncias spot serão executadas até que sejam interrompidas ou você as encerre.

Tópicos

- Estados das solicitações da Frota do EC2
- Pré-requisitos da Frota do EC2
- Criar uma Frota do EC2.
- Marcar uma solicitação nova ou atual de frota do EC2 e as instâncias e os volumes que ela inicializa
- Descrever uma frota do EC2, suas instâncias e seus eventos
- Modificar uma Frota do EC2
- Excluir uma solicitação de frota do EC2 e as instâncias da frota

Estados das solicitações da Frota do EC2

Uma solicitação de frota do EC2 pode ter um de vários estados, cada estado indicando um estágio diferente do ciclo de vida da solicitação e do gerenciamento das instâncias.

Uma solicitação de Frota do EC2 pode estar em um dos seguintes estados:

`submitted`

A solicitação de Frota do EC2 está sendo avaliada, e o Amazon EC2 está se preparando para executar o número de destino de instâncias. Se uma solicitação for exceder os limites da frota, ela será excluída imediatamente.

`active`

A solicitação de Frota do EC2 foi validada e o Amazon EC2 está tentando manter o número de destino das instâncias em execução. A solicitação permanece nesse estado até que seja alterada ou excluída.

`modifying`

A solicitação de Frota do EC2 está sendo modificada. A solicitação permanece nesse estado até que a modificação seja totalmente processada ou que a solicitação seja excluída. Apenas um tipo `maintain` de frota pode ser modificado. Esse estado não se aplica a outros tipos de solicitação.

`deleted_running`

A solicitação do EC2 Fleet foi excluída e não executará instâncias spot adicionais. Suas instâncias existentes continuam sendo executadas até que sejam interrompidas ou encerradas manualmente. A solicitação permanece nesse estado até que todas as instâncias sejam interrompidas ou encerradas. Apenas uma Frota do EC2 do tipo `maintain` ou `request` pode ter instâncias em execução após a solicitação de Frota do EC2 ser excluída. Não há suporte a uma frota `instant` excluída com instâncias em execução. Este estado não se aplica às frotas `instant`.

`deleted_terminating`

A solicitação de Frota do EC2 foi excluída, e as instâncias estão sendo encerradas. A solicitação permanece nesse estado até que todas as instâncias sejam encerradas.

`deleted`

A solicitação de Frota do EC2 foi excluída, e não há outras instâncias em execução. A solicitação foi excluída dois dias depois que as instâncias foram encerradas.

Pré-requisitos da Frota do EC2

Para criar uma Frota do EC2, observe os seguintes pré-requisitos:

- Modelo de execução
- Função vinculada ao serviço para Frota do EC2
- Conceder acesso às chaves gerenciadas pelo cliente para uso com AMIs criptografadas e snapshots do EBS
- Permissões para usuários da Frota do EC2

Modelo de execução

Um modelo de inicialização especifica as informações de configuração sobre as instâncias a serem inicializadas, como o tipo de instância e a zona de disponibilidade. Para obter mais informações sobre modelos de inicialização, consulte Armazenar os parâmetros de execução de instâncias nos modelos de execução do Amazon EC2.

Função vinculada ao serviço para Frota do EC2

O `AWSServiceRoleForEC2Fleet` concede à frota do EC2 permissão para solicitar, executar, encerrar e marcar instâncias em seu nome. O Amazon EC2 usa essa função vinculada ao serviço para concluir as seguintes ações:

- `ec2:RunInstances` – Executar instâncias
- `ec2:RequestSpotInstances` – Solicitação Instâncias spot.
- `ec2:TerminateInstances` – Encerrar instâncias
- `ec2:DescribeImages`: descrever imagens de máquina da Amazon (AMIs) para as instâncias.
- `ec2:DescribeInstanceStatus`: descrever o status das instâncias.
- `ec2:DescribeSubnets`: descrever as sub-redes das instâncias.
- `ec2:CreateTags` – Adicionar tags a Frota do EC2, instâncias e volumes.

Verifique se essa função está disponível antes de usar a AWS CLI ou uma API para criar uma frota do EC2.

> **Note**
>
> Uma Frota do EC2 `instant` não requer essa função.

Para criar a função, use o console do IAM da seguinte forma.

Para criar a função AWSServiceRoleForEC2Fleet para Frota do EC2

1. Abra o console do IAM em https://console.aws.amazon.com/iam/.
2. No painel de navegação, escolha Perfis.
3. Escolha Criar Perfil.
4. Na página Selecionar entidade confiável, faça o seguinte:
   a. Em Tipo de entidade confiável, escolha Serviços da AWS.
   b. Em Caso de uso, para Serviço ou caso de uso, escolha EC2 - Frota.

> **Tip**
>
> Certifique-se de escolher EC2 - Frota. Se você escolher EC2, o caso de uso EC2 - Frota não aparecerá na lista de Casos de uso. O caso de uso EC2 - Frota criará automaticamente uma política com as permissões necessárias do IAM e sugerirá AWSServiceRoleForEC2Fleet como nome do perfil.

c. Escolha Próximo.

5. Na página Adicionar permissões, escolha Próximo.
6. Na página Nomear, revisar e criar, escolha 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, será possível criar a função novamente se criar outra frota.

Para obter mais informações, consulte Perfis vinculados ao serviço no Guia do usuário do IAM.

Conceder acesso às chaves gerenciadas pelo cliente para uso com AMIs criptografadas e snapshots do EBS

Se você especificar uma AMI criptografada ou um snapshot criptografado do Amazon EBS na frota do EC2 e usar uma chave do AWS KMS para criptografia, será necessário conceder ao perfil AWSServiceRoleForEC2Fleet permissão para usar a chave gerenciada pelo cliente para que o Amazon EC2 possa iniciar instâncias em seu nome. Para isso, adicione uma concessão à chave gerenciada pelo cliente, conforme exibido no procedimento a seguir.

Durante a definição de permissões, as concessões são uma alternativa às políticas de chave. Para obter mais informações, consulte Usar concessões e Usar políticas de chave no AWS KMS, no Guia do desenvolvedor do AWS Key Management Service.

Para conceder as permissões para a função AWSServiceRoleForEC2Fleet para usar a chave gerenciada pelo cliente

- Use o comando create-grant para adicionar uma concessão à chave gerenciada pelo cliente e especificar a entidade principal (a função vinculada ao serviço AWSServiceRoleForEC2Fleet) que recebe permissão para executar as operações permitidas pela concessão. A chave gerenciada pelo cliente é especificada pelo parâmetro `key-id` e o ARN da chave gerenciada

pelo cliente. O principal é especificado pelo parâmetro `grantee-principal` e o ARN da função vinculada ao serviço AWSServiceRoleForEC2Fleet.

```
aws kms create-grant \
    --region us-east-1 \
    --key-id arn:aws:kms:us-
east-1:444455556666:key/1234abcd-12ab-34cd-56ef-1234567890ab \
    --grantee-principal arn:aws:iam::111122223333:role/AWSServiceRoleForEC2Fleet \
    --operations "Decrypt" "Encrypt" "GenerateDataKey"
 "GenerateDataKeyWithoutPlaintext" "CreateGrant" "DescribeKey" "ReEncryptFrom"
 "ReEncryptTo"
```

Permissões para usuários da Frota do EC2

Se os usuários pretenderem criar ou gerenciar uma Frota do EC2, certifique-se de conceder a eles as permissões necessárias.

Para criar uma frota do EC2

1. Abra o console do IAM em https://console.aws.amazon.com/iam/.
2. No painel de navegação, escolha Policies.
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).

   JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
```

```
            "Action": [
              "iam:ListRoles",
              "iam:PassRole",
              "iam:ListInstanceProfiles"
            ],
            "Resource":"arn:aws:iam::123456789012:role/DevTeam*"
        }
    ]
}
```

O `ec2:*` concede a um usuário 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.

O usuário deve ter permissão para chamar a ação `iam:ListRoles` para enumerar os perfis do IAM existentes, a ação `iam:PassRole` para especificar o perfil da frota do EC2 e a ação `iam:ListInstanceProfiles` para enumerar os perfis de instância existentes.

(Opcional) Para permitir que um usuário crie perfis ou perfis de instância usando o console do IAM, também é necessário adicionar as ações a seguir 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. Para conceder acesso, adicione as permissões aos seus usuários, grupos ou perfis:

   - Usuários e grupos no Centro de Identidade do AWS IAM:

     Crie um conjunto de permissões. Siga as instruções em Criação de um conjunto de permissões no Guia do usuário do Centro de Identidade do AWS IAM.

   - Usuários gerenciados no IAM com provedor de identidades:

Crie um perfil para a federação de identidades. Siga as instruções em Criando um perfil para um provedor de identidades de terceiros (federação) no Guia do Usuário do IAM.

- Usuários do IAM:
  - Crie um perfil que seu usuário possa assumir. Siga as instruções em Criação de um perfil para um usuário do IAM no Guia do usuário do IAM.
  - (Não recomendado) Vincule uma política diretamente a um usuário ou adicione um usuário a um grupo de usuários. Siga as instruções em Adição de permissões a um usuário (console) no Guia do usuário do IAM.

Criar uma Frota do EC2.

Para criar uma frota do EC2, defina a configuração da frota em um arquivo JSON e referencie esse arquivo com o comando create-fleet. No arquivo JSON, você deve especificar a capacidade total de destino da frota, as capacidades de destino separadas para instâncias spot e instâncias sob demanda e um modelo de inicialização que defina a configuração das instâncias na frota, como uma AMI, um tipo de instância, uma sub-rede ou uma zona de disponibilidade e um ou mais grupos de segurança. Como alternativa, você pode especificar configurações adicionais, como parâmetros para substituir a configuração do modelo de inicialização, estratégias de alocação para selecionar instâncias spot e instâncias sob demanda dos grupos de capacidade do EC2 e o valor máximo que você deseja pagar pela frota. Para obter mais informações, consulte Opções de configuração para frota do EC2 ou frota spot.

A frota do EC2 inicializa instâncias sob demanda quando há capacidade disponível e inicializa instâncias spot quando o preço máximo excede o preço spot e há capacidade disponível.

Se a frota incluir a instâncias spot e for do tipo `maintain`, o Amazon EC2 tentará manter a capacidade de destino da frota quando as instâncias spot forem interrompidas.

Limitações da Frota do EC2

As limitações a seguir se aplicam à Frota do EC2:

- A criação de uma frota do EC2 só está disponível por meio da API do Amazon EC2, da AWS CLI, dos AWS SDKs e do CloudFormation.
- Uma solicitação de EC2 Fleet não pode abranger regiões da AWS. Você precisa criar uma Frota do EC2 separada para cada região.

- Uma solicitação de Frota do EC2 não pode abranger sub-redes diferentes na mesma zona de disponibilidade.

Criar uma Frota do EC2.

Para inicializar uma frota de instâncias usando a frota do EC2, você só precisa especificar os seguintes parâmetros na solicitação de frota para que a frota use os valores padrão para os outros parâmetros:

- `LaunchTemplateId` ou `LaunchTemplateName`: especifica o modelo de inicialização a ser usado (que contém os parâmetros das instâncias a serem inicializadas, como o tipo de instância e a zona de disponibilidade)
- `TotalTargetCapacity`: especifica a capacidade-alvo total para a frota
- `DefaultTargetCapacityType`: especifica se a opção de compra padrão é sob demanda ou spot

Para substituir os parâmetros especificados no modelo de inicialização, você pode especificar uma ou mais substituições. 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. Como alternativa à especificação de um tipo de instância, você pode especificar os atributos que uma instância deve ter e o Amazon EC2 identificará todos os tipos de instância com esses atributos. Para obter mais informações, consulte Especificar atributos para seleção de tipo de instância para frota do EC2 ou frota spot.

Em frotas do EC2 do tipo `instant`, você pode especificar um parâmetro do Systems Manager em vez do ID da AMI. É possível especificar o parâmetro do Systems Manager na substituição ou no modelo de inicialização. Para obter mais informações, consulte Use um parâmetro de Systems Manager em vez de um ID de AMI.

É possível especificar os parâmetros da frota em um arquivo JSON. Para obter informações sobre todos os parâmetros possíveis que você pode especificar, consulte Visualizar todas as opções de configuração de frotas do EC2.

Para ver exemplos de configuração da frota, consulte Exemplo de configurações da CLI para frotas do EC2.

No momento, não há suporte de console para a criação de uma frota do EC2.

Criar uma frota do EC2

Use o comando create-fleet para criar a frota e especifique o arquivo JSON que contém os parâmetros de configuração da frota.

```
aws ec2 create-fleet --cli-input-json file://file_name.json
```

A seguir está um exemplo de saída de uma frota do tipo `request` ou `maintain`.

```
{
    "FleetId": "fleet-12a34b55-67cd-8ef9-ba9b-9208dEXAMPLE"
}
```

A seguir está um exemplo de saída de uma frota do tipo `instant` que executou a capacidade de destino.

```
{
  "FleetId": "fleet-12a34b55-67cd-8ef9-ba9b-9208dEXAMPLE",
  "Errors": [],
  "Instances": [
    {
      "LaunchTemplateAndOverrides": {
        "LaunchTemplateSpecification": {
          "LaunchTemplateId": "lt-01234a567b8910abcEXAMPLE",
          "Version": "1"
        },
        "Overrides": {
          "InstanceType": "c5.large",
          "AvailabilityZone": "us-east-1a"
        }
      },
      "Lifecycle": "on-demand",
      "InstanceIds": [
        "i-1234567890abcdef0",
        "i-9876543210abcdef9"
      ],
      "InstanceType": "c5.large",
      "Platform": null
    },
    {
      "LaunchTemplateAndOverrides": {
        "LaunchTemplateSpecification": {
```

```
          "LaunchTemplateId": "lt-01234a567b8910abcEXAMPLE",
          "Version": "1"
        },
        "Overrides": {
          "InstanceType": "c4.large",
          "AvailabilityZone": "us-east-1a"
        }
      },
      "Lifecycle": "on-demand",
      "InstanceIds": [
        "i-5678901234abcdef0",
        "i-5432109876abcdef9"
      ]
  ]
}
```

A seguir está um exemplo de saída de uma frota do tipo `instant` que executou parte da capacidade de destino com erros em instâncias que não foram executadas.

```
{
  "FleetId": "fleet-12a34b55-67cd-8ef9-ba9b-9208dEXAMPLE",
  "Errors": [
    {
      "LaunchTemplateAndOverrides": {
        "LaunchTemplateSpecification": {
          "LaunchTemplateId": "lt-01234a567b8910abcEXAMPLE",
          "Version": "1"
        },
        "Overrides": {
          "InstanceType": "c4.xlarge",
          "AvailabilityZone": "us-east-1a",
        }
      },
      "Lifecycle": "on-demand",
      "ErrorCode": "InsufficientInstanceCapacity",
      "ErrorMessage": ""
    },
  ],
  "Instances": [
    {
      "LaunchTemplateAndOverrides": {
        "LaunchTemplateSpecification": {
          "LaunchTemplateId": "lt-01234a567b8910abcEXAMPLE",
```

```
          "Version": "1"
        },
        "Overrides": {
          "InstanceType": "c5.large",
          "AvailabilityZone": "us-east-1a"
        }
      },
      "Lifecycle": "on-demand",
      "InstanceIds": [
        "i-1234567890abcdef0",
        "i-9876543210abcdef9"
      ]
  ]
}
```

A seguir está um exemplo de saída de uma frota do tipo `instant` que não executou nenhuma instância.

```
{
  "FleetId": "fleet-12a34b55-67cd-8ef9-ba9b-9208dEXAMPLE",
  "Errors": [
    {
      "LaunchTemplateAndOverrides": {
        "LaunchTemplateSpecification": {
          "LaunchTemplateId": "lt-01234a567b8910abcEXAMPLE",
          "Version": "1"
        },
        "Overrides": {
          "InstanceType": "c4.xlarge",
          "AvailabilityZone": "us-east-1a",
        }
      },
      "Lifecycle": "on-demand",
      "ErrorCode": "InsufficientCapacity",
      "ErrorMessage": ""
    },
    {
      "LaunchTemplateAndOverrides": {
        "LaunchTemplateSpecification": {
          "LaunchTemplateId": "lt-01234a567b8910abcEXAMPLE",
          "Version": "1"
        },
        "Overrides": {
```

```
          "InstanceType": "c5.large",
          "AvailabilityZone": "us-east-1a",
        }
      },
      "Lifecycle": "on-demand",
      "ErrorCode": "InsufficientCapacity",
      "ErrorMessage": ""
    },
  ],
  "Instances": []
}
```

Criar uma frota do EC2 que substitua instâncias spot não íntegras

A Frota do EC2 verifica o status de integridade das instâncias na frota a cada dois minutos. O status de integridade de uma instância é `healthy` ou `unhealthy`.

A Frota do EC2 determina o status de integridade de uma instância usando as verificações de status fornecidas pelo Amazon EC2. Uma instância é determinada como `unhealthy` quando o status da verificação de status da instância ou da verificação de status do sistema for `impaired` para três verificações de status de integridade consecutivas. Para obter mais informações, consulte Verificações do status das instâncias do Amazon EC2.

É possível configurar a sua frota para substituir Instâncias spot não íntegras. Depois de configurar `ReplaceUnhealthyInstances` para `true`, uma instância spot é substituída ao ser reportada como `unhealthy`. A frota poderá ficar abaixo de sua capacidade de destino por alguns minutos enquanto uma instância spot não íntegra estiver sendo substituída.

Requisitos

- A substituição da verificação de integridade é compatível apenas para Frotas do EC2 que mantenham uma capacidade de destino (frotas do tipo `maintain`) e não para as frotas únicas do tipo `request` ou `instant`.
- A substituição da verificação de integridade é compatível apenas para Instâncias spot. Este recurso não é compatível para Instâncias on-demand.
- É possível configurar a Frota do EC2 para substituir instâncias não íntegras somente durante sua criação.
- Os usuários só poderão usar a substituição de verificação de integridade se tiverem permissão para chamar a ação `ec2:DescribeInstanceStatus`.

Para configurar um Frota do EC2 para substituir uma Instâncias spot não íntegra

1. Use as informações para criar uma frota do EC2 em Criar uma Frota do EC2..
2. Para configurar a frota para substituir instâncias spot não íntegras no arquivo JSON, em `ReplaceUnhealthyInstances`, especifique `true`.

Visualizar todas as opções de configuração de frotas do EC2

Para visualizar a lista completa de parâmetros de configuração de frota do EC2, você pode gerar um arquivo JSON. Para obter uma descrição de cada parâmetro, consulte create-fleet.

Gerar um arquivo JSON com todos os parâmetros de frotas do EC2 possíveis

Use o comando create-fleet (AWS CLI) e o parâmetro `--generate-cli-skeleton` para gerar um arquivo JSON da Frota do EC2 e direcione a saída a um arquivo para salvá-la.

```
aws ec2 create-fleet \
    --generate-cli-skeleton input > ec2createfleet.json
```

O seguinte é um exemplo de saída.

```
{
    "DryRun": true,
    "ClientToken": "",
    "SpotOptions": {
        "AllocationStrategy": "price-capacity-optimized",
        "MaintenanceStrategies": {
            "CapacityRebalance": {
                "ReplacementStrategy": "launch"
            }
        },
        "InstanceInterruptionBehavior": "hibernate",
        "InstancePoolsToUseCount": 0,
        "SingleInstanceType": true,
        "SingleAvailabilityZone": true,
        "MinTargetCapacity": 0,
        "MaxTotalPrice": ""
    },
    "OnDemandOptions": {
        "AllocationStrategy": "prioritized",
        "CapacityReservationOptions": {
            "UsageStrategy": "use-capacity-reservations-first"
```

```
        },
        "SingleInstanceType": true,
        "SingleAvailabilityZone": true,
        "MinTargetCapacity": 0,
        "MaxTotalPrice": ""
    },
    "ExcessCapacityTerminationPolicy": "termination",
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateId": "",
                "LaunchTemplateName": "",
                "Version": ""
            },
            "Overrides": [
                {
                    "InstanceType": "r5.metal",
                    "MaxPrice": "",
                    "SubnetId": "",
                    "AvailabilityZone": "",
                    "WeightedCapacity": 0.0,
                    "Priority": 0.0,
                    "Placement": {
                        "AvailabilityZone": "",
                        "Affinity": "",
                        "GroupName": "",
                        "PartitionNumber": 0,
                        "HostId": "",
                        "Tenancy": "dedicated",
                        "SpreadDomain": "",
                        "HostResourceGroupArn": ""
                    },
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 0
                        },
                        "MemoryMiB": {
                            "Min": 0,
                            "Max": 0
                        },
                        "CpuManufacturers": [
                            "amd"
                        ],
```

```
                    "MemoryGiBPerVCpu": {
                        "Min": 0.0,
                        "Max": 0.0
                    },
                    "ExcludedInstanceTypes": [
                        ""
                    ],
                    "InstanceGenerations": [
                        "previous"
                    ],
                    "SpotMaxPricePercentageOverLowestPrice": 0,
                    "OnDemandMaxPricePercentageOverLowestPrice": 0,
                    "BareMetal": "included",
                    "BurstablePerformance": "required",
                    "RequireHibernateSupport": true,
                    "NetworkInterfaceCount": {
                        "Min": 0,
                        "Max": 0
                    },
                    "LocalStorage": "excluded",
                    "LocalStorageTypes": [
                        "ssd"
                    ],
                    "TotalLocalStorageGB": {
                        "Min": 0.0,
                        "Max": 0.0
                    },
                    "BaselineEbsBandwidthMbps": {
                        "Min": 0,
                        "Max": 0
                    },
                    "AcceleratorTypes": [
                        "inference"
                    ],
                    "AcceleratorCount": {
                        "Min": 0,
                        "Max": 0
                    },
                    "AcceleratorManufacturers": [
                        "amd"
                    ],
                    "AcceleratorNames": [
                        "a100"
                    ],
```

```
                        "AcceleratorTotalMemoryMiB": {
                            "Min": 0,
                            "Max": 0
                        }
                    }
                }
            ]
        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 0,
        "OnDemandTargetCapacity": 0,
        "SpotTargetCapacity": 0,
        "DefaultTargetCapacityType": "on-demand",
        "TargetCapacityUnitType": "memory-mib"
    },
    "TerminateInstancesWithExpiration": true,
    "Type": "instant",
    "ValidFrom": "1970-01-01T00:00:00",
    "ValidUntil": "1970-01-01T00:00:00",
    "ReplaceUnhealthyInstances": true,
    "TagSpecifications": [
        {
            "ResourceType": "fleet",
            "Tags": [
                {
                    "Key": "",
                    "Value": ""
                }
            ]
        }
    ],
    "Context": ""
}
```

Marcar uma solicitação nova ou atual de frota do EC2 e as instâncias e os volumes que ela inicializa

Para ajudar na categorização e no gerenciamento das solicitações de frota do EC2 e das instâncias e dos volumes que ela inicializa, você pode marcá-las com metadados personalizados. É possível atribuir uma tag a uma solicitação de Frota do EC2 ao criá-la ou posteriormente. Da mesma forma,

você pode atribuir uma tag às instâncias e aos volumes quando eles são inicializados pela frota, ou posteriormente.

Quando você marca uma solicitação de frota, as instâncias e os volumes que são executados pela frota não são marcados automaticamente. É necessário marcar explicitamente as instâncias e os volumes executados pela frota. É possível optar por atribuir tags somente à solicitação de frota, somente às instâncias inicializadas pela frota, somente aos volumes anexados às instâncias inicializadas pela frota ou a todos eles.

> **Note**
>
> Para tipos de frota `instant`, é possível marcar volumes anexados a Instâncias on-demand e Instâncias spot. Para os tipos de frota `request` ou `maintain`, só é possível marcar volumes anexados a Instâncias on-demand.

Para obter mais informações sobre como as tags funcionam, consulte Marcar com tag os recursos do Amazon EC2.

Pré-requisito

Conceda ao usuário permissão para marcar recursos. Para obter mais informações, consulte Exemplo: marcar recursos.

Para conceder a um usuário permissão para marcar recursos

Crie uma política do IAM que inclua o seguinte:

- A ação `ec2:CreateTags`. Isso concede ao usuário permissão para criar tags.
- A ação `ec2:CreateFleet`. Isso concede ao usuário permissão para criar uma solicitação de Frota do EC2.
- Para `Resource`, recomendamos que você especifique `"*"`. Permite que os usuários marquem todos os tipos de recursos.

Para conceder acesso, adicione as permissões aos seus usuários, grupos ou perfis:

- Usuários e grupos no Centro de Identidade do AWS IAM:

  Crie um conjunto de permissões. Siga as instruções em Criação de um conjunto de permissões no Guia do usuário do Centro de Identidade do AWS IAM.

- Usuários gerenciados no IAM com provedor de identidades:

  Crie um perfil para a federação de identidades. Siga as instruções em Criando um perfil para um provedor de identidades de terceiros (federação) no Guia do Usuário do IAM.

- Usuários do IAM:
  - Crie um perfil que seu usuário possa assumir. Siga as instruções em Criação de um perfil para um usuário do IAM no Guia do usuário do IAM.
  - (Não recomendado) Vincule uma política diretamente a um usuário ou adicione um usuário a um grupo de usuários. Siga as instruções em Adição de permissões a um usuário (console) no Guia do usuário do IAM.

Como marcar uma nova solicitação de Frota do EC2

Para marcar uma solicitação de Frota do EC2 ao criá-la, especifique o par de valor-chave no arquivo JSON usado para criar a frota. O valor de `ResourceType` deve ser `fleet`. Se você especificar outro valor, ocorrerá falha na frota.

Como marcar instâncias e volumes executado por uma Frota do EC2

Para marcar instâncias e volumes ao serem executados pela frota, especifique as tags no modelo de execução mencionado na solicitação de Frota do EC2.

> **Note**
>
> Não é possível marcar volumes anexados a Instâncias spot que são executados por um tipo de frota `request` ou `maintain`.

Marcar uma solicitação da frota do EC2, uma instância e um volume existentes

Use o comando create-tags para marcar os recursos existentes.

```
aws ec2 create-tags \
    --resources fleet-12a34b55-67cd-8ef9-
ba9b-9208dEXAMPLE i-1234567890abcdef0 vol-1234567890EXAMPLE \
    --tags Key=purpose,Value=test
```

Descrever uma frota do EC2, suas instâncias e seus eventos

É possível descrever a frota do EC2, relacionar as instâncias associadas à frota do EC2 e visualizar o histórico da frota do EC2.

Tarefas

- Descrever a frota do EC2
- Descrever todas as instâncias em sua frota do EC2
- Descrever o histórico de eventos para o EC2 Fleet

Descrever a frota do EC2

AWS CLI

Para descrever sua frota do EC2

Use o comando describe-fleets.

```
aws ec2 describe-fleets \
    --fleet-ids fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE
```

O seguinte é um exemplo de saída.

```
{
    "Fleets": [
        {
            "ActivityStatus": "fulfilled",
            "CreateTime": "2022-02-09T03:35:52+00:00",
            "FleetId": "fleet-364457cd-3a7a-4ed9-83d0-7b63e51bb1b7",
            "FleetState": "active",
            "ExcessCapacityTerminationPolicy": "termination",
            "FulfilledCapacity": 2.0,
            "FulfilledOnDemandCapacity": 0.0,
            "LaunchTemplateConfigs": [
                {
                    "LaunchTemplateSpecification": {
                        "LaunchTemplateName": "my-launch-template",
                        "Version": "$Latest"
                    }
                }
```

```
            ],
            "TargetCapacitySpecification": {
                "TotalTargetCapacity": 2,
                "OnDemandTargetCapacity": 0,
                "SpotTargetCapacity": 2,
                "DefaultTargetCapacityType": "spot"
            },
            "TerminateInstancesWithExpiration": false,
            "Type": "maintain",
            "ReplaceUnhealthyInstances": false,
            "SpotOptions": {
                "AllocationStrategy": "capacity-optimized",
                "InstanceInterruptionBehavior": "terminate"
            },
            "OnDemandOptions": {
                "AllocationStrategy": "lowestPrice"
            }
        }
    ]
}
```

PowerShell

Para descrever sua frota do EC2

Use o cmdlet Get-EC2FleetList.

```
Get-EC2FleetList `
    -FleetId fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE
```

Descrever todas as instâncias em sua frota do EC2

A lista retornada das instâncias em execução é atualizada periodicamente e pode estar desatualizada.

AWS CLI

Para descrever as instâncias da frota do EC2 especificada

Use o comando describe-fleet-instances.

```
aws ec2 describe-fleet-instances \
```

```
    --fleet-id fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE
```

O seguinte é um exemplo de saída.

```
{
    "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-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE"
}
```

PowerShell

Para descrever as instâncias da frota do EC2 especificada

Use o cmdlet Get-EC2FleetInstanceList.

```
Get-EC2FleetInstanceList `
    -FleetId fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE
```

Descrever o histórico de eventos para o EC2 Fleet

Para obter mais informações sobre os eventos no histórico de eventos, consulte Tipos de evento de Frota do EC2.

AWS CLI

Para descrever os eventos para a frota do EC2 especificada

Use o comando describe-fleet-history.

```
aws ec2 describe-fleet-history \
    --fleet-id fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
    --start-time 2020-06-01T00:00:00Z
```

O seguinte é um exemplo de saída.

```
{
    "HistoryRecords": [
        {
            "EventInformation": {
                "EventSubType": "submitted"
            },
            "EventType": "fleetRequestChange",
            "Timestamp": "2020-09-01T18:26:05.000Z"
        },
        {
            "EventInformation": {
                "EventSubType": "active"
            },
            "EventType": "fleetRequestChange",
            "Timestamp": "2020-09-01T18:26:15.000Z"
        },
        {
            "EventInformation": {
                "EventDescription": "t2.small, ami-07c8bc5c1ce9598c3, ...",
                "EventSubType": "progress"
            },
            "EventType": "fleetRequestChange",
            "Timestamp": "2020-09-01T18:26:17.000Z"
        },
        {
            "EventInformation": {
                "EventDescription": "{\"instanceType\":\"t2.small\", ...}",
                "EventSubType": "launched",
                "InstanceId": "i-083a1c446e66085d2"
            },
            "EventType": "instanceChange",
            "Timestamp": "2020-09-01T18:26:17.000Z"
        },
        {
            "EventInformation": {
                "EventDescription": "{\"instanceType\":\"t2.small\", ...}",
                "EventSubType": "launched",
```

```
                "InstanceId": "i-090db02406cc3c2d6"
            },
            "EventType": "instanceChange",
            "Timestamp": "2020-09-01T18:26:17.000Z"
        }
    ],
    "FleetId": "fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE",
    "LastEvaluatedTime": "1970-01-01T00:00:00.000Z",
    "StartTime": "2020-06-01T00:00:00.000Z"
}
```

PowerShell

Para descrever os eventos para a frota do EC2 especificada

Use o cmdlet Get-EC2FleetHistory.

```
Get-EC2FleetHistory `
    -FleetId fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE `
    -UtcStartTime 2020-06-01T00:00:00Z
```

Modificar uma Frota do EC2

É possível modificar a capacidade total de destino, a capacidade spot e a capacidade sob demanda de uma frota do EC2. Você também pode modificar se as instâncias em execução devem ser encerradas caso a nova capacidade total de destino fique abaixo do tamanho atual da frota.

Considerações

Considere o seguinte quando modificar uma frota do EC2:

- Tipo de frota: só é possível modificar uma frota do EC2 do tipo `maintain`. Você não pode modificar uma frota do EC2 do tipo `request` ou do tipo `instant`.
- Parâmetros da frota: você pode modificar os seguintes parâmetros de uma frota do EC2:
  - `target-capacity-specification`: aumentar ou diminuir a capacidade de destino de:
    - `TotalTargetCapacity`
    - `OnDemandTargetCapacity`
    - `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`
    - `termination`
- Comportamento da frota quando a capacidade total de destino é aumentada: quando você aumenta a capacidade total de destino, a frota do EC2 inicializa as instâncias adicionais de acordo com a opção de compra da instância especificada para `DefaultTargetCapacityType`, ou seja, instâncias sob demanda ou instâncias spot, e de acordo com a estratégia de alocação especificada.
- Comportamento da frota quando a capacidade de destino spot é diminuída: quando você diminui a capacidade de destino spot, a frota do EC2 exclui todas as solicitações abertas que excedem a nova capacidade de destino. É possível solicitar que a frota encerre as instâncias spot até que o tamanho da frota atinja a nova capacidade de destino. Quando uma EC2 Fleet encerra uma instância spot porque a capacidade pretendida foi diminuída, a instância recebe um aviso de interrupção de instância spot.

  As instâncias são selecionadas para encerramento com base na estratégia de alocação:
  - `capacity-optimized`: encerra instâncias de grupos com a menor capacidade disponível.
  - `price-capacity-optimized`: usa uma combinação de preço e capacidade disponível: encerra instâncias de grupos com a menor capacidade disponível e que têm o preço mais alto entre esses grupos.
  - `diversified`: encerra instâncias em todos os grupos.
  - `lowest-price`: encerra instâncias dos grupos com preços mais altos.

  Como alternativa, você pode solicitar que a frota do EC2 mantenha seu tamanho atual, mas não substitua nenhuma instância spot interrompida ou encerrada manualmente por você.
- Estado da frota: você pode modificar uma frota do EC2 que esteja no estado `submitted` ou no estado `active`. Quando você modifica uma frota, ela entra no estado `modifying`.

Comandos para modificar uma frota do EC2

AWS CLI

Modificar a capacidade total de destino de uma frota do EC2

Use o comando modify-fleet.

```
aws ec2 modify-fleet \
    --fleet-id fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
    --target-capacity-specification TotalTargetCapacity=20
```

Se você estiver diminuindo a capacidade de destino, mas quiser manter a frota com o tamanho atual, poderá modificar o exemplo anterior conforme mostrado a seguir.

```
aws ec2 modify-fleet \
    --fleet-id fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
    --target-capacity-specification TotalTargetCapacity=10 \
    --excess-capacity-termination-policy no-termination
```

PowerShell

Modificar a capacidade total de destino de uma frota do EC2

Use o cmdlet Edit-EC2Fleet.

```
Edit-EC2Fleet `
    -FleetId "fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE" `
    -TargetCapacitySpecification_TotalTargetCapacity 20
```

Se você estiver diminuindo a capacidade de destino, mas quiser manter a frota com o tamanho atual, poderá modificar o exemplo anterior conforme mostrado a seguir.

```
Edit-EC2Fleet `
    -FleetId "fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE" `
    -TargetCapacitySpecification_TotalTargetCapacity 20 `
    -ExcessCapacityTerminationPolicy "NoTermination"
```

Excluir uma solicitação de frota do EC2 e as instâncias da frota

Se você não precisar mais de uma frota do EC2, poderá excluí-la. Depois que você exclui uma frota, todas as solicitações spot associadas à frota são canceladas para que nenhuma nova instância spot seja iniciada.

Ao excluir uma frota do EC2, você deve também especificar se deseja encerrar todas as instâncias. Isso inclui tanto instâncias sob demanda quanto instâncias spot. Para frotas `instant`, a frota do

EC2 deve encerrar as instâncias quando a frota for excluída. Não há suporte a uma frota `instant` excluída com instâncias em execução.

> **Warning**
>
> O encerramento de uma instância é permanente e irreversível.
> Depois de encerrar uma instância, não será mais possível se conectar a ela e ela não poderá ser recuperada. Todos os volumes anexados do Amazon EBS configurados para serem excluídos no encerramento também serão excluídos permanentemente e não poderão ser recuperados. Todos os dados armazenados em volumes de armazenamento de instância serão perdidos permanentemente. Para obter mais informações, consulte Como funciona o encerramento de uma instância.
> Antes de encerrar uma instância, certifique-se de ter feito backup de todos os dados que você precise reter após o encerramento no armazenamento persistente.

Se você especificar que as instâncias deverão ser encerradas quando a solicitação de frota for excluída, a solicitação da frota 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.

Restrições

- É possível excluir até 25 frotas do tipo `instant` em uma única operação.
- É possível excluir até 100 frotas do tipo `maintain` ou `request` em uma única operação.
- É possível excluir até 125 frotas em uma única operação, desde que não exceda a cota para cada tipo de frota, conforme especificado acima.
- Nenhuma frota será excluída se você exceder o número especificado de frotas a serem excluídas.
- Não há suporte a uma frota `instant` excluída com instâncias em execução. Ao excluir uma frota `instant`, o Amazon EC2 encerra automaticamente todas as suas instâncias. Para frotas `instant` com mais de mil instâncias, a solicitação de exclusão pode não ser bem-sucedida. Caso sua frota contenha mais de mil instâncias, encerre manualmente a maioria delas, deixando mil ou menos. Em seguida, exclua a frota, e as instâncias restantes serão encerradas automaticamente.

AWS CLI

Para excluir uma solicitação de frota do EC2 e encerrar as instâncias

Use o comando delete-fleets com a opção `--terminate-instances`.

```
aws ec2 delete-fleets \
    --fleet-ids fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
    --terminate-instances
```

O seguinte é um exemplo de saída.

```
{
    "UnsuccessfulFleetDeletions": [],
    "SuccessfulFleetDeletions": [
        {
            "CurrentFleetState": "deleted_terminating",
            "PreviousFleetState": "active",
            "FleetId": "fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE"
        }
    ]
}
```

Para excluir uma solicitação de frota do EC2 sem encerrar as instâncias

Modifique o exemplo anterior usando a opção `--no-terminate-instances`. Observe que não há suporte a `--no-terminate-instances` para frotas `instant`.

```
aws ec2 delete-fleets \
    --fleet-ids fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
    --no-terminate-instances
```

O seguinte é um exemplo de saída.

```
{
    "UnsuccessfulFleetDeletions": [],
    "SuccessfulFleetDeletions": [
        {
            "CurrentFleetState": "deleted_running",
            "PreviousFleetState": "active",
            "FleetId": "fleet-4b8aaae8-dfb5-436d-a4c6-3dafa4c6b7dcEXAMPLE"
        }
    ]
}
```

PowerShell

Para excluir uma solicitação de frota do EC2 e encerrar as instâncias

Use o cmdlet Remove-EC2Fleet com o parâmetro `-TerminateInstance`.

```
Remove-EC2Fleet `
    -FleetId "fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE" `
    -TerminateInstance $true
```

Para excluir uma solicitação de frota do EC2 sem encerrar as instâncias

Modifique o exemplo anterior alterando o valor do parâmetro `-TerminateInstance`.

```
Remove-EC2Fleet `
    -FleetId "fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE" `
    -TerminateInstance $false
```

Solucionar problemas quando houver falha na exclusão da frota

Se a exclusão de uma solicitação de frota do EC2 falhar, `UnsuccessfulFleetDeletions` na saída mostrará o ID da solicitação de frota do EC2, um código de erro e uma mensagem de erro.

Os códigos de erro são:

- `ExceededInstantFleetNumForDeletion`
- `fleetIdDoesNotExist`
- `fleetIdMalformed`
- `fleetNotInDeletableState`
- `NoTerminateInstancesNotSupported`
- `UnauthorizedOperation`
- `unexpectedError`

Solução de problemas do **`ExceededInstantFleetNumForDeletion`**

Se você tentar excluir mais de 25 frotas `instant` em uma única solicitação, o erro `ExceededInstantFleetNumForDeletion` será retornado. Veja a seguir um exemplo de saída deste erro.

```
{
    "UnsuccessfulFleetDeletions": [
     {
          "FleetId": " fleet-5d130460-0c26-bfd9-2c32-0100a098f625",
          "Error": {
                 "Message": "Can’t delete more than 25 instant fleets in a single
 request.",
                 "Code": "ExceededInstantFleetNumForDeletion"
           }
     },
     {
           "FleetId": "fleet-9a941b23-0286-5bf4-2430-03a029a07e31",
           "Error": {
                 "Message": "Can’t delete more than 25 instant fleets in a single
 request.",
                 "Code": "ExceededInstantFleetNumForDeletion"
            }
     }
     .
     .
     .
     ],
     "SuccessfulFleetDeletions": []
}
```

Solução de problemas do **`NoTerminateInstancesNotSupported`**

Se você especificar que as instâncias em uma frota `instant` não devem ser encerradas quando você excluir a frota, o erro `NoTerminateInstancesNotSupported` será retornado. Não há suporte a `--no-terminate-instances` para frotas `instant`. Veja a seguir um exemplo de saída deste erro.

```
{
      "UnsuccessfulFleetDeletions": [
            {
                  "FleetId": "fleet-5d130460-0c26-bfd9-2c32-0100a098f625",
                  "Error": {
                         "Message": "NoTerminateInstances option is not supported for
 instant fleet",
                         "Code": "NoTerminateInstancesNotSupported"
                   }
            }
```

```
        ],
        "SuccessfulFleetDeletions": []
}
```

Solução de problemas do **`UnauthorizedOperation`**

Se você não tiver permissão para encerrar instâncias, você obterá o erro `UnauthorizedOperation` ao excluir uma frota que deve encerrar suas instâncias. A seguir está a resposta de erro.

```
<Response><Errors><Error><Code>UnauthorizedOperation</Code><Message>You are not
 authorized to perform this
operation. Encoded authorization failure message: VvuncIxj7Z_CPGNYXWqnuFV-
YjByeAU66Q9752NtQ-I3-qnDLWs6JLFd
KnSMMiq5s6cGqjjPtEDpsnGHzzyHasFHOaRYJpaDVravoW25azn6KNkUQQlFwhJyujt2dtNCdduJfrqcFYAjlEiRMkfDHt7
BHturzDK6A560Y2nDSUiMmAB1y9UNtqaZJ9SNe5sNxKMqZaqKtjRbk02RZu5V2vn9VMk6fm2aMVHbY9JhLvGypLcMUjtJ76
VPiU5v2s-
UgZ7h0p2yth6ysUdhlONg6dBYu8_y_HtEI54invCj4CoK0qawqzMNe6rcmCQHvtCxtXsbkgyaEbcwmrm2m01-
EMhekLFZeJLr
DtYOpYcEl4_nWFX1wtQDCnNNCmxnJZAoJvb3VMDYpDTsxjQv1PxODZuqWHs23YXWVywzgnLtHeRf2o4lUhGBw17mXsS07k7
PT9vrHtQiILor5VVTsjSPWg7edj__1rsnXhwPSu8gI48ZLRGrPQqFq0RmKO_QIE8N8s6NWzCK4yoX-9gDcheurOGpkprPIC
</Message></Error></Errors><RequestID>89b1215c-7814-40ae-a8db-41761f43f2b0</
RequestID></Response>
```

Para resolver o erro, você deve adicionar a ação `ec2:TerminateInstances` à política do IAM, conforme mostrado no exemplo a seguir.

Trabalhar com frotas spot

Para começar a usar uma frota spot, crie uma solicitação que inclua a capacidade total de destino para instâncias spot, uma parte opcional sob demanda, e especifique manualmente uma AMI e um par de chaves ou especifique um modelo de execução que inclua a configuração para as instâncias na frota. Como alternativa, você pode especificar parâmetros adicionais ou permitir que a frota use valores padrão. Você também pode marcar a solicitação da frota e suas instâncias e seus volumes quando criar a frota.

A frota executa instâncias sob demanda quando há capacidade disponível, e executa Instâncias spot quando o preço máximo excede o preço spot e há capacidade disponível.

Depois que a frota for inicializada, será possível descrever a solicitação, as instâncias e os eventos da frota. Você também poderá atribuir tags adicionais conforme necessário.

Caso precise alterar algum parâmetro da frota, como a capacidade total de destino, você pode modificar a frota, desde que ela tenha sido configurada para manter a capacidade. Você não pode modificar a capacidade de uma solicitação única depois que ela for enviada.

Uma solicitação de frota permanecerá ativa até que expire ou você a cancele (exclua). Ao cancelar a solicitação da frota, você pode encerrar as instâncias ou deixá-las em execução. Caso escolha deixá-las em execução, as instâncias sob demanda serão executadas até que você as encerre, e as Instâncias spot serão executadas até que sejam interrompidas ou você as encerre.

Tópicos

- Estados das solicitações de frota spot
- Permissões de frota spot
- Criar uma Frota spot
- Marcar uma solicitação nova ou existente da frota spot e as instâncias e os volumes que ela executa
- Descrever uma solicitação de frota spot, suas instâncias e o histórico de eventos
- Modificar uma solicitação de frota spot
- Cancelar (excluir) uma solicitação de frota spot
- Saiba mais sobre escalabilidade automática para frota spot

Estados das solicitações de frota spot

Uma solicitação de frota spot pode ser uma de vários estados, cada estado indicando um estágio diferente do ciclo de vida da solicitação e do gerenciamento de instâncias.

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. Se uma solicitação exceder as cotas da frota spot, ela será cancelada imediatamente.

`active`

A frota spot foi validada e o Amazon EC2 está tentando manter o número de destino de 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 seja cancelada. Apenas um tipo `maintain` de frota pode ser modificado. Esse estado não se aplica a um tipo de `request` única de frota.

`cancelled_running`

A frota spot foi cancelada (excluída) e não executará instâncias spot adicionais. Suas instâncias existentes continuam sendo executadas até que sejam interrompidas ou encerradas manualmente. A solicitação permanece nesse estado até que todas as instâncias sejam interrompidas ou encerradas.

`cancelled_terminating`

A frota spot foi cancelada (excluída) e suas instâncias estão sendo encerradas. A solicitação permanece nesse estado até que todas as instâncias sejam encerradas.

`cancelled`

A frota spot foi cancelada (excluída) e não há instâncias em execução. A solicitação foi excluída dois dias depois que as instâncias foram encerradas.

Permissões de frota spot

Se os usuários pretenderem criar ou gerenciar uma frota spot, será necessário conceder a eles as permissões necessárias.

Se você usar o console do Amazon EC2 para criar uma frota spot, ele criará duas funções vinculada ao serviço chamadas `AWSServiceRoleForEC2SpotFleet` e `AWSServiceRoleForEC2Spot`, além de uma função chamada `aws-ec2-spot-fleet-tagging-role` que concede à frota spot as permissões para solicitar, executar, encerrar e marcar recursos em seu nome. Se você usar a AWS CLI ou uma API, é necessário garantir que essas funções existam.

Use as instruções a seguir para conceder as permissões necessárias e criar as funções.

Permissões e funções

- Conceder aos usuários permissão para uma frota spot
- Função vinculada ao serviço para frota spot
- Função vinculada ao serviço para instâncias spot
- Função do IAM para marcar uma frota spot

Conceder aos usuários permissão para uma frota spot

Se os usuários pretenderem criar ou gerenciar uma frota spot, certifique-se de conceder a eles as permissões necessárias.

Para criar uma frota spot

1. Abra o console do IAM em https://console.aws.amazon.com/iam/.
2. No painel de navegação, escolha Policies, Create policy.
3. Na página Criar política, selecione JSON, e substitua o texto pelo indicado a seguir.

   JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances",
                "ec2:CreateTags",
                "ec2:RequestSpotFleet",
                "ec2:ModifySpotFleetRequest",
                "ec2:CancelSpotFleetRequests",
                "ec2:DescribeSpotFleetRequests",
                "ec2:DescribeSpotFleetInstances",
                "ec2:DescribeSpotFleetRequestHistory"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::*:role/aws-ec2-spot-fleet-tagging-role"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:CreateServiceLinkedRole",
                "iam:ListRoles",
                "iam:ListInstanceProfiles"
            ],
```

```
            "Resource": "*"
        }
    ]
}
```

A política de exemplo anterior concede a um usuário as permissões necessárias para a maioria dos casos de uso de frota spot. Para limitar o usuário a ações de API específicas, especifique somente essas ações de API.

APIs do EC2 e do IAM necessárias

As seguintes APIs devem ser incluídas na política:

- `ec2:RunInstances` – Necessária para executar instâncias em uma frota spot
- `ec2:CreateTags` – Necessária para marcar as solicitações, instâncias ou volumes da frota spot
- `iam:PassRole` – Necessária para especificar a função da frota spot
- `iam:CreateServiceLinkedRole` – Necessária para criar a função vinculada ao serviço
- `iam:ListRoles` – Necessária para enumerar funções do IAM existentes
- `iam:ListInstanceProfiles` – Necessária para enumerar perfis da instância existente

> **Important**
>
> Se você especificar um perfil para o perfil de instância do IAM na especificação ou no modelo de inicialização, deverá conceder ao usuário a permissão de passar o perfil para o serviço. Para fazer isso, na política do IAM inclua "`arn:aws:iam::*:role/`*`IamInstanceProfile-role`*" como um recurso para a ação `iam:PassRole`. Para obter mais informações, consulte Conceder permissões ao usuário para passar uma função a um produto da AWS no Guia do usuário do IAM.

APIs de frota spot

Adicione as seguintes ações da API de frota spot à política, conforme necessário:

- `ec2:RequestSpotFleet`

- `ec2:ModifySpotFleetRequest`
- `ec2:CancelSpotFleetRequests`
- `ec2:DescribeSpotFleetRequests`
- `ec2:DescribeSpotFleetInstances`
- `ec2:DescribeSpotFleetRequestHistory`

APIs opcionais do IAM

(Opcional) Para permitir que um usuário crie perfis ou perfis de instância usando o console do IAM, é necessário adicionar as seguintes ações à política:

- `iam:AddRoleToInstanceProfile`
- `iam:AttachRolePolicy`
- `iam:CreateInstanceProfile`
- `iam:CreateRole`
- `iam:GetRole`
- `iam:ListPolicies`

4. Escolha Revisar política.
5. Na página Review policy (Revisar política), digite um nome e uma descrição para a política e escolha Create policy (Criar política).
6. Para conceder acesso, adicione as permissões aos seus usuários, grupos ou perfis:

   - Usuários e grupos no Centro de Identidade do AWS IAM:

     Crie um conjunto de permissões. Siga as instruções em Criação de um conjunto de permissões no Guia do usuário do Centro de Identidade do AWS IAM.

   - Usuários gerenciados no IAM com provedor de identidades:

     Crie um perfil para a federação de identidades. Siga as instruções em Criando um perfil para um provedor de identidades de terceiros (federação) no Guia do Usuário do IAM.

   - Usuários do IAM:
     - Crie um perfil que seu usuário possa assumir. Siga as instruções em Criação de um perfil para um usuário do IAM no Guia do usuário do IAM.

- (Não recomendado) Vincule uma política diretamente a um usuário ou adicione um usuário a um grupo de usuários. Siga as instruções em Adição de permissões a um usuário (console) no Guia do usuário do IAM.

Função vinculada ao serviço para frota spot

O Amazon EC2 usa funções vinculadas ao serviço para as permissões de que ela precisa para chamar outros produtos da AWS em seu nome. Uma função vinculada ao serviço é um tipo exclusivo de função do IAM vinculado diretamente a um serviço da AWS. As funções vinculadas a serviços oferecem uma maneira segura de delegar permissões a serviços da AWS, pois somente o serviço vinculado pode assumir uma função vinculada ao serviço. Para obter mais informações, consulte Perfis vinculados ao serviço no Guia do usuário do IAM.

O Amazon EC2 usa a função vinculada ao serviço chamada AWSServiceRoleForEC2SpotFleet para executar e gerenciar instâncias em seu nome.

> **Important**
>
> Se você especificar uma AMI criptografada ou um snapshot do Amazon EBS criptografado na frota spot, será necessário conceder ao perfil AWSServiceRoleForEC2SpotFleet permissão para usar a CMK para que o Amazon EC2 possa executar instâncias em seu nome. Para obter mais informações, consulte Conceder acesso às CMKs para uso com AMIs criptografadas e snapshots do EBS.

Permissões concedidas por AWSServiceRoleForEC2SpotFleet

O perfil AWSServiceRoleForEC2SpotFleet concede à frota spot permissão para solicitar, executar, encerrar e marcar instâncias em seu nome. O Amazon EC2 usa essa função vinculada ao serviço para concluir as seguintes ações:

- `ec2:RequestSpotInstances` - Solicitar Instâncias spot
- `ec2:RunInstances` - executar instâncias
- `ec2:TerminateInstances` - encerrar instâncias
- `ec2:DescribeImages` - descrever imagens de máquina da Amazon (AMIs) para as instâncias
- `ec2:DescribeInstanceStatus` - descrever o status das instâncias
- `ec2:DescribeSubnets` – descrever as sub-redes das instâncias

- `ec2:CreateTags` - adiciona etiquetas à solicitação, às instâncias e aos volumes da frota spot
- `elasticloadbalancing:RegisterInstancesWithLoadBalancer` - adicionar as instâncias especificadas ao load balancer especificado.
- `elasticloadbalancing:RegisterTargets` - registrar os destinos especificados no grupo de destino especificado.

Criar a função vinculada ao serviço

Na maioria das circunstâncias, você não precisa criar manualmente uma função vinculada ao serviço. O Amazon EC2 cria a função AWSServiceRoleForEC2Spotleet vinculada ao serviço na primeira vez que você criar uma frota spot usando o console.

Se você tinha uma solicitação de frota spot ativa antes de outubro de 2017, quando o Amazon EC2 começou a oferecer suporte a essa função vinculada ao serviço, o Amazon EC2 criou a função AWSServiceRoleForEC2SpotFleet em sua conta da AWS. Para obter mais informações, consulte Uma nova função apareceu em minha conta da AWS no Guia do usuário do IAM.

Se você usar a AWS CLI ou uma API para criar uma frota spot, verifique se essa função existe.

Para criar o perfil AWSServiceRoleForEC2SpotFleet para a frota spot usando o console

1. Abra o console do IAM em https://console.aws.amazon.com/iam/.
2. No painel de navegação, escolha Perfis.
3. Escolha Criar Perfil.
4. Na página Selecionar entidade confiável, faça o seguinte:
   a. Em Tipo de entidade confiável, escolha Serviços da AWS.
   b. Em Caso de uso, para Serviço ou caso de uso, escolha EC2.
   c. Em Caso de uso, Escolha EC2 - Frota spot.

      > **Note**
      >
      > O caso de uso EC2: frota spot criará automaticamente uma política com as permissões necessárias do IAM e vai sugerir AWSEC2SpotFleetServiceRolePolicy como nome do perfil.

   d. Escolha Próximo.

5. Na página Adicionar permissões, escolha Próximo.
6. Na página Nomear, revisar e criar, escolha Criar função.

Para criar o perfil AWSServiceRoleForEC2SpotFleet para a frota spot usando a AWS CLI

Use o comando create-service-linked-role da seguinte forma.

```
aws iam create-service-linked-role --aws-service-name spotfleet.amazonaws.com
```

Se você não precisar mais usar a frota spot, é recomendável excluir a função AWSServiceRoleForEC2SpotFleet. Depois que a função for excluída da conta, o Amazon EC2 criará a função novamente se você solicitar uma frota spot usando o console. Para saber mais, consulte Excluir um perfil vinculado ao serviço no Guia do usuário do IAM.

Conceder acesso às CMKs para uso com AMIs criptografadas e snapshots do EBS

Se você especificar uma AMI criptografada ou um snapshot do Amazon EBS criptografado na solicitação de frota spot e usar uma chave gerenciada pelo cliente para criptografia, será necessário conceder ao perfil AWSServiceRoleForEC2SpotFleet permissão para usar a CMK para que o Amazon EC2 possa executar instâncias em seu nome. Para isso, adicione uma concessão à CMK, conforme exibido no procedimento a seguir.

Durante a definição de permissões, as concessões são uma alternativa às políticas de chave. Para obter mais informações, consulte Uso de concessões e Uso de políticas de chave no AWS KMS, no Guia do desenvolvedor do AWS Key Management Service.

Para conceder à função AWSServiceRoleForEC2SpotFleet permissões para usar a CMK

- Use o comando create-grant para adicionar uma concessão à CMK e especificar a entidade principal (a função vinculada ao serviço AWSServiceRoleForEC2SpotFleet) que recebe permissão para executar as operações permitidas pela concessão. A CMK é especificada pelo parâmetro `key-id` e pelo ARN da CMK. A entidade principal é especificada pelo parâmetro `grantee-principal` e pelo ARN da função vinculada ao serviço AWSServiceRoleForEC2SpotFleet.

```
aws kms create-grant \
    --region us-east-1 \
    --key-id arn:aws:kms:us-
east-1:444455556666:key/1234abcd-12ab-34cd-56ef-1234567890ab \
```

```
    --grantee-principal arn:aws:iam::111122223333:role/aws-service-role/
spotfleet.amazonaws.com/AWSServiceRoleForEC2SpotFleet \
    --operations "Decrypt" "Encrypt" "GenerateDataKey"
 "GenerateDataKeyWithoutPlaintext" "CreateGrant" "DescribeKey" "ReEncryptFrom"
 "ReEncryptTo"
```

Função vinculada ao serviço para instâncias spot

O Amazon EC2 usa a função vinculada ao serviço denominada AWSServiceRoleForEC2Spot para executar e gerenciar Instâncias spot em seu nome. Para obter mais informações, consulte Função vinculada ao serviço para solicitações de instâncias spot.

Função do IAM para marcar uma frota spot

A função do IAM `aws-ec2-spot-fleet-tagging-role` concede à frota spot permissão para marcar a solicitação, as instâncias e os volumes de frota spot. Para obter mais informações, consulte Marcar uma solicitação nova ou existente da frota spot e as instâncias e os volumes que ela executa.

> **Important**
>
> Se você optar por marcar as instâncias na frota e também por manter a capacidade visada (a solicitação de frota spot é do tipo `maintain`), as diferenças nas permissões definidas para o usuário e a `IamFleetRole` poderão levar a um comportamento inconsistente de marcação de instâncias na frota. Se o `IamFleetRole` não incluir a permissão `CreateTags`, algumas das instâncias executadas pela frota não serão marcadas. Embora estejamos trabalhando para corrigir essa inconsistência, para garantir que todas as instâncias executadas pela frota sejam marcadas, recomendamos que você use a função `aws-ec2-spot-fleet-tagging-role` para `IamFleetRole`. Outra opção é para usar uma função existente, anexe a `AmazonEC2SpotFleetTaggingRole`Política gerenciada da AWS à função existente. Caso contrário, você precisará adicionar manualmente a permissão `CreateTags` à política existente.

Para criar uma função do IAM para marcar uma frota spot

1. Abra o console do IAM em https://console.aws.amazon.com/iam/.
2. No painel de navegação, escolha Perfis.
3. Escolha Criar Perfil.

4. Na página Select trusted entity (Selecionar entidade confiável), em Trusted entity type (Tipo de entidade confiável), escolha AWS service (Serviço da).
5. Em Caso de uso, em Casos de uso para outros serviços da AWS, escolha EC2 e escolha EC2 - marcação de frota Spot.
6. Escolha Próximo.
7. Na página Adicionar permissões, escolha Próximo.
8. Na página Name, review, and create (Nomear, revisar e criar), para Role name (Nome da função), digite um nome para a função (por exemplo, **`aws-ec2-spot-fleet-tagging-role`**).
9. Revise as informações na página e escolha Create role (Criar função).

Prevenção contra o ataque do “substituto confuso” em todos os serviços

O problema “confused deputy” é um problema de segurança em que uma entidade que não tem permissão para executar uma ação pode coagir uma entidade mais privilegiada a executá-la. Recomendamos o uso das chaves de contexto de condição global `aws:SourceArn` e `aws:SourceAccount` na política de confiança `aws-ec2-spot-fleet-tagging-role` para limitar as permissões de acesso ao recurso que a frota spot concede a outro serviço.

Para adicionar as chaves de condição AWS:SourceArn e AWS:SourceAccount à política de confiança **`aws-ec2-spot-fleet-tagging-role`**

1. Abra o console do IAM em https://console.aws.amazon.com/iam/.
2. No painel de navegação, escolha Perfis.
3. Encontre o `aws-ec2-spot-fleet-tagging-role` criado anteriormente e escolha o link (não a caixa de seleção).
4. Em Summary (Resumo), escolha a guia Trust relationships (Relacionamentos de confiança) e, em seguida, escolha Edit trust policy (Editar política de confiança).
5. Na instrução JSON, adicione um elemento `Condition` que contenha suas chaves de contexto de condição global `aws:SourceAccount` e `aws:SourceArn` para evitar o problema confused deputy, como segue:

```
"Condition": {
      "ArnLike": {
        "aws:SourceArn": "arn:aws:ec2:us-east-1:111122223333:spot-fleet-request/
sfr-*"
      },
```

```
      "StringEquals": {
        "aws:SourceAccount": "111122223333"
      }
```

> **Note**
>
> Se você utilizar ambas as chaves de contexto de condição global, e o valor `aws:SourceArn` contiver o ID da conta, o valor `aws:SourceAccount` e a conta no valor `aws:SourceArn` deverão utilizar o mesmo ID de conta quando utilizados na mesma instrução de política.

A política de confiança final será a seguinte:

JSON

```
{
  "Version":"2012-10-17",
  "Statement": {
    "Sid": "ConfusedDeputyPreventionExamplePolicy",
    "Effect": "Allow",
    "Principal": {
      "Service": "spotfleet.amazonaws.com"
    },
    "Action": "sts:AssumeRole",
    "Condition": {
      "ArnLike": {
        "aws:SourceArn": "arn:aws:ec2:us-east-1:111122223333:spot-fleet-
request/sfr-*"
      },
      "StringEquals": {
        "aws:SourceAccount": "111122223333"
      }
    }
  }
}
```

6. Escolha Atualizar política.

A tabela a seguir fornece valores potenciais para `aws:SourceArn` para limitar o escopo do seu `aws-ec2-spot-fleet-tagging-role` em diferentes graus de especificidade.

Operação de API	Serviço chamado	Escopo	**aws:SourceArn**
RequestSpotFleet	AWS STS (AssumeRole)	Limita a capacidade de AssumeRole em aws-ec2-spot-fleet-tagging-role para solicitações de frota spot na conta especificada.	arn:aws:ec2:*: *123456789012* :spot-fleet-request/sfr-*
RequestSpotFleet	AWS STS (AssumeRole)	Limita a capacidade de AssumeRole em aws-ec2-spot-fleet-tagging-role para solicitações de frota spot na conta e na região especificada. Observe que essa função não será utilizável em outras regiões.	arn:aws:ec2: *us-east-1* :*123456789012* :spot-fleet-request/sfr-*
RequestSpotFleet	AWS STS (AssumeRole)	Limita a capacidade de AssumeRole em aws-ec2-spot-fleet-tagging-role para apenas ações que afetam a frota sfr-11111111-1111-1111-1111-111111111111. Observe que essa função pode não ser utilizável para	arn:aws:ec2: *us-east-1* :*123456789012* :spot-fleet-request/sfr-*11111111-1111-1111-1111-111111111111*

Operação de API	Serviço chamado	Escopo	`aws:SourceArn`
		outras frotas spot. Além disso, essa função não pode ser usada para lançar novas frotas spot por meio de request-spot-fleet.	

Criar uma Frota spot

Usando o Console de gerenciamento da AWS, é possível criar rapidamente uma solicitação de frota spot escolhendo apenas uma AMI e a capacidade total de destino pretendida. O Amazon EC2 vai configurar uma frota que melhor atenda às suas necessidades e siga as práticas recomendadas para instâncias spot. Como alternativa, você pode modificar qualquer uma das configurações padrão.

Se quiser incluir instâncias sob demanda em sua frota, você precisa especificar um modelo de execução em sua solicitação e especificar a capacidade sob demanda pretendida.

A frota executa instâncias sob demanda quando há capacidade disponível e inicializa instâncias spot quando o preço máximo excede o preço spot e há capacidade disponível.

Se a frota incluir a instâncias spot e for do tipo `maintain`, o Amazon EC2 tentará manter a capacidade de destino da frota quando as instâncias spot forem interrompidas.

Permissões obrigatórias

Para obter mais informações, consulte the section called “Permissões de frota spot”.

Tarefas

- Criar rapidamente uma solicitação de frota spot
- Criar uma solicitação de frota spot usando parâmetros definidos
- Criar uma frota spot que substitua instâncias spot não íntegras

Criar rapidamente uma solicitação de frota spot

Siga estas etapas para criar rapidamente uma solicitação de frota spot usando o console do Amazon EC2.

Para criar uma solicitação de frota spot usando as configurações recomendadas

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 spot, verá uma página de boas-vindas. Escolha Comece a usar. Caso contrário, escolha Criar solicitação de frota spot.
4. Em Launch parameters (Parâmetros de lançamento), escolha Manually configure launch parameters (Configurar parâmetros de lançamento manualmente).
5. Em AMI, escolha uma AMI.
6. Em Target capacity (Capacidade), especifique o número de unidades a serem solicitadas em Total target capacity (Capacidade-alvo total). Para o tipo de unidade, você pode escolher Instâncias, vCPUs ou Memória (GiB).
7. Em Visão rápida de sua solicitação de frota, analise a configuração da sua frota e selecione Iniciar.

Criar uma solicitação de frota spot usando parâmetros definidos

É possível criar uma frota spot usando parâmetros definidos por você.

Console

Para criar uma solicitação de frota spot usando parâmetros definidos

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 spot, verá uma página de boas-vindas. Escolha Comece a usar. Caso contrário, escolha Criar solicitação de frota spot.
4. Em Parâmetros de inicialização, você pode configurar manualmente os parâmetros de inicialização ou usar um modelo de inicialização, da seguinte forma:

a. [Configurar manualmente] Para definir os parâmetros de inicialização no console do Amazon EC2, escolha Configurar parâmetros de inicialização manualmente e, então, faça o seguinte:

   i. 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.

   > **Note**
   >
   > Se uma AMI especificada nos parâmetros de execução estiver descadastrada ou desabilitada, não será possível executar nenhuma instância nova com base na AMI. Para frotas configuradas para manter a capacidade de destino, a capacidade de destino não será mantida.

   ii. (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 Criar novo par de chaves para ir para a página Pares de chaves. Ao concluir, volte para a página Spot Requests (Solicitações de spot) e atualize a lista.

   iii. (Opcional) Expanda Additional launch parameters (Parâmetros de lançamento adicionais) e faça o seguinte:

      A. (Opcional) Para habilitar a otimização para o Amazon EBS, para EBS-optimized (Otimizada para EBS), escolha Launch EBS-optimized instances (Iniciar instâncias otimizadas para EBS).

      B. (Opcional) Para adicionar armazenamento temporário em nível de blocos para suas instâncias, em Instance store (Armazenamento de instâncias), escolha Attach at launch (Anexar na execução).

      C. (Opcional) Para adicionar armazenamento, escolha Add new volume (Adicionar novo volume) e especifique volumes adicionais do armazenamento de instâncias ou do Amazon EBS, dependendo do tipo de instância.

      D. (Opcional) Por padrão, o monitoramento básico está habilitado para suas instâncias. Para habilitar monitoramento detalhado, para 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 ir para a página Security Groups (Grupos de segurança). Ao concluir, volte para Spot Requests (Solicitações de spot) 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 Create tag (Criar tag), insira uma chave e valor da tag, e escolha Create (Criar). Repita esse procedimento para cada tag.

Para cada tag, para marcar as instâncias e a solicitação de frota spot com a mesma tag, verifique se as opções Instances (Instâncias) e Fleet (Frota) estão selecionadas. Para marcar apenas as instâncias iniciadas pela frota, desmarque Frota. Para aplicar tag apenas na solicitação de frota spot, desmarque Instances (Instâncias).

b. [Modelo de inicialização] Para usar uma configuração que você criou em um modelo de inicialização, escolha Usar um modelo de inicialização e, em Modelo de inicialização, escolha um modelo de inicialização.

> **Note**
>
> Caso deseje capacidade sob demanda na frota spot, você deve especificar um modelo de execução.

5. 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) Para criar uma solicitação que seja válida somente em um período específico, edite Request valid from e Request valid until.

   d. (Opcional) Por padrão, o Amazon EC2 encerra as instâncias spot quando a solicitação de frota spot 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).

   e. (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.

6. Em Modify target capacity (Modificar capacidade-alvo), faça o seguinte:

   a. Em Total target capacity (Capacidade-alvo total), especifique o número de unidades a serem solicitadas. Para o tipo de unidade, você pode escolher Instances (Instâncias), vCPUs ou Memory (MiB) [Memória (MiB)]. Para especificar uma capacidade de destino igual a 0 para que seja possível adicionar capacidade posteriormente, primeiro escolha Manter capacidade de destino.

   b. (Opcional) Em Include On-Demand base capacity (Incluir capacidade sob demanda de base), especifique o número de unidades sob demanda a serem solicitadas. O número deve ser menor que a Capacidade total pretendida. O Amazon EC2 calcula e aloca a diferença às unidades spot a serem solicitadas.

> **Important**
>
> Para especificar a capacidade sob demanda opcional, primeiro, escolha um modelo de lançamento.

c. (Opcional) Por padrão, o Amazon EC2 encerra instâncias spot quando elas são interrompidas. Para manter a capacidade do destino, selecione Maintain target capacity (Manter a capacidade de destino). Em seguida, será possível especificar se o Amazon EC2 vai encerrar, interromper ou hibernar as instâncias spot que forem interrompidas. Para fazer isso, escolha a opção correspondente em Interruption behavior.

> **Note**
>
> Se uma AMI especificada nos parâmetros de execução estiver descadastrada ou desabilitada, não será possível executar nenhuma instância nova com base na AMI. Nesse caso, para frotas configuradas para manter a capacidade de destino, a capacidade de destino não será mantida.

d. (Opcional) Para permitir que a frota spot inicie uma instância spot substituta quando uma notificação de rebalanceamento de instância for emitida para uma instância spot existente na frota, selecione Capacity rebalance (Rebalanceamento de capacidade) e escolha uma estratégia de substituição de instância. Se você escolher Inicializar antes de encerrar, especifique o atraso (em segundos) antes que o Amazon EC2 encerre as instâncias antigas. Para obter mais informações, consulte Use o rebalanceamento de capacidade na frota do EC2 e na frota spot para substituir instâncias spot em risco.

e. (Opcional) Para controlar o valor pago por hora por todas as instâncias spot da sua frota, selecione Manter custo pretendido para instâncias spot e insira o valor total máximo que você está disposto a pagar por hora. Quando o valor total máximo for alcançado, a frota spot interromperá a execução de instâncias spot mesmo que a capacidade do destino ainda não tenha sido atingida. Para obter mais informações, consulte Definir um limite de gastos para a frota do EC2 ou a frota spot.

7. Em Network (Rede), faça o seguinte:

a. Em Rede, escolha uma VPC existente ou crie uma nova.

[VPC existente] escolha a VPC.

[VPC nova] Escolha Create new VPC (Criar nova VPC) para acessar o console da Amazon VPC. Quando concluir, volte para esta tela e atualize a lista.

b. (Opcional) Em Zonas de disponibilidade, deixe que o Amazon EC2 escolha as zonas de disponibilidade para as 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. Quando concluir, volte para esta tela e atualize a lista.

8. Em Instance type requirements (Requisitos de tipo de instância), você pode especificar atributos de instância e deixar o Amazon EC2 identificar os tipos de instância com esses atributos ou pode especificar uma lista de instâncias. Para obter mais informações, consulte Especificar atributos para seleção de tipo de instância para frota do EC2 ou frota spot.

   a. Se escolher Specify instance attributes that match your compute requirements (Especificar atributos de instância que correspondam aos requisitos de computação), especifique os atributos da instância da seguinte forma:

      i. Em vCPUs, insira o número mínimo e máximo desejado de vCPUs. Para não especificar um limite, selecione Sem mínimo, Sem máximo ou ambos.

      ii. Em Memory (GiB) (Memória), insira a quantidade mínima e máxima de memória desejada. Para não especificar um limite, selecione Sem mínimo, Sem máximo ou ambos.

      iii. (Opcional) Em Atributos de instância adicionais, você pode, opcionalmente, especificar um ou mais atributos para expressar seus requisitos de computação com mais detalhes. Cada atributo adicional inclui mais uma restrição à solicitação. É possível omitir os atributos adicionais; quando omitidos, os valores padrão são usados. Para obter uma descrição de cada atributo e seus valores padrão, consulte get-spot-placement-scores.

      iv. (Opcional) Para visualizar os tipos de instância com os atributos especificados, expanda Preview matching instance types (Previsualizar os tipos de instância correspondentes). Para excluir tipos de instância dos tipos a serem usados na solicitação selecione as instâncias e escolha Exclude selected instance types (Excluir tipos de instância selecionados).

b. Se escolher Manually select instance types (Selecionar manualmente os tipos de instância), a frota spot fornecerá uma lista padrão de tipos de instância. Para selecionar mais tipos de instância, escolha Add instance types (Adicionar tipos de instância), selecione os tipos de instância a serem usados em sua solicitação e escolha Select (Selecionar). Para excluir tipos de instância, selecione os tipos de instância e escolha Delete (Excluir).

9. Em Estratégia de alocação, escolha uma estratégia de alocação spot e uma estratégia de alocação sob demanda que atenda às suas necessidades. Para obter mais informações, consulte Usar estratégias de alocação para determinar como a frota do EC2 ou a frota spot atende à capacidade spot e sob demanda.
10. Em Your fleet request at a glance (Visão rápida da sua solicitação de frota), revise a configuração de frota e faça os ajustes necessários.
11. (Opcional) Para fazer download de uma cópia da configuração de execução para uso com a AWS CLI, escolha JSON config.
12. Quando você estiver prestes a criar uma frota spot, escolha Inicializar.

    O tipo de solicitação de frota spot é `fleet`. Quando a solicitação for atendida, as solicitações do tipo `instance` serão adicionadas, onde o estado será `active` e o status será `fulfilled`.

AWS CLI

Para criar uma solicitação de frota spot

Use o comando request-spot-fleet.

```
aws ec2 request-spot-fleet --spot-fleet-request-config file://config.json
```

Para obter arquivos de configuração de exemplo, consulte Exemplo de configurações da CLI para frotas spot.

PowerShell

Para criar uma solicitação de frota spot

Use o cmdlet Request-EC2SpotFleet. O exemplo a seguir inicia instâncias spot em uma frota otimizada para capacidade.

```
Request-EC2SpotFleet `
```

```
    -SpotFleetRequestConfig_TargetCapacity 50 `
    -SpotFleetRequestConfig_AllocationStrategy "CapacityOptimized" `
    -SpotFleetRequestConfig_IamFleetRole "arn:aws:iam::123456789012:role/my-spot-
fleet-role" `
    -SpotFleetRequestConfig_LaunchTemplateConfig @($launchConfig)
```

Defina a configuração de execução conforme mostrado a seguir definindo o modelo de execução e substituindo as propriedades necessárias. Para obter configurações de exemplo, consulte Exemplo de configurações da CLI para frotas spot.

```
$lcSpec = Amazon.EC2.Model.FleetLaunchTemplateSpecification
# To do - Set FleetLaunchTemplateSpecification properties
$lcOverrides = New-Object Amazon.EC2.Model.LaunchTemplateOverrides
# To do - Set LaunchTemplateOverrides properties
$launchConfig = New-Object Amazon.EC2.Model.LaunchTemplateConfig
$launchConfig.LaunchTemplateSpecification $lcSpec
$launchConfig.Overrides @($lcOverrides)
```

Criar uma frota spot que substitua instâncias spot não íntegras

A frota spot verifica o status de integridade das instâncias spot na frota a cada dois minutos. O status de integridade de uma instância é `healthy` ou `unhealthy`.

A frota spot determina o status de integridade de uma instância usando as verificações de status fornecidas pelo Amazon EC2. É determinado que uma instância está `unhealthy` quando o status da verificação de status da instância ou da verificação de status do sistema é `impaired` em três verificações de integridade consecutivas. Para obter mais informações, consulte Verificações do status das instâncias do Amazon EC2.

É possível configurar a sua frota para substituir Instâncias spot não íntegras. Depois de habilitar a substituição da verificação de integridade, uma instância spot é substituída ao ser relatada como `unhealthy`. A frota pode ficar abaixo de sua capacidade de destino por até alguns minutos enquanto uma instância spot não íntegra está sendo substituída.

Requisitos

- A substituição da verificação de integridade é compatível apenas para Frotas spot que mantenham uma capacidade de destino (frotas do tipo `maintain`) e não para Frotas spot únicas (frotas do tipo `request`).

- A substituição da verificação de integridade é compatível apenas para Instâncias spot. Este recurso não é compatível para Instâncias on-demand.
- É possível configurar a frota spot para substituir instâncias não íntegras somente durante sua criação.
- Os usuários só poderão usar a substituição de verificação de integridade se tiverem permissão para chamar a ação `ec2:DescribeInstanceStatus`.

Console

Para configurar uma frota spot para substituir instâncias spot não íntegras

1. Siga as etapas para criar um frota spot em Criar uma solicitação de frota spot usando parâmetros definidos.
2. Para configurar a frota para substituir instâncias spot não íntegras, expanda Parâmetros adicionais de execução e, em Verificação de integridade, selecione Substituir instâncias não íntegras. Para habilitar essa opção, primeiramente você deve selecionar Maintain target capacity (Manter capacidade de destino).

AWS CLI

Para configurar uma frota spot para substituir instâncias spot não íntegras

Use o comando request-spot-fleet com a propriedade `ReplaceUnhealthyInstances` de `SpotFleetRequestConfig`.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "lowestPrice",
        "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-
role",
        "TargetCapacity": 10,
        "ReplaceUnhealthyInstances": true
    }
}
```

PowerShell

Para configurar uma solicitação de frota spot para substituir instâncias spot não íntegras

Use o cmdlet Request-EC2SpotFleet com o parâmetro -SpotFleetRequestConfig_ReplaceUnhealthyInstance.

```
-SpotFleetRequestConfig_ReplaceUnhealthyInstance $true
```

Marcar uma solicitação nova ou existente da frota spot e as instâncias e os volumes que ela executa

Para ajudar na categorização e no gerenciamento das solicitações de frota spot e das instâncias e dos volumes que ela executa, você pode marcá-las com metadados personalizados. É possível atribuir uma tag a uma solicitação de frota spot ao criá-la ou posteriormente. Da mesma forma, você pode atribuir uma tag às instâncias e aos volumes quando eles são inicializados pela frota, ou posteriormente.

Quando você marca uma solicitação de frota, as instâncias e os volumes que são executados pela frota não são marcados automaticamente. É necessário marcar explicitamente as instâncias e os volumes executados pela frota. É possível optar por atribuir tags somente à solicitação de frota, somente às instâncias inicializadas pela frota, somente aos volumes anexados às instâncias inicializadas pela frota ou a todos eles.

> **Note**
>
> Você só pode marcar volumes que estão anexados a instâncias sob demanda. Não é possível marcar volumes que estão anexados a Instâncias spot.

É possível atribuir tags usando o console do Amazon EC2 ou uma ferramenta da linha de comando.

Para obter mais informações sobre como as tags funcionam, consulte Marcar com tag os recursos do Amazon EC2.

Conteúdo

- Pré-requisito
- Marcar uma nova frota spot e as instâncias e os volumes que ela executa
- Marcar uma frota spot existente
- Exibir tags de solicitações de frota spot

Pré-requisito

Conceda ao usuário permissão para marcar recursos. Para obter mais informações, consulte Exemplo: marcar recursos.

Para conceder a um usuário permissão para marcar recursos

Crie uma política do IAM que inclua o seguinte:

- A ação `ec2:CreateTags`. Isso concede ao usuário permissão para criar tags.
- A ação `ec2:RequestSpotFleet`. Concede ao usuário permissão para criar uma solicitação de frota spot.
- Para `Resource`, você deve especificar `"*"`. Permite que os usuários marquem todos os tipos de recursos.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "TagSpotFleetRequest",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags",
                "ec2:RequestSpotFleet"
            ],
            "Resource": "*"
        }
    ]
}
```

Important

No momento, não oferecemos suporte para permissões no nível do recurso para o recurso `spot-fleet-request`. Se especificar `spot-fleet-request` como um recurso, você receberá uma exceção não autorizada quando tentar marcar a frota. O exemplo a seguir ilustra como não definir a política.

```
{
    "Effect": "Allow",
    "Action": [
        "ec2:CreateTags",
        "ec2:RequestSpotFleet"
    ],
    "Resource": "arn:aws:ec2:us-east-1:111122223333:spot-fleet-request/*"
}
```

Para conceder acesso, adicione as permissões aos seus usuários, grupos ou perfis:

- Usuários e grupos no Centro de Identidade do AWS IAM:

  Crie um conjunto de permissões. Siga as instruções em Criação de um conjunto de permissões no Guia do usuário do Centro de Identidade do AWS IAM.
- Usuários gerenciados no IAM com provedor de identidades:

  Crie um perfil para a federação de identidades. Siga as instruções em Criando um perfil para um provedor de identidades de terceiros (federação) no Guia do Usuário do IAM.
- Usuários do IAM:
  - Crie um perfil que seu usuário possa assumir. Siga as instruções em Criação de um perfil para um usuário do IAM no Guia do usuário do IAM.
  - (Não recomendado) Vincule uma política diretamente a um usuário ou adicione um usuário a um grupo de usuários. Siga as instruções em Adição de permissões a um usuário (console) no Guia do usuário do IAM.

Marcar uma nova frota spot e as instâncias e os volumes que ela executa

Para marcar uma nova solicitação de frota spot e as instâncias e os volumes que ela executa usando o console

1. Siga o procedimento do Criar uma solicitação de frota spot usando parâmetros definidos.
2. A forma como você adiciona uma tag depende se você configurou manualmente a frota ou se usou um modelo de execução.

   - Caso tenha configurado a frota manualmente, faça o seguinte:

Para adicionar uma tag, expanda Parâmetros adicionais de execução, escolha Criar tag e insira a chave e o valor para a tag. Repita esse procedimento para cada tag.

Para cada tag, você pode marcar a solicitação de frota spot e as instâncias com a mesma tag. Para marcar ambas, verifique se Instâncias e Frota estão selecionados. Para aplicar tag apenas na solicitação de frota spot, desmarque Instances (Instâncias). Para marcar apenas as instâncias iniciadas pela frota, desmarque Frota.

> **Note**
>
> Quando você configura manualmente uma frota, não há opção para marcar volumes. As tags de volume são compatíveis apenas para volumes que estão anexados a Instâncias on-demand. Ao configurar manualmente uma frota, você não pode especificar instâncias sob demanda.

- Caso tenha usado um modelo de execução, faça o seguinte:

  Para adicionar uma tag à solicitação de frota, em Tags, escolha Criar tag e insira a chave e o valor para a tag. Repita esse procedimento para cada tag.

  Para marcar os recursos em sua frota, você deve especificar as tags no modelo de execução.

Para marcar uma nova solicitação de frota spot e as instâncias e os volumes que ela executa usando a AWS CLI

Para marcar uma solicitação de frota spot ao criá-la e marcar as instâncias e os volumes quando elas são executadas pela frota, defina a configuração da solicitação de frota spot da seguinte maneira:

Tags de solicitações de frota spot:

- Especifique as etiquetas para a solicitação de frota spot em `SpotFleetRequestConfig`.
- Para `ResourceType`, especifique `spot-fleet-request`. Se você especificar outro valor, ocorrerá falha na frota.
- Em `Tags`, especifique o par de chave/valor. É possível especificar mais de um par de chave/valor.

Tags de instância:

- Especifique as tags das instâncias em `LaunchSpecifications`.
- Para `ResourceType`, especifique `instance`. Se você especificar outro valor, ocorrerá falha na frota.
- Em `Tags`, especifique o par de chave/valor. É possível especificar mais de um par de chave/valor.

  Como alternativa, você pode especificar as tags da instância no modelo de execução que é referenciado na solicitação de frota spot.

Tags de volume:

- Especifique as tags para os volumes no modelo de execução mencionado na solicitação de frota spot. A marcação de volume em `LaunchSpecifications` não é compatível.

No exemplo a seguir, a solicitação de frota spot é marcada com duas tags: Key=Environment e Value=Production, e Key=Cost-Center e Value=123. As instâncias executadas pela frota são marcadas com uma tag (que é a mesma que uma das tags da solicitação de frota spot): Keys=Cost-Center e Value=123.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "priceCapacityOptimized",
        "ExcessCapacityTerminationPolicy": "default",
        "IamFleetRole": "arn:aws:iam::111122223333:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchSpecifications": [
            {
                "ImageId": "ami-0123456789EXAMPLE",
                "InstanceType": "c4.large",
                "TagSpecifications": [
                    {
                        "ResourceType": "instance",
                        "Tags": [
                            {
                                "Key": "Cost-Center",
                                "Value": "123"
                            }
                        ]
                    }
```

```
                ]
            }
        ],
        "SpotPrice": "5",
        "TargetCapacity": 2,
        "TerminateInstancesWithExpiration": true,
        "Type": "maintain",
        "ReplaceUnhealthyInstances": true,
        "InstanceInterruptionBehavior": "terminate",
        "InstancePoolsToUseCount": 1,
        "TagSpecifications": [
            {
                "ResourceType": "spot-fleet-request",
                "Tags": [
                    {
                        "Key": "Environment",
                        "Value":"Production"
                    },
                    {
                        "Key": "Cost-Center",
                        "Value":"123"
                    }
                ]
            }
        ]
    }
}
```

Para marcar instâncias executadas por uma frota spot usando a AWS CLI

Para marcar instâncias quando elas são executadas pela frota, você pode especificar as tags no modelo de execução referenciado na solicitação de frota spot ou especificar as tags na configuração da solicitação de frota spot da seguinte maneira:

- Especifique as tags das instâncias em `LaunchSpecifications`.
- Para `ResourceType`, especifique `instance`. Se você especificar outro valor, ocorrerá falha na frota.
- Em `Tags`, especifique o par de chave/valor. É possível especificar mais de um par de chave/valor.

No exemplo a seguir, as instâncias que são executadas pela frota são marcadas com uma tag: Key=Cost-Center e Value=123.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "priceCapacityOptimized",
        "ExcessCapacityTerminationPolicy": "default",
        "IamFleetRole": "arn:aws:iam::111122223333:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchSpecifications": [
            {
                "ImageId": "ami-0123456789EXAMPLE",
                "InstanceType": "c4.large",
                "TagSpecifications": [
                    {
                        "ResourceType": "instance",
                        "Tags": [
                            {
                                "Key": "Cost-Center",
                                "Value": "123"
                            }
                        ]
                    }
                ]
            }
        ],
        "SpotPrice": "5",
        "TargetCapacity": 2,
        "TerminateInstancesWithExpiration": true,
        "Type": "maintain",
        "ReplaceUnhealthyInstances": true,
        "InstanceInterruptionBehavior": "terminate",
        "InstancePoolsToUseCount": 1
    }
}
```

Para marcar volumes anexados a instâncias sob demanda executadas por uma frota spot usando a AWS CLI

Para marcar volumes ao serem criados pela frota, é necessário especificar as tags no modelo de execução mencionado na solicitação de frota spot.

> **Note**
>
> As tags de volume são compatíveis apenas para volumes que estão anexados a Instâncias on-demand. Não é possível marcar volumes que estão anexados a Instâncias spot.
> A marcação de volume em `LaunchSpecifications` não é compatível.

Marcar uma frota spot existente

Para marcar uma solicitação de frota spot existente usando o console

Depois de criar uma solicitação de frota spot, você pode adicionar tags à solicitação de frota usando o console.

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Solicitações spot.
3. Selecione sua solicitação de frota spot.
4. Escolha a guia Tags e Create Tag (Criar tag).

Para marcar uma solicitação de frota spot existente usando a AWS CLI

É possível usar o comando create-tags para marcar os recursos existentes. No exemplo a seguir, a solicitação de frota spot existente é marcada com Key=purpose e Value=test.

```
aws ec2 create-tags \
    --resources sfr-11112222-3333-4444-5555-66666EXAMPLE \
    --tags Key=purpose,Value=test
```

Exibir tags de solicitações de frota spot

Para visualizar tags de solicitação de frota spot usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Solicitações spot.
3. Selecione sua solicitação de frota spot e escolha a guia Tags.

Para descrever as tags de solicitação de frota spot

Use o comando describe-tags para visualizar as tags para o recurso especificado. No exemplo a seguir, você descreve as tags da solicitação de frota spot especificada.

```
aws ec2 describe-tags \
    --filters "Name=resource-id,Values=sfr-11112222-3333-4444-5555-66666EXAMPLE"
```

```
{
    "Tags": [
        {
            "Key": "Environment",
            "ResourceId": "sfr-11112222-3333-4444-5555-66666EXAMPLE",
            "ResourceType": "spot-fleet-request",
            "Value": "Production"
        },
        {
            "Key": "Another key",
            "ResourceId": "sfr-11112222-3333-4444-5555-66666EXAMPLE",
            "ResourceType": "spot-fleet-request",
            "Value": "Another value"
        }
    ]
}
```

Você também pode visualizar as tags de uma solicitação de frota spot descrevendo a solicitação de frota spot.

Use o comando describe-spot-fleet-requests para visualizar a configuração da solicitação de frota spot especificada, que inclui todas as tags especificadas para a solicitação de frota.

```
aws ec2 describe-spot-fleet-requests \
    --spot-fleet-request-ids sfr-11112222-3333-4444-5555-66666EXAMPLE
```

```
{
    "SpotFleetRequestConfigs": [
        {
            "ActivityStatus": "fulfilled",
            "CreateTime": "2020-02-13T02:49:19.709Z",
            "SpotFleetRequestConfig": {
                "AllocationStrategy": "capacityOptimized",
                "OnDemandAllocationStrategy": "lowestPrice",
                "ExcessCapacityTerminationPolicy": "Default",
```

```
                "FulfilledCapacity": 2.0,
                "OnDemandFulfilledCapacity": 0.0,
                "IamFleetRole": "arn:aws:iam::111122223333:role/aws-ec2-spot-fleet-
tagging-role",
                "LaunchSpecifications": [
                    {
                        "ImageId": "ami-0123456789EXAMPLE",
                        "InstanceType": "c4.large"
                    }
                ],
                "TargetCapacity": 2,
                "OnDemandTargetCapacity": 0,
                "Type": "maintain",
                "ReplaceUnhealthyInstances": false,
                "InstanceInterruptionBehavior": "terminate"
            },
            "SpotFleetRequestId": "sfr-11112222-3333-4444-5555-66666EXAMPLE",
            "SpotFleetRequestState": "active",
            "Tags": [
                {
                    "Key": "Environment",
                    "Value": "Production"
                },
                {
                    "Key": "Another key",
                    "Value": "Another value"
                }
            ]
        }
    ]
}
```

Descrever uma solicitação de frota spot, suas instâncias e o histórico de eventos

É possível descrever a configuração, as instâncias e o histórico de eventos da frota spot.

Console

Para descrever sua frota spot

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

2. No painel de navegação, selecione Solicitações spot.
3. Selecione sua solicitação de frota spot. O ID começa com sfr-. Para ver os detalhes da configuração, escolha Description (Descrição).
4. Para listar as instâncias spot para a frota spot, escolha Instances (Instâncias).
5. Para visualizar o histórico da frota spot, escolha a guia History (Histórico).

AWS CLI

Para descrever sua solicitação de frota spot

Use o comando describe-spot-fleet-requests.

```
aws ec2 describe-spot-fleet-requests \
    --spot-fleet-request-ids sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE
```

Para descrever as instâncias em execução da frota spot especificada

Use o comando describe-spot-fleet-instances.

```
aws ec2 describe-spot-fleet-instances \
    --spot-fleet-request-id sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE
```

Para descrever o histórico de eventos da solicitação de frota spot especificada

Use o comando describe-spot-fleet-request-history.

```
aws ec2 describe-spot-fleet-request-history \
    --spot-fleet-request-id sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
    --start-time 2024-05-18T00:00:00Z
```

PowerShell

Para descrever sua solicitação de frota spot

Use o cmdlet Get-EC2SpotFleetRequest.

```
Get-EC2SpotFleetRequest
```

Para descrever as instâncias em execução da frota spot especificada

Use o cmdlet Get-EC2SpotFleetInstance.

```
Get-EC2SpotFleetInstance `
    -SpotFleetRequestId "sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE"
```

Para descrever o histórico de eventos da solicitação de frota spot especificada

Use o cmdlet Get-EC2SpotFleetRequestHistory.

```
Get-EC2SpotFleetRequestHistory `
    -SpotFleetRequestId "sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE" `
    -UtcStartTime 2024-05-18T00:00:00Z
```

Modificar uma solicitação de frota spot

É possível modificar uma solicitação de frota spot ativa para executar as seguintes tarefas:

- Aumentar a capacidade total de destino e a parte sob demanda
- Diminuir a capacidade total de destino e a parte sob demanda

Quando você aumenta a capacidade total de destino, a frota spot inicializa as instâncias spot adicionais de acordo com a estratégia de alocação da solicitação de frota spot. Quando você aumenta a parte sob demanda, a frota spot inicia Instâncias sob demanda adicionais.

Quando você diminui a capacidade total de destino, a frota spot cancela as solicitações abertas que excedem a nova capacidade de destino. É possível solicitar que a frota spot encerre instâncias spot até o tamanho da frota atingir a nova capacidade pretendida. Se a estratégia de alocação for `diversified`, a frota spot encerrará as instâncias nos grupos. Como alternativa, você pode solicitar que a frota spot mantenha seu tamanho atual, mas não substitua as instâncias spot interrompidas ou encerradas manualmente.

Considerações

- Você não pode modificar uma solicitação única de frota spot. É possível modificar uma solicitação de frota spot ao selecionar a opção Maintain target capacity (Manter capacidade de destino) ao criar a solicitação de frota spot.
- Quando uma frota spot encerra uma instância porque a capacidade pretendida foi diminuída, a instância recebe um aviso de interrupção de instância spot.

Console

Para modificar uma solicitação de frota spot

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Solicitações spot.
3. Selecione sua solicitação de frota spot.
4. Escolha Actions (Ações) e Modify target capacity (Modificar capacidade de destino).
5. Em Modify target capacity (Modificar capacidade de destino), faça o seguinte:
   a. Insira a nova capacidade de destino e a porção sob demanda
   b. (Opcional) Se você estiver reduzindo a capacidade de destino, mas deseja manter a frota no tamanho atual, desmarque Terminate instances (Encerrar instâncias).
   c. Selecione Enviar.

AWS CLI

Para modificar uma solicitação de frota spot

Use o comando modify-spot-fleet- request para atualizar a capacidade pretendida da solicitação de frota spot especificada.

```
aws ec2 modify-spot-fleet-request \
    --spot-fleet-request-id sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
    --target-capacity 20
```

É possível 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-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
    --target-capacity 10 \
    --excess-capacity-termination-policy NoTermination
```

PowerShell

Para modificar uma solicitação de frota spot

Use o cmdlet Edit-EC2SpotFleetRequest para atualizar a capacidade de destino da solicitação de frota spot especificada.

```
Edit-EC2SpotFleetRequest `
    -SpotFleetRequestId "sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE" `
    -TargetCapacity 20
```

É possível modificar o comando anterior da seguinte forma para diminuir a capacidade de destino da frota spot especificada sem encerrar instâncias spot como resultado.

```
Edit-EC2SpotFleetRequest `
    -SpotFleetRequestId "sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE" `
    -TargetCapacity 20 `
    -ExcessCapacityTerminationPolicy "NoTermination"
```

Cancelar (excluir) uma solicitação de frota spot

Caso não precise mais de uma frota spot, você cancelar a solicitação da frota spot, o que exclui a solicitação. Depois que você cancela uma solicitação de frota spot todas as solicitações spot associadas à frota são canceladas, para que nenhuma nova instância spot seja iniciada.

Ao canelar uma frota spot, você deve especificar se deseja encerrar todas as suas instâncias. Isso inclui tanto instâncias sob demanda quanto instâncias spot.

> **Warning**
>
> O encerramento de uma instância é permanente e irreversível.
> Depois de encerrar uma instância, não será mais possível se conectar a ela e ela não poderá ser recuperada. Todos os volumes anexados do Amazon EBS configurados para serem excluídos no encerramento também serão excluídos permanentemente e não poderão ser recuperados. Todos os dados armazenados em volumes de armazenamento de instância serão perdidos permanentemente. Para obter mais informações, consulte Como funciona o encerramento de uma instância.
> Antes de encerrar uma instância, certifique-se de ter feito backup de todos os dados que você precise reter após o encerramento no armazenamento persistente.

Se você especificar que as instâncias deverão ser encerradas quando a frota for cancelada, a frota entrará no estado `cancelled_terminating`. Caso contrário, ela entrará no estado `cancelled_running` e as instâncias continuarão em execução até que sejam interrompidas ou encerradas manualmente.

Restrições

- É possível cancelar até cem frotas com uma única solicitação. Se você exceder o número especificado, nenhuma frota será cancelada.

Console

Para cancelar (excluir) uma solicitação de frota spot

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Solicitações spot.
3. Selecione sua solicitação de frota spot.
4. Escolha Ações, Cancelar solicitação.
5. Na caixa de diálogo Adicionar regiões para replicação, faça o seguinte:
   a. Para encerrar as instâncias associadas ao mesmo tempo que cancela a solicitação de frota spot, deixe a caixa de seleção Encerrar instâncias marcada. Para cancelar a solicitação de frota spot sem encerar as instâncias associadas, desmarque a caixa de seleção Encerrar instâncias.
   b. Escolha Confirmar.

AWS CLI

Para cancelar (excluir) uma solicitação de frota spot e encerrar suas instâncias

Use o comando cancel-spot-fleet-requests com a opção `--terminate-instances`.

```
aws ec2 cancel-spot-fleet-requests \
    --spot-fleet-request-ids sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
    --terminate-instances
```

O seguinte é um exemplo de saída.

```
{
    "SuccessfulFleetRequests": [
        {
            "SpotFleetRequestId": "sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE",
            "CurrentSpotFleetRequestState": "cancelled_terminating",
            "PreviousSpotFleetRequestState": "active"
        }
    ],
    "UnsuccessfulFleetRequests": []
}
```

Para cancelar (excluir) uma solicitação de frota spot sem encerrar suas instâncias

Modifique o exemplo anterior usando a opção `--no-terminate-instances`.

```
aws ec2 cancel-spot-fleet-requests \
    --spot-fleet-request-ids sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
    --no-terminate-instances
```

O seguinte é um exemplo de saída.

```
{
    "SuccessfulFleetRequests": [
        {
            "SpotFleetRequestId": "sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE",
            "CurrentSpotFleetRequestState": "cancelled_running",
            "PreviousSpotFleetRequestState": "active"
        }
    ],
    "UnsuccessfulFleetRequests": []
}
```

PowerShell

Para cancelar (excluir) uma solicitação de frota spot e encerrar suas instâncias

Use o cmdlet Stop-EC2SpotFleetRequest com o parâmetro `-TerminateInstance`.

```
Stop-EC2SpotFleetRequest `
    -SpotFleetRequestId "sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE" `
    -TerminateInstance $true
```

Para cancelar (excluir) uma solicitação de frota spot sem encerrar suas instâncias

Modifique o exemplo anterior alterando o valor do parâmetro `-TerminateInstance`.

```
Stop-EC2SpotFleetRequest `
    -SpotFleetRequestId "sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE" `
    -TerminateInstance $false
```

Saiba mais sobre escalabilidade automática para frota spot

A escalabilidade automática permite que a frota spot aumente ou diminua sua capacidade com base na demanda. Com escalabilidade automática, uma frota spot pode executar instâncias (aumentar a escala horizontalmente) ou encerrar instâncias (reduzir a escala horizontalmente) no intervalo especificado, em resposta a uma ou mais políticas de escalabilidade.

A escalabilidade automática para frota spot é possível por uma combinação das APIs do Amazon EC2, do Amazon CloudWatch e do Application Auto Scaling. As solicitações de frota spot são criadas com o Amazon EC2, os alarmes são criados com o CloudWatch e as políticas de escalabilidade são criadas com o Application Auto Scaling.

Tipos de escalabilidade automática

A frota spot oferece suporte aos seguintes tipos de escalabilidade automática:

- Escalabilidade de rastreamento de destino: aumenta ou reduz a capacidade atual da frota com base em um valor pretendido para uma métrica específica. Isso é semelhante à forma como o termostato mantém a temperatura da sua casa, ou seja, você seleciona a temperatura desejada e o termostato faz o resto.
- Escalabilidade em etapas: aumenta ou diminui a capacidade atual da frota com base em um conjunto de ajustes de escalabilidade, conhecidos como ajustes em etapas, que variam com base no tamanho da ruptura do alarme.
- Escalabilidade programado: aumenta ou diminui a capacidade atual da frota com base em data e hora.

Considerações

Ao usar a escalabilidade automática para sua frota spot, considere o seguinte:

- Ponderação de instância: se estiver usando ponderação 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.
- Período de espera: as políticas de escalabilidade que você cria para a frota spot são compatíveis com um período de espera. Esse é o número de segundos após o encerramento de uma ação de escalabilidade em que as atividades de escalabilidade anteriores, relacionadas ao acionamento, podem influenciar eventos futuros de escalabilidade. Para expandir as políticas enquanto o período do desaquecimento estiver em vigor, a capacidade que foi adicionada pelo evento de expansão anterior que iniciou o desaquecimento é calculada como parte da capacidade desejada para a expansão seguinte. A intenção é expandir de forma contínua (mas não excessivamente). Para políticas de redução, o período do desaquecimento é utilizado para bloquear a escala subsequente nas solicitações até que expire. A intenção é reduzir de forma conservadora para proteger a disponibilidade de sua aplicação. Contudo, se outro alarme acionar uma política de expansão durante o período do desaquecimento após uma redução, a escalabilidade automática expandirá seu destino dimensionável imediatamente.
- Usar monitoramento detalhado: recomendamos que você escale com base nas métricas da instância com intervalos de um minuto, pois isso garante uma resposta mais rápida às mudanças de utilização. Aumentar a escalabilidade com base em métricas com intervalos de cinco minutos pode resultar em tempo de resposta mais lento e na escalabilidade com base em dados de métricas obsoletos. Para enviar dados de métrica das instâncias ao CloudWatch em períodos de 1 minuto, você deve habilitar especificamente o monitoramento detalhado. Para obter mais informações, consulte Gerenciar o monitoramento detalhado das instâncias do Amazon EC2 e Criar uma solicitação de frota spot usando parâmetros definidos.

- AWS CLI: caso use a AWS CLI para configurar o escalabilidade da frota spot, você usará o application-autoscaling.

Permissões do IAM obrigatórias para escalabilidade automática de frota spot

A escalabilidade automática para frota spot é possível por uma combinação das APIs do Amazon EC2, do Amazon CloudWatch e do Application Auto Scaling. As solicitações de frota spot são criadas com o Amazon EC2, os alarmes são criados com o CloudWatch e as políticas de escalabilidade são criadas com o Application Auto Scaling. Além das permissões do IAM obrigatórias para usar a frota spot e do Amazon EC2, o usuário que acessa as configurações de escalabilidade de frota deve ter as permissões adequadas para os serviços compatíveis com escalabilidade automática.

Para usar escalabilidade automática para frota spot, os usuários também precisam ter permissões para usar as ações na política de exemplo a seguir.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "application-autoscaling:*",
                "ec2:DescribeSpotFleetRequests",
                "ec2:ModifySpotFleetRequest",
                "cloudwatch:DeleteAlarms",
                "cloudwatch:DescribeAlarmHistory",
                "cloudwatch:DescribeAlarms",
                "cloudwatch:DescribeAlarmsForMetric",
                "cloudwatch:GetMetricStatistics",
                "cloudwatch:ListMetrics",
                "cloudwatch:PutMetricAlarm",
                "cloudwatch:DisableAlarmActions",
                "cloudwatch:EnableAlarmActions",
                "iam:CreateServiceLinkedRole",
                "sns:CreateTopic",
                "sns:Subscribe",
                "sns:Get*",
                "sns:List*"
            ],
```

```
            "Resource": "*"
        }
    ]
}
```

Também é possível criar suas próprias políticas do IAM que permitem permissões mais refinadas para chamadas à API do Application Auto Scaling. Para obter mais informações, consulte Identity and Access Management for Application Auto Scaling no Guia do usuário do Application Auto Scaling.

O serviço do Application Auto Scaling também precisa de permissão para descrever a frota spot e os alarmes do CloudWatch, além de permissões para modificar a capacidade de destino da frota spot em seu nome. Se você habilitar a escalabilidade automática para a frota spot, ela criará uma função vinculada ao serviço chamada `AWSServiceRoleForApplicationAutoScaling_EC2SpotFleetRequest`. Essa função vinculada ao serviço concede ao Application Auto Scaling permissão para descrever os alarmes das políticas, monitorar a capacidade atual da frota e modificar a capacidade da frota. A função de frota spot gerenciada original para o Application Auto Scaling era `aws-ec2-spot-fleet-autoscale-role`, mas ela não é mais necessária. Essa função vinculada ao serviço é a função padrão do Application Auto Scaling. Para ter mais informações, consulte Funções vinculadas a serviço do Application Auto Scaling, no Guia do usuário do Application Auto Scaling.

Escalabilidade de rastreamento de destino: escalar a frota spot definindo um valor para uma métrica específica

Com a escalabilidade de rastreamento de destino, você cria uma política de escalabilidade de rastreamento de destino ao selecionar uma métrica e definir um valor pretendido. A frota spot cria e gerencia os alarmes do CloudWatch que acionam a política de escalabilidade e calcula o ajuste de escalabilidade com base na métrica escolhida e no valor de destino. A política de escalabilidade ajusta a capacidade ao adicionar ou remover instâncias conforme necessário para manter a métrica no valor de destino especificado ou próxima a ele. Uma política de escalabilidade de rastreamento de destino não apenas mantém a métrica próxima do valor de destino, mas também se ajusta às flutuações na métrica devido a um padrão de carga de flutuação e minimiza as flutuações rápidas na capacidade.

É possível criar várias políticas de escalabilidade de rastreamento de destino para uma frota spot, desde que cada uma delas use uma métrica diferente. A frota escala com base na política que

especifica a maior capacidade da frota. Isso permite que você inclua vários cenários para garantir capacidade suficiente para suas workloads de aplicações.

Para garantir a disponibilidade da aplicação, a frota se expande proporcionalmente à métrica o mais rápido possível, mas se retrai gradualmente.

Quando uma frota spot encerra uma instância spot porque a capacidade pretendida foi reduzida, a instância recebe um aviso de interrupção de instância spot.

> **Note**
>
> Não edite ou exclua os alarmes do CloudWatch que a frota spot gerencia para uma política de dimensionamento com monitoramento do objetivo. A frota spot exclui os alarmes automaticamente quando você exclui a política de dimensionamento com monitoramento do objetivo.

Pré-requisitos

- A solicitação de frota spot deve ter o tipo de solicitação `maintain`. A escalação automática não é compatível com solicitações do tipo `request`.
- Configurar a Permissões do IAM obrigatórias para escalabilidade automática de frota spot.
- Revise as Considerações.

Para configurar uma política de rastreamento de destino

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Solicitações spot.
3. Selecione sua solicitação de frota spot.
4. Escolha a guia Ajuste de escala automático próxima à parte inferior da tela. Se você selecionou o link para sua frota spot, não há guia; em vez disso, role para baixo até a seção Ajuste de escala automático.
5. Se a escalabilidade automática não estiver configurada, escolha Configurar.
6. 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.
7. Em Policy Name (Nome da política), digite um nome para a política.

8. Escolha uma Target metric.
9. Digite um Target value (Valor de destino) para a métrica.
10. Em Período de esfriamento, especifique um novo valor (em segundos) ou mantenha o padrão.
11. (Opcional) Para omitir a criação de uma política de redução de escala na horizontal baseada na configuração atual, selecione Desabilitar redução de escala na horizontal. É possível criar uma política de redução de escala na horizontal usando uma configuração diferente.
12. Escolha Save (Salvar).

Para configurar uma política de rastreamento de destino usando a AWS CLI

1. Registre a solicitação de frota spot como um destino escalável usando o comando register-scalable-target.
2. Crie uma política de escalabilidade usando o comando put-scaling-policy.

Escalabilidade em etapas: escalar a 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 spot porque a capacidade pretendida foi reduzida, a instância recebe um aviso de interrupção de instância spot.

Pré-requisitos

- A solicitação de frota spot deve ter o tipo de solicitação `maintain`. A escalação automática não é compatível com solicitações do tipo `request`.
- Configurar a Permissões do IAM obrigatórias para escalabilidade automática de frota spot.
- Considere quais métricas do CloudWatch são importantes para sua aplicação. É possível criar alarmes do CloudWatch com base nas métricas fornecidas pela AWS ou nas suas próprias métricas personalizadas.
- Para as métricas da AWS que você usará em suas políticas de escalabilidade, habilite a coleta das métricas do CloudWatch se o serviço que fornece as métricas não for habilitado por padrão.
- Revise as Considerações.

Criar um alarme do CloudWatch

1. Abra o console do CloudWatch em https://console.aws.amazon.com/cloudwatch/.
2. No painel de navegação, expanda Alarmes e escolha Todos os alarmes.
3. Selecione Create alarm (Criar alarme).
4. Na página Specify metric and conditions (Especificar métrica e condições), selecione Select metric (Selecionar métrica).
5. Escolha Spot do EC2, Métricas de solicitação de frota e então uma métrica (por exemplo, TargetCapacity). Depois escolha Selecionar métrica.

   A página Specify metric and conditions (Especificar métrica e condições) será exibida, mostrando um gráfico e outras informações sobre a métrica selecionada.
6. Em Período, escolha o período de avaliação para o alarme, por exemplo, 1 minuto. Ao avaliar o alarme, todos os períodos são agregados em um único ponto de dados.

> **Note**
>
> Um período mais curto cria um alarme mais sensível.

7. Em Conditions (Condições), defina o alarme definindo a condição do limite. Por exemplo, é possível definir um limite para acionar o alarme sempre que o valor da métrica for maior que ou igual a 80%.
8. Em Additional configuration (Configuração adicional), para Datapoints to alarm (Pontos de dados para alarme), especifique quantos pontos de dados (períodos de avaliação) devem estar no estado ALARM para acionar o alarme, por exemplo, 1 período de avaliação para 2 de 3 períodos de avaliação. Isso cria um alarme que passará para o estado ALARM se houver violação de muitos períodos consecutivos. Para obter mais informações, consulte Avaliar um alarme no Guia do usuário do Amazon CloudWatch.
9. Para Missing data treatment (Tratamento de dados ausentes), selecione uma das opções (ou mantenha o padrão como Treat missing data as missing (Tratar dados ausentes como ausentes)). Para obter mais informações, consulte Configuração da forma como os alarmes do CloudWatch tratam dados ausentes no Manual do usuário do Amazon CloudWatch.
10. Escolha Next (Próximo).
11. (Opcional) Para receber notificações de um evento de dimensionamento, para Notification (Notificação), é possível escolher ou criar o tópico do Amazon SNS que você deseja usar para receber notificações. Caso contrário, será possível excluir a notificação agora e adicionar uma posteriormente, quando necessário.
12. Escolha Próximo.
13. Em Adicionar nome e descrição, insira um nome e uma descrição para o alarme e selecione Próximo.
14. Selecione Criar alarme.

Para configurar uma política de escalabilidade para a frota spot

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Solicitações spot.
3. Selecione sua solicitação de frota spot.

4. Escolha a guia Ajuste de escala automático próxima à parte inferior da tela. Se você selecionou o link para sua frota spot, não há guia; em vez disso, role para baixo até a seção Ajuste de escala automático.
5. Se a escalabilidade automática não estiver configurada, escolha Configurar.
6. Use Escalar capacidade entre para definir a capacidade mínima e máxima para sua frota. As políticas de ajuste de escala não escalam a frota abaixo da capacidade mínima ou acima da capacidade máxima.
7. Em Políticas de escalabilidade, para Tipo de política, escolha Política escalabilidade em etapas.
8. Inicialmente, a opção Políticas de escalação contêm políticas de escalação gradual denominadas ScaleUp e ScaleDown. É possível completar essas políticas ou escolher Remover política para excluí-las. Você também pode escolher Add policy (Adicionar política).
9. Para definir a política, faça o seguinte:

    a. Em Policy Name (Nome da política), digite um nome para a política.

    b. Em Gatilho de política, selecione um alarme existente ou escolha Criar alarme para abrir o console do Amazon CloudWatch e criar um.

    c. Em Modificar capacidade, defina a quantidade do ajuste de escala e os limites inferior e superior do ajuste da etapa. É possível adicionar ou remover um número específico de instâncias ou uma porcentagem do tamanho da frota atual ou definir a frota para um tamanho exato.

    Por exemplo, para criar uma política de escalabilidade em etapas que aumente a capacidade da frota em 30%, escolha Adicionar, insira 30 no próximo campo e escolha porcento. Por padrão, o limite inferior de uma política de adição é o limite do alarme e o limite superior é mais (+) infinito. Por padrão, o limite superior de uma política de remoção é o limite do alarme e o limite inferior é menos (-) infinito.

    d. (Opcional) Para adicionar outra etapa, escolha Adicionar etapa.

    e. Em Período de esfriamento, especifique um novo valor (em segundos) ou mantenha o padrão.
10. 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 escalável 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.

Escalabilidade programada: escalar a frota spot de acordo com uma programação

A escalabilidade da frota com base em uma programação permite que você escale sua aplicação em resposta a alterações previsíveis na demanda. Ao criar ações programadas, você pode instruir a frota spot a executar atividades de escalabilidade em momentos específicos. Ao criar uma ação programada, você deve especificar uma frota spot existente, a hora em que a atividade de escalabilidade deve ocorrer e a capacidade mínima e máxima desejada. As ações agendadas podem ser configuradas para escalar uma vez ou em uma programação recorrente. Caso precise fazer alterações, você pode editar ou excluir ações programadas.

Pré-requisitos

- As ações programadas somente podem ser criadas para as frotas spot existentes. Você não pode criar uma ação programada ao criar uma frota spot.
- A solicitação de frota spot deve ter o tipo de solicitação `maintain`. A escalação automática não é compatível com solicitações do tipo `request`.
- Configurar a Permissões do IAM obrigatórias para escalabilidade automática de frota spot.
- Revise as Considerações.

Para criar uma única ação programada

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Solicitações spot.
3. Selecione sua solicitação de frota spot.
4. Escolha a guia Escalabilidade programada próxima à parte inferior da tela. Caso tenha selecionado o link para sua frota spot, não há guia; em vez disso, role para baixo até a seção Escalabilidade programada.
5. Escolha Criar ação programada.
6. Em Name (Nome), especifique um nome para a ação programada.
7. Insira um valor para Minimum capacity (Capacidade mínima), Maximum capacity (Capacidade máxima), ou ambos.
8. Em Recurrence (Recorrência), escolha Once (Uma vez).

9. (Opcional) Escolha uma data e hora para Start time (Hora de início), End time (Hora de término), ou ambos.
10. Escolha Criar.

Para criar uma ação programada recorrente

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Solicitações spot.
3. Selecione sua solicitação de frota spot.
4. Escolha a guia Escalabilidade programada próxima à parte inferior da tela. Caso tenha selecionado o link para sua frota spot, não há guia; em vez disso, role para baixo até a seção Escalabilidade programada.
5. Em Name (Nome), especifique um nome para a ação programada.
6. Insira um valor para Minimum capacity (Capacidade mínima), Maximum capacity (Capacidade máxima), ou ambos.
7. Em Recurrence (Recorrência), escolha 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 Cron expressions no Guia do usuário do Amazon EventBridge.
8. (Opcional) Escolha uma data e hora para Start time (Hora de início), End time (Hora de término), ou ambos.
9. Selecione Enviar.

Para editar uma ação programada

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Solicitações spot.
3. Selecione sua solicitação de frota spot.
4. Escolha a guia Escalabilidade programada próxima à parte inferior da tela. Caso tenha selecionado o link para sua frota spot, não há guia; em vez disso, role para baixo até a seção Escalabilidade programada.
5. Selecione a ação programada e escolha Actions (Ações), Edit (Editar).
6. Faça as alterações necessárias e escolha Submit (Enviar).

Para excluir uma ação programada

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Solicitações spot.
3. Selecione sua solicitação de frota spot.
4. Escolha a guia Escalabilidade programada próxima à parte inferior da tela. Caso tenha selecionado o link para sua frota spot, não há guia; em vez disso, role para baixo até a seção Escalabilidade programada.
5. Selecione a ação programada e escolha Actions (Ações), Delete (Excluir).
6. Quando a confirmação for solicitada, escolha Excluir.

Para gerenciar a escalabilidade programada usando o AWS CLI

Use os seguintes comandos:

- put-scheduled-action
- describe-scheduled-actions
- delete-scheduled-action

Monitorar o EC2 Fleet ou a frota spot

O monitoramento eficaz do EC2 Fleet ou da frota spot é essencial para manter a performance ideal e garantir a confiabilidade. Há várias ferramentas para ajudar você a conseguir isso, incluindo o Amazon CloudWatch e o Amazon EventBridge, que são abordados neste tópico.

Com o CloudWatch, você pode coletar e rastrear métricas, definir alarmes e reagir automaticamente a alterações no status da frota.

Com o EventBridge, você pode monitorar e responder de forma programática aos eventos emitidos pela sua frota. Ao definir regras no EventBridge, você pode automatizar respostas a eventos específicos da frota, como encerramento de instâncias ou mudanças no estado da frota, melhorando sua eficiência operacional.

Tópicos

- Monitorar a frota do EC2 ou frota spot usando o CloudWatch

- Monitorar e responder de forma programática aos eventos emitidos pelo EC2 Fleet ou pela frota spot usando o Amazon EventBridge

Monitorar a frota do EC2 ou frota spot usando o CloudWatch

É possível monitorar a frota do EC2 ou a frota spot usando as métricas do Amazon CloudWatch descritas nesta seção.

> **Important**
>
> Para garantir uma precisão, recomendamos que você habilite o monitoramento detalhado para usar essas métricas. Para obter mais informações, consulte Gerenciar o monitoramento detalhado das instâncias do Amazon EC2.

Para obter mais informações sobre o uso de CloudWatch, consulte Monitorar instâncias usando o CloudWatch.

Métricas da frota do EC2 e da frota spot

O namespace `AWS/EC2Spot` inclui as métricas a seguir para a frota, além das métricas do CloudWatch para as instâncias spot na frota. Para obter mais informações, consulte Métricas de instância.

Métrica	Descrição
`AvailableInstancePoolsCount`	Os grupos de capacidade spot especificados na solicitação de frota. Unidades: contagem
`BidsSubmittedForCapacity`	A capacidade para a qual o Amazon EC2 enviou solicitações de frota. Unidades: contagem
`EligibleInstancePoolCount`	Os grupos de capacidade spot especificados na solicitação de frota em que o Amazon EC2 pode atender às solicitações. O Amazon EC2 não atende a solicitações em grupos

Métrica	Descrição
	nos quais o preço máximo que você está disposto a pagar por instâncias spot é menor que o preço spot ou o preço spot é maior que o preço das instâncias sob demanda. Unidades: contagem
`FulfilledCapacity`	A capacidade preenchida pelo Amazon EC2. Unidades: contagem
`MaxPercentCapacityAllocation`	O valor máximo de `PercentCapacityAllocation` em todos os grupos de frota spot especificados na solicitação de frota. Unidades: percentual
`PendingCapacity`	A diferença entre `TargetCapacity` e `FulfilledCapacity`. Unidades: contagem
`PercentCapacityAllocation`	A capacidade alocada para o grupo de capacidade spot para as dimensões especificadas. Para obter o valor máximo registrado em todos os grupos de capacidade spot, use `MaxPercentCapacityAllocation`. Unidades: percentual
`TargetCapacity`	A capacidade de destino da solicitação de frota. Unidades: contagem
`TerminatingCapacity`	A capacidade que está sendo encerrada, pois a capacidade provisionada é maior que a capacidade de destino. Unidades: contagem

Se a unidade de medida para uma métrica é `Count`, a estatística mais útil é `Average`.

Dimensões da frota do EC2 e da frota spot

Para filtrar os dados da frota, use as dimensões a seguir.

Dimensões	Descrição
`AvailabilityZone`	Filtre os dados por zona de disponibilidade.
`FleetRequestId`	Filtre os dados por solicitação de frota.
`InstanceType`	Filtre os dados por tipo de instância.

Visualizar as métricas do CloudWatch para a frota do EC2 ou a frota spot

É possível visualizar as métricas do CloudWatch para a 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 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 visualizar todas as métricas da frota ou grupos de métricas da frota pelo ID de solicitação da frota, tipo de instância ou zona de disponibilidade.

Visualizar métricas da frota

1. Abra o console do CloudWatch, em https://console.aws.amazon.com/cloudwatch/.
2. No painel de navegação, expanda Métricas e escolha Todas as métricas.
3. Escolha o namespace do EC2 Spot.

> **Note**
>
> Se o namespace do EC2 Spot não for exibido, há dois motivos para isso. Você nunca usou a frota do EC2 ou a frota spot na região. Somente os serviços da AWS em uso enviam métricas para o Amazon CloudWatch. Ou então, se você tiver usado a frota do EC2 ou a frota spot na região, mas não nas últimas duas semanas, o namespace não será exibido.

4. Para filtrar as métricas por dimensão, selecione uma das seguintes opções:

- Métricas de solicitação da frota: agrupar por solicitação de frota
- Por zona de disponibilidade: agrupar por solicitação de frota e zona de disponibilidade
- Por tipo de instância: agrupar por solicitação de frota e tipo de instância
- Por zona de disponibilidade/tipo de instância: agrupar por solicitação de frota, zona de disponibilidade e tipo de instância

5. Para visualizar os dados de uma métrica, marque a caixa de seleção ao lado da métrica.

Monitorar e responder de forma programática aos eventos emitidos pelo EC2 Fleet ou pela frota spot usando o Amazon EventBridge

Quando o estado de um EC2 Fleet ou frota spot é alterado, é emitida uma notificação. A notificação é disponibilizada como um evento que é enviado para Amazon EventBridge (anteriormente conhecido como Amazon CloudWatch Events). Os eventos são emitidos com base no melhor esforço.

É possível usar o Amazon EventBridge para criar regras que acionem ações programáticas em resposta a um evento. Por exemplo, você pode criar duas regras do EventBridge: uma acionada quando um estado da frota muda e outra acionada quando uma instância na frota é encerrada. Neste exemplo, você pode configurar a primeira regra para que, se o estado da frota for alterado, a regra invoque um tópico do SNS, enviando uma notificação por e-mail para você. É possível configurar a segunda regra para que, se uma instância na frota for encerrada, a regra invoque uma função do Lambda para executar uma nova instância.

> **Note**
>
> Apenas frotas do tipo `maintain` e `request` emitem eventos. As frotas do tipo `instant` não emitem eventos porque enviam solicitações únicas síncronas e o estado da frota é conhecido imediatamente na resposta. Para usar o Amazon EventBridge para monitorar eventos da frota, o tipo de solicitação deve ser `maintain` ou `request`.

Para obter instruções sobre como descrever o histórico de eventos de uma frota, consulte Descrever o histórico de eventos para o EC2 Fleet.

Tópicos

- Criar regras do Amazon EventBridge para monitorar eventos do EC2 Fleet ou da frota spot

- Tipos de evento de Frota do EC2
- Tipos de evento de frota spot

Criar regras do Amazon EventBridge para monitorar eventos do EC2 Fleet ou da frota spot

Quando uma notificação de alteração de estado é emitida para um EC2 Fleet ou frota spot, ela é enviada como um evento para o Amazon EventBridge como um arquivo JSON. Se o EventBridge detectar um padrão de evento que corresponda a um padrão definido em uma regra, o EventBridge invocará um destino (ou destinos) especificado(s) na regra.

É possível escrever regras do EventBridge para automatizar ações com base em padrões de eventos correspondentes.

Os seguintes campos no evento formam o padrão de evento que está definido na regra:

`"source": "aws.ec2fleet"`

Identifica que o evento é de Frota do EC2.

`"detail-type": "EC2 Fleet State Change"`

Identifica o tipo de evento.

`"detail": { "sub-type": "submitted" }`

Identifica o subtipo de evento.

Para obter a lista de eventos do EC2 Fleet e da frota spot e dados de eventos de exemplo, consulte Tipos de evento de Frota do EC2 e Tipos de evento de frota spot.

Exemplos

- Criar uma regra de EventBridge para enviar uma notificação
- Criar uma regra de EventBridge para acionar uma função do Lambda

Criar uma regra de EventBridge para enviar uma notificação

O exemplo a seguir cria uma regra de EventBridge para enviar um e-mail, mensagem de texto ou notificação por push móvel sempre que o Amazon EC2 emite uma notificação de Frota do EC2. O

sinal neste exemplo é emitido como um evento de `EC2 Fleet State Change`, que aciona a ação definida pela regra.

Pré-requisito

Antes de criar a regra EventBridge, você deve criar o tópico do Amazon SNS para e-mail, mensagem de texto ou notificação por push móvel.

Para criar uma regra de EventBridge para enviar uma notificação quando um estado de Frota do EC2 muda

1. Abra o console do Amazon EventBridge em https://console.aws.amazon.com/events/.
2. Selecione Criar regra.
3. Em Define rule detail (Definir detalhe da regra), faça o seguinte:
   a. Informe um Name (Nome) para a regra e, opcionalmente, uma descrição.

      Uma regra não pode ter o mesmo nome que outra regra na mesma região e no mesmo barramento de eventos.
   b. Em Event Bus (Barramento de eventos), escolha default (padrão). Quando um serviço da AWS em sua conta gerar um evento, ele sempre irá para o barramento de eventos padrão da sua conta.
   c. Em Rule type (Tipo de regra), escolha Rule with an event pattern (Regra com um padrão de evento).
   d. Escolha Próximo.
4. Em Build event pattern (Criar padrão de evento), faça o seguinte:
   a. Em Event source (Origem do evento), escolha Eventos da AWS ou eventos de parceiro do EventBridge.
   b. Em Event pattern (Padrão de evento), nesse exemplo, você especificará o seguinte padrão de evento para corresponder ao evento `EC2 Fleet Instance Change`.

```
{
 "source": ["aws.ec2fleet"],
 "detail-type": ["EC2 Fleet Instance Change"]
}
```

Para adicionar o padrão de evento, é possível usar um modelo escolhendo Event pattern form (Formulário de padrão de evento), ou especifique seu próprio padrão escolhendo Custom pattern (JSON editor) (Padrão personalizado (editor JSON)), como segue:

i. Para usar um modelo para criar o padrão de evento, faça o seguinte:

A. Escolha Event pattern form (Formulário de evento).

B. Em Event source (Origem do evento), escolha AWS services (Serviços da).

C. Para Service (Serviço da AWS), escolha EC2 Fleet (Frota do EC2).

D. Em Event type (Tipo de evento), escolha EC2 Fleet Instance Change (Alteração da instância da frota do EC2).

E. Para personalizar o modelo, escolha Edit pattern (Editar padrão) e faça as alterações para corresponder ao padrão de evento de exemplo.

ii. (Alternativa) Para especificar um padrão de evento personalizado, faça o seguinte:

A. Escolha Custom pattern (JSON editor) (Padrão personalizado (editor JSON)).

B. Na caixa Event pattern (Padrão de evento), adicione o padrão de evento para este exemplo.

c. Escolha Próximo.

5. Em Select target(s) (Selecionar destino(s)), faça o seguinte:

a. Em Tipos de destino, escolha Serviço da AWS.

b. Em Select a target (Selecione um destino), escolha SNS topic (Tópico do SNS) para enviar um email, mensagem de texto ou notificação por push móvel quando o evento ocorrer.

c. Em Topic (Tópico), escolha um tópico existente. Para fazer isso, você precisa criar um tópico do Amazon SNS usando o console do Amazon SNS. Para obter mais informações, consulte Usar o Amazon SNS para mensagens de aplicação para pessoa (A2P) no Guia do desenvolvedor do Amazon Simple Notification Service.

d. (Opcional) Em Additional settings (Configurações adicionais), é possível, opcionalmente, definir configurações adicionais. Para obter mais informações, consulte Criar regras do Amazon EventBridge que reajam a eventos (etapa 16) no Guia do usuário do Amazon EventBridge.

e. Escolha Próximo.

6. (Opcional) Em Tags (Etiquetas), é possível atribuir, opcionalmente, uma ou mais etiquetas à sua regra e, em seguida, escolher Next (Próximo).

7. Em Review and create (Revisar e criar), faça o seguinte:

   a. Revise os detalhes da regra e modifique-os conforme necessário.

   b. Escolha Criar regra.

Para obter mais informações, consulte Amazon EventBridge rules (Regras do Amazon EventBridge) e Amazon EventBridge event patterns (Padrões de eventos do Amazon EventBridge) no Amazon EventBridge User Guide (Manual do usuário do Amazon EventBridge).

Criar uma regra de EventBridge para acionar uma função do Lambda

O exemplo a seguir cria uma regra de EventBridge para acionar uma função do Lambda toda vez que Amazon EC2 emite uma notificação de Frota do EC2. O sinal neste exemplo é emitido como um evento de `EC2 Fleet Instance Change`, subtipo `launched`, que aciona a ação definida pela regra.

Antes de criar a regra de EventBridge, você deve criar a função do Lambda.

Como criar a função do Lambda a ser usada na regra EventBridge

1. Abra o console do AWS Lambda em https://console.aws.amazon.com/lambda/.
2. Escolha Create function.
3. Digite um nome para sua função, configure o código e escolha Create function (Criar função).

   Para ter mais informações, consulte Criar sua primeira função do Lambda no Guia do desenvolvedor do AWS Lambda.

Para criar uma regra de EventBridge para acionar uma função do Lambda quando uma instância em um estado de Frota do EC2 muda

1. Abra o console do Amazon EventBridge em https://console.aws.amazon.com/events/.
2. Selecione Criar regra.
3. Em Define rule detail (Definir detalhe da regra), faça o seguinte:

   a. Informe um Name (Nome) para a regra e, opcionalmente, uma descrição.

      Uma regra não pode ter o mesmo nome que outra regra na mesma região e no mesmo barramento de eventos.

b. Em Event Bus (Barramento de eventos), escolha default (padrão). Quando um serviço da AWS em sua conta gerar um evento, ele sempre irá para o barramento de eventos padrão da sua conta.

c. Em Rule type (Tipo de regra), escolha Rule with an event pattern (Regra com um padrão de evento).

d. Escolha Próximo.

4. Em Build event pattern (Criar padrão de evento), faça o seguinte:

a. Em Event source (Origem do evento), escolha Eventos da AWS ou eventos de parceiro do EventBridge.

b. Em Event pattern (Padrão de evento) nesse exemplo, você especificará o seguinte padrão de evento para corresponder ao evento `EC2 Fleet Instance Change` e ao subtipo `launched`.

```
{
 "source": ["aws.ec2fleet"],
 "detail-type": ["EC2 Fleet Instance Change"],
 "detail": {
   "sub-type": ["launched"]
}
```

Para adicionar o padrão de evento, é possível usar um modelo escolhendo Event pattern form (Formulário de padrão de evento), ou especifique seu próprio padrão escolhendo Custom pattern (JSON editor) (Padrão personalizado (editor JSON)), como segue:

i. Para usar um modelo para criar o padrão de evento, faça o seguinte:

A. Escolha Event pattern form (Formulário de evento).

B. Em Event source (Origem do evento), escolha AWS services (Serviços da).

C. Para Service (Serviço da AWS), escolha EC2 Fleet (Frota do EC2).

D. Em Event type (Tipo de evento), escolha EC2 Fleet Instance Change (Alteração da instância da frota do EC2).

E. Selecione Edit pattern (Editar padrão) e adicione `"detail": {"sub-type": ["launched"]` para corresponder ao padrão do evento de exemplo. Para o formato JSON adequado, insira uma vírgula (`,`) após o colchete anterior (`]`).

ii. (Alternativa) Para especificar um padrão de evento personalizado, faça o seguinte:

A. Escolha Custom pattern (JSON editor) (Padrão personalizado (editor JSON)).

B. Na caixa Event pattern (Padrão de evento), adicione o padrão de evento para este exemplo.

c. Escolha Próximo.

5. Em Select target(s) (Selecionar destino(s)), faça o seguinte:

   a. Em Tipos de destino, escolha Serviço da AWS.

   b. Em Select a target (Selecione um destino), escolha SNS topic (Tópico do SNS) para enviar um email, mensagem de texto ou notificação por push móvel quando o evento ocorrer.

   c. Para Topic (Tópico), escolha a Lambda function (função Lambda) e, para Function (Função), escolha a função que você criou para responder quando o evento ocorrer.

   d. (Opcional) Em Additional settings (Configurações adicionais), é possível, opcionalmente, definir configurações adicionais. Para obter mais informações, consulte Criar regras do Amazon EventBridge que reajam a eventos (etapa 16) no Guia do usuário do Amazon EventBridge.

   e. Escolha Próximo.

6. (Opcional) Em Tags (Etiquetas), é possível atribuir, opcionalmente, uma ou mais etiquetas à sua regra e, em seguida, escolher Next (Próximo).

7. Em Review and create (Revisar e criar), faça o seguinte:

   a. Revise os detalhes da regra e modifique-os conforme necessário.

   b. Escolha Criar regra.

Para obter um tutorial sobre como criar uma função do Lambda e uma EventBridge regra que executa a função do Lambda, consulte Tutorial: Log the State of an Amazon EC2 Instance Using EventBridge (Tutorial: Registrar em log o estado de uma instância do Amazon EC2 usando o EventBridge) no AWS Lambda User Guide (Guia do usuário do Amazon EventBridge).

Tipos de evento de Frota do EC2

Existem cinco tipos de eventos de Frota do EC2. Para cada tipo de evento, existem vários subtipos.

Tipos de eventos

- Alteração do estado da EC2 Fleet
- Alteração da solicitação de instância spot da EC2 Fleet

- Alteração da instância da EC2 Fleet
- Informações da EC2 Fleet
- Erro de EC2 Fleet

Alteração do estado da EC2 Fleet

A Frota do EC2 envia um evento `EC2 Fleet State Change` para Amazon EventBridge quando um estado Frota do EC2 mudar.

A seguir estão dados de exemplo para esse evento.

```
{
    "version": "0",
    "id": "715ed6b3-b8fc-27fe-fad6-528c7b8bf8a2",
    "detail-type": "EC2 Fleet State Change",
    "source": "aws.ec2fleet",
    "account": "123456789012",
    "time": "2020-11-09T09:00:20Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:fleet/fleet-598fb973-87b7-422d-
be4d-6b0809bfff0a"
    ],
    "detail": {
        "sub-type": "active"
    }
}
```

Os possíveis valores para `sub-type` são:

`active`

A solicitação de Frota do EC2 foi validada e o Amazon EC2 está tentando manter o número de destino das instâncias em execução.

`deleted`

A solicitação de Frota do EC2 foi excluída, e não há outras instâncias em execução. A solicitação de Frota do EC2 foi excluída dois dias depois que as instâncias foram encerradas.

`deleted_running`

A solicitação de Frota do EC2 foi excluída e não executará instâncias adicionais. Suas instâncias existentes continuam sendo executadas até que sejam interrompidas ou encerradas. A solicitação permanece nesse estado até que todas as instâncias sejam interrompidas ou encerradas.

`deleted_terminating`

A solicitação de Frota do EC2 foi excluída, e as instâncias estão sendo encerradas. A solicitação permanece nesse estado até que todas as instâncias sejam encerradas.

`expired`

A solicitação de Frota do EC2 expirou. Se a solicitação tiver sido criada com conjunto `TerminateInstancesWithExpiration`, um evento `terminated` subsequente indicará que as instâncias estão encerradas.

`modify_in_progress`

A solicitação de Frota do EC2 está sendo modificada. A solicitação permanece nesse estado até que a modificação seja totalmente processada.

`modify_succeeded`

A solicitação de Frota do EC2 foi modificada.

`submitted`

A solicitação de Frota do EC2 está sendo avaliada, e o Amazon EC2 está se preparando para executar o número de destino de instâncias.

`progress`

A solicitação de Frota do EC2 está em processo de ser atendida.

Alteração da solicitação de instância spot da EC2 Fleet

A Frota do EC2 envia um evento de `EC2 Fleet Spot Instance Request Change` para Amazon EventBridge quando uma solicitação de Instância spot na frota muda de estado.

A seguir estão dados de exemplo para esse evento.

```
{
```

```
    "version": "0",
    "id": "19331f74-bf4b-a3dd-0f1b-ddb1422032b9",
    "detail-type": "EC2 Fleet Spot Instance Request Change",
    "source": "aws.ec2fleet",
    "account": "123456789012",
    "time": "2020-11-09T09:00:05Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:fleet/
fleet-83fd4e48-552a-40ef-9532-82a3acca5f10"
    ],
    "detail": {
        "spot-instance-request-id": "sir-rmqske6h",
        "description": "SpotInstanceRequestId sir-rmqske6h, PreviousState:
 cancelled_running",
        "sub-type": "cancelled"
    }
}
```

Os possíveis valores para `sub-type` são:

`active`

A solicitação de instância spot foi atendida e tem uma instância spot associada.

`cancelled`

Você cancelou a solicitação de instância spot ou a solicitação de instância spot expirou.

`disabled`

Você interrompeu a instância spot.

`submitted`

A solicitação de instância spot foi enviada.

Alteração da instância da EC2 Fleet

O Frota do EC2 envia um evento de `EC2 Fleet Instance Change` para Amazon EventBridge quando uma instância na frota muda de estado.

A seguir estão dados de exemplo para esse evento.

```
{
    "version": "0",
    "id": "542ce428-c8f1-0608-c015-e8ed6522c5bc",
    "detail-type": "EC2 Fleet Instance Change",
    "source": "aws.ec2fleet",
    "account": "123456789012",
    "time": "2020-11-09T09:00:23Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:fleet/fleet-598fb973-87b7-422d-
be4d-6b0809bfff0a"
    ],
    "detail": {
        "instance-id": "i-0c594155dd5ff1829",
        "description": "{\"instanceType\":\"c5.large\",\"image\":\"ami-6057e21a\",
\"productDescription\":\"Linux/UNIX\",\"availabilityZone\":\"us-east-1d\"}",
        "sub-type": "launched"
    }
}
```

Os possíveis valores para `sub-type` são:

`launched`

Uma nova instância foi executada.

`terminated`

A instância foi encerrada.

`termination_notified`

Uma notificação de encerramento de instância foi enviada quando uma instância spot foi encerrada pelo Amazon EC2 durante a redução da escala na vertical, quando a capacidade de destino da frota foi modificada para baixo, p. ex., de uma capacidade de destino de 4 para uma capacidade de destino de 3.

Informações da EC2 Fleet

A Frota do EC2 envia um evento de `EC2 Fleet Information` para Amazon EventBridge quando há um erro durante a execução. O evento informativo não impede a frota de tentar atender à sua capacidade de destino.

A seguir estão dados de exemplo para esse evento.

```
{
    "version": "0",
    "id": "76529817-d605-4571-7224-d36cc1b2c0c4",
    "detail-type": "EC2 Fleet Information",
    "source": "aws.ec2fleet",
    "account": "123456789012",
    "time": "2020-11-09T08:17:07Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:fleet/fleet-8becf5fe-
bb9e-415d-8f54-3fa5a8628b91"
    ],
    "detail": {
        "description": "c4.xlarge, ami-0947d2ba12ee1ff75, Linux/UNIX, us-east-1a,
 Spot price in either SpotFleetRequestConfigData or SpotFleetLaunchSpecification or
 LaunchTemplate or LaunchTemplateOverrides is less than Spot market price $0.0619",
        "sub-type": "launchSpecUnusable"
    }
}
```

Os possíveis valores para `sub-type` são:

`fleetProgressHalted`

O preço em cada especificação de execução não é válido porque está abaixo do preço spot (todas as especificações de execução produziram `launchSpecUnusable` eventos). Uma especificação de execução pode se tornar válida se o preço spot mudar.

`launchSpecTemporarilyBlacklisted`

A configuração não é válida e várias tentativas de executar instâncias falharam. Para obter mais informações, consulte a descrição do evento.

`launchSpecUnusable`

O preço em uma especificação de execução não é válido porque está abaixo do preço spot.

`registerWithLoadBalancersFailed`

Falha na tentativa de registrar instâncias com balanceadores de carga. Para obter mais informações, consulte a descrição do evento.

Erro de EC2 Fleet

A Frota do EC2 envia um evento de `EC2 Fleet Error` para Amazon EventBridge quando há um erro durante a execução. O evento de erro impede a frota de tentar atender à sua capacidade de destino.

A seguir estão dados de exemplo para esse evento.

```
{
    "version": "0",
    "id": "69849a22-6d0f-d4ce-602b-b47c1c98240e",
    "detail-type": "EC2 Fleet Error",
    "source": "aws.ec2fleet",
    "account": "123456789012",
    "time": "2020-10-07T01:44:24Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:fleet/fleet-9bb19bc6-60d3-4fd2-ae47-
d33e68eafa08"
    ],
    "detail": {
        "description": "m3.large, ami-00068cd7555f543d5, Linux/UNIX: IPv6 is not
 supported for the instance type 'm3.large'. ",
        "sub-type": "spotFleetRequestConfigurationInvalid"
    }
}
```

Os possíveis valores para `sub-type` são:

`iamFleetRoleInvalid`

A frota do EC2 não tem as permissões necessárias para executar ou encerrar uma instância.

`allLaunchSpecsTemporarilyBlacklisted`

Nenhuma das configurações é válida e várias tentativas de executar instâncias falharam. Para obter mais informações, consulte a descrição do evento.

`spotInstanceCountLimitExceeded`

Você atingiu o limite do número de Instâncias spot que você pode executar.

`spotFleetRequestConfigurationInvalid`

A configuração não é válida. Para obter mais informações, consulte a descrição do evento.

Tipos de evento de frota spot

Existem cinco tipos de eventos de frota spot. Para cada tipo de evento, existem vários subtipos.

Tipos de eventos

- Alteração do estado da frota spot do EC2
- Alteração da solicitação de instância spot da frota spot do EC2
- Alteração da instância da frota spot do EC2
- Informações sobre a frota spot do EC2
- Erro na frota spot do EC2

Alteração do estado da frota spot do EC2

A Frota spot envia um `EC2 Spot Fleet State Change` evento para Amazon EventBridge quando uma frota spot muda de estado.

A seguir estão dados de exemplo para esse evento.

```
{
    "version": "0",
    "id": "d1af1091-6cc3-2e24-203a-3b870e455d5b",
    "detail-type": "EC2 Spot Fleet State Change",
    "source": "aws.ec2spotfleet",
    "account": "123456789012",
    "time": "2020-11-09T08:57:06Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:spot-fleet-request/sfr-4b6d274d-0cea-4b2c-
b3be-9dc627ad1f55"
    ],
    "detail": {
        "sub-type": "submitted"
    }
}
```

Os possíveis valores para `sub-type` são:

`active`

A solicitação de frota spot foi validada e o Amazon EC2 está tentando manter o número de destino das instâncias em execução.

`cancelled`

A solicitação de frota spot foi cancelada e não há instâncias em execução. A frota spot será excluída dois dias após o encerramento das instâncias.

`cancelled_running`

A solicitação de frota spot foi cancelada e não executará instâncias adicionais. Suas instâncias existentes continuam sendo executadas até que sejam interrompidas ou encerradas. A solicitação permanece nesse estado até que todas as instâncias sejam interrompidas ou encerradas.

`cancelled_terminating`

A solicitação de frota spot foi cancelada e as instâncias estão sendo encerradas. A solicitação permanece nesse estado até que todas as instâncias sejam encerradas.

`expired`

A solicitação de frota spot expirou. Se a solicitação tiver sido criada com conjunto `TerminateInstancesWithExpiration`, um evento `terminated` subsequente indicará que as instâncias estão encerradas.

`modify_in_progress`

A solicitação de frota spot está sendo modificada. A solicitação permanece nesse estado até que a modificação seja totalmente processada.

`modify_succeeded`

A solicitação de frota spot foi modificada.

`submitted`

A solicitação de frota spot está sendo avaliada, e o Amazon EC2 está se preparando para executar o número de destino de instâncias.

`progress`

A solicitação de frota spot está em processo de atendimento.

Alteração da solicitação de instância spot da frota spot do EC2

A Frota spot envia um evento de `EC2 Spot Fleet Spot Instance Request Change` para Amazon EventBridge quando uma solicitação de Instância spot da frota muda de estado.

A seguir estão dados de exemplo para esse evento.

```
{
    "version": "0",
    "id": "cd141ef0-14af-d670-a71d-fe46e9971bd2",
    "detail-type": "EC2 Spot Fleet Spot Instance Request Change",
    "source": "aws.ec2spotfleet",
    "account": "123456789012",
    "time": "2020-11-09T08:53:21Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:spot-fleet-request/sfr-
a98d2133-941a-47dc-8b03-0f94c6852ad1"
    ],
    "detail": {
        "spot-instance-request-id": "sir-a2w9gc5h",
        "description": "SpotInstanceRequestId sir-a2w9gc5h, PreviousState:
 cancelled_running",
        "sub-type": "cancelled"
    }
}
```

Os possíveis valores para `sub-type` são:

`active`

A solicitação de instância spot foi atendida e tem uma instância spot associada.

`cancelled`

Você cancelou a solicitação de instância spot ou a solicitação de instância spot expirou.

`disabled`

Você interrompeu a instância spot.

`submitted`

A solicitação de instância spot foi enviada.

Alteração da instância da frota spot do EC2

A frota spot envia um evento de `EC2 Spot Fleet Instance Change` para Amazon EventBridge quando uma instância na frota muda de estado.

A seguir estão dados de exemplo para esse evento.

```
{
    "version": "0",
    "id": "11591686-5bd7-bbaa-eb40-d46529c2710f",
    "detail-type": "EC2 Spot Fleet Instance Change",
    "source": "aws.ec2spotfleet",
    "account": "123456789012",
    "time": "2020-11-09T07:25:02Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:spot-fleet-request/sfr-c8a764a4-bedc-4b62-
af9c-0095e6e3ba61"
    ],
    "detail": {
        "instance-id": "i-08b90df1e09c30c9b",
        "description": "{\"instanceType\":\"r4.2xlarge\",\"image\":
\"ami-032930428bf1abbff\",\"productDescription\":\"Linux/UNIX\",\"availabilityZone\":
\"us-east-1a\"}",
        "sub-type": "launched"
    }
}
```

Os possíveis valores para `sub-type` são:

`launched`

Uma nova instância foi executada.

`terminated`

A instância foi encerrada.

`termination_notified`

Uma notificação de encerramento de instância foi enviada quando uma instância spot foi encerrada pelo Amazon EC2 durante a redução da escala na vertical, quando a capacidade de destino da frota foi modificada para baixo, p. ex., de uma capacidade de destino de 4 para uma capacidade de destino de 3.

Informações sobre a frota spot do EC2

A frota spot envia um evento do `EC2 Spot Fleet Information` para Amazon EventBridge quando há um erro durante o atendimento. O evento informativo não impede a frota de tentar atender à sua capacidade de destino.

A seguir estão dados de exemplo para esse evento.

```
{
    "version": "0",
    "id": "73a60f70-3409-a66c-635c-7f66c5f5b669",
    "detail-type": "EC2 Spot Fleet Information",
    "source": "aws.ec2spotfleet",
    "account": "123456789012",
    "time": "2020-11-08T20:56:12Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:spot-fleet-request/sfr-2531ea06-
af18-4647-8757-7d69c94971b1"
    ],
    "detail": {
        "description": "r3.8xlarge, ami-032930428bf1abbff, Linux/UNIX, us-east-1a, Spot
 bid price is less than Spot market price $0.5291",
        "sub-type": "launchSpecUnusable"
    }
}
```

Os possíveis valores para `sub-type` são:

`fleetProgressHalted`

O preço em cada especificação de execução não é válido porque está abaixo do preço spot (todas as especificações de execução produziram `launchSpecUnusable` eventos). Uma especificação de execução pode se tornar válida se o preço spot mudar.

`launchSpecTemporarilyBlacklisted`

A configuração não é válida e várias tentativas de executar instâncias falharam. Para obter mais informações, consulte a descrição do evento.

`launchSpecUnusable`

O preço em uma especificação de execução não é válido porque está abaixo do preço spot.

`registerWithLoadBalancersFailed`

Falha na tentativa de registrar instâncias com balanceadores de carga. Para obter mais informações, consulte a descrição do evento.

Erro na frota spot do EC2

A frota spot envia um evento do `EC2 Spot Fleet Error` para Amazon EventBridge quando há um erro durante o atendimento. O evento de erro impede a frota de tentar atender à sua capacidade de destino.

A seguir estão dados de exemplo para esse evento.

```
{
    "version": "0",
    "id": "10adc4e7-675c-643e-125c-5bfa1b1ba5d2",
    "detail-type": "EC2 Spot Fleet Error",
    "source": "aws.ec2spotfleet",
    "account": "123456789012",
    "time": "2020-11-09T06:56:07Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:spot-fleet-request/
sfr-38725d30-25f1-4f30-83ce-2907c56dba17"
    ],
    "detail": {
        "description": "r4.2xlarge, ami-032930428bf1abbff, Linux/UNIX: The
 associatePublicIPAddress parameter can only be specified for the network interface
 with DeviceIndex 0. ",
        "sub-type": "spotFleetRequestConfigurationInvalid"
    }
}
```

Os possíveis valores para `sub-type` são:

`iamFleetRoleInvalid`

A frota spot não tem as permissões necessárias para executar ou encerrar uma instância.

`allLaunchSpecsTemporarilyBlacklisted`

Nenhuma das configurações é válida e várias tentativas de executar instâncias falharam. Para obter mais informações, consulte a descrição do evento.

`spotInstanceCountLimitExceeded`

Você atingiu o limite do número de Instâncias spot que você pode executar.

`spotFleetRequestConfigurationInvalid`

A configuração não é válida. Para obter mais informações, consulte a descrição do evento.

Tutoriais para o EC2 Fleet

Há diferentes maneiras de configurar um EC2 Fleet. A configuração a escolher depende do seu caso de uso específico.

Os tutoriais a seguir abordam alguns dos possíveis casos de uso e fornecem as tarefas necessárias para implementá-los.

Caso de uso	Link para o tutorial
Use a ponderação de instâncias para gerenciar a disponibilidade e performance do EC2 Fleet. Com a ponderação de instâncias, você atribui um peso a cada tipo de instância no EC2 Fleet para representar sua capacidade computaci onal e a performance relativa entre elas. Com base nos pesos, a frota pode usar qualquer combinação dos tipos de instância especific ados, desde que possa atender à capacidade de destino desejada.	Tutorial: configurar o EC2 Fleet para usar ponderação de instâncias
Use a capacidade sob demanda para garantir a disponibilidade durante os períodos de pico, mas se beneficie da capacidade spot adicional a um custo menor. Configure o EC2 Fleet para usar instâncias sob demanda como capacidade principal para garantir a capacidade disponível durante os períodos de pico. Além disso, aloque alguma	Tutorial: configurar o EC2 Fleet para usar instâncias sob demanda como a capacidade principal

Caso de uso	Link para o tutorial
capacidade para as instâncias spot para se beneficiar de preços reduzidos, tendo em mente que as instâncias spot poderão ser interrompidas caso o Amazon EC2 precise da capacidade de volta.	
Use as reservas de capacidade para reservar capacidade computacional para as instâncias sob demanda. Configure o EC2 Fleet para usar primeiro reservas de capacidade `targeted` ao executar instâncias sob demanda. Se você tem requisitos rígidos de capacidade e está executando workloads essenciais para os negócios que exigem um certo nível de garantia de capacidade a longo ou curto prazo, recomendamos que você crie uma reserva de capacidade para garantir que sempre tenha acesso à capacidade do Amazon EC2 quando precisar, pelo tempo que precisar.	Tutorial: configurar o EC2 Fleet para executar instâncias sob demanda usando reservas de capacidade direcionadas
Use blocos de capacidade para reservar instâncias de GPU muito procuradas por suas workloads de ML. Configure o EC2 Fleet para executar instâncias em blocos de capacidade.	Tutorial: configurar o EC2 Fleet para executar instâncias em blocos de capacidade

Tutorial: configurar o EC2 Fleet para usar ponderação de instâncias

Este tutorial usa uma empresa fictícia chamada Example Corp para ilustrar o processo de solicitação de uma Frota do EC2 usando o peso da instância.

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 uma aplicação de uso intenso de memória e recursos de computação que funciona melhor com, pelo menos, 60 GB de memória e oito CPUs virtuais (vCPUs). Eles querem maximizar esses recursos para a aplicação com o menor preço possível. A Exemplo Corp decide que qualquer um dos seguintes tipos de instância do EC2 atenderá às suas necessidades:

Tipo de instância	Memória (GiB)	vCPUs
r3.2xlarge	61	8
r3.4xlarge	122	16
r3.8xlarge	244	32

Capacidade de destino em unidades

Com o peso da instância, a capacidade de destino pode igualar um número de instâncias (o padrão) ou uma combinação de fatores, como núcleos (vCPUs), memória (GiB) e armazenamento (GB). Considerando a base para sua aplicação (60 GB de RAM e oito vCPUs) como 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 do EC2 Fleet como 20 unidades.

Pesos das instâncias

Depois de determinar a capacidade de destino, a Exemplo Corp calcula os pesos das instâncias. Para calcular o peso para cada tipo de instância, eles determinam as unidades de cada tipo de instância que são necessárias para atingir a capacidade de destino da seguinte forma:

- r3.2xlarge (61,0 GB, 8 vCPUs) = 1 unidade de 20
- r3.4xlarge (122,0 GB, 16 vCPUs) = 2 unidades de 20
- r3.8xlarge (244,0 GB, 32 vCPUs) = 4 unidades de 20

Portanto, a Exemplo Corp atribui os pesos de instância 1, 2 e 4 às respectivas configurações de execução na solicitação de Frota do EC2.

Preço por hora

A Exemplo Corp usa o Preço sob demanda por hora de instância como o ponto inicial de preço. Eles também podem usar os preços spot recentes ou uma combinação dos dois. Para calcular o preço por hora, eles dividem o preço inicial por hora de instância pelo peso. Por exemplo:

Tipo de instância	Preço sob demanda	Peso da instância	Preço por hora
r3.2xLarge	0,7 USD	1	0,7 USD
r3.4xLarge	1,4 USD	2	0,7 USD
r3.8xLarge	$2,8	4	0,7 USD

A Exemplo Corp pode usar um preço global por hora de 0,7 USD e ser competitiva para todos os três tipos de instância. Eles também podem usar um preço global por hora de 0,7 USD e um preço específico por hora de 0,9 USD na especificação de execução `r3.8xlarge`.

Verificar permissões

Antes de criar uma Frota do EC2, a Exemplo Corp verifica se ela tem uma função do IAM com as permissões necessárias. Para obter mais informações, consulte Pré-requisitos da Frota do EC2.

Criar um modelo de execução

Em seguida, a Exemplo Corp cria um modelo de execução. O ID do modelo de execução é usado na próxima etapa. Para obter mais informações, consulte Criar um modelo de execução do Amazon EC2.

Criar a Frota do EC2

A Example Corp cria um arquivo, `config.json`, com a seguinte configuração para sua Frota do EC2: No exemplo a seguir, substitua os identificadores de recursos pelos seus identificadores de recursos.

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateId": "lt-07b3bc7625cdab851",
                "Version": "1"
            },
            "Overrides": [
                {
                    "InstanceType": "r3.2xlarge",
                    "SubnetId": "subnet-482e4972",
                    "WeightedCapacity": 1
                },
                {
                    "InstanceType": "r3.4xlarge",
                    "SubnetId": "subnet-482e4972",
                    "WeightedCapacity": 2
                },
                {
                    "InstanceType": "r3.8xlarge",
                    "MaxPrice": "0.90",
                    "SubnetId": "subnet-482e4972",
                    "WeightedCapacity": 4
                }
            ]
        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "DefaultTargetCapacityType": "spot"
    }
}
```

A Example Corp cria a Frota do EC2 usando o seguinte comando create-fleet:

```
aws ec2 create-fleet --cli-input-json file://config.json
```

Para obter mais informações, consulte Criar uma Frota do EC2..

Atendimento

A estratégia de alocação determina de quais grupos de capacidade spot os Instâncias spot procedem.

Com a estratégia `lowest-price` (que é uma estratégia padrão), as Instâncias spot vêm do grupo com o menor preço spot por unidade no momento do atendimento. Para fornecer 20 unidades de capacidade, a Frota do EC2 executa 20 instâncias `r3.2xlarge` (20 dividido por 1), 10 instâncias `r3.4xlarge` (20 dividido por 2) ou 5 instâncias `r3.8xlarge` (20 dividido por 4).

Se a Exemplo Corp usasse a estratégia `diversified`, as Instâncias spot viriam dos três grupos. A Frota do EC2 executaria seis instâncias `r3.2xlarge` (que fornecem 6 unidades), três instâncias `r3.4xlarge` (que fornecem 6 unidades), duas instâncias `r3.8xlarge` (que fornecem 8 unidades), totalizando 20 unidades.

Tutorial: configurar o EC2 Fleet para usar instâncias sob demanda como a capacidade principal

Este tutorial usa uma empresa fictícia chamada ABC Online para ilustrar o processo de solicitação de uma Frota do EC2 com opção sob demanda como capacidade principal e capacidade spot (se disponível).

Objetivo

A ABC Online, uma empresa de entrega para restaurantes, quer provisionar a capacidade do Amazon EC2 entre os tipos de instância do EC2 e as opções de compra para atingir a escala, a performance e o custo desejados.

Planejamento

A ABC Online precisa de uma capacidade fixa para operar durante períodos de pico, mas gostaria de se beneficiar de uma capacidade adicional com custo mais baixo. A empresa determina os seguintes requisitos para EC2 Fleet:

- Capacidade de instância sob demanda: a ABC Online requer 15 instâncias sob demanda para garantir a acomodação do tráfego em períodos de pico.
- Capacidade de instâncias spot: para aprimorar a performance, mas com um custo mais baixo, a ABC Online planeja provisionar cinco instâncias spot.

Verificar permissões

Antes de criar uma Frota do EC2, a ABC Online verifica se ela tem uma função do IAM com as permissões necessárias. Para obter mais informações, consulte Pré-requisitos da Frota do EC2.

Criar um modelo de execução

A ABC Online cria um modelo de execução. O ID do modelo de execução é usado na próxima etapa. Para obter mais informações, consulte Criar um modelo de execução do Amazon EC2.

Criar a Frota do EC2

A ABC Online cria um arquivo, `config.json`, com a seguinte configuração para sua Frota do EC2. No exemplo a seguir, substitua os identificadores de recursos pelos seus identificadores de recursos.

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateId": "lt-07b3bc7625cdab851",
                "Version": "2"
            }

        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "OnDemandTargetCapacity":15,
        "DefaultTargetCapacityType": "spot"
    }
}
```

A ABC Online cria a Frota do EC2 usando o seguinte comando create-fleet:

```
aws ec2 create-fleet --cli-input-json file://config.json
```

Para obter mais informações, consulte Criar uma Frota do EC2..

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.

Tutorial: configurar o EC2 Fleet para executar instâncias sob demanda usando reservas de capacidade direcionadas

Este tutorial orienta você por todas as etapas que você deve executar para que sua Frota do EC2 inicie Instâncias sob demanda nas Reservas de Capacidade `targeted`.

Você aprenderá a configurar uma frota para usar as Reservas de Capacidade sob demanda `targeted` primeiro ao iniciar Instâncias sob demanda. Você também aprenderá a configurar a frota para que, quando a capacidade total de destino sob demanda exceder o número de Reservas de Capacidade não utilizadas disponíveis, a frota use a estratégia de alocação especificada para selecionar os grupos de instâncias nos quais iniciar a capacidade de destino restante.

Configuração da Frota do EC2

Nesse tutorial, a frota é configurada da seguinte forma:

- Capacidade de destino: 10 Instâncias sob demanda
- Total de Reservas de Capacidade `targeted` não utilizadas: 6 (menor que a capacidade de destino sob demanda da frota de 10 Instâncias sob demanda)
- Número de grupos de Reservas de capacidade: 2 (`us-east-1a` e `us-east-1b`)
- Número de Reservas de Capacidade por grupo: 3
- Estratégia de alocação sob demanda: `lowest-price` (Quando o número de Reservas de Capacidade não utilizadas for menor que a capacidade de destino sob demanda, a frota determina os grupos nos quais iniciar a capacidade sob demanda restante com base na estratégia de alocação sob demanda.)

  Observe que você também pode usar a estratégia de alocação `prioritized` em vez da estratégia de alocação `lowest-price`.

Para iniciar as Instâncias sob demanda em Reservas de Capacidade targeted, você deve executar uma série de etapas, da seguinte forma:

- Etapa 1: Criar Reservas de Capacidade
- Etapa 2: Criar um grupo de recursos de Reservas de capacidade
- Etapa 3: Adicionar as Reservas de Capacidade ao grupo de recursos Reservas de Capacidade
- (Opcional) Etapa 4: Exibir Reservas de Capacidade no grupo de recursos
- Etapa 5: Criar um modelo de inicialização que especifique que a Reserva de Capacidade se destina a um grupo de recursos específico
- (Opcional) Etapa 6: Descrever o modelo de inicialização
- Etapa 7: Criar uma Frota EC2
- (Opcional) Etapa 8: Exibir o número de Reservas de Capacidade não utilizadas restantes

Etapa 1: Criar Reservas de Capacidade

Use o comando Create-capacity-reservation para criar as Reservas de Capacidade, três para `us-east-1a` e outras três para `us-east-1b`. Exceto para a Zona de disponibilidade, os outros atributos das Reservas de Capacidade são idênticos.

3 Reservas de Capacidade no **`us-east-1a`**

```
aws ec2 create-capacity-reservation \
    --availability-zone us-east-1a \
    --instance-type c5.xlarge \
    --instance-platform Linux/UNIX \
    --instance-count 3 \
    --instance-match-criteria targeted
```

Exemplo de ID de reserva de capacidade resultante

```
cr-1234567890abcdef1
```

3 Reservas de Capacidade no **`us-east-1b`**

```
aws ec2 create-capacity-reservation \
    --availability-zone us-east-1b \
    --instance-type c5.xlarge \
    --instance-platform Linux/UNIX \
    --instance-count 3 \
    --instance-match-criteria targeted
```

Exemplo de ID de reserva de capacidade resultante

```
cr-54321abcdef567890
```

Etapa 2: Criar um grupo de recursos de Reservas de capacidade

Use o serviço `resource-groups` e o comando create-group para criar um grupo de recursos de Reservas de capacidade. Neste exemplo, o grupo de recursos é chamado de `my-cr-group`. Para obter informações sobre por que você deve criar um grupo de recursos, consulte Use reservas de capacidade para reservar capacidade sob demanda na frota do EC2.

```
aws resource-groups create-group \
    --name my-cr-group \
    --configuration '{"Type":"AWS::EC2::CapacityReservationPool"}'
 '{"Type":"AWS::ResourceGroups::Generic", "Parameters": [{"Name": "allowed-resource-
types", "Values": ["AWS::EC2::CapacityReservation"]}]}'
```

Etapa 3: Adicionar as Reservas de Capacidade ao grupo de recursos Reservas de Capacidade

Use o serviço `resource-groups` e o comando group-resources para adicionar as Reservas de Capacidade que você criou na Etapa 1 para o grupo de recursos Reservas de Capacidade. Observe que você deve fazer referência às Reservas de Capacidade sob demanda por seus ARNs.

```
aws resource-groups group-resources \
    --group my-cr-group \
    --resource-arns \
      arn:aws:ec2:us-east-1:123456789012:capacity-reservation/cr-1234567890abcdef1 \
      arn:aws:ec2:us-east-1:123456789012:capacity-reservation/cr-54321abcdef567890
```

Exemplo de saída

```
{
   "Failed": [],
   "Succeeded": [
   "arn:aws:ec2:us-east-1:123456789012:capacity-reservation/cr-1234567890abcdef1",
   "arn:aws:ec2:us-east-1:123456789012:capacity-reservation/cr-54321abcdef567890"
   ]
}
```

(Opcional) Etapa 4: Exibir Reservas de Capacidade no grupo de recursos

Use o serviço `resource-groups` e o comando list-group-resources para descrever opcionalmente o grupo de recursos para visualizar suas Reservas de Capacidade.

```
aws resource-groups list-group-resources --group my-cr-group
```

Exemplo de saída

```
{
    "ResourceIdentifiers": [
        {
            "ResourceType": "AWS::EC2::CapacityReservation",
            "ResourceArn": "arn:aws:ec2:us-east-1:123456789012:capacity-reservation/
cr-1234567890abcdef1"
        },
        {
            "ResourceType": "AWS::EC2::CapacityReservation",
            "ResourceArn": "arn:aws:ec2:us-east-1:123456789012:capacity-reservation/
cr-54321abcdef567890"
        }
    ]
}
```

Etapa 5: Criar um modelo de inicialização que especifique que a Reserva de Capacidade se destina a um grupo de recursos específico

Use o comando create-launch-template para criar um modelo de execução no qual especifique as Reservas de Capacidade a serem usadas. Neste exemplo, a frota usará Reservas de Capacidade `targeted`, que foram adicionadas a um grupo de recursos. Portanto, os dados do modelo de inicialização especificam que a Reserva de Capacidade se destina a um grupo de recursos específico. Neste exemplo, o modelo de inicialização é chamado de `my-launch-template`.

```
aws ec2 create-launch-template \
    --launch-template-name my-launch-template \
    --launch-template-data \
        '{"ImageId": "ami-0123456789example",
          "CapacityReservationSpecification":
            {"CapacityReservationTarget":
                { "CapacityReservationResourceGroupArn": "arn:aws:resource-groups:us-
east-1:123456789012:group/my-cr-group" }
```

```
            }
        }'
```

(Opcional) Etapa 6: Descrever o modelo de inicialização

Use o comando describe-launch-template-versions para descrever opcionalmente o modelo de execução para visualizar a configuração.

```
aws ec2 describe-launch-template-versions --launch-template-name my-launch-template
```

Exemplo de saída

```
{
    "LaunchTemplateVersions": [
        {
            "LaunchTemplateId": "lt-01234567890example",
            "LaunchTemplateName": "my-launch-template",
            "VersionNumber": 1,
            "CreateTime": "2021-01-19T20:50:19.000Z",
            "CreatedBy": "arn:aws:iam::123456789012:user/Admin",
            "DefaultVersion": true,
            "LaunchTemplateData": {
                "ImageId": "ami-0947d2ba12ee1ff75",
                "CapacityReservationSpecification": {
                    "CapacityReservationTarget": {
                        "CapacityReservationResourceGroupArn": "arn:aws:resource-
groups:us-east-1:123456789012:group/my-cr-group"
                    }
                }
            }
        }
    ]
}
```

Etapa 7: Criar uma Frota EC2

Crie uma EC2 Fleet que especifique as informações de configuração para as instâncias que serão iniciadas. A configuração de frota EC2 a seguir mostra somente as configurações pertinentes a esse exemplo. O modelo de inicialização `my-launch-template` é o modelo de inicialização criado na Etapa 5. Há dois grupos de instâncias, cada um com o mesmo tipo de instância (`c5.xlarge`), mas com diferentes zonas de disponibilidade (`us-east-1a` e `us-east-1b`). O preço dos grupos de

instâncias é o mesmo porque o preço é definido para a região, não para a Zona de Disponibilidade. A capacidade de destino total é de 10 e o tipo de capacidade de destino padrão é `on-demand`. A estratégia de alocação sob demanda é `lowest-price`. A estratégia de uso para Reservas de Capacidade é `use-capacity-reservations-first`.

> **Note**
>
> O tipo da frota deve ser `instant`. Outros tipos de frota não são compatíveis com `use-capacity-reservations-first`.

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "my-launch-template",
                "Version": "1"
            },
            "Overrides": [
               {
                   "InstanceType": "c5.xlarge",
                   "AvailabilityZone": "us-east-1a"
               },
               {
                    "InstanceType": "c5.xlarge",
                    "AvailabilityZone": "us-east-1b"
               }
            ]
        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 10,
        "DefaultTargetCapacityType": "on-demand"
    },
    "OnDemandOptions": {
        "AllocationStrategy": "lowest-price",
        "CapacityReservationOptions": {
             "UsageStrategy": "use-capacity-reservations-first"
         }
    },
    "Type": "instant"
```

```
}
```

Depois de criar a frota `instant` usando a configuração anterior, as 10 instâncias a seguir serão iniciadas para atender à capacidade de destino:

- As Reservas de Capacidade são usadas primeiro para iniciar 6 Instâncias sob demanda da seguinte maneira:
  - 3 Instâncias sob demanda são iniciadas nas 3 `c5.xlarge` Reservas de Capacidade `targeted` no `us-east-1a`
  - 3 Instâncias sob demanda são iniciadas nas 3 `c5.xlarge` Reservas de Capacidade `targeted` no `us-east-1b`
- Para atender à capacidade de destino, 4 Instâncias sob demanda adicionais são iniciadas na capacidade sob demanda regular de acordo com a estratégia de alocação sob demanda, que é `lowest-price` neste exemplo. No entanto, como os grupos têm o mesmo preço (porque o preço é por região e não por zona de disponibilidade), a frota inicia as 4 Instâncias sob demanda restantes em qualquer um dos grupos.

(Opcional) Etapa 8: Exibir o número de Reservas de Capacidade não utilizadas restantes

Depois que a frota for lançada, você poderá, opcionalmente, executar describe-capacity-reservations para ver quantas Reservas de Capacidade não utilizadas restam. Neste exemplo, você deve ver a resposta a seguir, que mostra que todas as Reservas de Capacidade foram usadas em todos os grupos.

```
{ "CapacityReservationId":  "cr-111",
     "InstanceType":  "c5.xlarge",
     "AvailableInstanceCount":  0
}

 { "CapacityReservationId":  "cr-222",
     "InstanceType":  "c5.xlarge",
     "AvailableInstanceCount":  0
}
```

Tutorial: configurar o EC2 Fleet para executar instâncias em blocos de capacidade

Este tutorial mostra todas as etapas que você deve seguir para que a Frota do EC2 inicie Instâncias sob demanda em blocos de capacidade.

Na maioria dos casos, a capacidade de destino da solicitação do EC2 Fleet deve ser menor ou igual à capacidade disponível na reserva do bloco de capacidade pretendida. As solicitações de capacidade pretendida que excederem os limites da reserva de bloco de capacidade não serão atendidas. Se a solicitação da capacidade de destino exceder os limites da reserva de bloco de capacidade, você receberá uma `Insufficient Capacity Exception` para a capacidade que exceder os limites da reserva de bloco de capacidade.

> **Note**
>
> Para blocos de capacidade, a Frota do EC2 não recorrerá à inicialização de instâncias sob demanda para atender ao restante da capacidade pretendida.

Se a Frota do EC2 não puder atender à capacidade pretendida solicitada em uma reserva de bloco de capacidade disponível, a Frota do EC2 atenderá ao máximo de capacidade possível e retornará as instâncias que não conseguiu iniciar. Você pode repetir a chamada para a Frota do EC2 até que todas as instâncias sejam provisionadas.

Depois de configurar a solicitação da Frota do EC2, você deve esperar até a data de início da reserva do bloco de capacidade. Caso faça solicitações ao EC2 Fleet para executar um bloco de capacidade que ainda não foi iniciado, você receberá um `Insufficient Capacity Error`.

Depois que a reserva de bloco de capacidade se tornar ativa, você poderá fazer chamadas à API da Frota do EC2 e provisionar as instâncias no bloco de capacidade segundo os parâmetros selecionados. As instâncias em execução no bloco de capacidade continuam em execução até que você as interrompa ou encerre manualmente, ou até que o Amazon EC2 encerre as instâncias quando a reserva do bloco de capacidade terminar.

Para obter mais informações sobre blocos de capacidade, consulte Blocos de capacidade para ML.

Considerações

- Somente solicitações do EC2 Fleet do tipo `instant` são compatíveis para executar instâncias em blocos de capacidade. Para obter mais informações, consulte Configurar um EC2 Fleet do tipo instant.
- Não é possível ter vários blocos de capacidade na mesma solicitação do EC2 Fleet.
- Não é possível usar `OnDemandTargetCapacity` ou `SpotTargetCapacity` e, ao mesmo tempo, definir o `capacity-block` como `DefaultTargetCapacity`.
- Se o `DefaultTargetCapacityType` estiver definido como `capacity-block`, você não poderá fornecer `OnDemandOptions::CapacityReservationOptions`. Uma exceção ocorrerá.

Para configurar um EC2 Fleet para executar instâncias em blocos de capacidade

1. Crie um modelo de execução.

   No modelo de execução, faça o seguinte:

   - Para `InstanceMarketOptionsRequest`, defina `MarketType` como `capacity-block`.
   - Para direcionar a reserva do bloco de capacidade, para `CapacityReservationID`, especifique o ID da reserva do bloco de capacidade.

   Anote o nome e a versão do modelo de execução. Você usará essas informações na próxima etapa.

   Para obter mais informações sobre como criar um modelo de execução, consulte Criar um modelo de execução do Amazon EC2.
2. Configure o EC2 Fleet.

   Crie um arquivo, `config.json`, com a configuração do EC2 Fleet a seguir. No exemplo a seguir, substitua os identificadores de recursos pelos seus identificadores de recursos.

   Para obter mais informações sobre como configurar um EC2 Fleet, consulte Criar uma Frota do EC2..

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
```

```
                "LaunchTemplateName": "CBR-launch-template",
                "Version": "1"
            },
            "Overrides": [
                {
                    "InstanceType": "p5.48xlarge",
                    "AvailabilityZone": "us-east-1a"
                },
            ]
        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 10,
        "DefaultTargetCapacityType": "capacity-block"
    },
    "Type": "instant"
}
```

3. Execute a frota.

   Use o comando create-fleet a seguir.

   ```
   aws ec2 create-fleet --cli-input-json file://config.json
   ```

   Para obter mais informações, consulte Criar uma Frota do EC2..

Exemplo de configurações da CLI para frotas do EC2

É possível definir a configuração da frota do EC2 em um arquivo JSON e, em seguida, referenciar esse arquivo com o comando create-fleet para criar a frota, da maneira a seguir:

```
aws ec2 create-fleet --cli-input-json file://file_name.json
```

Os exemplos a seguir ilustram as configurações de inicialização para vários casos de uso de frotas do EC2. Para obter mais informações sobre os parâmetros de configuração, consulte create-fleet.

Exemplos

- Exemplo 1: Executar Instâncias spot como a opção de compra padrão
- Exemplo 2: Executar Instâncias on-demand como a opção de compra padrão
- Exemplo 3: Executar Instâncias on-demand como a capacidade principal

- Exemplo 4: Iniciar Instâncias sob demanda usando várias Reservas de Capacidade
- Exemplo 5: Iniciar Instâncias sob demanda usando Reservas de Capacidade quando a capacidade total de destino for maior que o número de Reservas de Capacidade não utilizadas
- Exemplo 6: Iniciar Instâncias sob demanda usando Reservas de Capacidade direcionadas
- Exemplo 7: Configurar o rebalanceamento de capacidade para executar a Instâncias spot de substituição
- Exemplo 8: iniciar instâncias spot em uma frota otimizada para capacidade
- Exemplo 9: iniciar instâncias spot em uma frota otimizada para capacidade com prioridades
- Exemplo 10: iniciar instâncias spot em uma frota otimizada para preço-capacidade
- Exemplo 11: configurar a seleção de tipo de instância baseada em atributos

Para obter mais exemplos da CLI para frotas do tipo `instant`, consulte Configurar um EC2 Fleet do tipo instant.

Exemplo 1: Executar Instâncias spot como a opção de compra padrão

O exemplo a seguir especifica os parâmetros mínimos necessários em uma Frota do EC2: um modelo de execução, a capacidade de destino e a opção de compra padrão. O modelo de execução é identificado pelo ID do seu modelo de execução e o número da versão. A capacidade de destino da frota é de 2 instâncias, e a opção de compra padrão é `spot`. Isso faz com que a frota execute duas Instâncias spot.

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateId": "lt-0e8c754449b27161c",
                "Version": "1"
            }

        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 2,
        "DefaultTargetCapacityType": "spot"
    }
}
```

Exemplo 2: Executar Instâncias on-demand como a opção de compra padrão

O exemplo a seguir especifica os parâmetros mínimos necessários em uma Frota do EC2: um modelo de execução, a capacidade de destino e a opção de compra padrão. O modelo de execução é identificado pelo ID do seu modelo de execução e o número da versão. A capacidade de destino da frota é de 2 instâncias, e a opção de compra padrão é `on-demand`. Isso faz com que a frota execute duas Instâncias on-demand.

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateId": "lt-0e8c754449b27161c",
                "Version": "1"
            }

        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 2,
        "DefaultTargetCapacityType": "on-demand"
    }
}
```

Exemplo 3: Executar Instâncias on-demand como a capacidade principal

O exemplo a seguir especifica a capacidade total de destino de duas instâncias para a frota e uma capacidade de destino de uma instância sob demanda. A opção de compra padrão é `spot`. A frota executa uma instância sob demanda, conforme especificado, mas precisa executar mais uma instância para atender à capacidade total desejada. A opção de compra para a diferença é calculada como `TotalTargetCapacity` – `OnDemandTargetCapacity` = `DefaultTargetCapacityType`, o que resulta na frota executando uma instância spot.

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateId": "lt-0e8c754449b27161c",
                "Version": "1"
```

```
            }

        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 2,
        "OnDemandTargetCapacity": 1,
        "DefaultTargetCapacityType": "spot"
    }
}
```

Exemplo 4: Iniciar Instâncias sob demanda usando várias Reservas de Capacidade

É possível configurar uma frota para usar Reservas de Capacidade sob demanda primeiro ao iniciar Instâncias on-demand definindo a estratégia de uso para Reservas de Capacidade como `use-capacity-reservations-first`. Este exemplo demonstra como a frota seleciona as Reservas de Capacidade a serem usadas quando há mais Reservas de Capacidade do que o necessário para atender à capacidade de destino.

Neste exemplo, a configuração da frota é a seguinte:

- Capacidade de destino: 12 Instâncias sob demanda
- Total de Reservas de Capacidade não utilizadas: 15 (mais do que a capacidade de destino da frota de 12 Instâncias sob demanda)
- Número de grupos de Reservas de capacidade: 3 (`m5.large`, `m4.xlarge` e `m4.2xlarge`)
- Número de Reservas de Capacidade por grupo: 5
- Estratégia de alocação sob demanda: `lowest-price` (Quando há várias Reservas de Capacidade não utilizadas em vários grupos de instâncias, a frota determina os grupos nos quais as Instâncias sob demanda serão iniciadas com base na estratégia de alocação sob demanda.)

  Observe que você também pode usar a estratégia de alocação `prioritized` em vez da estratégia de alocação `lowest-price`.

Reservas de capacidade

A conta tem as 15 Reservas de Capacidade não utilizadas a seguir em 3 grupos diferentes. O número de Reservas de Capacidade em cada grupo é indicado por `AvailableInstanceCount`.

```
{
    "CapacityReservationId": "cr-111",
    "InstanceType": "m5.large",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount": 5,
    "InstanceMatchCriteria": "open",
    "State": "active"
}

{
    "CapacityReservationId": "cr-222",
    "InstanceType": "m4.xlarge",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount": 5,
    "InstanceMatchCriteria": "open",
    "State": "active"
}

{
    "CapacityReservationId": "cr-333",
    "InstanceType": "m4.2xlarge",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount":5,
    "InstanceMatchCriteria": "open",
    "State": "active"
}
```

Configuração da frota

A configuração de frota a seguir mostra somente as configurações pertinentes a este exemplo. A capacidade de destino total é de 12 e o tipo de capacidade de destino padrão é `on-demand`. A estratégia de alocação sob demanda é `lowest-price`. A estratégia de uso para Reservas de Capacidade é `use-capacity-reservations-first`.

Neste exemplo, o preço da instância sob demanda é:

- `m5.large` – 0,096 USD por hora
- `m4.xlarge` – 0,20 USD por hora
- `m4.2xlarge` – 0,40 USD por hora

> **Note**
>
> O tipo da frota deve ser do tipo `instant`. Outros tipos de frota não são compatíveis com `use-capacity-reservations-first`.

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateId": "lt-abc1234567example",
                "Version": "1"
            },
            "Overrides": [
                {
                  "InstanceType": "m5.large",
                  "AvailabilityZone": "us-east-1a",
                  "WeightedCapacity": 1
                },
                {
                  "InstanceType": "m4.xlarge",
                  "AvailabilityZone": "us-east-1a",
                  "WeightedCapacity": 1
                },
                {
                  "InstanceType": "m4.2xlarge",
                  "AvailabilityZone": "us-east-1a",
                  "WeightedCapacity": 1
                }
              ]

        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 12,
        "DefaultTargetCapacityType": "on-demand"
    },
    "OnDemandOptions": {
        "AllocationStrategy": "lowest-price",
        "CapacityReservationOptions": {
            "UsageStrategy": "use-capacity-reservations-first"
        }
```

```
    },
    "Type": "instant"
}
```

Depois de criar a frota `instant` usando a configuração anterior, as 12 instâncias a seguir serão executadas para atender à capacidade de destino:

- 5 `m5.large` Instâncias sob demanda em `us-east-1a` – `m5.large` em `us-east-1a` é o preço mais baixo, e há 5 Reservas de Capacidade `m5.large` disponíveis não utilizadas
- 5 `m4.xlarge` Instâncias sob demanda em `m4.xlarge` – `us-east-1a` em us-east-1a é o próximo preço mais baixo, e há 5 Reservas de Capacidade `m4.xlarge` não utilizadas disponíveis
- 2 Instâncias sob demanda `m4.2xlarge` em us-east-1a – `m4.2xlarge` em `us-east-1a` é o terceiro preço mais baixo, e existem 5 Reservas de Capacidade `m4.2xlarge` não utilizadas disponíveis, das quais somente 2 são necessárias para atender à capacidade de destino

Depois que a frota for lançada, será possível executar describe-capacity-reservations para ver quantas Reservas de capacidade não utilizadas restam. Neste exemplo, você deve ver a resposta a seguir, que mostra que todas as Reservas de Capacidade `m5.large` e `m4.xlarge` foram usadas, com 3 Reservas de Capacidade `m4.2xlarge` restantes não utilizadas.

```
{
    "CapacityReservationId": "cr-111",
    "InstanceType": "m5.large",
    "AvailableInstanceCount": 0
}

{
    "CapacityReservationId": "cr-222",
    "InstanceType": "m4.xlarge",
    "AvailableInstanceCount": 0
}

{
    "CapacityReservationId": "cr-333",
    "InstanceType": "m4.2xlarge",
    "AvailableInstanceCount": 3
}
```

Exemplo 5: Iniciar Instâncias sob demanda usando Reservas de Capacidade quando a capacidade total de destino for maior que o número de Reservas de Capacidade não utilizadas

É possível configurar uma frota para usar Reservas de Capacidade sob demanda primeiro ao iniciar Instâncias on-demand definindo a estratégia de uso para Reservas de Capacidade como `use-capacity-reservations-first`. Este exemplo demonstra como a frota seleciona os grupos de instâncias nos quais iniciar Instâncias sob demanda quando a capacidade total de destino excede o número de Reservas de Capacidade não utilizadas disponíveis.

Neste exemplo, a configuração da frota é a seguinte:

- Capacidade de destino: 16 Instâncias sob demanda
- Total de Reservas de Capacidade não utilizadas: 15 (menor que a capacidade de destino da frota de 16 Instâncias sob demanda)
- Número de grupos de Reservas de capacidade: 3 (`m5.large`, `m4.xlarge` e `m4.2xlarge`)
- Número de Reservas de Capacidade por grupo: 5
- Estratégia de alocação sob demanda: `lowest-price` (Quando o número de Reservas de Capacidade não utilizadas for menor que a capacidade de destino sob demanda, a frota determina os grupos nos quais iniciar a capacidade sob demanda restante com base na estratégia de alocação sob demanda.)

  Observe que você também pode usar a estratégia de alocação `prioritized` em vez da estratégia de alocação `lowest-price`.

Reservas de capacidade

A conta tem as 15 Reservas de Capacidade não utilizadas a seguir em 3 grupos diferentes. O número de Reservas de Capacidade em cada grupo é indicado por `AvailableInstanceCount`.

```
{
    "CapacityReservationId": "cr-111",
    "InstanceType": "m5.large",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount": 5,
    "InstanceMatchCriteria": "open",
    "State": "active"
```

```
}

{
    "CapacityReservationId": "cr-222",
    "InstanceType": "m4.xlarge",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount": 5,
    "InstanceMatchCriteria": "open",
    "State": "active"
}

{
    "CapacityReservationId": "cr-333",
    "InstanceType": "m4.2xlarge",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount":5,
    "InstanceMatchCriteria": "open",
    "State": "active"
}
```

Configuração da frota

A configuração de frota a seguir mostra somente as configurações pertinentes a este exemplo. A capacidade de destino total é de 16 e o tipo de capacidade de destino padrão é `on-demand`. A estratégia de alocação sob demanda é `lowest-price`. A estratégia de uso para Reservas de Capacidade é `use-capacity-reservations-first`.

Neste exemplo, o preço da instância sob demanda é:

- m5.large – 0,096 USD por hora
- m4.xlarge – 0,20 USD por hora
- m4.2xlarge – 0,40 USD por hora

> **Note**
>
> O tipo da frota deve ser `instant`. Outros tipos de frota não são compatíveis com `use-capacity-reservations-first`.

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateId": "lt-0e8c754449b27161c",
                "Version": "1"
            },
            "Overrides": [
                {
                  "InstanceType": "m5.large",
                  "AvailabilityZone": "us-east-1a",
                  "WeightedCapacity": 1
                },
                {
                  "InstanceType": "m4.xlarge",
                  "AvailabilityZone": "us-east-1a",
                  "WeightedCapacity": 1
                },
                {
                  "InstanceType": "m4.2xlarge",
                  "AvailabilityZone": "us-east-1a",
                  "WeightedCapacity": 1
                }
              ]

        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 16,
        "DefaultTargetCapacityType": "on-demand"
    },
    "OnDemandOptions": {
        "AllocationStrategy": "lowest-price"
        "CapacityReservationOptions": {
            "UsageStrategy": "use-capacity-reservations-first"
        }
    },
    "Type": "instant",
}
```

Depois de criar a frota `instant` usando a configuração anterior, as 16 instâncias a seguir serão executadas para atender à capacidade de destino:

- 6 Instâncias sob demanda `m5.large` em `us-east-1a` – `m5.large` em `us-east-1a` é o preço mais baixo, e há 5 Reservas de Capacidade `m5.large` disponíveis não utilizadas As Reservas de Capacidade são usadas primeiro para iniciar 5 Instâncias sob demanda. Depois das Reservas de Capacidade `m4.xlarge` e `m4.2xlarge` restantes serem usadas, para atender à capacidade de destino, uma instância sob demanda adicional é iniciada, de acordo com a estratégia de alocação sob demanda, que é `lowest-price` neste exemplo.
- 5 `m4.xlarge` Instâncias sob demanda em `us-east-1a` – `m4.xlarge` em `us-east-1a` é o próximo preço mais baixo, e há 5 Reservas de Capacidade `m4.xlarge` disponíveis não utilizadas
- 5 `m4.2xlarge` Instâncias sob demanda em `us-east-1a` – `m4.2xlarge` em `us-east-1a` é o terceiro preço mais baixo, e há 5 Reservas de Capacidade `m4.2xlarge` disponíveis não utilizadas

Depois que a frota for lançada, será possível executar describe-capacity-reservations para ver quantas Reservas de capacidade não utilizadas restam. Neste exemplo, você deve ver a resposta a seguir, que mostra que todas as Reservas de capacidade foram usadas em todos os grupos.

```
{
    "CapacityReservationId": "cr-111",
    "InstanceType": "m5.large",
    "AvailableInstanceCount": 0
}

{
    "CapacityReservationId": "cr-222",
    "InstanceType": "m4.xlarge",
    "AvailableInstanceCount": 0
}

{
    "CapacityReservationId": "cr-333",
    "InstanceType": "m4.2xlarge",
    "AvailableInstanceCount": 0
}
```

Exemplo 6: Iniciar Instâncias sob demanda usando Reservas de Capacidade direcionadas

É possível configurar uma frota para usar Reservas de Capacidade `targeted` sob demanda primeiro ao iniciar Instâncias sob demanda definindo a estratégia de uso para Reservas de

Capacidade como `use-capacity-reservations-first`. Este exemplo demonstra como iniciar Instâncias sob demanda nas Reservas de Capacidade `targeted`, com os atributos das Reservas de Capacidade sendo os mesmos, exceto para suas Zonas de Disponibilidade (`us-east-1a` e `us-east-1b`). Ele também demonstra como a frota seleciona os grupos de instâncias nos quais iniciar Instâncias sob demanda quando a capacidade total de destino excede o número de Reservas de Capacidade não utilizadas disponíveis.

Neste exemplo, a configuração da frota é a seguinte:

- Capacidade de destino: 10 Instâncias sob demanda
- Total de Reservas de Capacidade `targeted` não utilizadas: 6 (menor que a capacidade de destino sob demanda da frota de 10 Instâncias sob demanda)
- Número de grupos de Reservas de capacidade: 2 (`us-east-1a` e `us-east-1b`)
- Número de Reservas de Capacidade por grupo: 3
- Estratégia de alocação sob demanda: `lowest-price` (Quando o número de Reservas de Capacidade não utilizadas for menor que a capacidade de destino sob demanda, a frota determina os grupos nos quais iniciar a capacidade sob demanda restante com base na estratégia de alocação sob demanda.)

  Observe que você também pode usar a estratégia de alocação `prioritized` em vez da estratégia de alocação `lowest-price`.

Para obter uma demonstração dos procedimentos que você deve executar para realizar este exemplo, consulte Tutorial: configurar o EC2 Fleet para executar instâncias sob demanda usando reservas de capacidade direcionadas.

Reservas de capacidade

A conta tem as 6 Reservas de Capacidade não utilizadas a seguir em 2 grupos diferentes. Neste exemplo, os grupos diferem de acordo com suas Zonas de disponibilidade. O número de Reservas de Capacidade em cada grupo é indicado por `AvailableInstanceCount`.


```
{
    "CapacityReservationId": "cr-111",
    "InstanceType": "c5.xlarge",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount": 3,
    "InstanceMatchCriteria": "open",
```

```
    "State": "active"
}

{
    "CapacityReservationId": "cr-222",
    "InstanceType": "c5.xlarge",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1b",
    "AvailableInstanceCount": 3,
    "InstanceMatchCriteria": "open",
    "State": "active"
}
```

Configuração da frota

A configuração de frota a seguir mostra somente as configurações pertinentes a este exemplo. A capacidade de destino total é de 10 e o tipo de capacidade de destino padrão é `on-demand`. A estratégia de alocação sob demanda é `lowest-price`. A estratégia de uso para Reservas de Capacidade é `use-capacity-reservations-first`.

Neste exemplo, o preço da instância sob demanda para `c5.xlarge` em `us-east-1` é 0,17 USD por hora.

> **Note**
>
> O tipo da frota deve ser `instant`. Outros tipos de frota não são compatíveis com `use-capacity-reservations-first`.

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "my-launch-template",
                "Version": "1"
            },
            "Overrides": [
               {
                   "InstanceType": "c5.xlarge",
                   "AvailabilityZone": "us-east-1a"
               },
               {
```

```
                    "InstanceType": "c5.xlarge",
                    "AvailabilityZone": "us-east-1b"
                }
            ]
        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 10,
        "DefaultTargetCapacityType": "on-demand"
    },
    "OnDemandOptions": {
        "AllocationStrategy": "lowest-price",
        "CapacityReservationOptions": {
             "UsageStrategy": "use-capacity-reservations-first"
         }
    },
    "Type": "instant"
}
```

Depois de criar a frota `instant` usando a configuração anterior, as 10 instâncias a seguir serão iniciadas para atender à capacidade de destino:

- As Reservas de Capacidade são usadas primeiro para iniciar 6 Instâncias sob demanda da seguinte maneira:
  - 3 Instâncias sob demanda são iniciadas nas 3 `c5.xlarge` Reservas de Capacidade `targeted` no `us-east-1a`
  - 3 Instâncias sob demanda são iniciadas nas 3 `c5.xlarge` Reservas de Capacidade `targeted` no `us-east-1b`
- Para atender à capacidade de destino, 4 Instâncias sob demanda adicionais são iniciadas na capacidade sob demanda regular de acordo com a estratégia de alocação sob demanda, que é `lowest-price` neste exemplo. No entanto, como os grupos têm o mesmo preço (porque o preço é por região e não por zona de disponibilidade), a frota inicia as 4 Instâncias sob demanda restantes em qualquer um dos grupos.

Depois que a frota for lançada, será possível executar describe-capacity-reservations para ver quantas Reservas de capacidade não utilizadas restam. Neste exemplo, você deve ver a resposta a seguir, que mostra que todas as Reservas de capacidade foram usadas em todos os grupos.

```
{
```

```
    "CapacityReservationId": "cr-111",
    "InstanceType": "c5.xlarge",
    "AvailableInstanceCount": 0
}

{
    "CapacityReservationId": "cr-222",
    "InstanceType": "c5.xlarge",
    "AvailableInstanceCount": 0
}
```

Exemplo 7: Configurar o rebalanceamento de capacidade para executar a Instâncias spot de substituição

O exemplo a seguir configura a EC2 Fleet para executar uma Instância spot de substituição quando o Amazon EC2 emite uma recomendação de rebalanceamento para uma Instância spot na frota. Para configurar a substituição automática da Instâncias spot, para `ReplacementStrategy`, especifique `launch-before-terminate`. Para configurar o tempo de espera entre o lançamento das novas instâncias spot substitutas até a exclusão automática das instâncias spot antigas, para `termination-delay`, especifique um valor em segundos. Para obter mais informações, consulte Opções de configuração.

> **Note**
>
> Recomendamos só usar `launch-before-terminate` se você puder prever quanto tempo os procedimentos de desligamento da instância levarão, de modo que as instâncias antigas só sejam terminadas após a conclusão desses procedimentos. Você é cobrado por todas as instâncias enquanto elas estão sendo executadas.

A eficácia da estratégia de rebalanceamento de capacidade depende do número de grupos de capacidade spot especificados na solicitação de Frota do EC2. Recomendamos que você configure a frota com um conjunto diversificado de tipos de instância e zonas de disponibilidade e para `AllocationStrategy`especifique `capacity-optimized`. Para obter mais informações sobre o que você deve considerar ao configurar uma Frota do EC2 para rebalanceamento de capacidade, consulte Use o rebalanceamento de capacidade na frota do EC2 e na frota spot para substituir instâncias spot em risco.

```
{
```

```
    "ExcessCapacityTerminationPolicy": "termination",
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "LaunchTemplate",
                "Version": "1"
            },
                 "Overrides": [
                       {
                           "InstanceType": "c3.large",
                           "WeightedCapacity": 1,
                            "Placement": {
                               "AvailabilityZone": "us-east-1a"
                           }
                       },
                       {
                           "InstanceType": "c4.large",
                           "WeightedCapacity": 1,
                            "Placement": {
                               "AvailabilityZone": "us-east-1a"
                           }
                       },
                       {
                           "InstanceType": "c5.large",
                           "WeightedCapacity": 1,
                            "Placement": {
                               "AvailabilityZone": "us-east-1a"
                           }
                       }
                ]
          }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 5,
        "DefaultTargetCapacityType": "spot"
    },
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized",
        "MaintenanceStrategies": {
            "CapacityRebalance": {
                "ReplacementStrategy": "launch-before-terminate",
                "TerminationDelay": "720"
            }
        }
```

```
    }
}
```

Exemplo 8: iniciar instâncias spot em uma frota otimizada para capacidade

O exemplo a seguir demonstra como configurar uma EC2 Fleet com uma estratégia de alocação spot que otimiza a capacidade. Para otimizar a capacidade, você deve definir `AllocationStrategy` como `capacity-optimized`.

No exemplo a seguir, as três especificações de lançamento especificam três grupos de capacidade spot. A capacidade pretendida é de 50 Instâncias spot. A EC2 Fleet tenta iniciar 50 instâncias spot no grupo de capacidade spot com a capacidade ideal para o número de instâncias em execução.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized",
        },
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "my-launch-template",
                "Version": "1"
            },
                 "Overrides": [
                       {
                           "InstanceType": "r4.2xlarge",
                           "Placement": {
                               "AvailabilityZone": "us-west-2a"
                           },
                      },
                       {
                           "InstanceType": "m4.2xlarge",
                           "Placement": {
                               "AvailabilityZone": "us-west-2b"
                           },
                       },
                       {
                           "InstanceType": "c5.2xlarge",
                           "Placement": {
                               "AvailabilityZone": "us-west-2b"
                           }
                       }
```

```
                ]
            }
    ],
    "TargetCapacitySpecification": {
            "TotalTargetCapacity": 50,
            "DefaultTargetCapacityType": "spot"

    }
}
```

Exemplo 9: iniciar instâncias spot em uma frota otimizada para capacidade com prioridades

O exemplo a seguir demonstra como configurar uma EC2 Fleet com uma estratégia de alocação spot que otimiza a capacidade enquanto usa a prioridade com base no melhor esforço.

Ao usar a estratégia de alocação `capacity-optimized-prioritized`, você pode usar o parâmetro `Priority` para especificar as prioridades dos grupos de capacidade spot, em que quanto menor o número, maior a prioridade. Você também pode definir a mesma prioridade para vários grupos de capacidade spot se você favorecê-los igualmente. Se você não definir uma prioridade para um grupo, ele será considerado o último em termos de prioridade.

Para priorizar grupos de capacidade spot, você deve definir `AllocationStrategy` como `capacity-optimized-prioritized`. A EC2 Fleet otimizará a capacidade primeiro, mas se empenhará em honrar as prioridades (por exemplo, se honrar as prioridades não afetará significativamente a capacidade da EC2 Fleet de provisionar a capacidade ideal). Essa é uma boa opção para workloads em que a possibilidade de interrupção deve ser minimizada e a preferência por determinados tipos de instância for importante.

No exemplo a seguir, as três especificações de lançamento especificam três grupos de capacidade spot. Cada grupo é priorizado, onde quanto menor o número, maior a prioridade. A capacidade pretendida é de 50 Instâncias spot. A EC2 Fleet tenta executar 50 instâncias Spot no grupo de capacidade spot com a maior prioridade com base no melhor esforço, mas otimiza a capacidade em primeiro lugar.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized-prioritized"
        },
    "LaunchTemplateConfigs": [
```

```
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "my-launch-template",
                "Version": "1"
            },
                 "Overrides": [
                        {
                            "InstanceType": "r4.2xlarge",
                            "Priority": 1,
                            "Placement": {
                                "AvailabilityZone": "us-west-2a"
                            },
                        },
                         {
                            "InstanceType": "m4.2xlarge",
                            "Priority": 2,
                            "Placement": {
                                "AvailabilityZone": "us-west-2b"
                            },
                         },
                         {
                            "InstanceType": "c5.2xlarge",
                            "Priority": 3,
                            "Placement": {
                                "AvailabilityZone": "us-west-2b"
                            }
                         }
                    ]
             }
    ],
    "TargetCapacitySpecification": {
            "TotalTargetCapacity": 50,
            "DefaultTargetCapacityType": "spot"
}
```

Exemplo 10: iniciar instâncias spot em uma frota otimizada para preço-capacidade

O exemplo a seguir demonstra como configurar uma Frota EC2 com uma estratégia de alocação spot que otimize tanto para capacidade quanto por menor preço. Para otimizar para capacidade e levar em consideração o preço, você deve definir a `AllocationStrategy` de spot como `price-capacity-optimized`.

No exemplo a seguir, as três especificações de lançamento especificam três grupos de capacidade spot. A capacidade pretendida é de 50 Instâncias spot. A frota do EC2 tenta iniciar 50 instâncias spot no grupo de capacidade spot com a capacidade ideal para o número de instâncias que estão sendo iniciadas e, ao mesmo tempo, escolher o grupo com menor preço.

```
{
    "SpotOptions": {
        "AllocationStrategy": "price-capacity-optimized",
        "MinTargetCapacity": 2,
        "SingleInstanceType": true
    },
    "OnDemandOptions": {
        "AllocationStrategy": "lowest-price"
    },
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "my-launch-template",
                "Version": "1"
            },
                 "Overrides": [
                       {
                           "InstanceType": "r4.2xlarge",
                           "Placement": {
                               "AvailabilityZone": "us-west-2a"
                           },
                      },
                       {
                           "InstanceType": "m4.2xlarge",
                           "Placement": {
                               "AvailabilityZone": "us-west-2b"
                           },
                       },
                       {
                           "InstanceType": "c5.2xlarge",
                           "Placement": {
                               "AvailabilityZone": "us-west-2b"
                           }
                       }
                 ]
           }
    ],
    "TargetCapacitySpecification": {
```

```
        "TotalTargetCapacity": 50,
        "OnDemandTargetCapacity":0,
        "SpotTargetCapacity":50,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

Exemplo 11: configurar a seleção de tipo de instância baseada em atributos

O exemplo a seguir demonstra como configurar uma Frota do EC2 para usar a seleção de tipo de instância baseada em atributos para identificar tipos de instância. Para especificar os atributos de instância necessários, especifique os atributos na estrutura `InstanceRequirements`.

No exemplo a seguir, dois atributos de instância são especificados:

- `VCpuCount`: é especificado um mínimo de 2 vCPUs. Como nenhum máximo é especificado, não há limite máximo.
- `MemoryMiB`: é especificado um mínimo de 4 MiB de memória. Como nenhum máximo é especificado, não há limite máximo.

Qualquer tipo de instância que tenha 2 ou mais vCPUs e 4 MiB ou mais de memória será identificado. Porém, a estratégia proteção de preços e de alocação pode excluir alguns tipos de instância quando a Frota do EC2 provisiona a frota.

Para obter uma lista e descrições de todos os atributos que você pode especificar, consulte InstanceRequirements na Amazon EC2 API Reference (Referência de API do Amazon EC2).

```
{
 "SpotOptions": {
  "AllocationStrategy": "price-capacity-optimized"
 },
 "LaunchTemplateConfigs": [{
  "LaunchTemplateSpecification": {
   "LaunchTemplateName": "my-launch-template",
   "Version": "1"
  },
  "Overrides": [{
   "InstanceRequirements": {
    "VCpuCount": {
     "Min": 2
```

```
    },
    "MemoryMiB": {
     "Min": 4
    }
   }
  }]
 }],
 "TargetCapacitySpecification": {
  "TotalTargetCapacity": 20,
  "DefaultTargetCapacityType": "spot"
 },
 "Type": "instant"
}
```

Exemplo de configurações da CLI para frotas spot

É possível definir a configuração da frota spot em um arquivo JSON e, em seguida, referenciar esse arquivo com o comando request-spot-fleet da AWS CLI para criar a frota, da seguinte maneira:

```
aws ec2 request-spot-fleet --spot-fleet-request-config file://file_name.json
```

Os exemplos a seguir ilustram as configurações de inicialização para vários casos de uso de frotas spot. Para obter mais informações sobre os parâmetros de configuração, consulte request-spot-fleet. Para obter mais informações sobre a criação de uma frota spot, consulte Criar uma Frota spot.

> **Note**
>
> Em frota spot, não é possível especificar um ID de interface de rede em uma especificação de execução. Omita o parâmetro `NetworkInterfaceID` no modelo ou na especificação de execução.

Exemplos

- Exemplo 1: executar instâncias spot usando a zona de disponibilidade com menor preço na região
- Exemplo 2: executar instâncias spot usando a zona de disponibilidade com o menor preço em uma lista especificada
- Exemplo 3: executar instâncias spot usando o tipo de instância com o menor preço em uma lista
- Exemplo 4. Cancelar o preço da solicitação

- Exemplo 5: executar uma frota spot usando a estratégia de alocação diversificada
- Exemplo 6: executar uma frota spot usando o peso da instância
- Exemplo 7: executar uma frota spot usando capacidade sob demanda
- Exemplo 8: Configurar o rebalanceamento de capacidade para executar a Instâncias spot de substituição
- Exemplo 9: iniciar instâncias spot em uma frota otimizada para capacidade
- Exemplo 10: iniciar instâncias spot em uma frota otimizada para capacidade com prioridades
- Exemplo 11: executar instâncias spot em uma frota priceCapacityOptimized
- Exemplo 12: configurar a seleção de tipo de instância baseada em atributos

Exemplo 1: executar instâncias spot usando a zona de disponibilidade com menor preço na região

O exemplo a seguir determina uma única especificação de execução sem uma zona de disponibilidade nem sub-rede. A frota spot executa as instâncias na zona de disponibilidade de menor preço que tem uma sub-rede padrão. O preço que você paga não excede o preço sob demanda.

```
{
  "TargetCapacity": 20,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "KeyName": "my-key-pair",
          "SecurityGroups": [
              {
                  "GroupId": "sg-1a2b3c4d"
              }
          ],
          "InstanceType": "m3.medium",
          "IamInstanceProfile": {
              "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"
          }
      }
  ]
}
```

Exemplo 2: executar instâncias spot usando a zona de disponibilidade com o menor preço em uma lista especificada

Os exemplos a seguir determinam duas especificações de execução com zonas de disponibilidade ou sub-redes diferentes, mas o mesmo tipo de instância e AMI.

Zonas de disponibilidade

A frota spot executa as instâncias na sub-rede padrão da zona de disponibilidade de menor preço especificada.

```
{
  "TargetCapacity": 20,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "KeyName": "my-key-pair",
          "SecurityGroups": [
              {
                  "GroupId": "sg-1a2b3c4d"
              }
          ],
          "InstanceType": "m3.medium",
          "Placement": {
              "AvailabilityZone": "us-west-2a, us-west-2b"
          },
          "IamInstanceProfile": {
              "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"
          }
      }
  ]
}
```

Sub-redes

É possível 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 grupo de segurança 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::123456789012:instance-profile/my-iam-role"
        }
    }
...
```

Exemplo 3: executar instâncias spot usando o tipo de instância com o menor preço em uma lista

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.

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": "c5.4xlarge",
          "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": "c5.4xlarge",
          "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.

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 Usar estratégias de alocação para determinar como a frota do EC2 ou a frota spot atende à capacidade spot e sob demanda.

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"
            }
        }
    ]
}
```

Sub-rede

```
{
    "SpotPrice": "0.70",
    "TargetCapacity": 30,
    "AllocationStrategy": "diversified",
    "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
    "LaunchSpecifications": [
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "c4.2xlarge",
            "SubnetId": "subnet-1a2b3c4d"
        },
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "m3.2xlarge",
            "SubnetId": "subnet-1a2b3c4d"
        },
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "r3.2xlarge",
            "SubnetId": "subnet-1a2b3c4d"
        }
    ]
}
```

Para aumentar a chance de que uma solicitação spot possa ser atendida pela capacidade do EC2 no caso de uma interrupção em uma das zonas de disponibilidade, uma prática recomendada é diversificar entre zonas. Nesse cenário, inclua cada zona de disponibilidade possível para você na especificação de execução. E, em vez de usar sempre a mesma sub-rede, use três sub-redes exclusivas (cada mapeamento para uma zona de disponibilidade diferente).

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"
          }
      }
  ]
}
```

Sub-rede

```
{
    "SpotPrice": "0.70",
```

```
    "TargetCapacity": 30,
    "AllocationStrategy": "diversified",
    "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
    "LaunchSpecifications": [
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "c4.2xlarge",
            "SubnetId": "subnet-1a2b3c4d"
        },
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "m3.2xlarge",
            "SubnetId": "subnet-2a2b3c4d"
        },
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "r3.2xlarge",
            "SubnetId": "subnet-3a2b3c4d"
        }
    ]
}
```

Exemplo 6: executar uma frota spot usando o peso da instância

Os exemplos a seguir usam o peso da instância, o que significa que o preço é por hora em vez de ser por hora de instância. Cada configuração de execução lista um tipo de instância e um peso diferentes. A frota spot seleciona o tipo de instância com o menor preço por hora de unidade. A frota spot calcula o número de instâncias spot a serem executadas dividindo a capacidade de destino pelo peso da instância. Se o resultado não for um valor inteiro, a frota spot o arredondará para o próximo valor inteiro, para que o tamanho de sua frota não fique abaixo de sua capacidade de destino.

Se a solicitação `r3.2xlarge` for feita com êxito, o spot provisionará 4 dessas instâncias. Divida 20 por 6 para um total de 3,33 instâncias, em seguida, arredonde para 4 instâncias.

Se a solicitação `c3.xlarge` for feita com êxito, o spot provisionará 7 dessas instâncias. Divida 20 por 3 para um total de 6,66 instâncias, em seguida, arredonde para 7 instâncias.

Para obter mais informações, consulte Usar ponderação de instâncias para gerenciar o custo e a performance da frota do EC2 ou da frota spot.

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
      }
    ]
}
```

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 usando capacidade sob demanda

Para garantir que você sempre tenha capacidade de instância, você pode incluir uma solicitação de capacidade sob demanda na solicitação de frota spot. Se houver capacidade, a solicitação de sob demanda sempre será atendida. O equilíbrio da capacidade de destino será atendido como Spot se houver capacidade e disponibilidade.

O exemplo a seguir especifica a capacidade desejada de destino como 10, da qual 5 deve ser sob demanda. A capacidade spot não é especificada. Ela está implícita no saldo da capacidade pretendida menos a capacidade sob demanda. O Amazon EC2 executará cinco unidades de capacidade como sob demanda e cinco unidades de capacidade (10-5=5) como spot se houver disponibilidade e capacidade do Amazon EC2 disponíveis.

```
{
  "IamFleetRole": "arn:aws:iam::123456789012: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"
        }
      ]
    }
  ]
```

```
}
```

Exemplo 8: Configurar o rebalanceamento de capacidade para executar a Instâncias spot de substituição

O exemplo a seguir configura a frota spot para executar uma instância spot de substituição quando o Amazon EC2 emite uma recomendação de rebalanceamento para uma instância spot na frota. Para configurar a substituição automática da Instâncias spot, para `ReplacementStrategy`, especifique `launch-before-terminate`. Para configurar o tempo de espera entre o lançamento das novas instâncias spot substitutas até a exclusão automática das instâncias spot antigas, para `termination-delay`, especifique um valor em segundos. Para obter mais informações, consulte Opções de configuração.

> **Note**
>
> Recomendamos só usar `launch-before-terminate` se você puder prever quanto tempo os procedimentos de desligamento da instância levarão. Isso garante que as instâncias antigas só sejam terminadas após a conclusão dos procedimentos de desligamento. Você é cobrado por todas as instâncias enquanto elas estão sendo executadas.

A eficácia da estratégia de rebalanceamento de capacidade depende do número de grupos de capacidade spot especificados na solicitação de frota spot. Recomendamos que você configure a frota com um conjunto diversificado de tipos de instância e zonas de disponibilidade e para `AllocationStrategy`especifique `capacityOptimized`. Para obter mais informações sobre o que você deve considerar ao configurar uma frota spot para rebalanceamento de capacidade, consulte Use o rebalanceamento de capacidade na frota do EC2 e na frota spot para substituir instâncias spot em risco.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "capacityOptimized",
        "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "LaunchTemplate",
```

```
                    "Version": "1"
                },
                 "Overrides": [
                       {
                           "InstanceType": "c3.large",
                           "WeightedCapacity": 1,
                           "Placement": {
                               "AvailabilityZone": "us-east-1a"
                           }
                       },
                       {
                           "InstanceType": "c4.large",
                           "WeightedCapacity": 1,
                           "Placement": {
                               "AvailabilityZone": "us-east-1a"
                           }
                       },
                       {
                           "InstanceType": "c5.large",
                           "WeightedCapacity": 1,
                           "Placement": {
                               "AvailabilityZone": "us-east-1a"
                           }
                       }
                ]
          }
    ],
        "TargetCapacity": 5,
        "SpotMaintenanceStrategies": {
            "CapacityRebalance": {
                "ReplacementStrategy": "launch-before-terminate",
                "TerminationDelay": "720"
            }
        }
    }
}
```

Exemplo 9: iniciar instâncias spot em uma frota otimizada para capacidade

O exemplo a seguir demonstra como configurar uma frota spot com uma estratégia de alocação spot que otimiza a capacidade. Para otimizar a capacidade, você deve definir `AllocationStrategy` como `capacityOptimized`.

No exemplo a seguir, as três especificações de lançamento especificam três grupos de capacidade spot. A capacidade pretendida é de 50 Instâncias spot. A frota spot tenta iniciar 50 instâncias spot no grupo de capacidade spot com a capacidade ideal para o número de instâncias em execução.

```
{
    "TargetCapacity": "50",
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "capacityOptimized",
    },
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "my-launch-template",
                "Version": "1"
            },
            "Overrides": [
                {
                    "InstanceType": "r4.2xlarge",
                    "AvailabilityZone": "us-west-2a"
                },
                {
                    "InstanceType": "m4.2xlarge",
                    "AvailabilityZone": "us-west-2b"
                },
                {
                    "InstanceType": "c5.2xlarge",
                    "AvailabilityZone": "us-west-2b"
                }
            ]
        }
    ]
}
```

Exemplo 10: iniciar instâncias spot em uma frota otimizada para capacidade com prioridades

O exemplo a seguir demonstra como configurar uma frota spot com uma estratégia de alocação spot que otimiza a capacidade enquanto usa a prioridade com base no melhor esforço.

Ao usar a estratégia de alocação `capacityOptimizedPrioritized`, você pode usar o parâmetro `Priority` para especificar as prioridades dos grupos de capacidade spot, em que quanto menor o

número, maior a prioridade. Você também pode definir a mesma prioridade para vários grupos de capacidade spot se você favorecê-los igualmente. Se você não definir uma prioridade para um grupo, ele será considerado o último em termos de prioridade.

Para priorizar grupos de capacidade spot, você deve definir `AllocationStrategy` como `capacityOptimizedPrioritized`. A frota spot otimizará a capacidade em primeiro lugar, mas honrará as prioridades com o melhor esforço (por exemplo, se honrar as prioridades não afetará significativamente a capacidade da frota spot de provisionar a capacidade ideal). Essa é uma boa opção para workloads em que a possibilidade de interrupção deve ser minimizada e a preferência por determinados tipos de instância for importante.

No exemplo a seguir, as três especificações de lançamento especificam três grupos de capacidade spot. Cada grupo é priorizado, onde quanto menor o número, maior a prioridade. A capacidade pretendida é de 50 Instâncias spot. A frota spot tenta executar 50 instâncias Spot no grupo de capacidade spot com a maior prioridade com base no melhor esforço, mas otimiza a capacidade em primeiro lugar.

```
{
    "TargetCapacity": "50",
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "capacityOptimizedPrioritized"
    },
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "my-launch-template",
                "Version": "1"
            },
            "Overrides": [
                {
                    "InstanceType": "r4.2xlarge",
                   "Priority": 1,
                    "AvailabilityZone": "us-west-2a"
                },
                {
                          "InstanceType": "m4.2xlarge",
                          "Priority": 2,
                          "AvailabilityZone": "us-west-2b"
                },
                {
                          "InstanceType": "c5.2xlarge",
                          "Priority": 3,
```

```
                        "AvailabilityZone": "us-west-2b"
                }
            ]
        }
    ]
}
```

Exemplo 11: executar instâncias spot em uma frota priceCapacityOptimized

O exemplo a seguir demonstra como configurar uma frota spot com uma estratégia de alocação spot que otimize tanto para capacidade quanto para o menor preço. Para otimizar para capacidade e levar em consideração o preço, você deve definir a `AllocationStrategy` de spot como `priceCapacityOptimized`.

No exemplo a seguir, as três especificações de lançamento especificam três grupos de capacidade spot. A capacidade pretendida é de 50 Instâncias spot. A frota spot tenta iniciar 50 instâncias spot no grupo de capacidade spot com a capacidade ideal para o número de instâncias que estão sendo iniciadas e ao mesmo tempo, escolher o grupo com menor preço.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "priceCapacityOptimized",
        "OnDemandAllocationStrategy": "lowestPrice",
        "ExcessCapacityTerminationPolicy": "default",
        "IamFleetRole": "arn:aws:iam::111111111111:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateId": "lt-0123456789example",
                    "Version": "1"
                },
                "Overrides": [
                     {
                          "InstanceType": "r4.2xlarge",
                          "AvailabilityZone": "us-west-2a"
                      },
                      {
                          "InstanceType": "m4.2xlarge",
                          "AvailabilityZone": "us-west-2b"
                      },
                      {
```

```
                        "InstanceType": "c5.2xlarge",
                        "AvailabilityZone": "us-west-2b"
                    }
                ]
            }
        ],
        "TargetCapacity": 50,
        "Type": "request"
    }
}
```

Exemplo 12: configurar a seleção de tipo de instância baseada em atributos

O exemplo a seguir demonstra como configurar uma frota spot para usar a seleção de tipo de instância baseada em atributos para identificar tipos de instância. Para especificar os atributos de instância necessários, especifique os atributos na estrutura `InstanceRequirements`.

No exemplo a seguir, dois atributos de instância são especificados:

- `VCpuCount`: é especificado um mínimo de 2 vCPUs. Como nenhum máximo é especificado, não há limite máximo.
- `MemoryMiB`: é especificado um mínimo de 4 MiB de memória. Como nenhum máximo é especificado, não há limite máximo.

Qualquer tipo de instância que tenha 2 ou mais vCPUs e 4 MiB ou mais de memória será identificado. Porém, a estratégia proteção de preços e de alocação pode excluir alguns tipos de instância quando a frota spot provisiona a frota.

Para obter uma lista e descrições de todos os atributos que você pode especificar, consulte InstanceRequirements na Amazon EC2 API Reference (Referência de API do Amazon EC2).

```
{
 "AllocationStrategy": "priceCapacityOptimized",
 "TargetCapacity": 20,
 "Type": "request",
 "LaunchTemplateConfigs": [{
  "LaunchTemplateSpecification": {
   "LaunchTemplateName": "my-launch-template",
   "Version": "1"
  },
  "Overrides": [{
```

```
   "InstanceRequirements": {
    "VCpuCount": {
     "Min": 2
    },
    "MemoryMiB": {
     "Min": 4
    }
   }
  }]
 }]
}
```

Cotas para frotas do EC2 e frotas spot

Sua Conta da AWS tem cotas padrão para cada serviço da AWS, que anteriormente eram chamadas de limites. A menos que especificado de outra forma, cada cota é específica da região.

As cotas normais do Amazon EC2 se aplicam a instâncias executadas por uma EC2 Fleet ou uma frota spot, como limites de instância spot e limites de volume.

Além disso, sua Conta da AWS tem as seguintes cotas relacionadas à frota do EC2 e à frota spot:

Descrição da cota	Quota
O número de frotas do EC2 e frotas spot por região dos tipos `maintain` e `request` nos estados `active`, `deleted_running` e `cancelled_running`	1.000 [1] [2] [3]
O número de frotas EC2 do tipo `instant`	Ilimitado
O número de grupos de capacidade spot (combinação exclusiva de tipo de instância e sub-rede) para frotas do EC2 e frotas spot dos tipos `maintain` e `request`	300 [1]
O número de grupos de capacidade spot (combinação exclusiva de tipo de instância e sub-rede) para frotas do EC2 do tipo `instant`	Ilimitado

Descrição da cota	Quota
O tamanho dos dados de usuário em uma especificação de inicialização	16 KB [2]
A capacidade pretendida por frota do EC2 ou frota spot	10.000
A capacidade de destino em todas as frotas do EC2 e frotas spot de uma região	100.000 [1]
Uma solicitação de EC2 Fleet ou de frota spot não pode abranger regiões.	
Uma solicitação de EC2 Fleet ou de frota spot não pode abranger sub-redes diferentes na mesma zona de disponibilidade.	

[1] Essas cotas aplicam-se a frotas do EC2 e frotas spot.

[2] Estas são cotas fixas. Você não pode solicitar um aumento dessas cotas.

[3] Depois de excluir uma frota do EC2 ou cancelar uma solicitação de frota spot, e se você especificou que a frota não deverá terminar suas instâncias spot quando excluiu ou cancelou a solicitação, a solicitação de frota inserirá o estado `deleted_running` (frota do EC2) ou `cancelled_running` (frota spot). As instâncias continuarão em execução até que sejam interrompidas ou terminadas manualmente. Se você terminar as instâncias, a solicitação de frota entrará no estado `deleted_terminating` (frota do EC2) ou `cancelled_terminating` (frota spot) e não contará para essa cota. Para obter mais informações, consulte Excluir uma solicitação de frota do EC2 e as instâncias da frota e Cancelar (excluir) uma solicitação de frota spot.

Solicitar um aumento de cota para a capacidade pretendida

Se precisar exceder a cota padrão da capacidade de destino, solicite um aumento de cota.

Como solicitar um aumento de cota para a capacidade pretendida

1. Abra o formulário Create case (Criar caso) no Suporte Center.
2. Escolha Service limit increase (Aumento de limite do serviço).

3. Em Limit type (Tipo de limite), escolha EC2 Fleet (Frota do EC2).
4. Em Region (Região), escolha a região da AWS na qual solicitar o aumento da cota.
5. Em Limit (Limite), escolha 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]), dependendo da cota que deseja aumentar.
6. Em New limit value (Novo valor de limite), insira o novo valor.
7. Para solicitar um aumento para outra cota, escolha Add another request (Adicionar outra solicitação) e repita as etapas de 4 a 6.
8. Em Use case description (Descrição do caso de uso), insira o motivo para solicitar um aumento de cota.
9. Em Contact options (Opções de contato), especifique o idioma de contato e o método de contato de sua preferência.
10. Selecione Enviar.

Redes no Amazon EC2

A Amazon VPC permite que você execute recursos da AWS, como as instâncias do Amazon EC2, em uma rede virtual dedicada à conta da AWS, conhecida como uma nuvem virtual privada (VPC). Ao executar uma instância, é possível selecionar uma sub-rede na VPC. A instância é configurada com uma interface de rede primária, que é uma placa de rede virtual lógica. A instância recebe um endereço IP privado primário do endereço IPv4 da sub-rede e é atribuída à interface da rede primária.

É possível controlar se a instância recebe um endereço IP público do grupo da Amazon de endereços IP públicos. O endereço IP público de uma instância é associado à sua instância somente até que ela seja interrompida ou encerrada. Se você precisar de um endereço IP público persistente, poderá alocar um endereço IP elástico para sua conta da AWS e associá-lo a uma instância ou uma interface de rede. Um endereço IP elástico permanece associado à sua conta AWS até que você o libere e possa movê-lo de uma instância à outra, conforme necessário. É possível trazer o seu próprio intervalo de endereços IP para sua conta AWS, onde ele aparece como um grupo de endereços e, em seguida, alocar endereços IP elásticos do seu grupo de endereços.

Para aumentar a performance da rede e reduzir a latência, é possível executar instâncias em um grupo de posicionamento. É possível obter uma performance significativamente superior de pacotes por segundo (PPS) usando redes aprimoradas. É possível acelerar aplicações de computação e machine learning de alta performance usando um Elastic Fabric Adapter (EFA), que é um dispositivo de rede que pode ser anexado a um tipo de instância compatível.

Recursos

- A VPC abrange as zonas de disponibilidade e a zona Wavelength.
- Endereçamento IP de instâncias do Amazon EC2
- Nomes de host e domínios de instâncias do EC2
- Trazer seus próprios endereços IP (BYOIP) para o Amazon EC2
- Endereços IP elásticos
- Interfaces de rede elástica
- Largura de banda de rede de instâncias do Amazon EC2
- Redes aperfeiçoadas para instâncias do Amazon EC2
- Elastic Fabric Adapter para workloads de IA/ML e HPC no Amazon EC2
- Topologia do Amazon EC2

- Grupos de posicionamento para as instâncias do Amazon EC2
- Unidade de transmissão máxima (MTU) de rede para a instância do EC2
- Nuvens privadas virtuais para as instâncias do EC2
- Redes secundárias

A VPC abrange as zonas de disponibilidade e a zona Wavelength.

O Amazon EC2 está hospedado em vários locais no mundo todo. Esses locais são compostos por Regiões da AWS, zonas de disponibilidade, zonas locais, AWS Outposts e zonas do Wavelength.

- Regiões são áreas geográficas distintas.
- Zonas de disponibilidade são vários locais isolados dentro de cada Região.
- Zonas locais fornecem a capacidade de colocar recursos, como computação e armazenamento, em vários locais mais próximos dos usuários finais.
- Zonas do Wavelength fornecem a capacidade de criar aplicações que oferecem baixíssimas latências para dispositivos 5G e usuários finais. O Wavelength implanta os serviços de armazenamento e computação padrão da AWS até a borda das redes 5G de operadoras de telecomunicação.
- O AWS Outposts leva serviços, infraestrutura e modelos operacionais nativos da AWS a praticamente qualquer data center, espaço de colocalização ou on-premises.

A AWS opera data centers de última geração com alta disponibilidade. Embora sejam raras, podem ocorrer falhas que afetam a disponibilidade das instâncias que estão no mesmo local. Se você hospedar todas as suas instâncias em um único local afetado por uma falha, nenhuma delas ficará disponível.

Para obter mais informações, consulte Infraestrutura global da AWS.

Conteúdo

- Regiões
- Zonas de disponibilidade
- zonas locais
- Zonas do Wavelength
- AWS Outposts

Regiões

Cada região é projetada para ser isolada das outras regiões. Isso proporciona a maior tolerância a falhas e estabilidade possível.

Ao executar uma instância, selecione uma região que deixe suas instâncias mais próximas de clientes específicos ou cumpra os requisitos legais ou outros. Você pode lançar instâncias em várias regiões.

Ao visualizar os recursos, você vê apenas os recursos que estão vinculados à região da especificada. Isso ocorre porque as regiões da são isoladas entre si e nós não replicamos os recursos entre regiões da automaticamente.

Regiões disponíveis

Para obter a lista de regiões disponíveis, consulte Regiões da AWS.

Endpoints regionais para o Amazon EC2

Ao trabalhar com uma instância usando a interface de linha de comando ou ações de API, é necessário especificar seu endpoint regional. Para obter mais informações sobre as regiões e os endpoints para o Amazon EC2, consulte Amazon EC2 service endpoints no Guia do desenvolvedor do Amazon EC2.

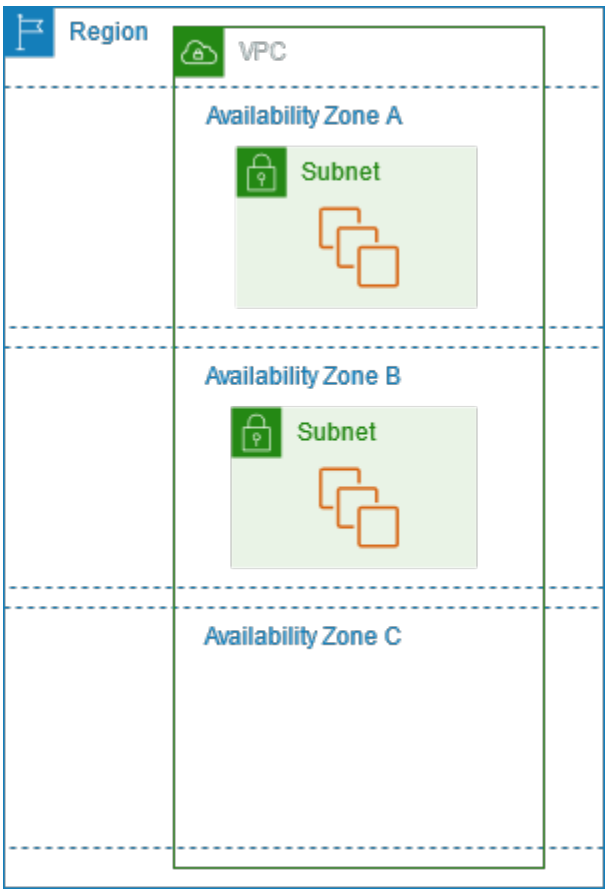
Para obter mais informações, consulte Regiões da AWS no Guia do usuário de zonas de disponibilidade e Regiões da AWS.

Zonas de disponibilidade

Cada região contém vários locais isolados conhecidos como Zonas de Disponibilidade. O código da zona de disponibilidade é o seu código de região seguido por um identificador de letra. Por exemplo, `.us-east-1a`

Ao lançar instâncias do EC2 em várias Zonas de disponibilidade, você pode proteger suas aplicações contra a falha de um único local na região.

O diagrama a seguir ilustra várias zonas de disponibilidade em uma região da AWS. A zona de disponibilidade A e a zona de disponibilidade B têm uma sub-rede, e cada sub-rede tem instâncias do EC2. A zona de disponibilidade C não tem sub-redes, portanto, não é possível iniciar instâncias nela.



Para obter mais informações, consulte Nuvens privadas virtuais para as instâncias do EC2.

Zonas de disponibilidade por região

Para ver a lista de Zonas de disponibilidade por região, consulte Zonas de disponibilidade da AWS.

Instâncias nas zonas de disponibilidade

Ao lançar uma instância, você seleciona uma Região e uma nuvem privada virtual (VPC). Em seguida, você pode selecionar uma sub-rede de uma das Zonas de disponibilidade ou permitir que escolhamos uma sub-rede para você. Ao lançar suas instâncias iniciais, recomendamos que você nos deixe selecionar uma Zona de disponibilidade para você com base na integridade do sistema e na 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 existentes.

Se distribuir instâncias em várias Zonas de disponibilidade e uma instância falhar, poderá projetar sua aplicação de modo que uma instância em outra Zona de disponibilidade trate das solicitações.

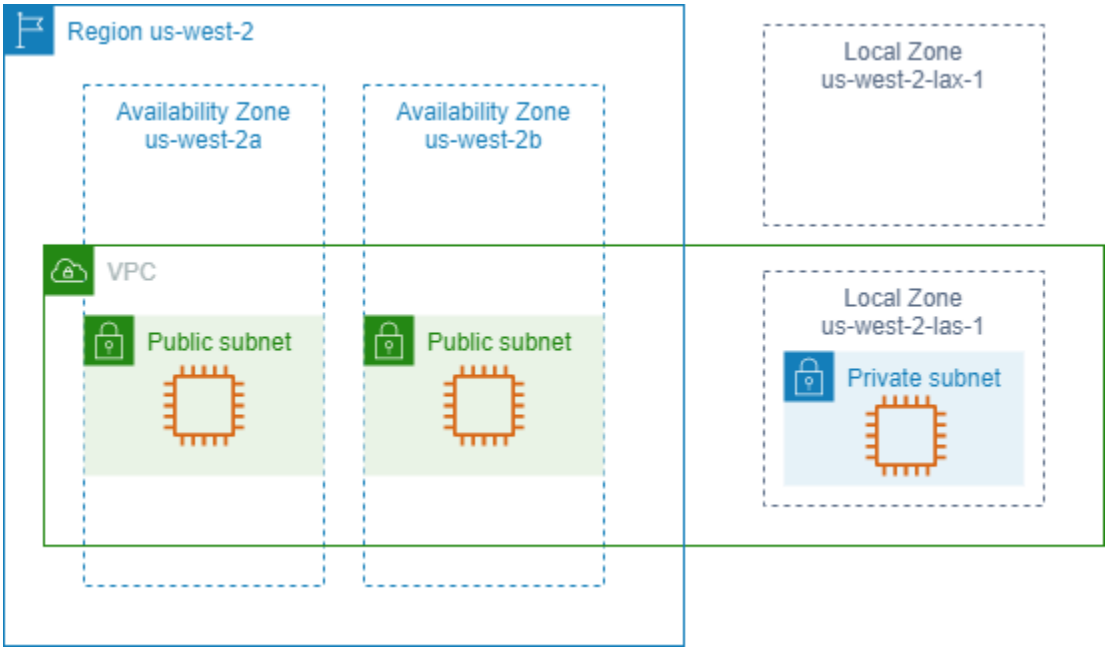
Para obter mais informações, consulte Zonas de disponibilidade da AWS no Guia do usuário de zonas de disponibilidade e Regiões da AWS.

zonas locais

Uma zona local é uma extensão de uma região da AWS na proximidade geográfica de seus usuários. As zonas locais têm suas próprias conexões com a Internet e são compatíveis com o Direct Connect para que os recursos criados em uma zona local possam atender usuários locais com comunicações de baixa latência. Para obter mais informações, consulte O que são zonas locais da AWS? no Guia do usuário de zonas locais da AWS.

O código da zona local é o código da região da seguido por um identificador que indica o local físico. Por exemplo, `us-west-2-lax-1` em Los Angeles.

O diagrama a seguir ilustra a região da AWS `us-west-2`, duas de suas zonas de disponibilidade e duas de suas zonas locais. A VPC abrange as zonas de disponibilidade e uma das zonas locais. Cada zona na VPC tem uma sub-rede, e cada sub-rede tem uma instância.



Zonas locais disponíveis

Para ver a lista de zonas locais disponíveis, consulte Available Local Zones no Guia do usuário de zonas locais da AWS. Para ver a lista de zonas locais anunciadas, consulte Localizações de zonas locais da AWS.

Instâncias em zonas locais

Para usar uma zona local, é necessário ativá-la primeiro. Depois, crie uma sub-rede na zona local. É possível especificar a sub-rede da zona local ao executar instâncias, o que a coloca na sub-rede da zona local na zona local.

Ao executar uma instância em uma zona local, você também aloca um endereço IP de um grupo de borda de rede. Um grupo de bordas de rede é um conjunto exclusivo de zonas de disponibilidade, zonas locais ou zonas do Wavelength, das quais a AWS anuncia endereços IP, por exemplo, `us-west-2-lax-1a`. É possível alocar os endereços IP de um grupo de bordas de rede:

- Endereços IPv4 elásticos fornecidos pela Amazon
- Endereços IPv6 da VPC fornecidos pela Amazon (disponíveis somente nas zonas de Los Angeles)

Para obter mais informações sobre como iniciar uma instância em uma zona local, consulte Conceitos básicos do AWS Local Zones no Guia do usuário do AWS Local Zones.

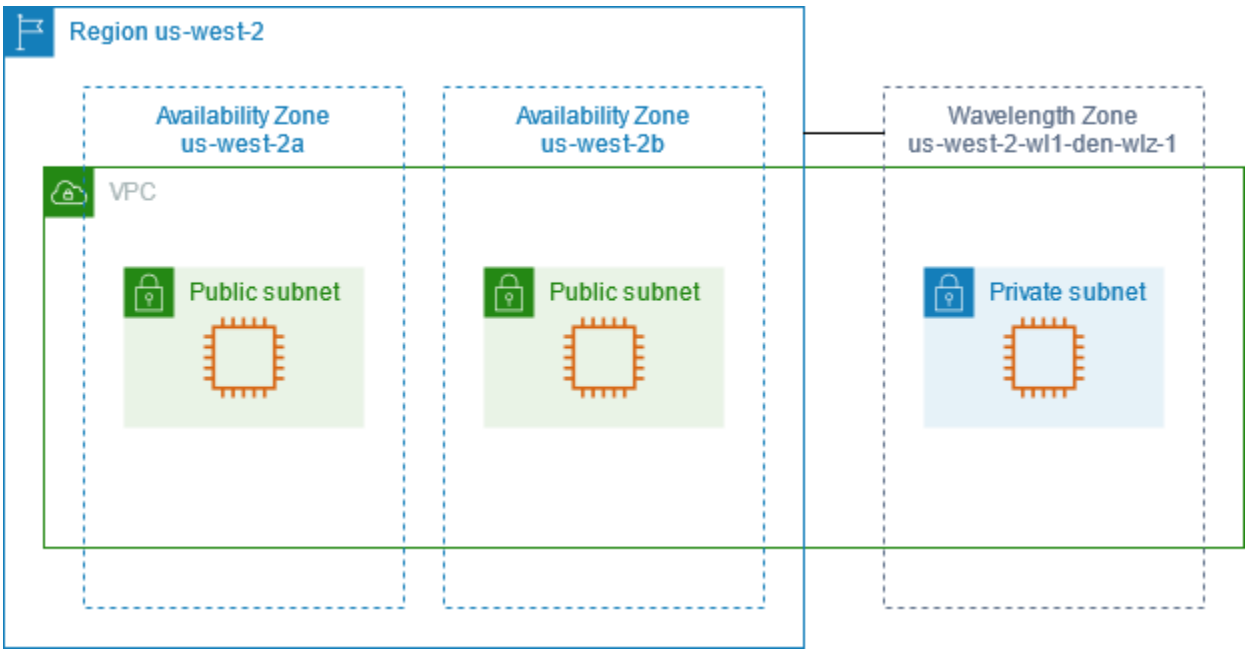
Zonas do Wavelength

O AWS Wavelength permite que os desenvolvedores criem aplicações que oferecem baixíssimas latências para dispositivos móveis e usuários finais. O Wavelength implanta os serviços de armazenamento e computação padrão da AWS até a borda das redes 5G de operadoras de telecomunicação. Os desenvolvedores podem estender uma nuvem privada virtual (VPC) para uma ou mais zonas do Wavelength e usar os recursos da AWS, como instâncias do Amazon EC2, para executar aplicações que exigem baixíssima latência e uma conexão com serviços da AWS na região.

Uma Wavelength Zone é uma zona isolada no local da transportadora em que a infraestrutura de Wavelength é implantada. As zonas de Wavelength estão vinculadas a uma região. Uma zona de Wavelength é uma extensão lógica de uma região e é gerenciada pelo plano de controle na região.

O código para uma zona Wavelength é seu código de região seguido por um identificador que indica o local físico. Por exemplo, `us-east-1-wl1-bos-wlz-1` em Boston.

O diagrama a seguir ilustra a região da AWS `us-west-2`, duas de suas zonas de disponibilidade e uma zona Wavelength. A VPC abrange as zonas de disponibilidade e a zona Wavelength. Cada zona na VPC tem uma sub-rede, e cada sub-rede tem uma instância.



As Wavelength Zones não estão disponíveis em todas as regiões. Para obter informações sobre as regiões compatíveis com as zonas do Wavelength consulte Zonas do Wavelength disponíveis no Guia do desenvolvedor da AWS Wavelength.

Zonas do Wavelength disponíveis

Para ver uma lista das zonas do Wavelength disponíveis, consulte Available Wavelength Zones no Guia do AWS Wavelength.

Instâncias nas zonas do Wavelength

Para usar uma zona de Wavelength, é necessário primeiro escolher a zona. Depois, crie uma sub-rede na zona do Wavelength. É possível especificar a sub-rede do Wavelength ao executar instâncias. Você também aloca o endereço IP de uma operadora de um grupo de bordas de rede, que é um conjunto exclusivo de zonas de disponibilidade, zonas locais ou zonas do Wavelength, das quais a AWS anuncia endereços IP, por exemplo, `us-east-1-wl1-bos-wlz-1`.

Para obter instruções detalhadas para executar uma instância em uma zona do Wavelength, consulte Get started with AWS Wavelength no Guia do desenvolvedor do AWS Wavelength.

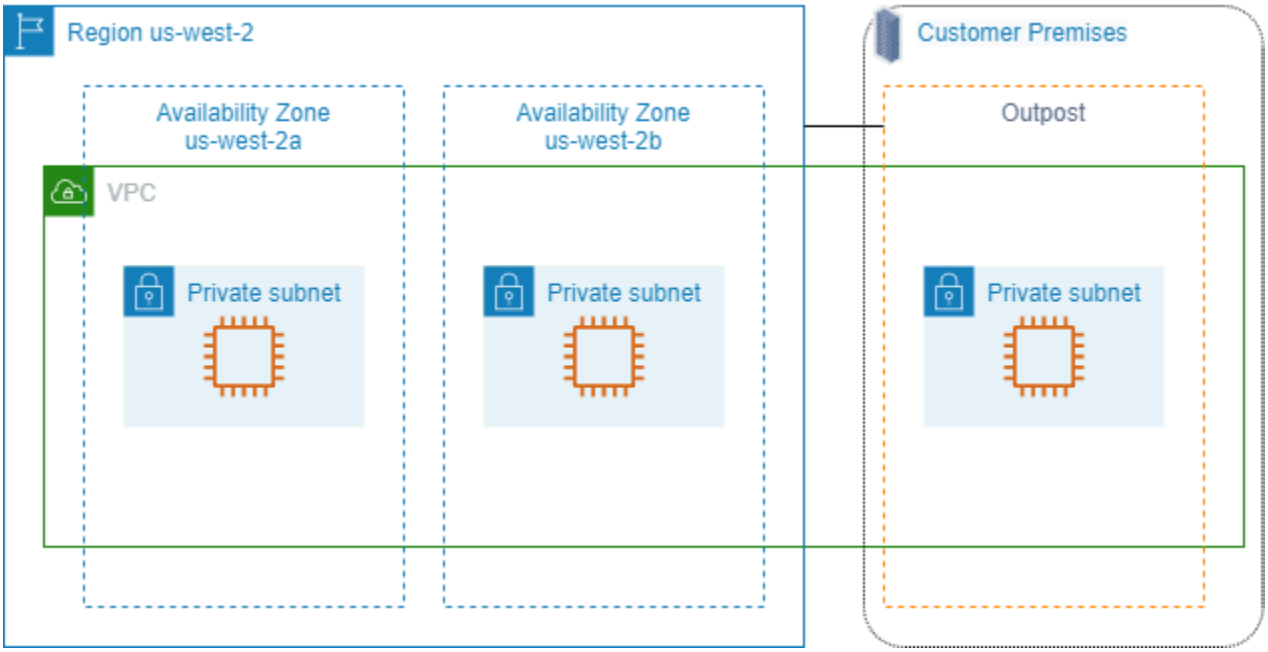
AWS Outposts

O AWS Outposts é um serviço totalmente gerenciado que estende a infraestrutura, os serviços, as APIs e as ferramentas da AWS no local do cliente. Ao fornecer acesso local à infraestrutura gerenciada pela AWS, o AWS Outposts permite que os clientes criem e executem aplicações on-

premises usando as mesmas interfaces de programação que nas regiões da AWS, ao mesmo tempo que usam recursos locais de computação e armazenamento para menor latência e necessidades de processamento de dados locais.

Um Outpost é um grupo de capacidade de computação e armazenamento da AWS implantado em um local do cliente. A AWS opera, monitora e gerencia essa capacidade como parte de uma região da AWS. É possível criar sub-redes no Outpost e especificá-las ao criar recursos da AWS. As instâncias nas sub-redes do Outpost se comunicam com outras instâncias na região da AWS usando endereços IP privados, tudo na mesma VPC.

O diagrama a seguir ilustra a região `us-west-2` da AWS, duas de suas zonas de disponibilidade e um Outpost. A VPC abrange as zonas de disponibilidade e o Outpost. O Outpost está em um data center on-premises do cliente. Cada zona na VPC tem uma sub-rede, e cada sub-rede tem uma instância.



Instâncias em um Outpost

Para começar a usar o AWS Outposts, crie um Outpost e solicite capacidade para o Outpost. O AWS Outposts oferece dois formatos, racks e servidores do Outposts. Para obter mais informações sobre configurações de Outposts, consulte Família do AWS Outposts. Após a instalação do equipamento do Outpost, a capacidade de computação e de armazenamento estará disponível quando você executar instâncias do EC2 em seu Outpost.

Para executar instâncias do EC2, você deve criar uma sub-rede do Outposts. Os grupos de segurança controlam o tráfego de entrada e saída de instâncias em uma sub-rede do Outpost,

assim como fazem para instâncias em uma sub-rede de zona de disponibilidade. Para se conectar a instâncias em sub-redes do Outpost usando SSH, especifique um par de chaves ao lançá-las, da mesma forma que você faz para instâncias em sub-redes da Zona de disponibilidade.

Para obter mais informações, consulte Get started with Outposts racks ou Get started with Outposts servers.

Volumes em um rack do Outpost

Se sua capacidade de computação do Outpost estiver em um rack do Outpost, será possível criar volumes do EBS na sub-rede do Outpost que você criou. Ao criar o volume, especifique o nome de recurso da Amazon (ARN) do Outpost.

O seguinte comando create-volume cria um volume vazio de 50 GB no Outpost especificado.

```
aws ec2 create-volume --availability-zone us-east-2a --outpost-arn arn:aws:outposts:us-east-2:123456789012:outpost/op-03e6fecad652a6138 --size 50
```

É possível modificar dinamicamente o tamanho dos volumes gp2 Amazon EBS sem desanexá-los. Para obter mais informações sobre como modificar um volume sem desassociá-lo, consulte Solicitar modificações para seus volumes do EBS no Guia de usuário do Amazon EBS.

Recomendamos limitar o volume raiz de uma instância em um rack do Outpost a até 30 GiB. É possível especificar volumes de dados no mapeamento de dispositivo de bloco da AMI ou na instância para fornecer armazenamento adicional. Para eliminar blocos não utilizados do volume de inicialização, consulte Como criar volumes de EBS esparsos no blog da rede de parceiros da AWS.

Recomendamos aumentar o tempo limite de NVMe para o volume raiz. Para obter mais informações, consulte Tempo limite de operação de E/S no Guia do usuário do Amazon EBS.

Volumes em um servidor do Outpost

As instâncias nos servidores do Outpost fornecem volumes de armazenamento de instâncias, mas não volumes do EBS. Escolha uma AMI baseada no Amazon EBS com apenas um único snapshot do EBS. Escolha um tamanho de instância com armazenamento de instâncias suficiente para atender às necessidades da sua aplicação. Para obter mais informações, consulte Limites de volume de armazenamento de instância.

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 VPC usa o protocolo de endereçamento IPv4. Não é possível desabilitar esse comportamento. Ao criar uma VPC, especifique um bloco CIDR IPv4 (um intervalo de endereços IPv4 privados). Opcionalmente, é possível atribuir um bloco CIDR IPv6 à VPC e atribuir os endereços IPv6 desse bloco às instâncias nas sub-redes.

Ao iniciar uma instância do EC2, você especifica uma VPC e uma sub-rede. A instância recebe um endereço IPv4 privado do intervalo CIDR da sub-rede. Opcionalmente, você pode configurar suas instâncias com endereços IPv4 públicos e endereços IPv6. Se as instâncias do EC2 em diferentes VPCs se comunicarem usando endereços IP públicos, o tráfego permanecerá na rede global privada da AWS e não atravessará a Internet pública.

Conteúdo

- Endereços IPv4 privados
- Endereços IPv4 públicos
- Otimização de endereço IPv4 público
- Endereços IPv6
- Vários endereços IP
- Hostnames de instância do EC2
- Endereços locais de link
- Gerenciar os endereços IPv4 para as instâncias do EC2
- Gerenciar os endereços IPv6 para as instâncias do EC2
- Endereços IP secundários para suas instâncias do EC2
- Configurar endereços IPv4 privados secundários para instâncias do Windows

Endereços IPv4 privados

Um endereço IPv4 privado é um endereço IP que não é acessível pela Internet. É possível 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**
>
> É possível 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.

As sub-redes da VPC podem ser de um destes tipos:

- Sub-redes somente IPv4: você só pode criar recursos nessas sub-redes com endereços IPv4 atribuídos a eles.
- Sub-redes somente IPv6: você só pode criar recursos nessas sub-redes com endereços IPv6 atribuídos a eles.
- Sub-redes IPv4 e IPv6: você pode criar recursos nessas sub-redes com endereços IPv4 ou IPv6 atribuídos a eles.

Quando você inicia uma instância do EC2 em uma sub-rede somente IPv4 ou de pilha dupla (IPv4 e IPv6), a instância recebe um endereço IP privado primário do intervalo de endereços IPv4 da sub-rede. Para obter mais informações, consulte Endereçamento IP no Manual 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 (index 0) que recebe o endereço IPv4 privado primário. Também é possível 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.

Um endereço IPv4 privado, independentemente de ser um endereço primário ou secundário, permanece associado à interface de rede quando a instância é interrompida e reiniciada ou é hibernada e iniciada, e é liberado quando a instância é encerrada.

Endereços IPv4 públicos

Um endereço IP público é um endereço IPv4 que é acessível pela Internet. É possível usar endereços públicos para comunicação entre as instâncias e a Internet.

Quando você inicia uma instância em uma VPC padrão, atribuímos a ela um endereço IP público por padrão. Quando você executa uma instância em uma VPC não padrão, a sub-rede tem um atributo que determina se as instâncias executadas naquela sub-rede recebem um endereço IP público do grupo de endereços IPv4 públicos. Por padrão, não atribuímos um endereço IP público a instâncias iniciadas em uma sub-rede não padrão.

É possível controlar se sua instância recebe um endereço IP público fazendo o seguinte:

- Modifique o atributo de endereçamento IP público da sua sub-rede. Para obter mais informações, consulte Modificar o atributo de endereçamento IPv4 público para a sub-rede no Guia do usuário da Amazon VPC.
- Habilite ou desabilite o atributo de endereçamento de IP público durante a instância. Isso substitui o atributo de endereçamento de IP público da sub-rede. Para obter mais informações, consulte Atribuir um endereço IPv4 público na inicialização.
- Cancele a atribuição de um endereço IP público da sua instância após a inicialização. Para obter mais informações, consulte the section called “Gerenciar endereços IP”.

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.

Liberamos o endereço IP público de sua instância e atribuímos um novo nos seguintes casos:

- Liberamos o endereço IP público quando a instância é interrompida, hibernada ou encerrada. Atribuímos um novo endereço IP público quando você inicia sua instância parada ou hibernada.
- Liberamos o endereço IP público quando você associa um endereço IP da Elastic à instância. Atribuímos um novo endereço IP público quando você desassociar o endereço IP elástico da sua instância.
- Se liberarmos o endereço IP público da instância e ela tiver uma interface de rede secundária, não atribuiremos um novo endereço IP público.
- Se liberarmos o endereço IP público da sua instância e ela tiver um endereço IP privado secundário associado a um endereço IP elástico, não atribuiremos um novo endereço IP público.

Se você precisar de um endereço IP público persistente que possa ser associado às instâncias e das instâncias conforme necessário, use um endereço IP elástico.

Se você usar o DNS dinâmico para mapear um nome DNS existente para o endereço IP público de uma nova instância, poderá demorar até 24 horas para o endereço IP ser propagado via Internet. Como resultado, as novas instâncias não poderão receber tráfego quando as instâncias encerradas continuarem a receber solicitações. Para resolver o problema, use um endereço IP elástico. É possível alocar seu próprio endereço IP elástico e associá-lo à instância. Para obter mais informações, consulte Endereços IP elásticos.

Se você estiver usando o Gerenciador de endereços IP (IPAM) do Amazon VPC IP), pode obter um bloco contíguo de endereços IPv4 públicos da AWS e usá-lo para alocar endereços IP elásticos aos recursos da AWS. O uso de blocos de endereços IPv4 contíguos pode reduzir significativamente a sobrecarga de gerenciamento das listas de controle de acesso de segurança e simplificar a alocação e o rastreamento de endereços IP para empresas em expansão na AWS. Para obter mais informações, consulte Allocate sequential Elastic IP addresses from an IPAM pool no Guia do usuário do IPAM da Amazon VPC.

Considerações

- A AWS cobra por todos os endereços IPv4 públicos, incluindo endereços IPv4 públicos associados a instâncias em execução e endereços IP elásticos. Para obter mais informações, consulte a guia Endereço IPv4 público na página de preços da Amazon VPC.
- 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.

Otimização de endereço IPv4 público

A AWS cobra por todos os endereços IPv4 públicos, incluindo endereços IPv4 públicos associados a instâncias em execução e endereços IP elásticos. Para obter mais informações, consulte a guia Endereço IPv4 público na página de preços da Amazon VPC.

A lista a seguir contém ações que você pode tomar para otimizar o número de endereços IPv4 públicos que você usa:

- Use um balanceador de carga elástico para balancear a carga do tráfego para suas instâncias do EC2 e desabilitar a atribuição automática de IP público na ENI primária atribuída às instâncias. Os balanceadores de carga usam um único endereço IPv4 público, o que reduz o número de endereços IPv4 público. Talvez você também queira consolidar os balanceadores de carga existentes para reduzir ainda mais a contagem de endereços IPv4 públicos.

- Se o único motivo para usar um gateway NAT for usar SSH em uma instância do EC2 em uma sub-rede privada para manutenção ou emergências, considere usar o Endpoint do EC2 Instance Connect no lugar. Com o Endpoint do EC2 Instance Connect, você pode se conectar a uma instância da Internet sem a necessidade de que a instância tenha um endereço IPv4 público.
- Se suas instâncias do EC2 estiverem em uma sub-rede pública com endereços IP públicos alocados a elas, considere mover as instâncias para uma sub-rede privada, remover os endereços IP públicos e usar um gateway NAT público para permitir o acesso de e para suas instâncias do EC2. Há considerações de custo para usar gateways NAT. Use este método de cálculo para decidir se os gateways NAT são econômicos. É possível obter o `Number of public IPv4 addresses` necessário para esse cálculo criando um relatório de uso e custo de cobrança da AWS.

  ```
  NAT gateway per hour + NAT gateway public IPs + NAT gateway transfer / Existing
   public IP cost
  ```

  Em que:

  - `NAT gateway per hour = $0.045 * 730 hours in a month * Number of Availability Zones the NAT gateways are in`
  - `NAT gateway public IPs = $0.005 * 730 hours in a month * Number of IPs associated with your NAT gateways`
  - `NAT gateway transfer = $0.045 * Number of GBs that will go through the NAT gateway in a month`
  - `Existing public IP cost = $0.005 * 730 hours in a month * Number of public IPv4 addresses`

  Se o total for menor que 1, os gateways NAT são mais baratos que os endereços IPv4 públicos.
- Use AWS PrivateLink para se conectar de forma privada a serviços da AWS ou serviços hospedados por outras contas da AWS, em vez de usar endereços IPv4 públicos e gateways da Internet.
- Traga seu próprio intervalo de endereços IP (BYOIP) para a AWS e use-o para endereços IPv4 públicos em vez de usar endereços IPv4 públicos de propriedade da Amazon.
- Desative o endereço IPv4 público atribuído automaticamente à instância executada em sub-redes. Essa opção geralmente é desabilitada por padrão para VPCs quando você cria uma sub-rede, mas você deve verificar suas sub-redes existentes para garantir que ela esteja desabilitada.

- Se você tiver instâncias do EC2 que não precisam de endereços IPv4 públicos, verifique se as interfaces de rede anexadas às suas instâncias têm a atribuição automática de IP público desabilitada.
- Configure endpoints do acelerador no AWS Global Accelerator para instâncias do EC2 em sub-redes privadas para permitir que o tráfego da Internet flua diretamente para os endpoints em suas VPCs sem exigir endereços IP públicos. Você também pode trazer seus próprios endereços para o AWS Global Accelerator e usar seus próprios endereços IPv4 para os endereços IP estáticos do seu acelerador.

Endereços IPv6

Os endereços IPv6 são globalmente exclusivos e podem ser configurados para permanecer privados ou acessíveis pela Internet. O endereçamento IPv6 público e privado está disponível na AWS:

- IPv6 privado: a AWS considera endereços IPv6 privados aqueles que não são anunciados e não podem ser anunciados na internet da AWS.
- IPv6 público: a AWS considera endereços IPv6 públicos aqueles que são anunciados na internet da AWS.

Para obter mais informações sobre o endereçamento IPv6, consulte Endereços IPv6 no Manual do usuário da Amazon VPC.

Todos os tipos de instância oferecem suporte a endereços IPv6, exceto as a seguir: C1, M1, M2, M3 e T1.

As instâncias EC2 receberão um endereço IPv6 se um bloco CIDR IPv6 estiver associado à VPC e à sub-rede, e se uma das seguintes afirmações for verdadeira:

- A sub-rede está configurada para atribuir automaticamente um endereço IPv6 a uma instância durante a execução. Para obter mais informações, consulte Modificar os atributos de endereçamento IP da sua 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 (index 0) da instância. É possível gerenciar os endereços IPv6 das interfaces de rede primárias das suas instâncias da seguinte forma:

- Desassociar um endereço IPv6 de uma interface de rede. O número de endereços IPv6 que é possível atribuir a uma interface de rede e o número de interfaces de rede que é possível anexar a uma instância varia de acordo com o tipo de instância. Para obter mais informações, consulte Máximo de endereços IP por interface de rede.
- Habilite um endereço IPv6 primário. Um endereço IPv6 primário permite evitar a interrupção do tráfego para instâncias ou ENIs. Para ter mais informações, consulte Criar uma interface de rede para sua instância do EC2 ou Gerenciar os endereços IP para a interface de rede.

Um endereço IPv6 persiste quando você interrompe e inicia ou hiberna e inicia a instância, e é liberado quando você encerra a instância. Você não pode atribuir novamente um endereço IPv6 enquanto ele estiver atribuído a outra interface de rede — é necessário primeiro cancelar a atribuição.

É possível controlar se as instâncias são acessíveis através de seus endereços IPv6, controlando o roteamento da sua sub-rede ou usando o grupo de segurança e as regras de ACL de rede. Para obter mais informações, consulte Privacidade do tráfego entre redes no Guia do usuário da Amazon VPC.

Para obter mais informações sobre intervalos de endereço IPv6 reservados, consulte Registro de endereço para finalidades especiais IANA IPv6 e RFC4291.

Vários endereços IP

É possível 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 é possível especificar para uma instância depende do tipo da instância. Para obter mais informações, consulte Máximo de endereços IP por interface de rede.

Casos de uso

- Hospedar vários sites em um único servidor usando vários certificados SSL em um único servidor e associando cada certificado a um endereço IP específico.
- Operar aplicações de rede, como firewalls ou load balancers, que têm vários endereços IP para cada interface de rede.

- Redirecionar o tráfego interno para uma instância em espera em caso de falha na instância, atribuindo novamente o endereço IP secundário à instância em espera.

Como funcionam vários endereços IP

- É possível atribuir um endereço IPv4 privado secundário a qualquer interface de rede.
- É possível atribuir vários endereços IPv6 a uma interface de rede que esteja em uma sub-rede que tem um bloco CIDR IPv6 associado.
- É necessário escolher um endereço IPv4 secundário no intervalo de bloco CIDR IPv4 da sub-rede para a interface de rede.
- É necessário escolher endereços IPv6 no intervalo de bloco CIDR IPv6 da sub-rede para a interface de rede.
- Você associa grupos de segurança a interfaces de rede, não a endereços IP individuais. Portanto, cada endereço IP especificado em uma interface de rede está sujeito ao grupo de segurança de sua interface de rede.
- Vários endereços IP podem ser atribuídos e ter a atribuição cancelada para interfaces de rede anexadas ou instâncias paradas.
- Os endereços IPv4 privados secundários que são atribuídos a uma interface de rede podem ser atribuídos novamente para outra interface de rede se você permitir isso explicitamente.
- Um endereço IPv6 não pode ser atribuído novamente a outra interface de rede. É necessário primeiro cancelar a atribuição do endereço IPv6 da interface de rede existente.
- Ao atribuir vários endereços IP a uma interface de rede usando as ferramentas da linha de comando ou a API, a operação inteira falhará se um dos endereços IP não puder ser atribuído.
- Os endereços IPv4 privados primários, os endereços IPv4 privados secundários, os endereços IP elásticos e os endereços IPv6 permanecem com a interface de rede secundária quando ela é desanexada de uma instância ou anexada a uma instância.
- Embora não seja possível desanexar a interface de rede primária de uma instância, é possível atribuir novamente o endereço IPv4 privado secundário da interface de rede primária para outra interface de rede.

Para obter mais informações, consulte the section called “Endereços IP secundários”.

Hostnames de instância do EC2

Quando você cria uma instância do EC2, o AWS cria um hostname para essa instância. Para obter mais informações sobre os tipos de nome de host e como são provisionados pela AWS, consulte Nomes de host e domínios de instâncias do EC2. A Amazon fornece um servidor DNS que resolve hostnames fornecidos pela Amazon em endereços IPv4 e IPv6. O servidor DNS da Amazon está localizado na base de seu intervalo de rede VPC mais dois. Para ter mais informações, consulte Atributos de DNS para sua VPC no Guia do usuário da Amazon VPC.

Endereços locais de link

Os endereços de link local são endereços IP bem conhecidos e não roteáveis. O Amazon EC2 usa endereços do espaço de endereços locais de link para fornecer serviços que são acessíveis somente por uma instância do EC2. Esses serviços não são executados na instância, mas sim no host subjacente. Ao acessar os endereços locais de link desses serviços, você está se comunicando com o hipervisor Xen ou o controlador do Nitro.

Intervalos de endereços locais de link

- IPv4: 169.254.0.0/16 (169.254.0.0 a 169.254.255.255)
- IPv6: fe80::/10

Serviços acessados usando endereços locais de link

- Serviço de metadados da instância
- Amazon Route 53 Resolver (também conhecido como servidor DNS da Amazon)
- Serviço de Sincronização Temporal da Amazon
- Servidores do AWS KMS

Gerenciar os endereços IPv4 para as instâncias do EC2

É possível atribuir um endereço IPv4 à instância ao executá-la. É possível ver os endereços IPv4 no console nas páginas Instances (Instâncias) ou Network Interfaces (Interfaces de rede).

Tarefas

- Atribuir um endereço IPv4 público na inicialização

- Atribuir um endereço IPv4 privado na inicialização
- Visualizar o endereço IPv4 primário
- Visualizar os endereços IPv4 usando metadados de instância

Atribuir um endereço IPv4 público na inicialização

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. É possível 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 0. Esse recurso depende de determinadas condições no momento em que você executa a instância.

Considerações

- É possível cancelar a atribuição do endereço IP público da sua instância após a execução gerenciando os endereços IP associados a uma interface de rede. Para mais informações sobre endereços IPv4 públicos, consulte Endereços IPv4 públicos.
- 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 atributo de atribuição automática de endereço IP público, se especificar uma interface de rede existente com o índice de dispositivo 0.
- Independentemente de você atribuir ou não um endereço IP público à instância ao iniciá-la, é possível associar um endereço IP elástico à instância depois que ela for executada. Para obter mais informações, consulte Endereços IP elásticos. Também é possível modificar o comportamento do endereçamento IPv4 público da sub-rede. Para obter mais informações, consulte Modificar o atributo de endereçamento IPv4 público para a sub-rede.

Console

Para atribuir um endereço IPv4 público na inicialização

Siga o procedimento para iniciar uma instância e, ao definir as Network Settings (Configurações de rede), escolha a opção Auto-assign Public IP (Atribuir IP público automaticamente).

AWS CLI

Para atribuir um endereço IPv4 público na inicialização

Use o comando run-instances com a opção `--associate-public-ip-address`.

```
--associate-public-ip-address
```

PowerShell

Para atribuir um endereço IPv4 público na inicialização

Use o cmdlet New-EC2Instance com o parâmetro `-AssociatePublicIp`.

```
-AssociatePublicIp $true
```

Atribuir um endereço IPv4 privado na inicialização

É possível especificar um endereço IPv4 privado no intervalo de endereços IPv4 da sub-rede ou deixar que o Amazon EC2 escolha um para você. Esse endereço é atribuído à interface de rede primária.

Para atribuir endereços IPv4 após a inicialização, consulte the section called “Atribuir endereços IP secundários a uma instância”.

Console

Para atribuir um endereço IPv4 privado na inicialização

Siga o procedimento para iniciar uma instância. Ao definir Configurações de rede, expanda Configuração avançada de rede e insira um valor para IP primário.

AWS CLI

Para atribuir um endereço IPv4 privado na inicialização

Use o comando run-instances com a opção `--private-ip-address`.

```
--private-ip-addresses 10.251.50.12
```

Para permitir que o Amazon EC2 escolha o endereço IP, omita essa opção.

PowerShell

Para atribuir um endereço IPv4 privado na inicialização

Use o cmdlet New-EC2Instance com o parâmetro `-PrivateIpAddress`.

```
-PrivateIpAddress 10.251.50.12
```

Para permitir que o Amazon EC2 escolha o endereço IP, omita esse parâmetro.

Visualizar o endereço IPv4 primário

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.

Console

Para visualizar os endereços IPv4 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.
4. Na guia Rede, encontre Endereço IPv4 público e Endereço IPv4 privado.
5. (Opcional) A guia Rede também contém as interfaces de rede e os endereços IP elásticos da instância.

AWS CLI

Para visualizar o endereço IPv4 primário de uma instância

Use o comando describe-instances.

```
aws ec2 describe-instances \
    --instance-ids i-1234567890abcdef0 \
    --query "Reservations[].Instances[].PrivateIpAddress" \
```

```
    --output text
```

O seguinte é um exemplo de saída.

```
10.251.50.12
```

PowerShell

Para visualizar o endereço IPv4 primário de uma instância

Use o cmdlet Get-EC2Instance.

```
(Get-EC2Instance `
    -InstanceId i-1234567890abcdef0).Instances.PrivateIpAddress
```

O seguinte é um exemplo de saída.

```
10.251.50.12
```

Visualizar os endereços IPv4 usando metadados de instância

Você pode obter os endereços IPv4 para a instância recuperando os metadados da instância. Para obter mais informações, consulte Usar metadados da instância para gerenciar a instância do EC2.

Para visualizar os endereços IPv4 usando metadados de instância

1. Conecte-se à sua instância. Para obter mais informações, consulte Conexão com a instância do EC2.
2. Execute um dos seguintes comandos:

   IMDSv2

   Linux

   Execute o seguinte comando em sua instância Linux.

   ```
   TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-
   metadata-token-ttl-seconds: 21600"` \
   && curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
   meta-data/local-ipv4
   ```

Windows

Execute o seguinte comando em sua instância Windows.

```
[string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-
seconds" = "21600"} `
    -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} `
    -Method GET -Uri http://169.254.169.254/latest/meta-data/local-ipv4
```

IMDSv1

Linux

Execute o seguinte comando em sua instância Linux.

```
curl http://169.254.169.254/latest/meta-data/local-ipv4
```

Windows

Execute o seguinte comando em sua instância Windows.

```
Invoke-RestMethod http://169.254.169.254/latest/meta-data/local-ipv4
```

3. Use um dos seguintes comandos para acessar o endereço IP público. Se houver um endereço IP elástico associado à instância, o comando retornará o endereço IP elástico.

IMDSv2

Linux

Execute o seguinte comando em sua instância Linux.

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H
 "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
meta-data/public-ipv4
```

Windows

Execute o seguinte comando em sua instância Windows.

```
[string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-
seconds" = "21600"} `
    -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} `
    -Method GET -Uri http://169.254.169.254/latest/meta-data/public-ipv4
```

IMDSv1

Linux

Execute o seguinte comando em sua instância Linux.

```
curl http://169.254.169.254/latest/meta-data/public-ipv4
```

Windows

Execute o seguinte comando em sua instância Windows.

```
Invoke-RestMethod http://169.254.169.254/latest/meta-data/public-ipv4
```

Gerenciar os endereços IPv6 para as instâncias do EC2

Se a VPC e a sub-rede tiverem blocos CIDR IPv6 associados a elas, será possível atribuir um endereço IPv6 à instância durante ou após a execução. É possível acessar os endereços IPv6 de suas instâncias no console, nas páginas Instâncias ou Interfaces de rede. As tarefas a seguir configuram endereços IP para suas instâncias. Para configurar endereços IP nas interfaces de rede, consulte the section called “Gerenciar endereços IP”.

Tarefas

- Atribuir um endereço IPv6 a uma instância
- Visualizar os endereços IPv6 de uma instância
- Visualizar endereços IPv6 usando metadados de instância
- Cancelar a atribuição de um endereço IPv6 de uma instância

Atribuir um endereço IPv6 a uma instância

É possível especificar um endereço IPv6 no intervalo de endereços IPv6 da sub-rede ou deixar que o Amazon EC2 escolha um para você. Esse endereço é atribuído à interface de rede primária. Observe que os tipos de instância a seguir não oferecem suporte a endereços IPv6: C1, M1, M2, M3 e T1.

Console

Para atribuir um endereço IPv6 na inicialização

Siga o procedimento para iniciar uma instância. Ao definir as Configurações de rede, escolha a opção Atribuir IP IPv6 automaticamente. Se você não vir essa opção, a sub-rede selecionada não tem um bloco CIDR IPv6 associado.

Para atribuir um endereço IPv6 após a inicialização

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância e escolha Actions (Ações), Networking (Redes), Manage IP Addresses (Gerenciar endereços IP).
4. Expanda a interface de rede. Em IPv6 addresses (Endereços IPv6), escolha Assign new IP address (Atribuir novo endereço IP).
5. Insira um endereço IPv6 no intervalo da sub-rede ou deixe o campo em branco para permitir que o Amazon EC2 escolha o endereço IPv6 para você. Se você não vir essa opção, a sub-rede da instância não tem um bloco CIDR IPv6 associado.
6. Escolha Salvar.

AWS CLI

Para atribuir um endereço IPv6 na inicialização

Use o comando run-instances com a opção `--ipv6-addresses`. O exemplo a seguir atribui dois endereços IPv6.

```
--ipv6-addresses Ipv6Address=2001:db8::1234:5678:1.2.3.4
 Ipv6Address=2001:db8::1234:5678:5.6.7.8
```

Para permitir que o Amazon EC2 escolha os endereços IPv6, use a opção `--ipv6-address-count`. O exemplo a seguir atribui dois endereços IPv6.

```
--ipv6-address-count 2
```

Para atribuir um endereço IPv6 após a inicialização

Use o comando assign-ipv6-addresses. O exemplo a seguir atribui dois endereços IPv6.

```
aws ec2 assign-ipv6-addresses \
    --network-interface-id eni-1234567890abcdef0 \
    --ipv6-addresses 2001:db8::1234:5678:1.2.3.4 2001:db8::1234:5678:5.6.7.8
```

Para permitir que o Amazon EC2 escolha os endereços IPv6, use a opção `--ipv6-address-count`. O exemplo a seguir atribui dois endereços IPv6.

```
aws ec2 assign-ipv6-addresses \
    --network-interface-id eni-1234567890abcdef0 \
    --ipv6-address-count 2
```

PowerShell

Para atribuir um endereço IPv6 na inicialização

Use o cmdlet New-EC2Instance com o parâmetro `-Ipv6Address`. O exemplo a seguir atribui dois endereços IPv6.

```
-Ipv6Address $ipv6addr1,$ipv6addr2
```

Defina os endereços IPv6 da seguinte maneira.

```
$ipv6addr1 = New-Object Amazon.EC2.Model.InstanceIpv6Address
$ipv6addr1.Ipv6Address = "2001:db8::1234:5678:1.2.3.4"
$ipv6addr2 = New-Object Amazon.EC2.Model.InstanceIpv6Address
$ipv6addr2.Ipv6Address = "2001:db8::1234:5678:5.6.7.8"
```

Para permitir que o Amazon EC2 escolha os endereços IPv6, use o parâmetro `-Ipv6AddressCount`. O exemplo a seguir atribui dois endereços IPv6.

```
-Ipv6AddressCount 2
```

Para atribuir um endereço IPv6 após a inicialização

Use o cmdlet Register-EC2Ipv6AddressList. O exemplo a seguir atribui dois endereços IPv6.

```
Register-EC2Ipv6AddressList `
    -NetworkInterfaceId eni-1234567890abcdef0 `
    -Ipv6Address "2001:db8::1234:5678:1.2.3.4","2001:db8::1234:5678:5.6.7.8"
```

Para permitir que o Amazon EC2 escolha os endereços IPv6, use o parâmetro `-Ipv6AddressCount`. O exemplo a seguir atribui dois endereços IPv6.

```
Register-EC2Ipv6AddressList `
    -NetworkInterfaceId eni-1234567890abcdef0 `
    -Ipv6AddressCount 2
```

Visualizar os endereços IPv6 de uma instância

É possível visualizar os endereços IPv6 da sua instância.

Console

Para visualizar os endereços 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.
4. Na guia Networking (Redes), localize IPv6 addresses (Endereços IPv6).

AWS CLI

Para visualizar o endereço IPv6 de uma instância

Use o comando describe-instances.

```
aws ec2 describe-instances \
    --instance-ids i-1234567890abcdef0 \
    --query "Reservations[*].Instances[].Ipv6Address" \
    --output text
```

O seguinte é um exemplo de saída.

```
2001:db8::1234:5678:1.2.3.4
```

PowerShell

Para visualizar o endereço IPv6 de uma instância

Use o cmdlet Get-EC2Instance.

```
(Get-EC2Instance `
    -InstanceId i-1234567890abcdef0).Instances.Ipv6Address
```

O seguinte é um exemplo de saída.

```
2001:db8::1234:5678:1.2.3.4
```

Visualizar endereços IPv6 usando metadados de instância

Depois de se conectar à sua instância, é possível recuperar os endereços IPv6 usando metadados de instância. Primeiro, é necessário obter o endereço MAC da instância em `http://169.254.169.254/latest/meta-data/network/interfaces/macs/`.

IMDSv2

Linux

Execute o seguinte comando em sua instância Linux.

```
TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-
token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-
data/network/interfaces/macs/mac-address/ipv6s
```

Windows

Execute os seguintes cmdlets na sua instância Windows.

```
[string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds"
 = "21600"} `
```

```
    -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} `
    -Method GET -Uri http://169.254.169.254/latest/meta-data/network/interfaces/
macs/mac-address/ipv6s
```

IMDSv1

Linux

Execute o seguinte comando em sua instância Linux.

```
curl http://169.254.169.254/latest/meta-data/network/interfaces/macs/mac-address/
ipv6s
```

Windows

Execute o seguinte cmdlet na sua instância Windows.

```
Invoke-RestMethod -Uri http://169.254.169.254/latest/meta-data/network/interfaces/
macs/mac-address/ipv6s
```

Cancelar a atribuição de um endereço IPv6 de uma instância

É possível cancelar a atribuição de um endereço IPv6 de uma instância a qualquer momento.

Console

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. Expanda a interface de rede. Em IPv6 addresses (Endereços IPv6), selecione Unassign (Cancelar atribuição) ao lado de endereços IPv6.
5. Escolha Salvar.

AWS CLI

Para cancelar a atribuição de um endereço IPv6 de uma instância

Use o comando unassign-ipv6-addresses.

```
aws ec2 unassign-ipv6-addresses \
    --network-interface-id eni-1234567890abcdef0 \
    --ipv6-addresses 2001:db8::1234:5678:1.2.3.4
```

PowerShell

Para cancelar a atribuição de um endereço IPv6 de uma instância

Use o cmdlet Unregister-EC2Ipv6AddressList.

```
Unregister-EC2Ipv6AddressList `
    -NetworkInterfaceId eni-1234567890abcdef0 `
    -Ipv6Address 2001:db8::1234:5678:1.2.3.4
```

Endereços IP secundários para suas instâncias do EC2

O primeiro endereço IPv4 atribuído a uma interface de rede é conhecido como endereço IP primário. Os endereços IP secundários são endereços IPv4 adicionais atribuídos a uma interface de rede. Para obter mais informações, consulte the section called “Vários endereços IP”.

Também é possível atribuir vários endereços IPv6 a uma instância. Para obter mais informações, consulte the section called “Endereços IPv6”.

Tarefas

- Atribuir endereços IP secundários a uma instância
- Configurar o sistema operacional para usar endereços IP secundários
- Remover um endereço IP secundário de uma instância

Atribuir endereços IP secundários a uma instância

É possível atribuir endereços IP secundários à interface de rede para uma instância ao executar a instância ou após a instância estar em execução.

Console

Para atribuir um endereço IP secundário na inicialização

1. Siga o procedimento para iniciar uma instância. Ao definir Configurações de rede, expanda Configuração avançada de rede.
2. Em IP secundário, escolha Atribuir automaticamente e insira o número de endereços IP para o Amazon EC2 atribuir. Como alternativa, escolha Atribuir manualmente e insira os endereços IPv4.
3. Conclua as etapas restantes para iniciar a instância.

Para atribuir um endereço IP secundário após a inicialização

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância e escolha Actions (Ações), Networking (Redes), Manage IP Addresses (Gerenciar endereços IP).
4. Expanda a interface de rede.
5. Para adicionar um endereço IPv4, em Endereços IPv4, escolha Atribuir novo endereço IP. Insira um endereço IPv4 no intervalo da sub-rede ou deixe o campo em branco para deixar que o Amazon EC2 escolha um para você.
6. Escolha Salvar.

AWS CLI

Para atribuir um endereço IP secundário na inicialização

Use o comando run-instances com a opção `--secondary-private-ip-addresses`.

```
--secondary-private-ip-addresses 10.251.50.12
```

Para permitir que o Amazon EC2 escolha o endereço IP, use a opção `--secondary-private-ip-address-count`. O exemplo a seguir atribui um endereço IP secundário.

```
--secondary-private-ip-address-count 1
```

Como alternativa, você pode criar uma interface de rede. Para obter mais informações, consulte the section called “Criar uma interface de rede”.

Para atribuir um endereço IP secundário após a inicialização

Use o comando assign-private-ip-addresses com a opção `--private-ip-addresses`.

```
aws ec2 assign-private-ip-addresses \
    --network-interface-ids eni-1234567890abcdef0 \
    --private-ip-addresses 10.251.50.12
```

Para permitir que o Amazon EC2 escolha o endereço IPv4, use o parâmetro `--secondary-private-ip-address-count`. O exemplo a seguir atribui um endereço IPv4.

```
aws ec2 assign-private-ip-addresses \
    --network-interface-ids eni-1234567890abcdef0 \
    --secondary-private-ip-address-count 1
```

PowerShell

Para atribuir um endereço IP secundário na inicialização

É necessário criar uma interface de rede. Para obter mais informações, consulte the section called “Criar uma interface de rede”.

Para atribuir um endereço IP secundário após a inicialização

Use o cmdlet Register-EC2PrivateIpAddress com o parâmetro `-PrivateIpAddress`.

```
Register-EC2PrivateIpAddress `
    -NetworkInterfaceId eni-1234567890abcdef0 `
    -PrivateIpAddress 10.251.50.12
```

Para permitir que o Amazon EC2 escolha os endereços IPv4, use o parâmetro `-SecondaryPrivateIpAddressCount`. O exemplo a seguir atribui um endereço IPv4.

```
Register-EC2PrivateIpAddress `
    -NetworkInterfaceId eni-1234567890abcdef0 `
    -SecondaryPrivateIpAddressCount 1
```

Configurar o sistema operacional para usar endereços IP secundários

Depois de atribuir um endereço IP secundário à sua instância, é necessário configurar o sistema operacional na instância para reconhecer o endereço IPv4 privado adicional.

Instâncias do Linux

- Se estiver usando o Amazon Linux, o pacote ec2-net-utils poderá cuidar desta etapa para você. Ele configura interfaces de rede adicionais que você anexa enquanto a instância está em execução, atualiza os endereços IPv4 secundários durante a renovação da concessão DHCP e atualiza a regras de roteamento relacionadas. Você pode atualizar imediatamente a lista de interfaces usando um dos seguintes comandos, dependendo do sistema: `sudo systemctl restart systemd-networkd` (AL2023) ou `sudo service network restart` (Amazon Linux 2). Você pode visualizar a lista atualizada usando o seguinte comando: `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 Configure your network interface using ec2-net-utils.
- 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.

Instâncias do Windows

Para obter mais informações, consulte Configurar endereços IPv4 privados secundários para instâncias do Windows.

Remover um endereço IP secundário de uma instância

Se você não precisar mais de um endereço IP 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.

Console

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 Ações, Redes, Gerencia endereços IP.

4. Expanda a interface de rede. Em Endereços IPv4, escolha Cancelar atribuição para cancelar a atribuição do endereço IPv4.
5. Escolha Salvar.

AWS CLI

Para remover a atribuição de um endereço IP privado secundário

Use o comando unassign-private-ip-addresses.

```
aws ec2 unassign-private-ip-addresses \
    --network-interface eni-1234567890abcdef0\
    --private-ip-addresses 10.251.50.12
```

PowerShell

Para remover a atribuição de um endereço IP privado secundário

Use o cmdlet Unregister-EC2PrivateIpAddress.

```
Unregister-EC2PrivateIpAddress `
    -NetworkInterface eni-1234567890abcdef0 `
    -PrivateIpAddress 10.251.50.12
```

Configurar endereços IPv4 privados secundários para instâncias do Windows

É possível especificar vários endereços IPv4 privados para as instâncias. Depois de atribuir um endereço IPv4 privado secundário a uma instância, você precisa configurar o sistema operacional na instância para reconhecer o endereço IPv4 privado secundário.

> **Note**
>
> Essas instruções são baseadas no Windows Server 2022. A implantação dessas etapas pode variar dependendo do sistema operacional da instância do Windows.

Tarefas

- Pré-requisitos

- Etapa 1: configurar o endereçamento IP estático na sua instância
- Etapa 2: Configurar um endereço IP privado secundário para a instância
- Etapa 3: Configurar as aplicações para usar o endereço IP privado secundário

Pré-requisitos

- Atribua o endereço IPv4 privado secundário à interface de rede para a instância. É possível atribuir o endereço IPv4 privado secundário ao iniciar a instância ou após a instância estar em execução. Para obter mais informações, consulte Atribuir endereços IP secundários a uma instância.

Etapa 1: configurar o endereçamento IP estático na sua instância

Para permitir que sua instância do Windows use vários endereços IP, configure sua instância para usar o endereçamento IP estático em vez de um servidor DHCP.

> **Important**
>
> Quando você configura o endereçamento IP estático na sua instância, o endereço IP deve corresponder exatamente o que é exibido no console, na CLI ou na API. Se você inserir esses endereços IP incorretamente, a instância poderia tornar-se inacessível.

Para configurar o endereçamento IP estático em uma instância do Windows

1. Conecte-se à sua instância.
2. Encontre o endereço IP, a máscara da sub-rede e os endereços gateway padrão para a instância ao executar as seguintes etapas:
   - Execute o seguinte comando no PowerShell:

     ```
     ipconfig /all
     ```

     Examine a saída e anote os valores de Endereço IPv4, Máscara de sub-rede, Gateway padrão e Servidores DNS da interface de rede. A saída deve ser semelhante ao exemplo apresentado a seguir:

     ```
     ...
     ```

```
Ethernet adapter Ethernet 4:

   Connection-specific DNS Suffix  . : us-west-2.compute.internal
   Description . . . . . . . . . . . : Amazon Elastic Network Adapter #2
   Physical Address. . . . . . . . . : 02-9C-3B-FC-8E-67
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::f4d1:a773:5afa:cd1%7(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.200.0.128(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Monday, April 8, 2024 12:19:29 PM
   Lease Expires . . . . . . . . . . : Monday, April 8, 2024 4:49:30 PM
   Default Gateway . . . . . . . . . : 10.200.0.1
   DHCP Server . . . . . . . . . . . : 10.200.0.1
   DHCPv6 IAID . . . . . . . . . . . : 151166011
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2D-67-AC-FC-12-34-9A-BE-A5-
E7
   DNS Servers . . . . . . . . . . . : 10.200.0.2
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

3. Abra o Centro de Rede e Compartilhamento executando o seguinte comando no PowerShell:

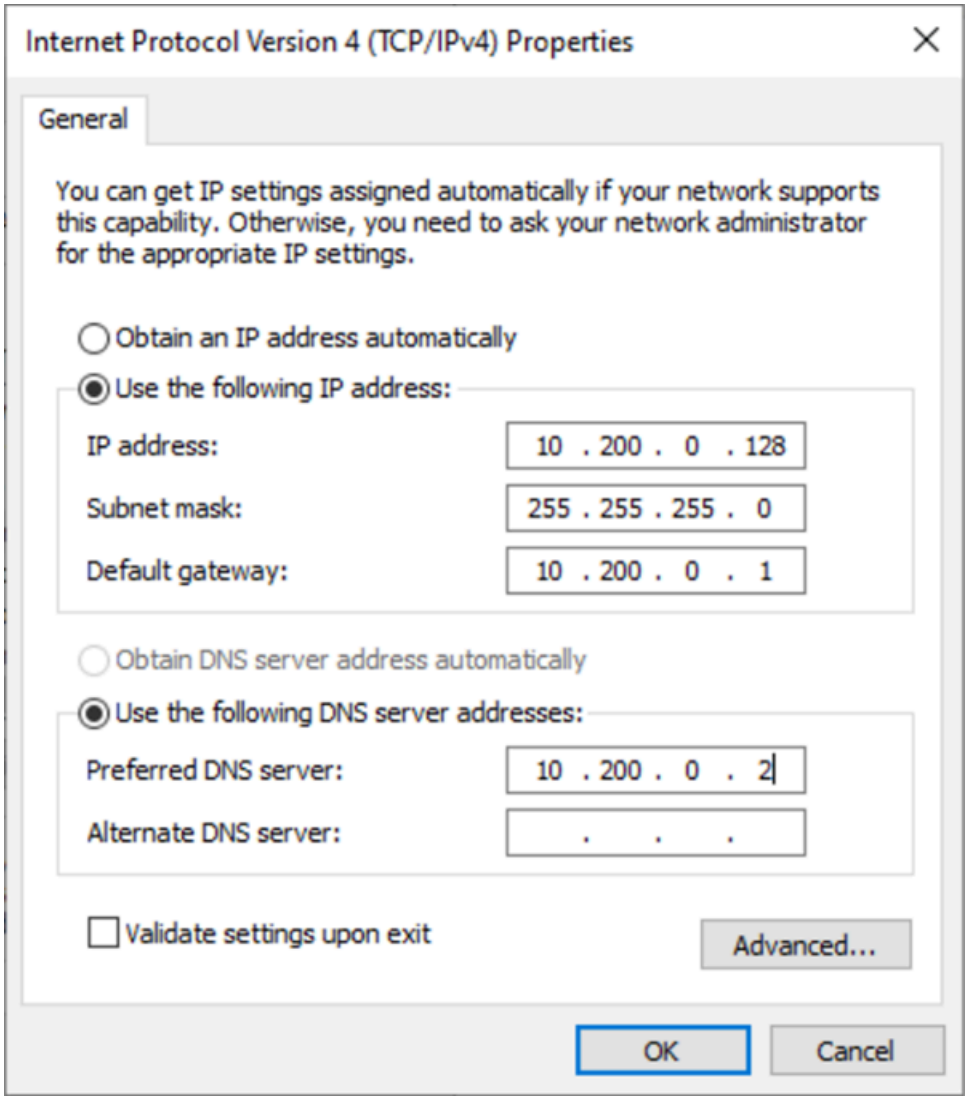
```
& $env:SystemRoot\system32\control.exe ncpa.cpl
```

4. Abra o menu contextual (botão direito do mouse) para interface de rede (Conexão Local ou Ethernet) e selecione Propriedades.
5. Escolha Protocolo TCP/IP Versão 4 (TCP/IPv4), Propriedades.
6. Na caixa de diálogo Propriedades do Protocolo TCP/IP Versão 4 (TCP/IPv4), selecione Usar o seguinte endereço IP, insira os valores a seguir e escolha OK.

Campo	Valor
IP address	O endereço IPv4 obtido na etapa 2 acima.
Máscara de sub-rede	A máscara de sub-rede obtida na etapa 2 acima.
Gateway padrão	O endereço do gateway padrão obtido na etapa 2 acima.

Campo	Valor
Servidor DNS preferido	O servidor DNS obtido na etapa 2 acima.
Servidor DNS alternativo	O servidor DNS alternativo obtido na etapa 2 acima. Se um servidor DNS alternativo não estiver listado, deixe esse campo em branco.

> **Important**
>
> Se você definir o endereço IP para qualquer valor além do endereço IP atual, perderá conectividade com a instância.



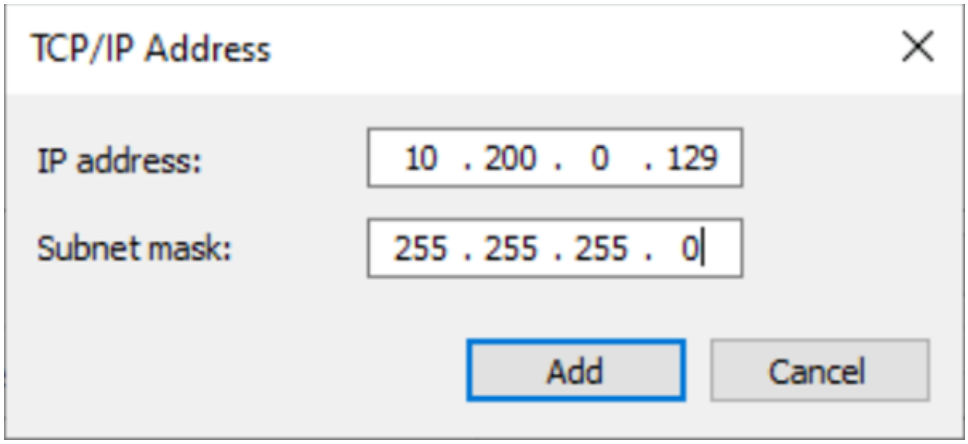
Você perderá conectividade do RDP com a instância do Windows por alguns segundos enquanto a instância converte entre uso de DHCP para endereçamento estático. A instância retém a mesma informação de endereços IP que antes, mas agora essa informação é estática e não é gerenciada por DHCP.

Etapa 2: Configurar um endereço IP privado secundário para a instância

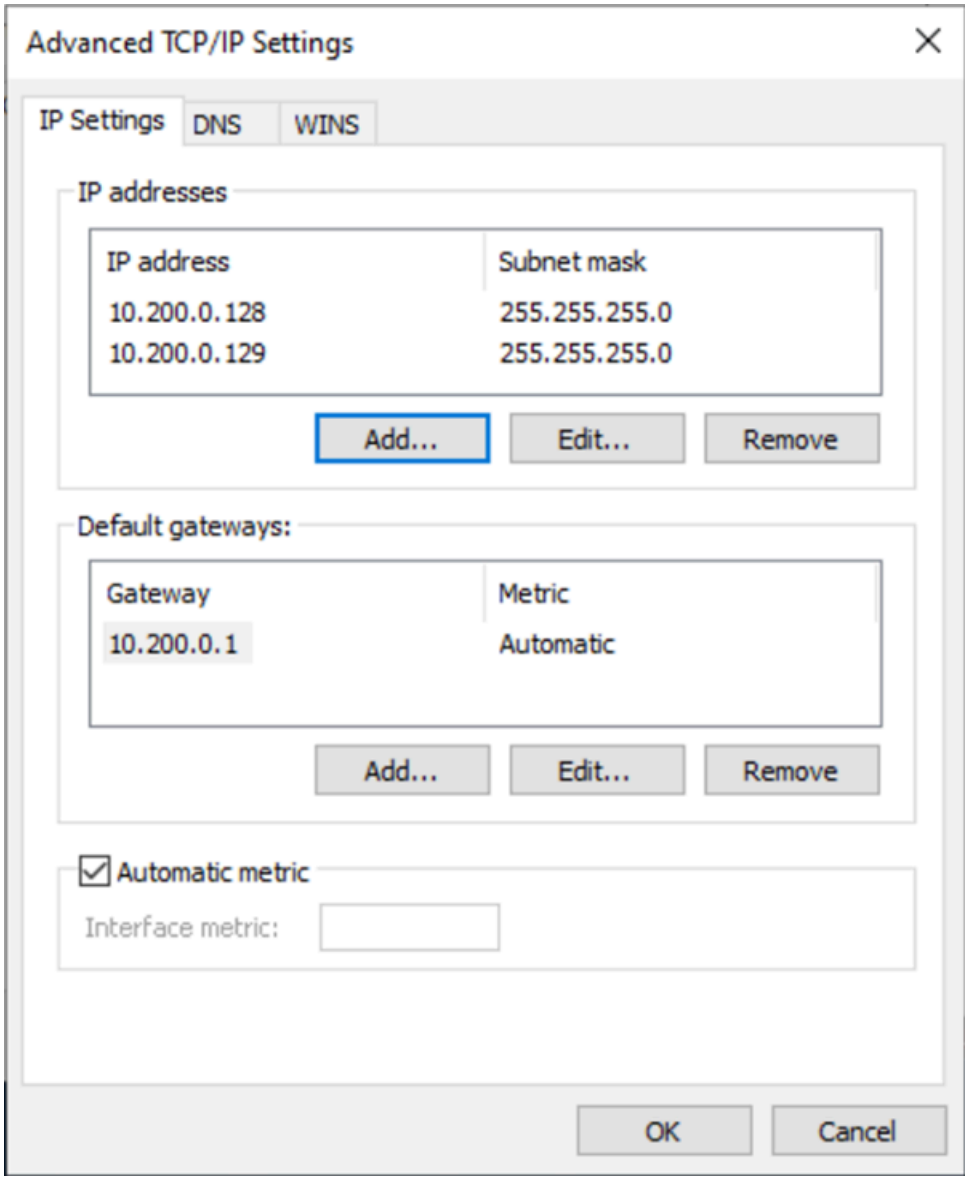
Depois de configurar o endereçamento IP estático na sua instância do Windows, você estará pronto para preparar um segundo endereço IP privado.

Como configurar um endereço IP secundário

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Instâncias e selecione sua instância.
3. Na (Networking (Rede), observe o endereço IP secundário.
4. Conecte-se à sua instância.
5. Na sua instância do Windows, selecione Iniciar, Painel de Controle.
6. Escolha Rede e Internet, Central de Rede e Compartilhamento.
7. Selecione a interface de rede (Conexão Local ou Ethernet) e escolha Propriedades.
8. Na página Propriedades da Conexão Local, escolha Protocolo TCP/IP Versão 4 (TCP/IPv4), Propriedades, Avançado.
9. Escolha Adicionar.
10. Na caixa de diálogo Endereço TCP/IP, digite o endereço IP privado secundário para o endereço IP. Em Subnet mask (Máscara de sub-rede), digite a mesma máscara de sub-rede inserida para o endereço IP privado primário em Etapa 1: configurar o endereçamento IP estático na sua instância e selecione Add (Adicionar).



11. Verifique as configurações de endereço IP e selecione OK.



12. Escolha OK, Fechar.
13. Para confirmar se o endereço IP secundário foi adicionado ao sistema operacional, execute o comando `ipconfig /all` no PowerShell. A saída deve ser semelhante à seguinte:

```
Ethernet adapter Ethernet 4:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Amazon Elastic Network Adapter #2
   Physical Address. . . . . . . . . : 02-9C-3B-FC-8E-67
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::f4d1:a773:5afa:cd1%7(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.200.0.128(Preferred)
```

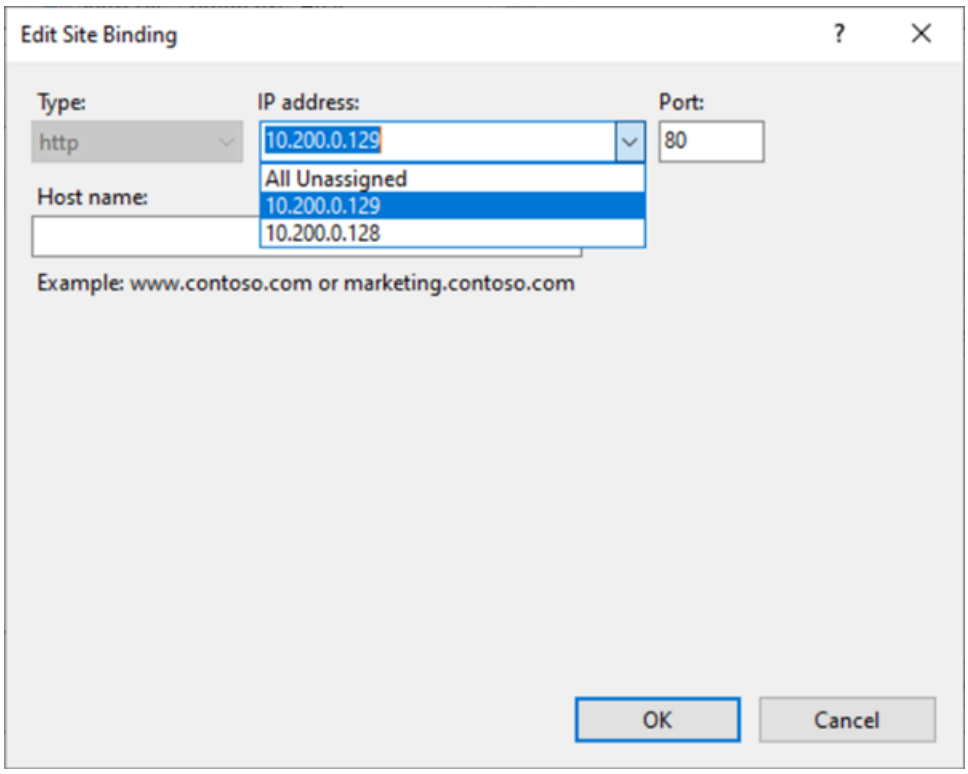
```
Subnet Mask . . . . . . . . . . . : 255.255.255.0
IPv4 Address. . . . . . . . . . . : 10.200.0.129(Preferred)
Subnet Mask . . . . . . . . . . . : 255.255.255.0
Default Gateway . . . . . . . . . : 10.200.0.1
DHCPv6 IAID . . . . . . . . . . . : 151166011
DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2D-67-AC-FC-12-34-9A-BE-A5-E7
DNS Servers . . . . . . . . . . . : 10.200.0.2
NetBIOS over Tcpip. . . . . . . . : Enabled
```

Etapa 3: Configurar as aplicações para usar o endereço IP privado secundário

É possível configurar quaisquer aplicações para usar o endereço IP privado secundário. Por exemplo, se sua instância estiver executando um site no IIS, é possível configurar o IIS para usar o endereço IP privado secundário.

Para configurar o IIS para usar o endereço IP privado secundário

1. Conecte-se à sua instância.
2. Abra o Gerenciador do Serviços de Informações da Internet (IIS).
3. No painel Conexões, expanda Sites.
4. Abra o menu contextual (botão direito do mouse) para seu site ou selecione Editar Ligações.
5. Na caixa de diálogo Ligações do Site, para Tipo, escolha http, Editar.
6. Na caixa de diálogo Editar Ligação do Site, para Endereço IP, selecione o endereço IP privado secundário. (Por padrão, cada site aceita solicitações HTTP de todos os endereços IP.)



7. Escolha OK, Fechar.

Nomes de host e domínios de instâncias do EC2

Compreender nomes de host e domínios de instâncias do EC2 é importante para gerenciar e acessar com eficácia suas instâncias do Amazon EC2. Cada instância do EC2 pode ter diferentes tipos de nomes de host, privados e públicos, que servem a propósitos diferentes e seguem convenções de nomenclatura específicas.

Este tópico explica a estrutura dos nomes de host de instâncias do EC2, como eles são construídos e os diferentes tipos de nomes de host disponíveis. Você aprenderá a visualizar e modificar as configurações de nome de host, entender quando usar cada tipo e aprenderá as melhores práticas para gerenciamento de nomes de host em seu ambiente da AWS.

Conteúdo

- Entendendo nomes de host e domínios de instâncias do EC2
- Tipos de nomes de host

Entendendo nomes de host e domínios de instâncias do EC2

Um endereço de instância do EC2 é formado por vários componentes. Exemplo de um endereço de instância do EC2 que usa o endereço IPv4 privado da instância:

```
   IP address         Domain name
   #--------# #-----------------------#
ip-10-24-34-0.us-west-2.compute.internal
#-----------#
  Hostname
#-------------------------------------#
    Fully qualified domain name (FQDN)
```

Em que:

- Endereço IP: o endereço IPv4 principal da interface de rede primária associada a uma instância.
- Nome de host: o nome local de uma instância do EC2 específica (usado pelo sistema operacional e para identificação da rede local)
- Nome de domínio: a parte do FQDN fornecida pela AWS.
- Nome de domínio totalmente qualificado (FQDN): o endereço completo que inclui tanto o nome do host quanto o nome do domínio. Esse é o identificador completo e globalmente exclusivo usado para acessar sua instância em todas as redes.

Dependendo do tipo de nome de host escolhido para a instância ou interface de rede primária anexada à instância, os formatos de nome de host e nome de domínio serão diferentes do exemplo acima. Esta seção explica as opções de tipos de nome de host.

Tipos de nomes de host

A AWS fornece dois tipos de nomes de host: privados e públicos. A tabela a seguir compara as principais diferenças entre nomes de host privados e públicos, incluindo como eles são resolvidos, como são configurados e quando cada tipo deve ser usado.

	Nomes de host privados	Nomes de host públicos
Resolução do DNS	Os nomes de host privados permitem utilizar FQDNs privados que não são acessíveis via Internet pública. Os	Os nomes de host públicos permitem utilizar FQDNs públicos que são acessíveis via Internet pública. Os

	Nomes de host privados	Nomes de host públicos
	nomes de host privados só permitem que as solicitações sejam resolvidas para endereços GUA IPv4 e IPv6 privados dentro da VPC.	nomes de host públicos permitem que as solicitações sejam resolvidas para GUA IPv4 e IPv6 privados dentro da VPC e IPs públicos da Internet (DNS de horizonte dividido).
Configuração	Os nomes de host privados são configurados em nível de instância.	Os nomes de host públicos são configurados em nível de interface de rede.
Quando usar	• Para nomes de host que são resolvidos somente em sua VPC, para comunicação interna • Para manter seu esquema de nomenclatura interno privado • Para simplificar o gerenciamento interno de recursos sem considerações de DNS externo	• Para acessar instâncias via IPv4 e IPv6 pela Internet • Para simplificar a migração de ambientes IPv4 para IPv6

Conteúdo

- Nomes de host públicos
- Nomes de host privados

Nomes de host públicos

É possível usar nomes de host públicos para acessar instâncias do EC2 usando nomes de host que se resolvem no endereço IPv4 ou IPv6 público da instância e facilitar sua transição para IPv6.

Os nomes de host públicos permitem:

- Acessar suas instâncias do EC2 via IPv4 e IPv6, oferecendo mais flexibilidade na forma como você se conecta aos seus recursos.
- Migrar de ambientes IPv4 para IPv6 no seu próprio ritmo. Você pode, por exemplo, desacoplar suas migrações de banco de dados e aplicações, reduzindo a complexidade e o risco.

- Usar várias opções de nome de host (somente IPv4, somente IPv6 e pilha dupla) que são resolvidos automaticamente nos endereços IP apropriados.
- Beneficiar-se da segurança aprimorada com DNS de horizonte dividido, que resolve nomes de host em endereços IP privados quando consultados de dentro da sua VPC.

Conteúdo

- Tipos de nomes de host públicos e quando usá-los
- Visualizar nomes de host públicos
- Modificar tipos de nomes de host públicos

Tipos de nomes de host públicos e quando usá-los

Para usar nomes de host públicos, é necessário modificar uma interface de rede existente. Esta seção descreve as três opções de tipo de nome de host público e ajuda você a decidir qual usar:

- Pilha dupla: nome baseado em IP
  - Essa é a melhor opção se você está migrando ou planejando migrar de IPv4 para IPv6. Essa opção permite a conectividade via IPv4 e IPv6, oferecendo flexibilidade a clientes que podem estar usando qualquer um dos protocolos, além de permitir que os clientes mantenham o mesmo nome de host durante a migração para IPv6.
  - As solicitações de dentro da VPC são resolvidas no endereço IPv4 privado e no endereço unicast global (GUA) IPv6 da interface de rede. As solicitações da Internet são resolvidas tanto no endereço IPv4 público quanto no GUA IPv6 da interface de rede.
  - Exemplo
    - Quando você escolhe essa opção, um FQDN de pilha dupla é gerado para essa interface de rede. Este é um exemplo do FQDN que será gerado:
      - f5lnz-0khrm-nt2u3-gyqqt-nbdl5-q3cdpO.ap-southeast-2.ip.aws
    - Em que:
      - f5lnz-0khrm-nt2u3-gyqqt-nbdl5-q3cdpO é o nome do host em uma representação base36 do endereço IPv6 público primário (f5lnz-0khrm-nt2u3-gyqqt-nbdl5) na interface de rede junto com uma representação base36 do endereço IPv4 público primário (q3cdpO) na interface de rede.

        - f5lnz-0khrm-nt2u3-gyqqt-nbdl5 é resolvido pelo resolvedor de DNS da Amazon no endereço GUA IPv6 FFFF:1407:4:f000:81d:2689:1066:4489. Esse é o primeiro GUA IPv6 atribuído à interface de rede.
        - q3cdpo é resolvido no endereço IPv4 52.54.55.56. Esse é o endereço IPv4 público vinculado à interface de rede primária.
        - ap-southeast-2 é a região da sub-rede em que a interface de rede está localizada.
        - ip.aws é o domínio fornecido pela AWS.
- IPv6: nome baseado em IP
    - Essa é uma boa opção se você já migrou para IPv6 e precisa de conectividade somente via IPv6.
    - As solicitações de dentro da VPC ou da internet são resolvidas no GUA IPv6 da interface de rede.
    - Exemplo
        - Quando você escolhe essa opção, um FQDN é gerado para essa interface de rede. Este é um exemplo do FQDN que será gerado:
            - f5lnz-0khrm-nt2u3-gyqqt-nbdl5.ap-southeast-2.ip.aws
        - Em que:
            - f5lnz-0khrm-nt2u3-gyqqt-nbdl5 é um nome de host que é uma representação base36 do endereço IPv6 público primário da interface de rede.
            - f5lnz-0khrm-nt2u3-gyqqt-nbdl5 é resolvido pelo resolvedor de DNS da Amazon no endereço GUA IPv6 FFFF:1407:4:f000:81d:2689:1066:4489. Esse é o primeiro GUA IPv6 atribuído à interface de rede.
            - ap-southeast-2 é a região da sub-rede em que a interface de rede está localizada.
            - ip.aws é o domínio fornecido pela AWS.
- IPv4: nome baseado em IP
    - Essa é uma boa opção se a instância que usa essa interface de rede precisa manter o acesso IPv4 durante a transição para IPv6 ou se as aplicações ou os sistemas em execução na instância oferecem suporte somente a IPv4. Essa é a melhor opção se você precisa apenas manter a conectividade IPv4 e suas workloads não exigem suporte a IPv6. Por exemplo, se você estiver migrando para IPv6, poderá decidir manter algumas aplicações em IPv4 enquanto migra outras para IPv6.

- As solicitações de dentro da VPC são resolvidas no endereço IPv4 primário privado da interface de rede. As solicitações da Internet são resolvidas no endereço IPv4 público da interface de rede.
- Exemplo
  - Se você escolher essa opção, um nome de host público habilitado para IPv4 será gerado para essa interface de rede. Este é um exemplo do nome de DNS que será gerado:
    - ec2-52-54-55-66.ap-southeast-2.compute.amazonaws.com
  - Em que:
    - ec2-52-54-55-66 é um nome de host que é uma representação base36 do endereço IPv4 público primário da interface de rede.
    - ec2-52-54-55-66 é resolvido no endereço IPv4 52.54.55.56. Esse é o endereço IPv4 público vinculado à interface de rede primária.
    - ap-southeast-2 é a região da sub-rede em que a interface de rede está localizada.
    - ip.aws é o domínio fornecido pela AWS.

> **Important**
>
> Nos exemplos acima, é possível ver que os endereços IP são usados para gerar o nome do host. Se você alterar o endereço IPv4 privado primário ou o primeiro GUA IPv6 atribuído à interface de rede, a parte do nome do host que se traduz no endereço IP mudará e o nome de host público gerado anteriormente deixará de ser válido. Além disso, alterar o endereço público IPv4 primário força uma atualização downstream do Instance Metadata Service (IMDS) no Guia do usuário do Amazon EC2, fazendo com que os metadados IMDS da instância do EC2 sejam atualizados automaticamente.

Visualizar nomes de host públicos

Se a VPC na qual a interface de rede está não tiver EnableDnsHostnames e EnableDnsSupport habilitados, não haverá nenhum tipo de nome de host definido ou gerado.

Console

É possível visualizar os nomes de host públicos para uma instância ou interface de rede primária.

Para visualizar o tipo de nome de host e os nomes DNS 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. Marque a caixa de seleção da instância.
4. Na guia Rede, em Nome do host e DNS, procure:
   - Tipo de nome de host público
   - DNS público
   - Somente IPv4: nome baseado em IP
   - Somente IPv6: nome baseado em IP
   - Pilha dupla: nome baseado em IP

Para visualizar o tipo de nome de host e os nomes DNS 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. No campo de pesquisa, insira o ID da instância. Selecione o ID da interface de rede para abrir sua página de detalhes.
4. Na guia Nome de host e DNS, procure:
   - Tipo de nome de host público
   - Nome público do DNS
   - Nome DNS IPv4 público
   - Nome DNS IPv6 público
   - Nome DNS de pilha dupla público

AWS CLI

Para visualizar o tipo de nome de host e os nomes DNS de uma interface de rede

Use o comando describe-network-interfaces.

```
aws ec2 describe-network-interfaces \
    --network-interface-id eni-1234567890abcdef0 \
```

```
    --query NetworkInterfaces[].PublicIpDnsNameOptions
```

O seguinte é um exemplo de saída. Como o tipo de nome de host é `public-dual-stack-dns-name`, o nome de host DNS é o mesmo que `PublicDualStackDnsName`.

```
[
     {
          "DnsHostnameType": "public-dual-stack-dns-name",
          "PublicIpv4DnsName": "ec2-52-54-55-66.ap-
southeast-2.compute.amazonaws.com",
          "PublicIpv6DnsName": "f5lnz-0khrm-nt2u3-gyqqt-nbdl5.ap-
southeast-2.ip.aws",
          "PublicDualStackDnsName": "f5lnz-0khrm-nt2u3-gyqqt-nbdl5-q3cdp0.ap-
southeast-2.ip.aws"
     }
]
```

PowerShell

Para visualizar o tipo de nome de host e os nomes DNS de uma interface de rede

Use o cmdlet Get-EC2NetworkInterface.

```
(Get-EC2NetworkInterface `
    -NetworkInterfaceId eni-1234567890abcdef0).PublicIpDnsNameOptions
```

O seguinte é um exemplo de saída. Como o tipo de nome de host é `public-dual-stack-dns-name`, o nome de host DNS é o mesmo que `PublicDualStackDnsName`.

```
DnsHostnameType        : public-dual-stack-dns-name
PublicDualStackDnsName : f5lnz-0khrm-nt2u3-gyqqt-nbdl5-q3cdp0.ap-southeast-2.ip.aws
PublicIpv4DnsName      : ec2-52-54-55-66.ap-southeast-2.compute.amazonaws.com
PublicIpv6DnsName      : f5lnz-0khrm-nt2u3-gyqqt-nbdl5.ap-southeast-2.ip.aws
```

Modificar tipos de nomes de host públicos

As opções de tipo de nome de host público dependem dos endereços IP associados à interface de rede:

- Se a interface de rede tiver apenas um endereço IPv4 público, o tipo de nome de host será IPv4: nome baseado em IP.

- Se a interface de rede tiver apenas um endereço IPv6, o tipo de nome de host será IPv6: nome baseado em IP.
- Se a interface de rede tiver um endereço IPv4 público e um IPv6, o tipo de nome de host será Pilha dupla: nome baseado em IP.

Pré-requisitos

- A interface de rede deve ter um endereço IPv4 público ou um endereço IPv6 associado.
- A VPC na qual a interface de rede está deve ter as opções EnableDnsHostnames e EnableDnsSupport habilitadas. Consulte Visualizar e atualizar atributos de DNS para sua VPC no Guia do usuário do Amazon VPC.

Console

Para modificar o tipo de nome de host público

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Network Interfaces.
3. No campo de pesquisa, insira o ID da instância. Marque a caixa de seleção para a interface de rede.

   Como alternativa, na página de detalhes da instância, escolha a guia Rede e selecione o ID da interface de rede para o índice de dispositivo 0.
4. Escolha Ações, Modificar tipo de nome de host público.
5. Escolha uma opção:

   - Pilha dupla: nome baseado em IP: um nome de host público de pilha dupla para uma interface de rede. As solicitações de dentro da VPC são resolvidas no endereço IPv4 privado e no endereço unicast global IPv6 da interface de rede. As solicitações da Internet são resolvidas tanto no endereço IPv4 público quanto no GUA IPv6 da interface de rede.
   - IPv4: nome baseado em IP: um nome de host público habilitado para IPv4 para uma interface de rede. As solicitações de dentro da VPC são resolvidas no endereço IPv4 primário privado da interface de rede. As solicitações da Internet são resolvidas no endereço IPv4 público da interface de rede.

- IPv6: nome baseado em IP: um nome de host público habilitado para IPv6 para uma interface de rede. As solicitações de dentro da VPC ou da internet são resolvidas no GUA IPv6 da interface de rede.

6. Escolha Modificar.

AWS CLI

Para modificar o tipo de nome de host público

Use o comando modify-public-ip-dns-name-options.

```
aws ec2 modify-public-ip-dns-name-options \
    --network-interface-id eni-1234567890abcdef0 \
    --hostname-type public-dual-stack-dns-name
```

O seguinte é um exemplo de saída.

```
{
    "Successful": true
}
```

PowerShell

Para modificar o tipo de nome de host público

Use o cmdlet Edit-EC2PublicIpDnsNameOption.

```
Edit-EC2PublicIpDnsNameOption `
    -NetworkInterfaceId eni-1234567890abcdef0 `
    -HostNameType public-dual-stack-dns-name
```

Nomes de host privados

Esta seção descreve os nomes de host privados da instância do Amazon EC2 disponíveis quando você inicia as instâncias nas sub-redes da sua VPC.

O nome do host privado diferencia as instâncias do EC2 em sua rede. Você pode usar o nome de host privado de uma instância se, por exemplo, quiser executar scripts para se comunicar com algumas ou todas as instâncias de sua rede.

Conteúdo

- Tipos de nomes de host privados
- Onde encontrar nomes de recursos e nomes de IP
- Escolher entre nomes de recursos e nomes de IP
- Alterar as opções de nomenclatura baseada em recursos para o Amazon EC2

Tipos de nomes de host privados

Existem dois tipos de nomes de host privados para o nome de host do sistema operacional guest quando as instâncias do EC2 são executadas em uma VPC:

- IP name (Nome de IP): o esquema de nomenclatura herdado em que, quando você inicia uma instância, o endereço IPv4 privado da instância está incluído no nome de host da instância. O nome de IP existe durante todo o ciclo de vida da instância do EC2. Quando usado como hostname de DNS privado, ele só retorna o endereço IPv4 privado (registro A).
- Resource name (Nome do recurso): quando você inicia uma instância, o ID da instância do EC2 está incluído no nome de host da instância. O nome do recurso existe durante todo o ciclo de vida da instância do EC2. Quando usado como hostname de DNS privado, ele pode retornar o endereço IPv4 privado (registro A) e/ou o endereço IPv6 Global Unicast (registro AAAA).

O tipo de nome de host do sistema operacional convidado da instância do EC2 depende das configurações de sub-rede:

- Se a instância for iniciada em uma sub-rede somente IPv4, será possível selecionar nome de IP ou nome do recurso.
- Se a instância for iniciada em uma sub-rede de pilha dual (IPv4+IPv6), será possível selecionar nome de IP ou nome do recurso.
- Se a instância for iniciada em uma sub-rede somente IPv6, o nome do recurso será usado automaticamente.

Conteúdo

- Nome de IP
- Nome do recurso
- Diferença entre o nome de IP e o nome do recurso

Nome de IP

Quando você inicia uma instância do EC2 com o Hostname type (Tipo de nome de host) de IP name (Nome de IP), o nome de host do sistema operacional convidado será configurado para usar o endereço IPv4 privado.

- Formato para uma instância em us-east-1: *private-ipv4-address*.ec2.internal
- Exemplo: *ip-10-24-34-0*.ec2.internal
- Formato para uma instância em qualquer outra região da AWS: *private-ipv4-address.region*.compute.internal
- Exemplo: *ip-10-24-34-0.us-west-2*.compute.internal

Nome do recurso

Quando você inicia instâncias do EC2 em sub-redes somente IPv6, o Hostname type (Tipo de nome de host) do Resource name (Nome do recurso) é selecionado por padrão. Quando você inicia uma instância em sub-redes somente IPv4 ou pilha dupla (IPv4+IPv6), é possível selecionar a opção Resource name (Nome do recurso). Após iniciar uma instância, é possível gerenciar a configuração de nome de host. Para obter mais informações, consulte Alterar as opções de nomenclatura baseada em recursos para o Amazon EC2.

Quando você inicia uma instância do EC2 com um Hostname type (Tipo de nome de host) de Resource name (Nome de recurso), o hostname do sistema operacional convidado é configurado para usar o ID da instância do EC2.

- Formato para uma instância em us-east-1: *ec2-instance-id*.ec2.internal
- Exemplo: *i-0123456789abcdef*.ec2.internal
- Formato para uma instância em qualquer outra região da AWS: *ec2-instance-id.region*.compute.internal
- Exemplo: *i-0123456789abcdef.us-west-2*.compute.internal

Diferença entre o nome de IP e o nome do recurso

Consultas ao DNS para nomes de IP e nomes de recurso coexistem para garantir compatibilidade com versões anteriores e permitir a migração de nomenclatura baseada em IP para nomes de host para nomenclatura baseada em recursos. Para hostnames de DNS privados baseados em nomes de IP, você não pode configurar se uma consulta de registro de DNS A para a instância é

respondida ou não. As consultas de registro de DNS A são sempre respondidas independentemente das configurações de nome de host do sistema operacional convidado. Entretanto, para nomes de host de DNS privados baseados em nome do recurso, é possível configurar se as consultas de DNS A ou DNS AAAA para a instância são respondidas ou não. Você configura o comportamento de resposta quando inicia uma instância ou modifica uma sub-rede. Para obter mais informações, consulte Alterar as opções de nomenclatura baseada em recursos para o Amazon EC2.

Onde encontrar nomes de recursos e nomes de IP

Você pode ver os tipos de nome de host, o nome do recurso e o nome do IP no console do Amazon EC2.

Conteúdo

- Ao criar uma instância do EC2
- Ao visualizar os detalhes de uma instância do EC2 existente

Ao criar uma instância do EC2

Quando você cria uma instância do EC2, dependendo do tipo de sub-rede selecionada, Hostname type (Tipo de nome de host) de Resource name (Nome de recurso) pode estar disponível ou pode estar selecionada e não poder ser modificada. Esta seção explica em que cenários você encontra os tipos de nome de host do nome do recurso e o nome de IP.

Cenário 1

Crie uma instância do EC2 no assistente (consulte Executar uma instância do EC2 usando o assistente de inicialização de instâncias no console) e, ao configurar os detalhes, escolha uma sub-rede que você configurou para ser somente IPv6.

Neste caso, Hostname type (Tipo de nome de host) de Resource name (Nome do recurso) é selecionado automaticamente e não pode ser modificado. As opções de DNS Hostname (Nome de host DNS) em Enable IP name IPv4 (A record) DNS requests (Habilitar solicitações DNS IPv4 [registro A] de nome de IP) e Enable resource-based IPv4 (A record) DNS requests (Habilitar solicitações DNS IPv4 [registro A] baseadas em recursos) são desmarcadas automaticamente, não sendo possível modificá-las. A opção Enable resource-based IPv6 (AAAA record) DNS requests (Habilitar solicitações DNS IPv6 [registro AAAA] baseadas em recursos) é selecionada por padrão, mas é possível modificá-la. Se estiver selecionada, as solicitações DNS para o nome do recurso serão resolvidas como o endereço IPv6 (registro AAAA) dessa instância do EC2.

Cenário 2

Crie uma instância do EC2 no assistente (consulte Executar uma instância do EC2 usando o assistente de inicialização de instâncias no console) e, ao configurar os detalhes, escolha uma sub-rede configurada com um bloco CIDR IPv4 ou um bloco CIDR IPv4 e IPv6 (“pilha dupla”).

Nesse caso, a opção Enable IP name IPV4 (A record) DNS requests (Habilitar solicitações DNS de IPV4 de nome de IP [registro A]) é selecionada automaticamente e não pode ser alterada. Isso significa que as solicitações para o nome IP serão resolvidas como o endereço IPv4 (registro A) dessa instância do EC2.

As opções são padrão para as configurações da sub-rede, mas é possível modificar as opções para essa instância, dependendo das configurações de sub-rede:

- Hostname type (Tipo de nome de host): determina se você deseja que o nome de host do sistema operacional convidado da instância do EC2 seja o nome do recurso ou o nome de IP. O valor padrão é IP name (Nome de IP).
- Enable resource-based IPv4 (A record) DNS requests (Habilitar solicitações DNS IPv4 baseado em recursos [registro A]): determina se as solicitações ao nome do recurso são resolvidas como o endereço IPv4 privado (registro A) dessa instância do EC2. Essa opção não é selecionada por padrão.
- Enable resource-based IPv6 (AAAA record) DNS requests (Habilitar solicitações DNS IPv6 baseado em recursos [registro AAAA]): determina se as solicitações ao nome do recurso são resolvidas como o endereço GUA IPv6 (registro AAAA) dessa instância do EC2. Essa opção não é selecionada por padrão.

Ao visualizar os detalhes de uma instância do EC2 existente

É possível ver os valores do nome de host de uma instância do EC2 existente na guia Details (Detalhes) para a instância do EC2:

- Hostname type (Tipo de nome de host): o nome de host em nome de IP ou formato de nome do recurso.
- Private IP DNS name (IPv4 only) (Nome de DNS do IP privado [somente IPv4]): o nome de IP que sempre é resolvido como o endereço IPv4 privado da instância.
- Private resource DNS name (Nome de DNS de recurso privado): o nome do recurso que pode ser resolvido como registros de DNS para essa instância.

- Answer private resource DNS name (Responder ao nome de DNS de recurso privado): o nome de recurso é resolvido como registros de DNS IPv4 (A), IPv6 (AAAA) ou IPv4 e IPv6 (A e AAAA).

Além disso, se você se conectar à instância do EC2 diretamente por SSH e inserir o comando `hostname`, verá o nome de host no formato nome de IP ou nome do recurso.

Escolher entre nomes de recursos e nomes de IP

Ao iniciar uma instância do EC2 (consulte Executar uma instância do EC2 usando o assistente de inicialização de instâncias no console), se você escolher um Hostname type (Tipo de nome de host) do Resource name (Nome do recurso), a instância do EC2 será executada com um nome de host no formato de nome do recurso. Nesses casos, o registro DNS dessa instância do EC2 também poderá apontar para o nome do recurso. Isso permite a flexibilidade de escolher se esse nome de host será resolvido para o endereço IPv4, o endereço IPv6 ou para ambos os endereços IPv4 e IPv6 da instância. Se você planeja usar o IPv6 no futuro ou se estiver usando sub-redes de pilha dupla atualmente, é melhor usar um Hostname type (Tipo de nome de host) do Resource name (Nome do recurso) para alterar a resolução de DNS para os nomes de host de suas instâncias sem fazer alterações nos registros DNS por conta própria. O nome do recurso permite adicionar e remover a resolução de DNS IPv4 e IPv6 em uma instância do EC2.

Se, em vez disso, você escolher um Hostname type (Tipo de nome de host) de IP name (Nome de IP) e usá-lo como nome de host DNS, ele só poderá resolver para o endereço IPv4 da instância. Ele não será resolvido para o endereço IPv6 da instância, mesmo que a instância tenha um endereço IPv4 e um endereço IPv6 associado a ela.

Alterar as opções de nomenclatura baseada em recursos para o Amazon EC2

Você pode alterar o tipo de nome de host e as configurações de nome de host DNS para sub-redes, o que afetará todas as execuções de instâncias subsequentes nesse assunto, ou você pode alterá-los para uma instância do EC2 depois de iniciá-la.

Opções de nomenclatura baseada em recursos

- Tipo de nome de host: determina a configuração padrão para o nome de host do sistema operacional hospedado das instâncias do EC2 executadas na sub-rede. Esse é o nome do recurso ou o nome do IP.
- Habilitar solicitações de nome de host DNS IPv4 (registro A): determina se as solicitações/consultas de DNS ao nome do recurso são resolvidas como o endereço IPv4 (registro A) privado da instância do EC2.

- Habilitar solicitações de nome de host DNS IPv6 (registro AAAA): determina se as solicitações/consultas de DNS ao nome do recurso são resolvidas como o endereço IPv6 (registro A) da instância do EC2.

Sub-redes

Alterar as configurações de sub-rede não altera a configuração das instâncias do EC2 que já foram executadas na sub-rede.

Console

Para modificar as opções de uma sub-rede

Abra o console do Amazon VPC e selecione a sub-rede. Escolha Ações, Editar configurações de sub-rede. Modifique as configurações conforme necessário e salve suas alterações.

AWS CLI

Para modificar as opções de uma sub-rede

Use o comando modify-subnet-attribute.

```
aws ec2 modify-subnet-attribute \
    --subnet-id subnet-0abcdef1234567890 \
    --private-dns-hostname-type-on-launch resource-name \
    --enable-resource-name-dns-a-record-on-launch \
    --enable-resource-name-dns-aaaa-record-on-launch
```

PowerShell

Para modificar as opções de uma sub-rede

Use o cmdlet Edit-EC2SubnetAttribute.

```
Edit-EC2SubnetAttribute `
    -SubnetId subnet-0abcdef1234567890 `
    -PrivateDnsHostnameTypeOnLaunch ResourceName `
    -EnableResourceNameDnsAAAARecordOnLaunch $true `
    -EnableResourceNameDnsARecordOnLaunch $true
```

Instâncias do EC2

Considerações

- Para alterar o tipo do nome de host, primeiro você deve interromper a instância. Não é necessário interromper uma instância para alterar as outras duas opções.
- Uma vez que instâncias com volume raiz de armazenamento de instância não podem ser interrompidas, as configurações de tipo de nome do host e nome do host DNS só podem ser definidas durante a inicialização da instância. Somente os seguintes tipos de instância são compatíveis com volumes raiz de armazenamento de instância: C1, C3, D2, I2, M1, M2, M3, R3 e X1.

Console

Para modificar o tipo de nome de host e as opções de nome de host DNS para uma instância

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Se você for alterar a configuração Use resource based naming as guest OS hostname (Usar nomenclatura baseada em recursos como nome de host do sistema operacional convidado), primeiro interrompa a instância do EC2. Caso contrário, ignore essa etapa.

   Para interromper a instância, selecione-a e escolha Instance state (Estado da instância) e Start instance (Iniciar instância).
3. Selecione a instância e escolha Actions (Ações), Instance settings (Configurações da instância), Change resource based naming options (Alterar opções de nomenclatura baseada em recurso).

   - Use resource based naming as guest OS hostname (Usar nomenclatura baseada em recursos como nome de host do sistema operacional convidado): determina se você deseja que o nome de host do sistema operacional convidado da instância do EC2 seja o nome do recurso ou o nome de IP.
   - Answer DNS hostname IPv4 (A record) requests (Responder solicitações de nome de host DNS IPv4 (registro A)): determina se as solicitações/consultas de DNS ao nome do recurso são resolvidas como o endereço IPv4 privado desta instância do EC2.
   - Answer DNS hostname IPv6 (AAAA record) requests (Responder solicitações de nome de host DNS IPv6 (registro AAAA)): determina se as solicitações/consultas de DNS ao nome do recurso são resolvidas como o endereço IPv6 (registro AAAA) desta instância do EC2.

4. Escolha Salvar.
5. Se você interrompeu a instância, inicie-a novamente.

AWS CLI

Para modificar o tipo de nome de host e as opções de nome de host DNS para uma instância

Use o comando modify-private-dns-name-options.

```
aws ec2 modify-private-dns-name-options \
    --instance-id i-1234567890abcdef0 \
    --private-dns-hostname-type resource-name \
    --enable-resource-name-dns-a-record \
    --enable-resource-name-dns-aaaa-record
```

PowerShell

Para modificar o tipo de nome de host e as opções de nome de host DNS para uma instância

Use o cmdlet Edit-EC2PrivateDnsNameOption.

```
Edit-EC2PrivateDnsNameOption `
    -InstanceId i-1234567890abcdef0 `
    -PrivateDnsHostnameType ResourceName `
    -EnableResourceNameDnsAAAARecord $true`
    -EnableResourceNameDnsARecord $true
```

Trazer seus próprios endereços IP (BYOIP) para o Amazon EC2

É possível trazer parte ou todo o seu intervalo de endereços IPv4 ou IPv6 publicamente roteáveis da rede on-premises para sua Conta da AWS. Você continua controlando o intervalo de endereços e pode anunciar o intervalo de endereços na Internet via AWS. Depois de trazer o intervalo de endereços para o Amazon EC2, ele aparecerá em sua Conta da AWS como um grupo de endereços.

> **Note**
>
> Esta documentação descreve como trazer seu próprio intervalo de endereços IP para uso somente no Amazon EC2. Para trazer seu próprio intervalo de endereços IP para uso no AWS Global Accelerator, consulte Trazer seus próprios endereços IP (BYOIP) no Guia do

desenvolvedor do AWS Global Accelerator. Para usar seu próprio intervalo de endereços IP para uso no Amazon VPC IP Address Manager, consulte o Tutorial: traga seus endereços IP para o IPAM no Guia do usuário do IPAM da Amazon VPC.

Quando você traz um intervalo de endereços IP para a AWS, a AWS valida que você controla o intervalo de endereços IP. Existem dois métodos que você pode usar para mostrar que controla o intervalo:

- Se seu intervalo de endereços IP estiver registrado em um Registro da Internetcompatível com RDAP (como ARIN, RIPE e APNIC), será possível verificar o controle do domínio com um certificado X.509 usando o processo mostrado nesta página. O certificado apenas deve ser válido durante o processo de provisionamento. É possívelrá remover o certificado do seu registro do RIR após a conclusão do provisionamento.
- Independentemente do seu Registro da Internet ser compatível com RDAP, você pode usar o IPAM da Amazon VPC para verificar o controle do seu domínio com um registro DNS TXT. Esse processo está documentado no Tutorial: trazer seus endereços IP para o IPAM no Guia do usuário do IPAM da Amazon VPC.

Para obter mais informações, consulte o Conversa técnica online da AWS Mergulho profundo em Traga seu próprio IP.

Conteúdo

- Definições BYOIP
- Requisitos e cotas
- Disponibilidade regional
- Disponibilidade da zona local
- Pré-requisitos para o BYOIP no Amazon EC2
- Integrar seu intervalo de endereços para uso no Amazon EC2
- Usar seu intervalo de endereços BYOIP no Amazon EC2

Definições BYOIP

- Certificado autoassinado X.509: um padrão de certificado mais comumente usado para criptografar e autenticar dados dentro de uma rede. É um certificado usado pela AWS para validar o controle

do espaço IP a partir de um registro RDAP. Para obter mais informações sobre certificados X.509, consulte RFC 3280.

- Número de sistema autônomo (ASN): um identificador global exclusivo que define um grupo de prefixos de IP executados por uma ou mais operadoras de rede que mantêm uma política de roteamento única e claramente definida.
- Registro regional da Internet (RIR): uma organização que gerencia a alocação e o registro de endereços IP e ASNs em uma região do mundo.
- Registry Data Access Protocol (RDAP): um protocolo somente de leitura para consultar dados de registro atuais em um RIR. As entradas no banco de dados do RIR consultado são chamadas de "registros RDAP". Certos tipos de registros precisam ser atualizados pelos clientes por meio de um mecanismo fornecido pelo RIR. Esses registros são consultados pela AWS para verificar o controle de um espaço de endereço no RIR.
- Autorização de origem de rota (ROA): um objeto criado por RIRs para que os clientes autentiquem anúncios IP em sistemas autônomos específicos. Para obter uma visão geral, consulte Autorizações de origem de rota (ROAs) no site do ARIN.
- Registro local da Internet (LIR):: organizações, como provedores de serviços de Internet, que alocam um bloco de endereços IP de um RIR para seus clientes.

Requisitos e cotas

- O intervalo de endereços deve ser registrado no seu Registro Regional da Internet (RIR). Consulte seu RIR para ver quaisquer políticas relacionadas a regiões geográficas. O BYOIP atualmente oferece suporte ao registro no American Registry for Internet Numbers (ARIN), Réseaux IP Européens Network Coordination Centre (RIPE) ou no Asia-Pacific Network Information Centre (APNIC). Ele deve ser registrado para uma entidade empresarial ou institucional e não pode ser registrado para uma única pessoa.
- O intervalo de endereços IPv4 mais específico que é possível trazer é /24.
- O intervalo mais específico de endereços IPv6 que é possível trazer é /48 para CIDRs anunciáveis publicamente e /60 para CIDRs que não são anunciáveis publicamente.
- As ROAs não são necessárias para intervalos CIDR que não são anunciáveis publicamente, mas os registros RDAP ainda precisam ser atualizados.
- É possível trazer cada intervalo de endereços para uma região da AWS de cada vez.
- É possível trazer um total de cinco intervalos de endereços IPv4 e IPv6 BYOIP por região da AWS para sua conta da AWS. Não é possível ajustar as cotas para CIDRs BYOIP usando o console do

Service Quotas, mas você pode solicitar um aumento da cota entrando em contato com o AWS Support Center, conforme descrito em Cotas de serviços da AWS, na Referência geral da AWS.

- Você não pode compartilhar seu intervalo de endereços IP com outras contas usando AWS RAM a menos que você use o IP Address Manager (IPAM) da Amazon VPC e integre o IPAM com o AWS Organizations. Para obter mais informações, consulte Integrar IPAM com o AWS Organizations no Guia do usuário do Amazon VPC IPAM.
- Os endereços no intervalo de endereços IP devem ter um histórico limpo. Podemos investigar a reputação do intervalo de endereços IP e reservar o direito de rejeitar um intervalo de endereços IP, se ele contiver um endereço IP que tenha má reputação ou esteja associado a comportamento mal-intencionado.
- O espaço de endereço herdado, o espaço de endereço IPv4 que foi distribuído pelo registro central da Internet Assigned Numbers Authority (IANA) antes da formação de Regional Internet Registries (RIR), ainda requer um objeto ROA correspondente.
- Para LIRs, é comum o uso de um processo manual para atualizar os registros. Dependendo do LIR, a implantação pode levar dias.
- Um único objeto ROA e registro RDAP são necessários para um bloco CIDR grande. É possível trazer vários blocos CIDR menores desse intervalo para a AWS, mesmo em várias regiões da AWS, usando o único objeto e registro.
- Não há suporte para BYOIP em zonas de comprimento de onda ou em AWS Outposts.
- Não faça alterações manuais no BYOIP no RADb ou em qualquer outro IRR. O BYOIP atualizará automaticamente o RADb. Qualquer alteração manual que inclua o ASN do BYOIP fará com que a operação de provisão do BYOIP falhe.
- Se você trouxer um intervalo de endereços IPv4 para a AWS, poderá usar todos os endereços IP do intervalo, incluindo o primeiro endereço (o endereço de rede) e o último endereço (o endereço de broadcast).

Disponibilidade regional

No momento, o recurso BYOIP está disponível em todas as regiões da AWS comerciais, exceto nas regiões localizadas na China.

Disponibilidade da zona local

Uma Local Zone é uma extensão de uma região da AWS na proximidade geográfica dos usuários. As zonas locais são agrupadas em “grupos de borda de rede”. Na AWS, um grupo de borda de

rede é uma coleção de zonas de disponibilidade (AZs), zonas locais ou zonas de comprimento de onda das quais a AWS anuncia um endereço IP público. As zonas locais podem ter grupos de borda de rede diferentes das AZs em uma região da AWS para garantir a latência ou a distância física mínimas entre a rede da AWS e os clientes que acessam os recursos nessas zonas.

É possível provisionar intervalos de endereços BYOIPv4 e anunciá-los nos seguintes grupos de borda de rede da zona local usando a opção `--network-border-group`:

- af-south-1-los-1
- ap-northeast-1-tpe-1
- ap-south-1-ccu-1
- ap-south-1-del-1
- ap-southeast-1-bkk-1
- ap-southeast-1-mnl-1
- ap-southeast-2-akl-1
- ap-southeast-2-per-1
- eu-central-1-ham-1
- eu-central-1-waw-1
- eu-north-1-cph-1
- eu-north-1-hel-1
- me-south-1-mct-1
- us-east-1-atl-2
- us-east-1-bos-1
- us-east-1-bue-1
- us-east-1-chi-2
- us-east-1-dfw-2
- us-east-1-iah-2
- us-east-1-lim-1
- us-east-1-mci-1
- us-east-1-mia-2
- us-east-1-msp-1

- us-east-1-nyc-1
- us-east-1-nyc-2
- us-east-1-phl-1
- us-east-1-qro-1
- us-east-1-scl-1
- us-west-2-den-1
- us-west-2-hnl-1
- us-west-2-las-1
- us-west-2-lax-1
- us-west-2-pdx-1
- us-west-2-phx-2
- us-west-2-sea-1

Se você tiver zonas locais habilitadas (consulte Enable a Local Zone), é possível escolher um grupo de borda de rede para zonas locais ao provisionar e anunciar um CIDR BYOIPv4. Escolha o grupo de bordas de rede com cuidado, pois o EIP e o AWS recurso ao qual ele está associado devem residir no mesmo grupo de bordas de rede.

> **Note**
>
> No momento, não é possível provisionar ou anunciar intervalos de endereços BYOIPv6 em zonas locais.

Pré-requisitos para o BYOIP no Amazon EC2

O processo de integração do BYOIP tem duas fases, para as quais é necessário executar três etapas. Essas etapas estão descritas no diagrama a seguir. Incluímos etapas manuais nesta documentação, mas seu RIR pode oferecer serviços gerenciados para ajudar você nessas etapas.

> **Tip**
>
> As tarefas nesta seção exigem um terminal Linux e podem ser executadas usando o Linux, o AWS CloudShell ou o Subsistema Windows para Linux..

Conteúdo

- Visão geral
- Crie uma chave privada e gere um certificado X.509
- Carregue o certificado X.509 no registro RDAP no RIR
- Criar um objeto ROA no seu RIR

Visão geral

Fase de preparação

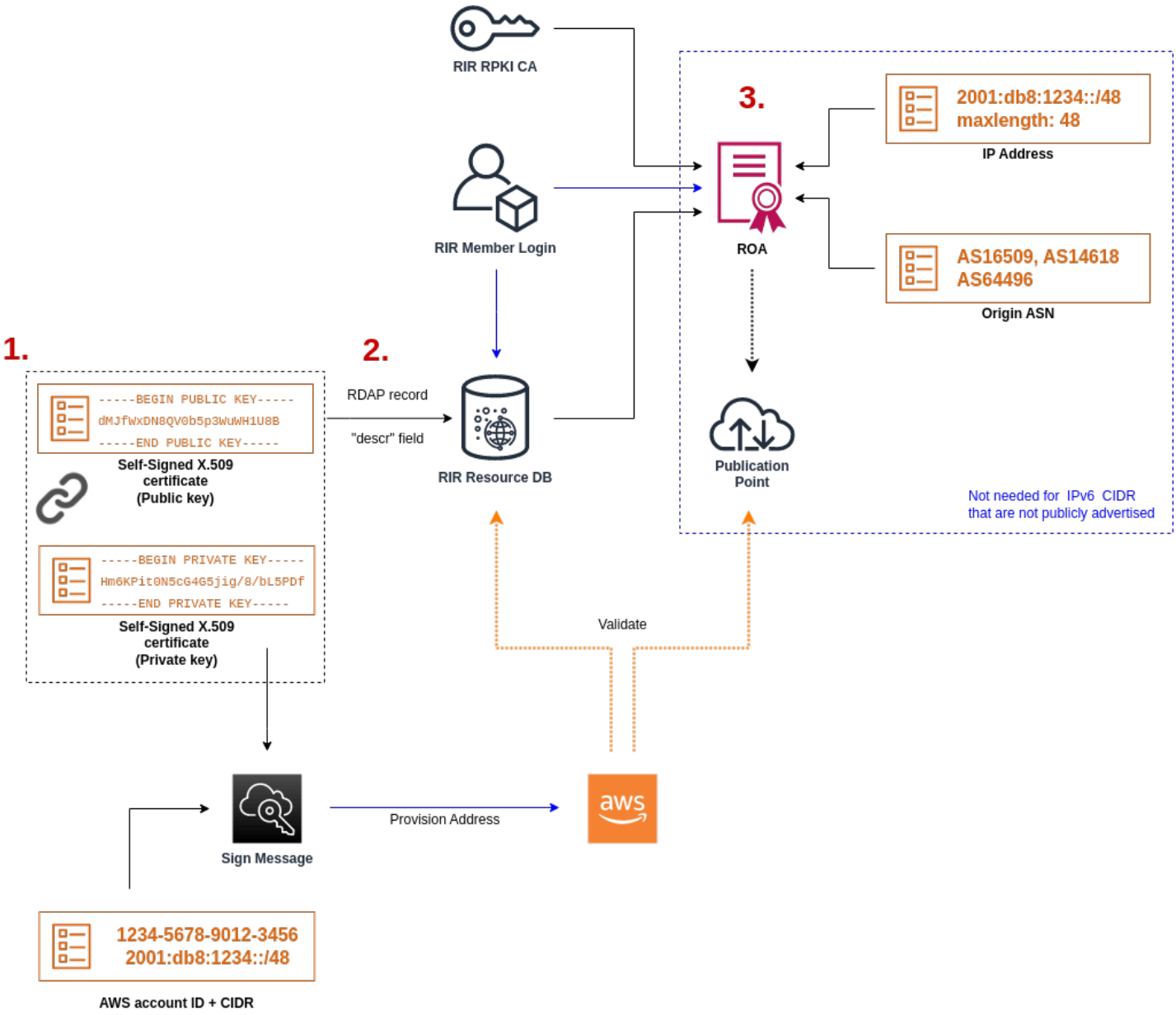
[1] Crie uma chave privada e use-a para gerar um certificado X.509 autoassinado para fins de autenticação. Esse certificado é usado somente durante a fase de provisionamento. É possívelrá remover o certificado do seu registro do RIR após a conclusão do provisionamento

Fase de configuração do RIR

[2] Carregue o certificado autoassinado nos comentários do registro do RDAP.

[3] Crie um objeto ROA no seu RIR. Uma ROA define o intervalo de endereços desejado, os Autonomous System Numbers (ASNs – Números de Sistema Autônomo) autorizados a anunciar o intervalo de endereços e uma data de validade para registro do RIR na Resource Public Key Infrastructure (RPKI – Infraestrutura de Chave Pública de Recursos).

> **Note**
>
> Não é necessário ter uma ROA para o espaço de endereços IPv6 não anunciáveis publicamente.



Para trazer vários intervalos de endereços, é necessário repetir esse processo com cada um deles. No entanto, as etapas de preparação e configuração do RIR não precisam ser repetidas, basta dividir um bloco contíguo em várias regiões da AWS diferentes.

Colocar em um intervalo de endereços não tem efeito em quaisquer intervalos de endereços que você trouxe anteriormente.

Crie uma chave privada e gere um certificado X.509

Siga o procedimento a seguir para criar um certificado autoassinado X.509 e adicione-o ao registro RDAP para seu RIR. Esse par de chaves é usado para autenticar o intervalo de endereços com o RIR. Os comandos openssl requerem o OpenSSL versão 1.0.2 ou posterior.

Copie os comandos a seguir e substitua apenas os valores de espaço reservado (em texto itálico colorido).

Esse procedimento segue a prática recomendada de criptografar sua chave RSA privada e exigir uma frase para acessá-la.

1. Gere uma chave privada RSA de 2048 bits, como mostrado a seguir.

```
$ openssl genpkey -aes256 -algorithm RSA -pkeyopt rsa_keygen_bits:2048 -out
 private-key.pem
```

O parâmetro `-aes256` especifica o algoritmo usado para criptografar a chave privada. O comando retorna a seguinte saída, incluindo prompts para definir uma frase de acesso:

```
......+++
.+++
Enter PEM pass phrase: xxxxxxx
Verifying - Enter PEM pass phrase: xxxxxxx
```

É possível fazer inspecionar a chave pública com o seguinte comando:

```
$ openssl pkey -in private-key.pem -text
```

Isso retorna um prompt de frase de acesso e o conteúdo da chave, que deve ser semelhante ao seguinte:

```
Enter pass phrase for private-key.pem: xxxxxxx
-----BEGIN PRIVATE KEY-----
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQDFBXHRI4HVKAhh
3seiciooizCRTbJe1+YsxNTja4XyKypVGIFWDGhZs44FCHlPOOSVJ+NqP74w96oM
7DPS3xo9kaQyZBFn2YEp2EBq5vf307KHNRmZZUmkn0zHOSEpNmY2fMxISBxewlxR
FAniwmSd/8TDvHJMY9FvAIvWuTsv5l0tJKk+a91K4+tO3UdDR7Sno5WXExfsBrW3
g1ydo3TBsx8i5/YiVOcNApy7ge2/FiwY3aCXJB6r6nuF6H8mRgI4r4vkMRsOlAhJ
DnZPNeweboo+K3Q3lwbgbmOKD/z9svk8N/+hUTBtIX0fRtbG+PLIw3xWRHGrMSn2
```

```
BzsPVuDLAgMBAAECggEACiJUj2hfJkKv47Dc3es3Zex67A5uDVjXmxfox2Xhdupn
fAcNqAptV6fXt0SPUNbhUxbBKNbshoJGufFwXPli1SXnpzvkdU4Hyco4zgbhXFsE
RNYjYfOGzTPwdBLpNMB6k3Tp4RHse6dNrlH0jDhpioL8cQEBdBJyVF5X0wymEbmV
mC0jgH/MxsBAPWW6ZKicg9ULMlWiAZ3MRAZPjHHgpYkAAsUWKAbCBwVQcVjGO59W
jfZjzTX5pQtVVH68ruciH88DTZCwjCkjBhxg+OIkJBLE5wkh82jIHSivZ63flwLw
z+E0+HhELSZJrn2MY6Jxmik3qNNUOF/Z+3msdj2luQKBgQDjwlC/3jxp8zJy6P8o
JQKv7TdvMwUj4VSWOHZBHLv4evJaaia0uQjIo1UDa8AYitqhX1NmCCehGH8yuXj/
v6V3CzMKDkmRr1NrONnSz5QsndQ04Z6ihAQlPmJ96g4wKtgoC7AYpyP0g1a+4/sj
b1+o3YQI4pD/F71c+qaztH7PRwKBgQDdc23yNmT3+Jyptf0fKjEvONK+xwUKzi9c
L/OzBq5yOIC1Pz2T85gOe1i8kwZws+xlpG6uBT6lmIJELd0k59FyupNu4dPvX5SD
6GGqdx4jk9KvI74usGeOBohmF0phTHkrWKBxXiyT0oS8zjnJlEn8ysIpGgO28jjr
LpaHNZ/MXQKBgQDfLNcnS0LzpsS2aK0tzyZU8SMyqVHOGMxj7quhneBq2T6FbiLD
T9TVlYaGNZ0j71vQaLI19qOubWymbautH0Op5KV8owdf4+bf1/NJaPIOzhDUSIjD
Qo01WW31Z9XDSRhKFTnWzmCjBdeIcajyzf10YKsycaAW9lItu8aBrMndnQKBgQDb
nNp/JyRwqjOrNljk7DHEs+SD39kHQzzCfqd+dnTPv2sc06+cpym3yulQcbokULpy
fmRo3bin/pvJQ3aZX/Bdh9woTXqhXDdrrSwWInVYMQPyPk8f/D9mIOJp5FUWMwHD
U+whIZSxsEeE+jtixlWtheKRYkQmzQZXbWdIhYyI3QKBgD+F/6wcZ85QW8nAUykA
3WrSIx/3cwDGdm4NRGct8ZOZjTHjiy9ojMOD1L7iMhRQ/3k3hUsin5LDMp/ryWGG
x4uIaLat40kiC7T4I66DM7P59euqdz3w0PD+VU+h7GSivvsFDdySUt7bNK0AUVLh
dMJfWxDN8QV0b5p3WuWH1U8B
-----END PRIVATE KEY-----
Private-Key: (2048 bit)
modulus:
    00:c5:05:71:d1:23:81:d5:28:08:61:de:c7:a2:72:
    2a:28:8b:30:91:4d:b2:5e:d7:e6:2c:c4:d4:e3:6b:
    85:f2:2b:2a:55:18:81:56:0c:68:59:b3:8e:05:08:
    79:4f:38:e4:95:27:e3:6a:3f:be:30:f7:aa:0c:ec:
    33:d2:df:1a:3d:91:a4:32:64:11:67:d9:81:29:d8:
    40:6a:e6:f7:f7:d3:b2:87:35:19:99:65:49:a4:9f:
    4c:c7:39:21:29:36:66:36:7c:cc:48:48:1c:5e:c2:
    5c:51:14:09:e2:c2:64:9d:ff:c4:c3:bc:72:4c:63:
    d1:6f:00:8b:d6:b9:3b:2f:e6:5d:2d:24:a9:3e:6b:
    dd:4a:e3:eb:4e:dd:47:43:47:b4:a7:a3:95:97:13:
    17:ec:06:b5:b7:83:5c:9d:a3:74:c1:b3:1f:22:e7:
    f6:22:54:e7:0d:02:9c:bb:81:ed:bf:16:2c:18:dd:
    a0:97:24:1e:ab:ea:7b:85:e8:7f:26:46:02:38:af:
    8b:e4:31:1b:0e:94:08:49:0e:76:4f:35:ec:1e:6e:
    8a:3e:2b:74:37:97:06:e0:6e:63:8a:0f:fc:fd:b2:
    f9:3c:37:ff:a1:51:30:6d:21:7d:1f:46:d6:c6:f8:
    f2:c8:c3:7c:56:44:71:ab:31:29:f6:07:3b:0f:56:
    e0:cb
publicExponent: 65537 (0x10001)
privateExponent:
    0a:22:54:8f:68:5f:26:42:af:e3:b0:dc:dd:eb:37:
```

```
    65:ec:7a:ec:0e:6e:0d:58:d7:9b:17:e8:c7:65:e1:
    76:ea:67:7c:07:0d:a8:0a:6d:57:a7:d7:b7:44:8f:
    50:d6:e1:53:16:c1:28:d6:ec:86:82:46:b9:f1:70:
    5c:f9:62:d5:25:e7:a7:3b:e4:75:4e:07:c9:ca:38:
    ce:06:e1:5c:5b:04:44:d6:23:61:f3:86:cd:33:f0:
    74:12:e9:34:c0:7a:93:74:e9:e1:11:ec:7b:a7:4d:
    ae:51:f4:8c:38:69:8a:82:fc:71:01:01:74:12:72:
    54:5e:57:d3:0c:a6:11:b9:95:98:2d:23:80:7f:cc:
    c6:c0:40:3d:65:ba:64:a8:9c:83:d5:0b:32:55:a2:
    01:9d:cc:44:06:4f:8c:71:e0:a5:89:00:02:c5:16:
    28:06:c2:07:05:50:71:58:c6:3b:9f:56:8d:f6:63:
    cd:35:f9:a5:0b:55:54:7e:bc:ae:e7:22:1f:cf:03:
    4d:90:b0:8c:29:23:06:1c:60:f8:e2:24:24:12:c4:
    e7:09:21:f3:68:c8:1d:28:af:67:ad:df:97:02:f0:
    cf:e1:34:f8:78:44:2d:26:49:ae:7d:8c:63:a2:71:
    9a:29:37:a8:d3:54:38:5f:d9:fb:79:ac:76:3d:a5:
    b9
prime1:
    00:e3:c2:50:bf:de:3c:69:f3:32:72:e8:ff:28:25:
    02:af:ed:37:6f:33:05:23:e1:54:96:38:76:41:1c:
    bb:f8:7a:f2:5a:6a:26:b4:b9:08:c8:a3:55:03:6b:
    c0:18:8a:da:a1:5f:53:66:08:27:a1:18:7f:32:b9:
    78:ff:bf:a5:77:0b:33:0a:0e:49:91:af:53:6b:38:
    d9:d2:cf:94:2c:9d:d4:34:e1:9e:a2:84:04:25:3e:
    62:7d:ea:0e:30:2a:d8:28:0b:b0:18:a7:23:f4:83:
    56:be:e3:fb:23:6f:5f:a8:dd:84:08:e2:90:ff:17:
    bd:5c:fa:a6:b3:b4:7e:cf:47
prime2:
    00:dd:73:6d:f2:36:64:f7:f8:9c:a9:b5:fd:1f:2a:
    31:2f:38:d2:be:c7:05:0a:ce:2f:5c:2f:f3:b3:06:
    ae:72:38:80:b5:3f:3d:93:f3:98:0e:7b:58:bc:93:
    06:70:b3:ec:65:a4:6e:ae:05:3e:a5:98:82:44:2d:
    dd:24:e7:d1:72:ba:93:6e:e1:d3:ef:5f:94:83:e8:
    61:aa:77:1e:23:93:d2:af:23:be:2e:b0:67:8e:06:
    88:66:17:4a:61:4c:79:2b:58:a0:71:5e:2c:93:d2:
    84:bc:ce:39:c9:94:49:fc:ca:c2:29:1a:03:b6:f2:
    38:eb:2e:96:87:35:9f:cc:5d
exponent1:
    00:df:2c:d7:27:4b:42:f3:a6:c4:b6:68:ad:2d:cf:
    26:54:f1:23:32:a9:51:ce:18:cc:63:ee:ab:a1:9d:
    e0:6a:d9:3e:85:6e:22:c3:4f:d4:d5:95:86:86:35:
    9d:23:ef:5b:d0:68:b2:35:f6:a3:ae:6d:6c:a6:6d:
    ab:ad:1f:43:a9:e4:a5:7c:a3:07:5f:e3:e6:df:d7:
    f3:49:68:f2:0e:ce:10:d4:48:88:c3:42:8d:35:59:
```

```
    6d:f5:67:d5:c3:49:18:4a:15:39:d6:ce:60:a3:05:
    d7:88:71:a8:f2:cd:fd:74:60:ab:32:71:a0:16:f6:
    52:2d:bb:c6:81:ac:c9:dd:9d
exponent2:
    00:db:9c:da:7f:27:24:70:aa:33:ab:36:58:e4:ec:
    31:c4:b3:e4:83:df:d9:07:43:3c:c2:7e:a7:7e:76:
    74:cf:bf:6b:1c:d3:af:9c:a7:29:b7:ca:e9:50:71:
    ba:24:50:ba:72:7e:64:68:dd:b8:a7:fe:9b:c9:43:
    76:99:5f:f0:5d:87:dc:28:4d:7a:a1:5c:37:6b:ad:
    2c:16:22:75:58:31:03:f2:3e:4f:1f:fc:3f:66:20:
    e2:69:e4:55:16:33:01:c3:53:ec:21:21:94:b1:b0:
    47:84:fa:3b:62:c6:55:ad:85:e2:91:62:44:26:cd:
    06:57:6d:67:48:85:8c:88:dd
coefficient:
    3f:85:ff:ac:1c:67:ce:50:5b:c9:c0:53:29:00:dd:
    6a:d2:23:1f:f7:73:00:c6:76:6e:0d:44:67:2d:f1:
    93:99:8d:31:e3:8b:2f:68:8c:c3:83:d4:be:e2:32:
    14:50:ff:79:37:85:4b:22:9f:92:c3:32:9f:eb:c9:
    61:86:c7:8b:88:68:b6:ad:e3:49:22:0b:b4:f8:23:
    ae:83:33:b3:f9:f5:eb:aa:77:3d:f0:d0:f0:fe:55:
    4f:a1:ec:64:a2:be:fb:05:0d:dc:92:52:de:db:34:
    ad:00:51:52:e1:74:c2:5f:5b:10:cd:f1:05:74:6f:
    9a:77:5a:e5:87:d5:4f:01
```

Mantenha sua chave privada em um local seguro quando ela não estiver em uso.

2. Gere um certificado X.509 usando a chave privada criada na etapa anterior. Neste exemplo, o certificado expira em 365 dias, após o qual ele não é mais confiável. Defina a expiração adequadamente. O certificado apenas deve ser válido durante o processo de provisionamento. É possívelrá remover o certificado do seu registro do RIR após a conclusão do provisionamento. O comando `tr -d "\n"` remove caracteres de nova linha (quebras de linha) da saída. Você precisa fornecer um nome comum quando solicitado, mas os outros campos podem ser deixados em branco.

```
$ openssl req -new -x509 -key private-key.pem -days 365 | tr -d "\n" >
 certificate.pem
```

Isso resulta em uma saída semelhante à seguinte:

```
Enter pass phrase for private-key.pem: xxxxxxx
You are about to be asked to enter information that will be incorporated
into your certificate request.
```

```
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) []:
State or Province Name (full name) []:
Locality Name (eg, city) []:
Organization Name (eg, company) []:
Organizational Unit Name (eg, section) []:
Common Name (eg, fully qualified host name) []:example.com
Email Address []:
```

> **Note**
>
> O nome comum não é necessário para provisionamento da AWS. Pode ser qualquer nome de domínio interno ou público.

É possível inspecionar o certificado usando o seguinte comando:

```
$ cat certificate.pem
```

A saída deve ser uma string longa, codificada em PEM, sem quebras de linha, prefaciada por `-----BEGIN CERTIFICATE-----` e seguida por `-----END CERTIFICATE-----`.

Carregue o certificado X.509 no registro RDAP no RIR

Adicione o certificado criado anteriormente ao registro RDAP do RIR. Certifique-se de incluir as strings `-----BEGIN CERTIFICATE-----` e `-----END CERTIFICATE-----` antes e depois da parte codificada. Todo esse conteúdo deve estar em uma única e longa linha. O procedimento para atualizar o RDAP depende do RIR:

- Para o ARIN, use o portal do Account Manager para adicionar o certificado na seção “Comentários públicos” para o objeto “Informações de rede” que representa seu intervalo de endereços. Não o adicione à seção de comentários da sua organização.
- Para o RIPE, adicione o certificado como um novo campo “descr” ao objeto “inetnum” ou “inet6num” que representa seu intervalo de endereços. Geralmente, eles podem ser encontrados

na seção “Meus recursos” do portal do banco de dados RIPE. Não o adicione à seção de comentários da sua organização ou ao campo “comentários” dos objetos acima.

- Para o APNIC, adicione o certificado editando as observações no registro “inetnum” ou “inet6num”.

É possível remover o certificado do seu registro do RIR após a conclusão da etapa de provisionamento abaixo.

Criar um objeto ROA no seu RIR

Crie um objeto ROA para autorizar os Amazon ASNs 16509 e 14618 a anunciar o intervalo de endereços, bem como os ASNs atualmente autorizados a anunciar o intervalo de endereços. Para as AWS GovCloud (US) Regions, autorize o ASN 8987 em vez do 16509 e 14618. É necessário definir o tamanho máximo para o CIDR que você está incluindo. O prefixo IPv4 mais específico que você pode incluir é /24. O intervalo de endereços IPv6 /48 é o intervalo mais específico que você trazer para CIDRs anunciáveis publicamente e /60 para CIDRs que não são anunciáveis publicamente.

> **Important**
>
> Se você estiver criando um objeto ROA para o IP Address Manager (IPAM) da Amazon VPC, ao criar as ROAs, para CIDRs IPv4, é necessário definir o comprimento máximo de um prefixo de endereço IP como `/24`. Para CIDRs IPv6, se você estiver adicionando-os a um grupo anunciável, o tamanho máximo de um prefixo de endereço IP deve ser `/48`. Isso garante que você tenha total flexibilidade para dividir seu endereço IP público nas regiões da AWS. O IPAM impõe o comprimento máximo que você definiu. Para obter mais informações sobre endereços BYOIP para IPAM, consulte Tutorial: CIDRs de endereço BYOIP para IPAM no Guia do usuário do IPAM da Amazon VPC.

Pode demorar até 24 horas para que a ROA se torne disponível para a Amazon. Para obter mais informações, consulte o seu RIR:

- ARIN — Solicitações de ROA
- RIPE — Gerenciamento de ROAs
- APNIC — Gerenciamento de rotas

Ao migrar anúncios de uma workload on-premises para a AWS, crie uma ROA para seu ASN existente antes de criar as ROAs para ASNs da Amazon. Caso contrário, talvez você perceba um impacto no roteamento e nos anúncios existentes.

> **Important**
>
> Para que a Amazon anuncie e continue anunciando seu intervalo de endereços IP, as ROAs com os ASNs da Amazon devem estar em conformidade com as diretrizes acima. Se seus ROAs forem inválidos ou não estiverem em conformidade com as diretrizes acima, a Amazon se reserva o direito de parar de anunciar seu intervalo de endereços IP.

> **Note**
>
> Essa etapa não é necessária para o espaço de endereços IPv6 não anunciável publicamente.

Integrar seu intervalo de endereços para uso no Amazon EC2

O processo de integração para BYOIP inclui as tarefas apresentadas a seguir, conforme suas necessidades.

Tarefas

- Provisionamento de um intervalo de endereços anunciado publicamente na AWS
- Como provisionar um intervalo de endereços IPv6 que não seja anunciável publicamente
- Anunciar o intervalo de endereços por meio da AWS
- Desprovisionar o intervalo de endereços
- Validar o BYOIP

Provisionamento de um intervalo de endereços anunciado publicamente na AWS

Ao provisionar um intervalo de endereços para uso com a AWS, você está confirmando que controla o intervalo de endereços e autoriza a Amazon a anunciá-lo. Também verificamos se você controla o intervalo por meio de uma mensagem de autorização assinada. Essa mensagem é assinada com o par de chaves X.509 autoassinadas que você usou ao atualizar o registro RDAP com o certificado X.509. A AWS requer uma mensagem de autorização assinada criptograficamente que é

apresentada ao RIR. O RIR autentica a assinatura em relação ao certificado que você adicionou ao RDAP e verifica os detalhes da autorização em relação ao ROA.

Para provisionar o intervalo de endereços

1. Compose message

   Componha a mensagem de autorização de texto simples. O formato da mensagem é o seguinte, em que a data é a data de expiração da mensagem:

   ```
   1|aws|account|cidr|YYYYMMDD|SHA256|RSAPSS
   ```

   Substitua o número da conta, o intervalo de endereços e a data de expiração por seus próprios valores para criar uma mensagem semelhante à seguinte:

   ```
   text_message="1|aws|0123456789AB|198.51.100.0/24|20211231|SHA256|RSAPSS"
   ```

   Não confundir com uma mensagem ROA, que tem uma aparência semelhante.

2. Assinar mensagens

   Assine a mensagem de texto sem formatação usando a chave privada criada anteriormente. A assinatura retornada pelo comando é uma string longa que você precisará copiar para uso na próxima etapa.

   > **Important**
   >
   > Recomendamos que você copie e cole esse comando. Com exceção do conteúdo da mensagem, não modifique nem substitua nenhum dos valores.

   ```
   signed_message=$( echo -n $text_message | openssl dgst -sha256 -sigopt
    rsa_padding_mode:pss -sigopt rsa_pss_saltlen:-1 -sign private-key.pem -keyform PEM
    | openssl base64 | tr -- '+=/' '-_~' | tr -d "\n")
   ```

3. Endereço de provisão

   Use o comando provisiona-byoip-cidr da AWS CLI para provisionar o intervalo de endereços. A opção `--cidr-authorization-context` usa as strings de mensagem e assinatura que você criou anteriormente.

> **Important**
>
> Você deve especificar a região da AWS em que o intervalo do BYOIP deve ser provisionado caso ele seja diferente da sua configuração da AWS CLI da `Default region name`.

```
aws ec2 provision-byoip-cidr --cidr address-range --cidr-authorization-context
 Message="$text_message",Signature="$signed_message" --region us-east-1
```

O provisionamento de um intervalo de endereços é uma operação assíncrona, de modo que a chamada retorna imediatamente, mas o intervalo de endereços não está pronto para uso até que seu status mude de `pending-provision` para `provisioned`.

4. Monitorar o andamento

   Embora a maior parte do provisionamento seja concluída em duas horas, a conclusão do processo de provisionamento pode levar até uma semana para intervalos que permitam anúncios públicos. Use o comando describe-byoip-cidrs para monitorar seu progresso, como neste exemplo:

   ```
   aws ec2 describe-byoip-cidrs --max-results 5 --region us-east-1
   ```

   Se houver problemas durante o provisionamento e o status for para `failed-provision`, o comando `provision-byoip-cidr` deverá ser executado novamente após os problemas terem sido resolvidos.

Como provisionar um intervalo de endereços IPv6 que não seja anunciável publicamente

Por padrão, um intervalo de endereços é provisionado para ser publicamente anunciável na Internet. É possível provisionar um intervalo de endereços IPv6 que não será anunciável publicamente. Para rotas que não permitem anúncios públicos, o processo de provisionamento geralmente é concluído em minutos. Quando você associa um bloco CIDR IPv6 de um intervalo de endereços não públicos a uma VPC, o CIDR IPv6 só pode ser acessado por opções de conectividade híbrida compatíveis com IPv6, como Direct Connect, AWS Site-to-Site VPN, ouGateways de trânsito da Amazon VPC.

Não é necessário ter um ROA para provisionar um intervalo de endereços não públicos.

> **Important**
>
> - Você só pode especificar se um intervalo de endereços é anunciável publicamente durante o provisionamento. Não é possível alterar o status de anúncio de um intervalo de endereços posteriormente.
> - A Amazon VPC não oferece suporte a CIDRs de endereço local exclusivo (ULA). Todas as VPCs devem ter CIDRs IPv6 exclusivos. Duas VPCs não podem ter o mesmo intervalo CIDR IPv6.

Para provisionar um intervalo de endereços IPv6 que não será anunciável publicamente, use o comando provision-byoip-cidr a seguir.

```
aws ec2 provision-byoip-cidr --cidr address-range --cidr-authorization-context
 Message="$text_message",Signature="$signed_message" --no-publicly-advertisable --
region us-east-1
```

Anunciar o intervalo de endereços por meio da AWS

Após ser provisionado, o intervalo de endereços estará pronto para ser anunciado. É necessário anunciar o intervalo de endereço exato que você provisionou. Não é possível anunciar apenas uma parte do intervalo de endereço provisionado.

Se você provisionou um intervalo de endereços IPv6 que não será anunciado publicamente, não será necessário concluir esta etapa.

Recomendamos que você interrompa o anúncio do intervalo de endereços, ou qualquer parte dele, em outros locais antes de anunciá-lo por meio da AWS. Se você continuar a anunciar o seu intervalo de endereços IP, ou qualquer parte dele, em outros locais, não poderemos oferecer suporte nem solucionar os problemas do intervalo de forma confiável. Especificamente, não podemos garantir que o tráfego para o intervalo de endereços, ou qualquer parte dele, entre em nossa rede.

Para minimizar o tempo de inatividade, é possível configurar os recursos da AWS para usar um endereço do grupo de endereços antes de ele ser anunciado e, em seguida, interromper simultaneamente o anúncio no local atual e iniciar o anúncio por meio da AWS. Para obter mais informações sobre a alocação de um endereço IP elástico em seu grupo de endereços, consulte Alocar um endereço IP elástico.

Limitações

- É possível 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.
- É possível executar o comando withdraw-byoip-cidr no máximo uma vez a cada 10 segundos, mesmo que você especifique diferentes intervalos de endereços de cada vez.

Para anunciar o intervalo de endereços, use o seguinte comando advertise-byoip-cidr.

```
aws ec2 advertise-byoip-cidr --cidr address-range --region us-east-1
```

Para interromper o anúncio do intervalo de endereços, use o seguinte comando withdraw-byoip-cidr.

```
aws ec2 withdraw-byoip-cidr --cidr address-range --region us-east-1
```

Desprovisionar o intervalo de endereços

Para interromper o uso do intervalo de endereços com a AWS, primeiro libere todos os endereços IP elásticos e desassocie todos os blocos CIDR IPv6 que ainda estiverem alocados do grupo de endereços. Depois, pare de anunciar o intervalo de endereços e, por fim, desprovisione o intervalo de endereços.

Não é possível desprovisionar uma parte do intervalo de endereços. Se você quiser usar um intervalo de endereços mais específico com a AWS, cancele o provisionamento de todo o intervalo de endereços e provisione um intervalo de endereços mais específico.

(IPv4) Para liberar cada endereço IP elástico, use o seguinte comando release-address.

```
aws ec2 release-address --allocation-id eipalloc-12345678abcabcabc --region us-east-1
```

(IPv6) Para desassociar um bloco CIDR IPv6, use o seguinte comando disassociate-vpc-cidr-block.

```
aws ec2 disassociate-vpc-cidr-block --association-id vpc-cidr-assoc-12345abcd1234abc1
 --region us-east-1
```

Para interromper o anúncio do intervalo de endereços, use o seguinte comando withdraw-byoip-cidr.

```
aws ec2 withdraw-byoip-cidr --cidr address-range --region us-east-1
```

Para desprovisionar o intervalo de endereços, use o seguinte comando deprovision-byoip-cidr.

```
aws ec2 deprovision-byoip-cidr --cidr address-range --region us-east-1
```

Pode levar até um dia para desprovisionar um intervalo de endereços.

Validar o BYOIP

1. Valide o par de chaves x.509 autoassinado

   Valide se o certificado foi carregado e é válido por meio do comando whois.

   Para ARIN, use `whois -h whois.arin.net r + 2001:0DB8:6172::/48` para procurar o registro RDAP do intervalo de endereços. Verifique a seção `Public Comments` para o `NetRange` (Intervalo de rede) na saída do comando. O certificado deve ser adicionado na seção `Public Comments` do intervalo de endereços.

   É possível inspecionar o `Public Comments` que contém o certificado usando o seguinte comando:

   ```
   whois -h whois.arin.net r + 2001:0DB8:6172::/48 | grep Comments | grep BEGIN
   ```

   Isso retorna a saída com o conteúdo da chave, que deve ser semelhante ao seguinte:

   ```
   Public Comments:
   -----BEGIN CERTIFICATE-----
   MIID1zCCAr+gAwIBAgIUBkRPNSLrPqbRAFP8RDAHSP+I1TowDQYJKoZIhvcNAQE
   LBQAwezELMAkGA1UEBhMCTloxETAPBgNVBAgMCEF1Y2tsYW5kMREwDwYDVQQHDA
   hBdWNrbGFuZDEcMBoGA1UECgwTQW1hem9uIFdlYiBTZXJ2aWNlczETMBEGA1UEC
   wwKQllPSVAgRGVtbzETMBEGA1UEAwwKQllPSVAgRGVtbzAeFw0yMTEyMDcyMDI0
   NTRaFw0yMjEyMDcyMDI0NTRaMHsxCzAJBgNVBAYTAk5aMREwDwYDVQQIDAhBdWN
   rbGFuZDERMA8GA1UEBwwIQXVja2xhbmQxHDAaBgNVBAoME0FtYXpvbiBXZWIgU2
   VydmljZXMxEzARBgNVBAsMCkJZT0lQIERlbW8xEzARBgNVBAMMCkJZT0lQIERlb
   W8wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCfmacvDp0wZ0ceiXXc
   R/q27mHI/U5HKt7SST4X2eAqufR9wXkfNanAEskgAseyFypwEEQr4CJijI/5hp9
   prh+jsWHWwkFRoBRR9FBtwcU/45XDXLga7D3stsI5QesHVRwOaXUdprAnndaTug
   mDPkD0vrl475JWDSIm+PUxGWLy+60aBqiaZq35wU/x+wXlAqBXg4MZK2KoUu27k
   Yt2zhmy0S7Ky+oRfRJ9QbAiSu/RwhQbh5Mkp1ZnVIc7NqnhdeIW48QaYjhMlUEf
   xdaqYUinzz8KpjfADZ4Hvqj9jWZ/eXo/9b2rGlHWkJsbhr0VEUyAGu1bwkgcdww
   3A7NjOxQbAgMBAAGjUzBRMB0GA1UdDgQWBBStFyujN6SYBr2glHpGt0XGF7GbGT
   AfBgNVHSMEGDAWgBStFyujN6SYBr2glHpGt0XGF7GbGTAPBgNVHRMBAf8EBTADA
   ```

```
QH/MA0GCSqGSIb3DQEBCwUAA4IBAQBX6nn6YLhz521lfyVfxY0t6o3410bQAeAF
08ud+ICtmQ4IO4A4B7zV3zIVYr0clrOOaFyLxngwMYN0XY5tVhDQqk4/gmDNEKS
Zy2QkX4Eg0YUWVzOyt6fPzjOvJLcsqc1hcF9wySL507XQz76Uk5cFypBOzbnk35
UkWrzA9KK97cXckfIESgK/k1N4ecwxwG6VQ8mBGqVpPpey+dXpzzzv1iBKN/VY4
ydjgH/LBfdTsVarmmy2vtWBxwrqkFvpdhSGCvRDl/qdO/GIDJi77dmZWkh/ic90
MNk1f38gs1jrCj8lThoar17Uo9y/Q5qJIsoNPyQrJRzqFU9F3FBjiPJF
-----END CERTIFICATE-----
```

Para RIPE, use `whois -r -h whois.ripe.net` *2001:0DB8:7269::/48* para procurar o registro RDAP do intervalo de endereços. Verifique a seção `descr` para o objeto `inetnum` (intervalo de rede) na saída do comando. O certificado deve ser adicionado como um novo campo `descr` para o intervalo de endereços.

É possível inspecionar o `descr` que contém o certificado usando o seguinte comando:

```
whois -r -h whois.ripe.net 2001:0DB8:7269::/48 | grep descr | grep BEGIN
```

Isso retorna a saída com o conteúdo da chave, que deve ser semelhante ao seguinte:

```
descr:
-----BEGIN CERTIFICATE-----MIID1zCCAr+gAwIBAgIUBkRPNSLrPqbRAFP8
RDAHSP+I1TowDQYJKoZIhvcNAQELBQAwezELMAkGA1UEBhMCTloxETAPBgNVBAg
MCEF1Y2tsYW5kMREwDwYDVQQHDAhBdWNrbGFuZDEcMBoGA1UECgwTQW1hem9uIF
dlYiBTZXJ2aWNlczETMBEGA1UECwwKQllPSVAgRGVtbzETMBEGA1UEAwwKQllPS
VAgRGVtbzAeFw0yMTEyMDcyMDI0NTRaFw0yMjEyMDcyMDI0NTRaMHsxCzAJBgNV
BAYTAk5aMREwDwYDVQQIDAhBdWNrbGFuZDERMA8GA1UEBwwIQXVja2xhbmQxHDA
aBgNVBAoME0FtYXpvbiBXZWIgU2VydmljZXMxEzARBgNVBAsMCkJZT0lQIERlbW
8xEzARBgNVBAMMCkJZT0lQIERlbW8wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwg
gEKAoIBAQCfmacvDp0wZ0ceiXXcR/q27mHI/U5HKt7SST4X2eAqufR9wXkfNanA
EskgAseyFypwEEQr4CJijI/5hp9prh+jsWHWwkFRoBRR9FBtwcU/45XDXLga7D3
stsI5QesHVRwOaXUdprAnndaTugmDPkD0vrl475JWDSIm+PUxGWLy+60aBqiaZq
35wU/x+wXlAqBXg4MZK2KoUu27kYt2zhmy0S7Ky+oRfRJ9QbAiSu/RwhQbh5Mkp
1ZnVIc7NqnhdeIW48QaYjhMlUEfxdaqYUinzz8KpjfADZ4Hvqj9jWZ/eXo/9b2r
GlHWkJsbhr0VEUyAGu1bwkgcdww3A7NjOxQbAgMBAAGjUzBRMB0GA1UdDgQWBBS
tFyujN6SYBr2glHpGt0XGF7GbGTAfBgNVHSMEGDAWgBStFyujN6SYBr2glHpGt0
XGF7GbGTAPBgNVHRMBAf8EBTADAQH/MA0GCSqGSIb3DQEBCwUAA4IBAQBX6nn6Y
Lhz521lfyVfxY0t6o3410bQAeAF08ud+ICtmQ4IO4A4B7zV3zIVYr0clrOOaFyL
xngwMYN0XY5tVhDQqk4/gmDNEKSZy2QkX4Eg0YUWVzOyt6fPzjOvJLcsqc1hcF9
wySL507XQz76Uk5cFypBOzbnk35UkWrzA9KK97cXckfIESgK/k1N4ecwxwG6VQ8
mBGqVpPpey+dXpzzzv1iBKN/VY4ydjgH/LBfdTsVarmmy2vtWBxwrqkFvpdhSGC
vRDl/qdO/GIDJi77dmZWkh/ic90MNk1f38gs1jrCj8lThoar17Uo9y/Q5qJIsoN
PyQrJRzqFU9F3FBjiPJF
```

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

Para AONIC, use `whois -h whois.apnic.net` *`2001:0DB8:6170::/48`* para procurar o registro RDAP do intervalo de endereços BYOIP. Verifique a seção `remarks` para o objeto `inetnum` (intervalo de rede) na saída do comando. O certificado deve ser adicionado como um novo campo `remarks` para o intervalo de endereços.

É possível inspecionar o `remarks` que contém o certificado usando o seguinte comando:

```
whois -h whois.apnic.net 2001:0DB8:6170::/48 | grep remarks | grep BEGIN
```

Isso retorna a saída com o conteúdo da chave, que deve ser semelhante ao seguinte:

```
remarks:
-----BEGIN CERTIFICATE-----
MIID1zCCAr+gAwIBAgIUBkRPNSLrPqbRAFP8RDAHSP+I1TowDQYJKoZIhvcNAQE
LBQAwezELMAkGA1UEBhMCTloxETAPBgNVBAgMCEF1Y2tsYW5kMREwDwYDVQQHDA
hBdWNrbGFuZDEcMBoGA1UECgwTQW1hem9uIFdlYiBTZXJ2aWNlczETMBEGA1UEC
wwKQllPSVAgRGVtbzETMBEGA1UEAwwKQllPSVAgRGVtbzAeFw0yMTEyMDcyMDI0
NTRaFw0yMjEyMDcyMDI0NTRaMHsxCzAJBgNVBAYTAk5aMREwDwYDVQQIDAhBdWN
rbGFuZDERMA8GA1UEBwwIQXVja2xhbmQxHDAaBgNVBAoME0FtYXpvbiBXZWIgU2
VydmljZXMxEzARBgNVBAsMCkJZT0lQIERlbW8xEzARBgNVBAMMCkJZT0lQIERlb
W8wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCfmacvDp0wZ0ceiXXc
R/q27mHI/U5HKt7SST4X2eAqufR9wXkfNanAEskgAseyFypwEEQr4CJijI/5hp9
prh+jsWHWwkFRoBRR9FBtwcU/45XDXLga7D3stsI5QesHVRwOaXUdprAnndaTug
mDPkD0vrl475JWDSIm+PUxGWLy+60aBqiaZq35wU/x+wXlAqBXg4MZK2KoUu27k
Yt2zhmy0S7Ky+oRfRJ9QbAiSu/RwhQbh5Mkp1ZnVIc7NqnhdeIW48QaYjhMlUEf
xdaqYUinzz8KpjfADZ4Hvqj9jWZ/eXo/9b2rGlHWkJsbhr0VEUyAGu1bwkgcdww
3A7NjOxQbAgMBAAGjUzBRMB0GA1UdDgQWBBStFyujN6SYBr2glHpGt0XGF7GbGT
AfBgNVHSMEGDAWgBStFyujN6SYBr2glHpGt0XGF7GbGTAPBgNVHRMBAf8EBTADA
QH/MA0GCSqGSIb3DQEBCwUAA4IBAQBX6nn6YLhz521lfyVfxY0t6o3410bQAeAF
08ud+ICtmQ4IO4A4B7zV3zIVYr0clrOOaFyLxngwMYN0XY5tVhDQqk4/gmDNEKS
Zy2QkX4Eg0YUWVzOyt6fPzjOvJLcsqc1hcF9wySL507XQz76Uk5cFypBOzbnk35
UkWrzA9KK97cXckfIESgK/k1N4ecwxwG6VQ8mBGqVpPpey+dXpzzzv1iBKN/VY4
ydjgH/LBfdTsVarmmy2vtWBxwrqkFvpdhSGCvRDl/qdO/GIDJi77dmZWkh/ic90
MNk1f38gs1jrCj8lThoar17Uo9y/Q5qJIsoNPyQrJRzqFU9F3FBjiPJF
-----END CERTIFICATE-----
```

2. Validar a criação de um objeto ROA

Valide a criação bem-sucedida de objetos ROA usando a API RIPEstat Data. Certifique-se de testar o intervalo de endereços em relação aos Amazon ASNs 16509 e 14618, além dos ASNs atualmente autorizados a anunciar o intervalo de endereços.

É possível inspecionar os objetos ROA de diferentes Amazon ASNs com seu intervalo de endereços usando o seguinte comando:

```
curl --location --request GET "https://stat.ripe.net/data/rpki-validation/data.json?
resource=ASN&prefix=CIDR
```

Neste exemplo de saída, a resposta tem resultado de `"status": "valid"` para o Amazon ASN 16509. Isso indica que o objeto ROA para o intervalo de endereços foi criado com êxito:

```
{
    "messages": [],
    "see_also": [],
    "version": "0.3",
    "data_call_name": "rpki-validation",
    "data_call_status": "supported",
    "cached": false,
    "data": {
        "validating_roas": [
            {
                "origin": "16509",
                "prefix": "2001:0DB8::/32",
                "max_length": 48,
                "validity": "valid"
            },
            {
                "origin": "14618",
                "prefix": "2001:0DB8::/32",
                "max_length": 48,
                "validity": "invalid_asn"
            },
            {
                "origin": "64496",
                "prefix": "2001:0DB8::/32",
                "max_length": 48,
                "validity": "invalid_asn"
            }
        ],
```

```
        "status": "valid",
        "validator": "routinator",
        "resource": "16509",
        "prefix": "2001:0DB8::/32"
    },
    "query_id": "20230224152430-81e6384e-21ba-4a86-852a-31850787105f",
    "process_time": 58,
    "server_id": "app116",
    "build_version": "live.2023.2.1.142",
    "status": "ok",
    "status_code": 200,
    "time": "2023-02-24T15:24:30.773654"
}
```

Um status de "`unknown`" indica que o objeto ROA para o intervalo de endereços não foi criado. Um status de "`invalid_asn`" indica que o objeto ROA para o intervalo de endereços não foi criado com êxito.

Usar seu intervalo de endereços BYOIP no Amazon EC2

É possível visualizar e trabalhar com os intervalos de endereços IPv4 e IPv6 que você provisionou na conta. Para obter mais informações, consulte the section called "Integrar seu intervalo de endereços".

Intervalos de endereços IPv4

É possível criar um endereço IP elástico no grupo de endereços IPv4 e usá-lo com os recursos da AWS como instâncias do EC2, gateways NAT e balanceadores de carga da rede.

Para visualizar informações sobre os grupos de endereços IPv4 que você provisionou na conta, use o seguinte comando describe-public-ipv4-pools.

```
aws ec2 describe-public-ipv4-pools --region us-east-1
```

Para criar um endereço IP elástico pelo grupo de endereços IPv4, use o comando allocate-address. É possível usar a opção `--public-ipv4-pool` para especificar o ID do grupo de endereços retornado por `describe-byoip-cidrs`. Ou usar a opção `--address` para especificar um endereço do intervalo de endereços que você provisionou.

Intervalos de endereços IPv6

Para visualizar informações sobre os grupos de endereços IPv6 que você provisionou na conta, use o seguinte comando describe-ipv6-pools.

```
aws ec2 describe-ipv6-pools --region us-east-1
```

Para criar uma VPC e especificar um CIDR IPv6 pelo grupo de endereços IPv6, use o seguinte comando create-vpc. Para permitir que a Amazon escolha o CIDR IPv6 do grupo de endereços IPv6, omita a opção `--ipv6-cidr-block`.

```
aws ec2 create-vpc --cidr-block 10.0.0.0/16 --ipv6-cidr-block ipv6-cidr --ipv6-
pool pool-id --region us-east-1
```

Para associar um bloco CIDR IPv6 do grupo de endereços IPv6 a uma VPC, use o seguinte comando associate-vpc-cidr-block. Para permitir que a Amazon escolha o CIDR IPv6 do grupo de endereços IPv6, omita a opção `--ipv6-cidr-block`.

```
aws ec2 associate-vpc-cidr-block --vpc-id vpc-123456789abc123ab --ipv6-cidr-block ipv6-
cidr --ipv6-pool pool-id --region us-east-1
```

Para visualizar as VPCs e as informações do grupo de endereços IPv6 associado, use o comando describe-vpcs. Para visualizar informações sobre blocos CIDR IPv6 associados de um grupo de endereços IPv6 específico, use o seguinte comando get-associated-ipv6-pool-cidrs.

```
aws ec2 get-associated-ipv6-pool-cidrs --pool-id pool-id --region us-east-1
```

Se você desassociar o bloco CIDR IPv6 da VPC, ele será liberado de volta para o grupo de endereços IPv6.

Endereços IP elásticos

Um Endereço IP elástico é um endereço IPv4 estático projetado para computação em nuvem dinâmica. Um endereço IP elástico é alocado para a conta da AWS e será seu até que você o libere. Com um endereço IP elástico, é possível mascarar a falha de uma instância ou software remapeando rapidamente o endereço para outra instância na conta. Como alternativa, é possível

especificar o endereço IP elástico em um registro DNS para o seu domínio, para que ele acione a sua instância. Para obter mais informações, consulte a documentação para o registro de domínio.

Um endereço IP elástico é um endereço IPv4 público, que é acessível pela Internet. Caso precise se conectar a uma instância que não tenha um endereço IPv4 público, você pode associar um endereço IP elástico a ela para permitir a comunicação com a internet.

Conteúdo

- Definição de preço de endereços IP elásticos
- Noções básicas sobre endereços IP elásticos
- Cota de endereços IP elásticos
- Para associar um endereço IP elástico a uma instância
- Transferir um endereço IP elástico entre Contas da AWS
- Liberar um endereço IP elástico
- Criar um registro de DNS reverso para e-mails no Amazon EC2

Definição de preço de endereços IP elásticos

Há uma cobrança por todos os endereços IP elásticos, independentemente de eles estarem em uso (alocados a um recurso, como uma instância do EC2) ou ociosos (criados em sua conta, mas não alocados).

A AWS cobra por todos os endereços IPv4 públicos, incluindo endereços IPv4 públicos associados a instâncias em execução e endereços IP elásticos. Para obter mais informações, consulte a guia Endereço IPv4 público na página de preços da Amazon VPC.

Noções básicas sobre endereços IP elásticos

As seguintes são as características básicas de um endereço IP elástico:

- Um endereço IP elástico é estático; ele não muda ao longo do tempo.
- Um endereço IP elástico é destinado ao uso somente em uma região específica e não pode ser movido para uma região diferente.
- Um endereço IP elástico é proveniente do grupo de endereços IPv4 da Amazon ou de um grupo de endereços IPv4 personalizados transferido para sua Conta da AWS. Não oferecemos suporte a endereços IP elásticos para IPv6.

- Para usar um endereço IP elástico, você primeiro aloca um para sua conta e o associa à instância ou a uma interface de rede.
- Quando você associa um endereço IP elástico a uma instância, ele também é associado à interface de rede principal da instância. Quando você associa um endereço IP elástico a uma interface de rede anexada a uma instância, ele também é associado à instância.
- Quando você associa um endereço IP elástico a uma instância ou à sua interface de rede primária, se a instância já tiver um endereço IPv4 público associado, esse endereço IPv4 público será liberado de volta ao grupo de endereços IPv4 públicos da Amazon, e o endereço IP elástico será associado à instância em vez disso. Não é possível reutilizar o endereço IPv4 público anteriormente associado à instância ou converter esse endereço IPv4 público em um endereço IP elástico. Para obter mais informações, consulte Endereços IPv4 públicos.
- É possível desassociar um endereço IP elástico de um recurso e reassociá-lo a outro recurso. Para evitar um comportamento inesperado, certifique-se de que todas as conexões ativas com o recurso nomeado na associação existente sejam fechadas antes de fazer a alteração. Depois de associar seu endereço IP elástico a um recurso diferente, será possível reabrir suas conexões com o recurso recém-associado.
- Um endereço IP elástico desassociado permanece alocado à sua conta até você liberá-lo explicitamente. Você recebe cobranças por todos os endereços IP elásticos em sua conta, independentemente de estarem associados ou desassociados a uma instância. Para obter mais informações, consulte a guia Endereço IPv4 público na página de preços da Amazon VPC.
- 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 na 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. Para obter mais informações, consulte Cota de endereços IP elásticos.
- Ao alocar os endereços IP elásticos, é possível associar os endereços IP elásticos a um grupo de borda de rede. Esse é o local a partir do qual anunciamos o bloco CIDR. Definir o grupo de borda de rede limita o bloco CIDR a esse grupo. Se você não especificar o grupo de borda de rede, definiremos o grupo de borda que contém todas as zonas de disponibilidade na região (por exemplo, `us-west-2`).
- Um endereço IP elástico deve ser usado somente um grupo de borda de rede específico.

Cota de endereços IP elásticos

Por padrão, todas as Contas da AWS têm uma cota de cinco (5) endereços IP elásticos por região, pois os endereços públicos da internet (IPv4) são um recurso público escasso. Recomendamos fortemente usar endereços IP elásticos, principalmente devido à sua capacidade de remapear o endereço para outra instância no caso de falha da instância, e usar nomes de host DNS para qualquer outra comunicação entre nós.

Se achar que a arquitetura justifica endereços IP elásticos adicionais, será possível solicitar um aumento de cota diretamente no console do Service Quotas. Para solicitar um aumento de cota, escolha Solicitar aumento no nível da conta. Para obter mais informações, consulte Service Quotas do Amazon EC2.

Para associar um endereço IP elástico a uma instância

Depois de alocar um endereço IP elástico, você pode associá-lo a um recurso da AWS, como uma instância do EC2, um gateway NAT ou um Network Load Balancer. Para associar um endereço IP elástico com outro recurso da AWS mais tarde, você pode desassociá-lo do seu recurso atual e depois associá-lo a um novo recurso.

Tarefas

- Alocar um endereço IP elástico
- Associar um endereço IP elástico
- Dissociar um endereço IP elástico

Alocar um endereço IP elástico

É possível alocar um endereço IP elástico para uso em uma região. Há uma cobrança por todos os endereços IP elásticos, independentemente de eles estarem em uso (associados a um recurso, como uma instância do EC2) ou ociosos (criados em sua conta, mas desassociados).

Console

Para alocar um endereço IP elástico

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Network & Security (Rede e segurança) e Elastic IPs (IPs elásticos).

3. Escolha Allocate Elastic IP address (Alocar endereço IP elástico).
4. (Opcional) Ao alocar um endereço IP elástico (EIP), você escolhe o Grupo de borda de rede no qual alocar o EIP. Um grupo de bordas de rede é uma coleção de zonas de disponibilidade (AZs), das AWS quais a anuncia um endereço IP público. As Zonas Locais (Local Zones) e Zonas Wavelength (Wavelength Zones) podem ter grupos de fronteira de rede diferentes das Zonas de Disponibilidade (AZs) em uma Região para garantir a latência mínima ou distância física entre a rede AWS e os clientes que acessam os recursos nessas Zonas.

   > **Important**
   >
   > Você deve alocar um EIP no mesmo grupo de fronteiras de rede do AWS recurso que será associado ao EIP. Um EIP (Endereço IP Elástico) em um grupo de fronteira de rede só pode ser anunciado em zonas dentro desse grupo de fronteira de rede e não em nenhuma outra zona representada por outros grupos de fronteira de rede.

   Se você tiver Zonas Locais ou Zonas de Comprimento de Wavelength ativadas (para obter mais informações, consulte Habilitar uma Zona Local ou Ativar zonas de comprimento de onda), você pode escolher um grupo de borda de rede para AZs, Zonas Locais ou Zonas de Comprimento de Onda. Escolha o grupo de bordas de rede com cuidado, pois o EIP e o AWS recurso ao qual ele está associado devem residir no mesmo grupo de bordas de rede. É possível usar o console do EC2 para visualizar o grupo de borda de rede em que estão as zonas de disponibilidade, as zonas locais ou as zonas de Wavelength. Normalmente, todas as zonas de disponibilidade em uma região pertencem ao mesmo grupo de fronteiras de rede, enquanto as zonas locais ou zonas de comprimento de onda pertencem a seus próprios grupos de fronteiras de rede separados.

   Se você não tiver zonas locais ou zonas de comprimento de onda habilitadas, ao alocar um EIP, o grupo de bordas de rede que representa todas as AZs da região (como `us-west-2`) será predefinido para você e não será possível alterá-lo. Isso significa que o EIP alocado para esse grupo de borda de rede será anunciado em todas as AZs da região em que você está.
5. Em Public IPv4 address pool (Grupo de endereços IPv4 público), escolha uma das seguintes opções:

- Amazon's pool of IPv4 addresses (Grupo de endereços IPv4 da Amazon) — Se você deseja que um endereço IPv4 seja alocado a partir do grupo de endereços IPv4 da Amazon.
- Endereço IPv4 público que você traz para sua conta da AWS: se deseja alocar um endereço IPv4 não contíguo (não sequencial) de um grupo de endereços IP que você trouxe para sua conta da AWS. Essa opção será desabilitada se você não tiver nenhum pool de endereços IP. Para obter mais informações sobre como levar seu próprio intervalo de endereços IP para sua conta da AWS, consulte Trazer seus próprios endereços IP (BYOIP) para o Amazon EC2.
- Customer owned pool of IPv4 addresses (Grupo de endereços IPv4 de propriedade do cliente): se você quiser alocar um endereço IPv4 de um grupo criado a partir de sua rede on-premises para uso com um AWS Outpost. Essa opção será desativada se você não tiver um Outpost da AWS.
- Aloque usando um grupo de IPv4 IPAM: se você quiser alocar endereços IP elásticos sequenciais de um bloco IPv4 público contíguo em um grupo de IPAM. A alocação de endereços IP elásticos sequenciais pode reduzir significativamente a sobrecarga de gerenciamento das listas de controle de acesso de segurança e simplificar a alocação e o rastreamento de endereços IP para empresas em expansão na AWS. Para obter mais informações, consulte Allocate sequential Elastic IP addresses from an IPAM pool no Guia do usuário do Amazon VPC IPAM.

6. (Opcional) Para adicionar uma tag, escolha Adicionar nova tag e insira uma chave e um valor de tag.

AWS CLI

Para alocar um endereço IP elástico

Use o comando da AWS CLI allocate-address.

No exemplo a seguir, o Amazon EC2 seleciona um endereço do conjunto de endereços da Amazon.

```
aws ec2 allocate-address
```

No exemplo a seguir, o Amazon EC2 seleciona um endereço do pool especificado que você trouxe para AWS usando o BYOIP.

```
aws ec2 allocate-address \
    --public-ipv4-pool ipv4pool-ec2-012345abcdef67890
```

O exemplo a seguir especifica um endereço do pool IPAM IPv4 especificado.

```
aws ec2 allocate-address \
    --ipam-pool-id ipam-pool-1234567890abcdef0 \
    --address 192.0.2.0
```

PowerShell

Para alocar um endereço IP elástico

Use o cmdlet New-EC2Address.

No exemplo a seguir, o Amazon EC2 seleciona um endereço do conjunto de endereços da Amazon.

```
New-EC2Address
```

No exemplo a seguir, o Amazon EC2 seleciona um endereço do pool especificado que você trouxe para AWS usando o BYOIP.

```
New-EC2Address \
    --PublicIpv4Pool ipv4pool-ec2-012345abcdef67890
```

O exemplo a seguir especifica um endereço do pool IPAM IPv4 especificado.

```
New-EC2Address \
    --IpamPoolId ipam-pool-1234567890abcdef0 \
    --Address 192.0.2.0
```

Associar um endereço IP elástico

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 Habilitar o acesso à internet usando gateways da internet no Guia do usuário da Amazon VPC.

Console

Para associar um endereço Elastic IP a uma instância

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha IPs elásticos.
3. Selecione o endereço IP elástico a ser associado e escolha Actions (Ações), Associate Elastic IP address (Associar endereço IP elástico).
4. Em Resource type (Tipo de recurso), escolha Instance (Instância).
5. Por exemplo, escolha a instância à qual associar o endereço IP elástico. Também é possível inserir texto para pesquisar uma instância específica.
6. (Opcional) Em Private IP address (Endereço IP privado), especifique um endereço IP privado ao qual associar o endereço IP elástico.
7. Escolha Associate.

Como associar um endereço IP elástico a uma interface de rede

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha IPs elásticos.
3. Selecione o endereço IP elástico a ser associado e escolha Actions (Ações), Associate Elastic IP address (Associar endereço IP elástico).
4. Em Resource type (Tipo de recurso), selecione Network interface (Interface de rede).
5. Em Network interface (Interface de rede), escolha a interface de rede à qual associar o endereço IP elástico. Também é possível inserir texto para pesquisar uma interface de rede específica.
6. (Opcional) Em Private IP address (Endereço IP privado), especifique um endereço IP privado ao qual associar o endereço IP elástico.
7. Escolha Associate.

AWS CLI

Como associar um endereço IP elástico

Use o comando da AWS CLI associate-address.

```
aws ec2 associate-address \
```

```
    --instance-id i-0b263919b6498b123 \
    --allocation-id eipalloc-64d5890a
```

PowerShell

Como associar um endereço IP elástico

Use o cmdlet Register-EC2Address.

```
Register-EC2Address `
    -InstanceId i-0b263919b6498b123 `
    -AllocationId eipalloc-64d5890a
```

Dissociar um endereço IP elástico

É possível desassociar um endereço IP elástico de uma instância ou interface de rede a qualquer momento. Depois de desassociar o endereço IP elástico, será possível associá-lo a outro recurso.

Console

Como desassociar e reassociar um endereço IP elástico

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha IPs elásticos.
3. Selecione o endereço IP elástico a ser desassociado e escolha Actions (Ações), Disassociate Elastic IP address (Desassociar endereço IP elástico).
4. Escolha Disassociate (Desassociar).

AWS CLI

Para dissociar um endereço IP elástico

Use o comando da AWS CLI disassociate-address.

```
aws ec2 disassociate-address --association-id eipassoc-12345678
```

PowerShell

Para dissociar um endereço IP elástico

Use o cmdlet do Unregister-EC2Address.

```
Unregister-EC2Address -AssociationId eipassoc-12345678
```

Transferir um endereço IP elástico entre Contas da AWS

É possível transferir um endereço IP elástico de uma Conta da AWS para outra. Isso pode ser útil nas seguintes situações:

- Recuperação de desastres: remapeie rapidamente endereços IP para workloads da internet voltadas ao público durante eventos de emergência.
- Reestruturação organizacional: mova rapidamente uma workload de uma Conta da AWS para outra. Uma transferência de endereços evita a necessidade de esperar que novos endereços IP elásticos sejam permitidos por seus grupos de segurança e ACLs de rede.
- Administração de segurança centralizada: use uma conta de segurança da AWS centralizada para rastrear e transferir endereços IP elásticos que tiver a conformidade de segurança verificada.

Preços

Não há cobrança pela transferência de endereços IP elásticos.

Tarefas

- Habilitar a transferência de endereços IP elásticos
- Aceitar um endereço IP elástico transferido
- Desabilitar a transferência de endereços IP elásticos

Habilitar a transferência de endereços IP elásticos

Esta seção descreve como aceitar um endereço IP elástico transferido. Observe as seguintes limitações relacionadas à habilitação de endereços IP elásticos para transferência:

- Os endereços IP elásticos podem ser transferidos de qualquer Conta da AWS (conta de origem) para qualquer outra Conta da AWS na mesma Região da AWS (conta de transferência). Não é possível transferir endereços IP elásticos para outra região.
- Ao transferir um endereço IP elástico, há um handshake de duas etapas entre as Contas da AWS. Quando a conta de origem inicia a transferência, as contas de transferência têm sete dias para

aceitar a transferência do endereço IP elástico. Durante esses sete dias, a conta de origem pode visualizar a transferência pendente (por exemplo, no console da AWS ou ao usar o comando describe-address-transfers). Após sete dias, a transferência expira e a propriedade do endereço IP elástico retorna à conta de origem.

- As transferências aceitas ficam visíveis para a conta de origem (por exemplo, no console da AWS ou usando o comando describe-address-transfers) por 14 dias após a aceitação das transferências.
- AWSA não notifica as contas de transferência sobre solicitações pendentes de transferência de endereços IP elásticos. O proprietário da conta de origem deve notificar o proprietário da conta de transferência sobre uma solicitação de transferência de endereços IP que este deve aceitar.
- Todas as tags associadas a um endereço IP elástico que está sendo transferido são redefinidas quando a transferência é concluída.
- Não é possível transferir endereços IP elásticos alocados de grupos de endereços IPv4 públicos que você traz para sua conta da Conta da AWS (comumente chamados de grupos de endereços traga seu próprio IP (BYOIP)).
- Você não pode transferir endereços IP elásticos alocados de um grupo de Gerenciador de endereços IP (IPAM) público contíguo do Amazon VPC IPv4. Em vez disso, o IPAM permite que você compartilhe grupos do IPAM entre contas da AWS integrando o IPAM com o AWS Organizations e usando o AWS RAM. Para obter mais informações, consulte Allocate sequential Elastic IP addresses from an IPAM pool no Guia do usuário do Amazon VPC IPAM.
- Caso tente transferir um endereço IP elástico que tenha um registro DNS reverso associado a ele, será possível iniciar o processo de transferência, mas a conta de transferência não poderá aceitar a transferência até que o registro DNS associado seja removido.
- Se tiver habilitado e configurado o AWS Outposts, talvez você tenha alocado endereços IP elásticos de um grupo de endereços IP pertencentes ao cliente (CoIPs). Não é possível transferir endereços IP elásticos alocados de um CoIP. No entanto, você pode usar o AWS RAM para compartilhar um CoIP com outra conta. Para obter mais informações, consulte Customer-owned IP addresses (Endereços IP pertencentes ao cliente) no Guia do usuário do AWS Outposts Outposts.
- É possível usar o Amazon VPC IPAM para rastrear a transferência de endereços IP elásticos para contas em uma organização da AWS Organizations. Para obter mais informações, consulte Visualizar histórico de endereços IP. Se um endereço IP elástico for transferido para uma Conta da AWS fora da organização, o histórico de auditoria IPAM do endereço IP elástico será perdido.

Essas etapas devem ser concluídas pela conta de origem.

Console

Para habilitar a transferência de endereços IP elásticos

1. Verifique se você está usando a conta da AWS de origem.
2. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
3. No painel de navegação, escolha IPs elásticos.
4. Selecione um ou mais endereços IP elásticos para habilitar para transferência e escolha Actions (Ações), Enable transfer (Habilitar transferência).
5. Se você estiver transferindo vários endereços IP elásticos, verá a opção Transfer type (Tipo de transferência). Escolha uma das seguintes opções:
   - Escolha Single account (Conta única) se estiver transferindo os endereços IP elásticos para uma única conta da AWS.
   - Escolha Multiple accounts (Várias contas) se estiver transferindo os endereços IP elásticos para várias contas da AWS.
6. Em Transfer account ID (ID da conta de transferência), insira os IDs das contas da AWS para as quais deseja transferir os endereços IP elásticos.
7. Confirme a transferência inserindo **`enable`** na caixa de texto.
8. Selecione Enviar.
9. Para aceitar a transferência, consulte Aceitar um endereço IP elástico transferido. Para desabilitar a transferência, consulte Desabilitar a transferência de endereços IP elásticos.

AWS CLI

Para habilitar a transferência de endereços IP elásticos

Use o comando enable-address-transfer.

```
aws ec2 enable-address-transfer \
    --allocation-id eipalloc-09ad461b0d03f6aaf \
    --transfer-account-id 123456789012
```

PowerShell

Para habilitar a transferência de endereços IP elásticos

Use o cmdlet Enable-EC2AddressTransfer.

```
Enable-EC2AddressTransfer `
    -AllocationId eipalloc-09ad461b0d03f6aaf `
    -TransferAccountId 123456789012
```

Aceitar um endereço IP elástico transferido

Esta seção descreve como aceitar um endereço IP elástico transferido.

Ao transferir um endereço IP elástico, há um handshake de duas etapas entre as Contas da AWS. Quando a conta de origem inicia a transferência, as contas de transferência têm sete dias para aceitar a transferência do endereço IP elástico. Durante esses sete dias, a conta de origem pode visualizar a transferência pendente (por exemplo, no console da AWS ou ao usar o comando describe-address-transfers). Após sete dias, a transferência expira e a propriedade do endereço IP elástico retorna à conta de origem.

Ao aceitar transferências, observe as seguintes exceções que podem ocorrer e como resolvê-las:

- AddressLimitExceeded: se sua conta de transferência tiver excedido a cota de endereços IP elásticos, a conta de origem poderá habilitar a transferência de endereços IP elásticos, mas essa exceção ocorrerá quando a conta de transferência tentar aceitar a transferência. Por padrão, todas as contas da AWS estão limitadas a 5 endereços IP elásticos por região. Consulte Cota de endereços IP elásticos para obter instruções sobre como aumentar o limite.
- InvalidTransfer.AddressCustomPtrSet: se você ou alguém da sua organização tiver configurado o endereço IP elástico que você está tentando transferir para usar pesquisa reversa de DNS, a conta de origem poderá habilitar a transferência para o endereço IP elástico, mas essa exceção ocorrerá quando a conta de transferência tentar aceitar a transferência. Para resolver esse problema, a conta de origem deverá remover o registro de DNS do endereço IP elástico. Para obter mais informações, consulte Criar um registro de DNS reverso para e-mails no Amazon EC2.
- InvalidTransfer.AddressAssociated: se houver um endereço IP elástico associado a uma instância do ENI ou EC2, a conta de origem poderá habilitar a transferência para o endereço IP elástico, mas essa exceção ocorrerá quando a conta de transferência tentar aceitar a transferência. Para resolver esse problema, a conta de origem deve desassociar o endereço IP elástico. Para obter mais informações, consulte Dissociar um endereço IP elástico.

Para quaisquer outras exceções, entre em contato com o Suporte.

Essas etapas devem ser concluídas pela conta de transferência.

Console

Para aceitar uma transferência de endereço IP elástico

1. Verifique se você está usando a conta de transferência.
2. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
3. No painel de navegação, escolha IPs elásticos.
4. Escolha Actions (Ações), Accept transfer (Aceitar transferência).
5. Quando a transferência for aceita, nenhuma tag associada ao endereço IP elástico que está sendo transferido será transferida com o endereço IP elástico. Se desejar definir uma etiqueta Name (Nome) para o endereço IP elástico que está aceitando, selecione Create a tag with a key of 'Name' and a value that you specify (Criar uma tag com uma chave “Nome” e um valor especificado por você).
6. Insira o endereço IP elástico que deseja transferir.
7. Se você estiver aceitando vários endereços IP elásticos transferidos, escolha Add address (Adicionar endereço) para inserir um endereço IP elástico adicional.
8. Selecione Enviar.

AWS CLI

Para aceitar uma transferência de endereço IP elástico

Use o comando accept-address-transfer.

```
aws ec2 accept-address-transfer --address 100.21.184.216
```

PowerShell

Para aceitar uma transferência de endereço IP elástico

Use o cmdlet Approve-EC2AddressTransfer.

```
Approve-EC2AddressTransfer -Address 100.21.184.216
```

Desabilitar a transferência de endereços IP elásticos

Esta seção descreve como desabilitar uma transferência de IP elásticos após a habilitação da transferência.

Estas etapas devem ser concluídas pela conta de origem que habilitou a transferência.

Console

Para desabilitar uma transferência de endereço IP elástico

1. Certifique-se de que esteja usando a Conta da AWS de origem.
2. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
3. No painel de navegação, escolha IPs elásticos.
4. Na lista de recursos de IPs elásticos, verifique se a propriedade que mostra o status de transferência da coluna está habilitada.
5. Selecione um ou mais endereços IP elásticos que tenham Transfer status (Status de transferência) Pending (Pendente) e escolha Actions (Ações), Disable transfer (Desabilitar transferência).
6. Confirme digitando **`disable`** na caixa de texto.
7. Selecione Enviar.

AWS CLI

Para desabilitar a transferência de endereços IP elásticos

Use o comando disable-address-transfer.

```
aws ec2 disable-address-transfer --allocation-id eipalloc-09ad461b0d03f6aaf
```

PowerShell

Para desabilitar a transferência de endereços IP elásticos

Use o cmdlet Disable-EC2AddressTransfer.

```
Disable-EC2AddressTransfer -AllocationId eipalloc-09ad461b0d03f6aaf
```

Liberar um endereço IP elástico

Se não for mais necessário um endereço IP elástico, recomendamos liberá-lo. O endereço IP elástico a ser liberado não deve estar associado atualmente a um recurso da AWS.

Console

Para liberar um endereço IP elástico

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Elastic IPs.
3. Selecione o endereço IP elástico a ser liberado e escolha Actions (Ações), Release Elastic IP addresses (Liberar endereços IP elásticos).
4. Escolha Release (Liberar).

AWS CLI

Para liberar um endereço IP elástico

Use o comando da AWS CLI release-address.

```
aws ec2 release-address --allocation-id eipalloc-64d5890a
```

PowerShell

Para liberar um endereço IP elástico

Use o cmdlet Remove-EC2Address.

```
Remove-EC2Address -AllocationId eipalloc-64d5890a
```

Depois de liberar o endereço IP elástico, você talvez possa recuperá-lo. As seguintes regras se aplicam:

- Você não poderá recuperar um endereço IP elástico caso ele tenha sido alocado para outra conta da AWS, ou caso você vá exceder seu limite de endereços IP elásticos.
- Você não pode recuperar tags associadas a um endereço IP elástico.

AWS CLI

Como recuperar um endereço IP elástico

Use o comando da allocate-address.

```
aws ec2 allocate-address \
    --domain vpc \
    --address 203.0.113.3
```

PowerShell

Como recuperar um endereço IP elástico

Use o cmdlet New-EC2Address.

```
New-EC2Address `
    -Address 203.0.113.3 `
    -Domain vpc `
    -Region us-east-1
```

Criar um registro de DNS reverso para e-mails no Amazon EC2

Se você pretende enviar e-mails a terceiros de uma instância do EC2, recomendamos que provisione um ou mais endereços IP elásticos e atribua registros de DNS reverso estático aos endereços IP elásticos que você usa para enviar e-mails. Isso pode ajudar a evitar que o seu e-mail seja sinalizado como spam por algumas organizações antispam. O AWS trabalha com ISPs e organizações antispam da Internet para reduzir a chance de que e-mails enviados desses endereços sejam sinalizados como spam.

Considerações

- Antes de criar um registro DNS reverso, é necessário definir um registro DNS de encaminhamento correspondente (registro do tipo A) que acione o seu endereço IP elástico.
- Se um registro DNS reverso estiver associado a um endereço IP elástico, o endereço IP elástico será bloqueado para sua conta e não poderá ser liberado de sua conta até que o registro seja removido.
- Caso tenha entrado em contato com o Suporte para configurar o DNS reverso para um endereço IP elástico, será possível remover o DNS reverso, mas não poderá liberar o endereço IP elástico

porque ele foi bloqueado pelo Suporte. Para desbloquear o endereço IP elástico, entre em contato com AWS Support. Depois que o endereço IP elástico for desbloqueado, será possível liberá-lo.

- [AWS GovCloud (US) Region] Você não pode criar um registro de DNS reverso. A AWS deve atribuir os registros de DNS reverso estático para você. Abra um caso de suporte para remover as limitações de DNS reverso e envio de e-mail. Você deve fornecer seus endereços IP elásticos e registros de DNS reverso.

Crie um registro de DNS reverso

É possível criar um registro de DNS reverso para o endereço IP elástico, conforme a seguir.

Console

Para criar um registro de DNS reverso

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha IPs elásticos.
3. Selecione o endereço IP elástico e escolha Actions (Ações) e Update reverse DNS (Atualizar DNS reverso).
4. Em Nome do domínio de DNS reverso, digite o nome do domínio.
5. Digite **`update`** para confirmar.
6. Escolha Update.

AWS CLI

Para criar um registro de DNS reverso

Use o comando modify-address-attribute.

```
aws ec2 modify-address-attribute \
    --allocation-id eipalloc-abcdef01234567890 \
    --domain-name example.com
```

O seguinte é um exemplo de saída.

```
{
    "Addresses": [
        {
```

```
            "PublicIp": "192.0.2.0",
            "AllocationId": "eipalloc-abcdef01234567890",
            "PtrRecord": "example.net.",
            "PtrRecordUpdate": {
                "Value": "example.com.",
                "Status": "PENDING"
            }
        }
    ]
}
```

PowerShell

Para criar um registro de DNS reverso

Use o cmdlet Edit-EC2AddressAttribute.

```
Edit-EC2AddressAttribute `
    -AllocationId 'eipalloc-abcdef01234567890' `
    -DomainName 'example.com' |
Format-List `
    AllocationId, PtrRecord, PublicIp,
    @{Name='PtrRecordUpdate';Expression={$_.PtrRecordUpdate | Format-List | Out-
String}}
```

O seguinte é um exemplo de saída.

```
AllocationId    : eipalloc-abcdef01234567890
PtrRecord       : example.net.
PublicIp        : 192.0.2.0
PtrRecordUpdate :
                  Reason :
                  Status : PENDING
                  Value  : example.com.
```

Remover um registro de DNS reverso

É possível remover um registro de DNS reverso do seu endereço IP elástico, conforme a seguir.

Caso receba o erro a seguir, será possível enviar uma Solicitação para remover restrições ao envio de e-mail ao Suporte para obter assistência.

```
The address cannot be released because it is locked to your account.
```

Console

Para remover um registro de DNS reverso

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha IPs elásticos.
3. Selecione o endereço IP elástico e escolha Actions (Ações) e Update reverse DNS (Atualizar DNS reverso).
4. Em Nome do domínio de DNS reverso, limpe o nome do domínio.
5. Digite **`update`** para confirmar.
6. Escolha Update.

AWS CLI

Para remover um registro de DNS reverso

Use o comando reset-address-attribute.

```
aws ec2 reset-address-attribute \
    --allocation-id eipalloc-abcdef01234567890 \
    --attribute domain-name
```

O seguinte é um exemplo de saída.

```
{
    "Addresses": [
        {
            "PublicIp": "192.0.2.0",
            "AllocationId": "eipalloc-abcdef01234567890",
            "PtrRecord": "example.com.",
            "PtrRecordUpdate": {
                "Value": "example.net.",
                "Status": "PENDING"
            }
        }
    ]
```

```
}
```

PowerShell

Para remover um registro de DNS reverso

Use o cmdlet Reset-EC2AddressAttribute.

```
Reset-EC2AddressAttribute `
    -AllocationId 'eipalloc-abcdef01234567890' `
    -Attribute domain-name |
Format-List `
    AllocationId, PtrRecord, PublicIp,
    @{Name='PtrRecordUpdate';Expression={$_.PtrRecordUpdate | Format-List | Out-
String}}
```

O seguinte é um exemplo de saída.

```
AllocationId    : eipalloc-abcdef01234567890
PtrRecord       : example.com.
PublicIp        : 192.0.2.0
PtrRecordUpdate :
                  Reason :
                  Status : PENDING
                  Value  : example.net.
```

Interfaces de rede elástica

Uma interface de rede elástica é um componente lógico de redes em uma VPC que representa uma cartão de rede virtual. É possível criar e configurar interfaces de rede e anexá-las a instâncias que você executa na mesma zona de disponibilidade. 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 da instância original para a nova instância.

Observe que esse recurso da AWS é chamado de interface de rede no Console de gerenciamento da AWS e na API do Amazon EC2. Portanto, usamos "interface de rede" nesta documentação em vez de "interface de rede elástica". O termo "interface de rede" nesta documentação significa sempre "interface de rede elástica".

Atributos da interface de rede

Uma interface de rede pode incluir os seguintes atributos:

- Um endereço IPv4 privado primário do intervalo de endereços IPv4 da sua rede
- Um endereço IPv6 primário do intervalo de endereços IPv6 da sua rede
- Endereços IPv4 privados secundários do intervalo de endereços IPv4 da sua sub-rede
- Um endereço IP elástico (IPv4) por cada endereço IPv4 privado
- Um endereço IPv4 público
- Endereços IPv6 secundários
- Grupos de segurança
- Um endereço MAC
- Um indicador de verificação de origem/destino
- Uma descrição

Monitoramento do tráfego

É possível habilitar um log de fluxo da VPC na sua interface de rede para capturar informações sobre o tráfego que vai de e para a 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.

Conteúdo

- Conceitos da interface de rede
- Placas de rede
- Máximo de endereços IP por interface de rede
- Criar uma interface de rede para sua instância do EC2
- Anexos de interface de rede para sua instância do EC2
- Gerenciar os endereços IP para a interface de rede
- Modificar atributos da interface de rede
- Várias interfaces de rede para as instâncias do Amazon EC2
- Interfaces de rede gerenciadas pelo solicitante
- Delegação de prefixo para interfaces de rede do Amazon EC2
- Excluir uma interface de rede

Conceitos da interface de rede

Veja a seguir conceitos importantes que você deve compreender ao começar a usar interfaces de rede.

Interface de rede primária

Cada instância tem uma interface de rede padrão, chamada interface de rede primária. Você não pode desanexar uma interface de rede primária de uma instância.

Interfaces de rede secundárias

É possível criar e anexar interfaces de rede secundárias à sua instância. O número máximo de interfaces de rede varia por tipo de instância. Para obter mais informações, consulte Máximo de endereços IP por interface de rede.

Endereços IPv4 públicos para interfaces de rede

Quando você executa uma instância do EC2 em uma sub-rede somente IPv4 ou de pilha dupla, a instância recebe um endereço IP privado primário do intervalo de endereços IPv4 da sub-rede. Também é possível 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.

Endereços IPv4 públicos para interfaces de rede

Todas as sub-redes têm um atributo modificável que determina se será atribuído um endereço IPv4 público às interfaces de rede criadas na sub-rede (e, portanto, instâncias executadas nessa sub-rede). Para obter mais informações, consulte Configurações de sub-redes no Guia do usuário da Amazon VPC. Quando você executa uma instância, o endereço IP é atribuído à interface de rede primária. Caso especifique uma interface de rede existente como a interface de rede primária ao executar uma instância, o endereço IPv4 público será determinado por essa interface de rede.

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.

Liberamos o endereço IP público quando a instância é interrompida, hibernada ou encerrada. Atribuímos um novo endereço IP público quando você inicia sua instância interrompida ou hibernada, a não ser que ela tenha uma interface de rede secundária ou um endereço IPv4 privado secundário associado a um endereço IP elástico.

Endereços IPv6 públicos para interfaces de rede

Caso associe blocos CIDR IPv6 à VPC e sub-rede, será possível atribuir endereços IPv6 do intervalo de sub-redes a uma interface de rede. Cada endereço IPv6 pode ser atribuído a uma interface de rede.

Todas as sub-redes têm um atributo modificável que determina se às interfaces de rede criadas naquela sub-rede (e, portanto, em instâncias executadas nessa sub-rede) é atribuído automaticamente um endereço de público IPv6 do intervalo da sub-rede. Quando você executa uma instância, o endereço IPv6 é atribuído à interface de rede primária.

Endereços IP elásticos para interfaces de rede

É possível associar um endereço IP elástico com endereços IPv4 privados para a interface de rede. É possível associar um endereço IP elástico a cada endereço IPv4 privado. Caso desassocie um endereço IP elástico de uma interface de rede, será possível liberá-lo ou associá-lo a outra instância.

Comportamento de encerramento

É possível definir o comportamento de encerramento para uma interface de rede que está anexada a uma instância. É possível especificar se a interface de rede deve ser excluída automaticamente quando você encerrar a instância à qual está anexada.

Verificação de origem/destino

É possível ativar ou desativar as verificações de origem/destino, que garantem que a instância seja a origem ou o destino de qualquer tráfego recebido. A verificação da origem/destino está ativada por padrão. É necessário desabilitar as verificações de origem/destino se a instância executa serviços como tradução de endereço de rede, roteamento ou firewalls.

Interfaces de rede gerenciadas pelo solicitante

Essas interfaces de rede são criadas e gerenciadas pelos Serviços da AWS para que você possa usar alguns recursos e serviços. Você não pode gerenciar por si mesmo essas interfaces de rede. Para obter mais informações, consulte Interfaces de rede gerenciadas pelo solicitante.

Delegação de prefixo

Um prefixo é um intervalo de CIDR IPv4 ou IPv6 privado reservado que você aloca para atribuição automática ou manual para interfaces de rede associadas a uma instância. Usando prefixos delegados, é possível iniciar serviços mais rapidamente atribuindo um intervalo de endereços IP como um único prefixo.

Interfaces de rede gerenciadas

Uma interface de rede gerenciada é gerenciada por um provedor de serviços, como o Modo Automático do Amazon EKS. Você não pode modificar diretamente as configurações de uma interface de rede gerenciada. Interfaces de rede gerenciadas são identificadas por um valor true no campo Gerenciada. Para obter mais informações, consulte Instâncias gerenciadas do Amazon EC2.

Placas de rede

A maioria dos tipos de instância é compatível com uma placa de rede. As instâncias compatíveis com várias placas de rede oferecem maior performance de rede, incluindo recursos de largura de banda acima de 100 Gbps e maior performance da taxa de pacotes. Quando você anexa uma interface de rede a uma instância compatível com várias placas de rede, você pode selecionar a placa de rede para a interface de rede. A interface de rede primária deve ser atribuída ao índice 0 da placa de rede.

As interfaces de rede EFA e exclusivamente EFA contam como uma interface de rede. Pode-se atribuir apenas uma interface de rede EFA ou exclusivamente EFA por placa de rede. A interface de rede primária não pode ser uma interface de rede exclusivamente EFA.

Os tipos de instância a seguir são compatíveis com várias placas de rede. Para obter informações sobre o número de interfaces de rede compatíveis com um tipo de instância, consulte Máximo de endereços IP por interface de rede.

Tipo de instância	Quantidade de placas de rede
c6in.32xlarge	2
c6in.metal	2
c8gb.48xlarge	2
c8gb.metal-48xl	2
c8gn.48xlarge	2
c8gn.metal-48xl	2
dl1.24xlarge	4

Tipo de instância	Quantidade de placas de rede
g6e.24xlarge	2
g6e.48xlarge	4
g7e.24xlarge	2
g7e.48xlarge	4
hpc6id.32xlarge	2
hpc7a.12xlarge	2
hpc7a.24xlarge	2
hpc7a.48xlarge	2
hpc7a.96xlarge	2
hpc8a.96xlarge	2
m6idn.32xlarge	2
m6idn.metal	2
m6in.32xlarge	2
m6in.metal	2
m8gb.48xlarge	2
m8gn.48xlarge	2
p4d.24xlarge	4
p4de.24xlarge	4
p5.48xlarge	32
p5e.48xlarge	32

Tipo de instância	Quantidade de placas de rede
p5en.48xlarge	16
p6-b200.48xlarge	8
p6-b300.48xlarge	17
p6e-gb200.36xlarge	17
r8gb.48xlarge	2
r8gb.metal-48xl	2
r8gn.48xlarge	2
r8gn.metal-48xl	2
r6idn.32xlarge	2
r6idn.metal	2
r6in.32xlarge	2
r6in.metal	2
trn1.32xlarge	8
trn1n.32xlarge	16
trn2.48xlarge	16
trn2u.48xlarge	16
u7in-16tb.224xlarge	2
u7in-24tb.224xlarge	2
u7in-32tb.224xlarge	2
u7inh-32tb.480xlarge	2

Máximo de endereços IP por interface de rede

Cada tipo de instância oferece suporte a um número máximo de interfaces de rede, um número máximo de endereços IPv4 privados por interface de rede e um número máximo de endereços IPv6 por interface de rede. O limite de endereços IPv6 é separado do limite para endereços IPv4 privados por interface de rede. Observe que todos os tipos de instância oferecem suporte a endereçamento IPv6, exceto as a seguir: C1, M1, M2, M3 e T1.

Interfaces de rede disponíveis

O Guia de tipos de instância do Amazon EC2 fornece informações sobre as interfaces de rede disponíveis para cada tipo de instância. Para saber mais, consulte:

- Network specifications: General purpose
- Network specifications: Compute optimized
- Network specifications: Memory optimized
- Network specifications: Storage optimized
- Network specifications: Accelerated computing
- Network specifications: High-performance computing
- Network specifications: Previous generation

Console

Para recuperar o máximo de interfaces de rede

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Instance Types (Tipos de instância).
3. Adicione um filtro para especificar o tipo de instância (Instance type=c5.12xlarge) ou família de instâncias (Instance family=c5).
4. (Opcional) Clique no ícone Preferências e ative Número máximo de interfaces de rede. Essa coluna indica o número máximo de interfaces de rede para cada tipo de instância.
5. (Opcional) Selecione o tipo de instância. Na guia Rede, encontre Número máximo de interfaces de rede.

AWS CLI

Para recuperar o máximo de interfaces de rede

É possível usar o comando describe-instance-types para exibir informações sobre um tipo de instância, como as interfaces de rede com suporte e os endereços IP por interface. O exemplo a seguir exibe essas informações para todas as instâncias C5.

```
aws ec2 describe-instance-types \
    --filters "Name=instance-type,Values=c5.*" \
    --query "InstanceTypes[].{ \
        Type: InstanceType, \
        MaxENI: NetworkInfo.MaximumNetworkInterfaces, \
        IPv4addr: NetworkInfo.Ipv4AddressesPerInterface}" \
    --output table
```

O seguinte é um exemplo de saída.

```
-------------------------------------
|        DescribeInstanceTypes      |
+----------+----------+--------------+
| IPv4addr | MaxENI   |     Type     |
+----------+----------+--------------+
|  30      |  8       |  c5.4xlarge  |
|  50      |  15      |  c5.24xlarge |
|  15      |  4       |  c5.xlarge   |
|  30      |  8       |  c5.12xlarge |
|  10      |  3       |  c5.large    |
|  15      |  4       |  c5.2xlarge  |
|  50      |  15      |  c5.metal    |
|  30      |  8       |  c5.9xlarge  |
|  50      |  15      |  c5.18xlarge |
+----------+----------+--------------+
```

PowerShell

Para recuperar o máximo de interfaces de rede

É possível usar o comando Get-EC2InstanceType do PowerShell para exibir informações sobre um tipo de instância, como as interfaces de rede compatíveis e os endereços IP por interface. O exemplo a seguir exibe essas informações para todas as instâncias C5.

```
Get-EC2InstanceType -Filter @{Name="instance-type"; Values="c5.*"} | `
```

```
Select-Object `
    @{Name='Ipv4AddressesPerInterface';
 Expression={($_.Networkinfo.Ipv4AddressesPerInterface)}},
    @{Name='MaximumNetworkInterfaces';
 Expression={($_.Networkinfo.MaximumNetworkInterfaces)}},
    InstanceType | `
Format-Table -AutoSize
```

O seguinte é um exemplo de saída.

```
Ipv4AddressesPerInterface MaximumNetworkInterfaces InstanceType
------------------------- ------------------------ ------------
                       30                        8 c5.4xlarge
                       15                        4 c5.xlarge
                       30                        8 c5.12xlarge
                       50                       15 c5.24xlarge
                       30                        8 c5.9xlarge
                       50                       15 c5.metal
                       15                        4 c5.2xlarge
                       10                        3 c5.large
                       50                       15 c5.18xlarge
```

Criar uma interface de rede para sua instância do EC2

É possível criar uma interface de rede para uso de suas instâncias do EC2. Ao criar uma interface de rede, você especifica a sub-rede para a qual ela foi criada. Você não pode mover a interface de rede para outra sub-rede depois que ela é criada. É necessário associar uma interface de rede a uma instância na mesma zona de disponibilidade. É possível desanexar uma interface de rede secundária de uma instância e anexá-la a outra instância na mesma zona de disponibilidade. Você não pode desanexar uma interface de rede primária de uma instância. Para obter mais informações, consulte the section called “Anexos de interface de rede”.

Console

Para criar 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. Clique em Create network interface (Criar interface de rede).

4. (Opcional) Em Description (Descrição), insira um nome descritivo.
5. Em Subnet (Sub-rede), selecione uma sub-rede. As opções disponíveis nas etapas subsequentes mudam dependendo do tipo de sub-rede selecionada [somente IPv4, somente IPv6 ou pilha dupla (IPv4 e IPv6)].
6. Em Tipo de interface, escolha uma das seguintes opções:

   - ENA: uma interface de rede de alta performance projetada para lidar com throughput elevado e altas taxas de pacotes por segundo para protocolos TCP/IP ao mesmo tempo que minimiza o uso da CPU. Este é o valor padrão. Para obter mais informações sobre ENA, consulte Elastic Fabric Adapter.
   - EFA com ENA: uma interface de rede que oferece suporte a dispositivos ENA e EFA para transporte tradicional baseado em TCP/IP junto com transporte baseado em SRD. Se você escolher EFA com ENA, a instância à qual ela está sendo associada deverá oferecer suporte a EFA. Para obter mais informações sobre EFA, consulte Elastic Fabric Adapter.
   - Somente EFA: uma interface de rede de alta performance projetada para lidar com comunicação entre nós com throughput elevado e baixa latência para transporte baseado em SRD enquanto ignora a pilha do sistema operacional. Se você escolher essa opção, a instância à qual ela está sendo associada deverá oferecer suporte a EFA. As interfaces de rede somente EFA não oferecem suporte a endereços IP. Para obter mais informações sobre EFA, consulte Elastic Fabric Adapter.

7. Em Private IPv4 address (Endereço IPv4 privado), siga um dos seguintes procedimentos:

   - Clique em Auto-assign (Atribuição automática) para permitir que Amazon EC2 selecione um endereço IPv4 na sub-rede.
   - Clique em Custom (Personalizado) e insira um endereço IPv4 selecionado na sub-rede.

8. (Somente sub-redes com endereços IPv6) Para IPv6 address (Endereço IPv6), execute um dos seguintes procedimentos:

   - Clique em None (Nenhum) se você não quiser atribuir um endereço IPv6 à interface de rede.
   - Clique em Auto-assign (Atribuição automática) para permitir que Amazon EC2 selecione um endereço IPv6 na sub-rede.
   - Clique em Custom (Personalizado) e insira um endereço IPv6 selecionado na sub-rede.

9. (Opcional) Se estiver criando uma interface de rede em uma sub-rede de pilha dupla ou somente IPv6, você terá a opção de Atribuir IP IPv6 primário. Isso atribui um endereço unicast global (GUA) IPv6 primário à interface de rede. A atribuição de um endereço IPv6

primário permite evitar a interrupção do tráfego para instâncias ou ENIs. Escolha Habilitar se a instância à qual essa ENI será anexada depender do seu endereço IPv6 permanecer inalterado. A AWS atribuirá automaticamente um endereço IPv6 associado à ENI anexada à sua instância como o endereço IPv6 primário. Após habilitar um endereço GUA IPv6 para ser um IPv6 primário, não será possível desabilitá-lo. Quando você habilita um endereço GUA IPv6 para ser um IPv6 primário, o primeiro GUA IPv6 se tornará o endereço IPv6 primário até que a instância seja encerrada ou a interface de rede seja desconectada. Se você tiver vários endereços IPv6 associados a uma ENI anexada à sua instância e habilitar um endereço IPv6 primário, o primeiro endereço GUA IPv6 associado à ENI se tornará o endereço IPv6 primário.

10. (Opcional) Para criar um Elastic Fabric Adapter, clique em Elastic Fabric Adapter e em Enable (Habilitar).
11. (Opcional) Em Configurações avançadas, existe a opção de definir a delegação do prefixo IP. Para obter mais informações, consulte Delegação de prefixo.

    - Atribuição automática: a AWS escolhe o prefixo dos blocos CIDR IPv4 ou IPv6 para a sub-rede e o atribui à interface de rede.
    - Personalizada: você especifica o prefixo dos blocos CIDR IPv4 ou IPv6 para a sub-rede, e a AWS verifica se o prefixo ainda não foi atribuído a outros recursos antes de atribuí-lo à interface de rede.
12. (Opcional) Em Configurações avançadas, para Tempo limite de rastreamento de conexão ociosa, modifique os tempos limite de conexão ociosa padrão. Para obter mais informações, consulte Tempo limite de rastreamento de conexão ociosa.

    - Tempo limite para TCP estabelecido: tempo limite (em segundos) para conexões TCP ociosas em um estado estabelecido.
        - Mín: `60` segundos
        - Máx: `432000` segundos
        - Padrão: `350` segundos para tipos de instância Nitrov6, excluindo P6e-GB200. E `432000` segundos para outros tipos de instâncias, incluindo P6e-GB200.
        - Recomendado: menos de `432000` segundos
    - Tempo limite de UDP: tempo limite (em segundos) para fluxos UDP ociosos que só tiverem tráfego em uma única direção ou uma única transação de solicitação-resposta.
        - Mín: `30` segundos
        - Máx: `60` segundos

- Padrão: 30 segundos

- Tempo limite de fluxo UDP: tempo limite (em segundos) para fluxos UDP ociosos classificados como fluxos que tiveram mais de uma transação de solicitação-resposta.
  - Mín: 60 segundos
  - Máx: 180 segundos
  - Padrão: 180 segundos

13. Para Security groups, selecione um ou mais security groups.
14. (Opcional) Para cada tag, escolha Add new tag (Adicionar nova tag) e insira uma chave de tag e um valor de tag opcional.
15. Clique em Create network interface (Criar interface de rede).

AWS CLI

Exemplo 1: criar uma interface de rede com endereços IP escolhidos pelo Amazon EC2

Use o seguinte comando create-network-interface. Esse exemplo cria uma interface de rede com um endereço IPv4 público e um endereço IPv6 escolhido pelo Amazon EC2.

```
aws ec2 create-network-interface \
    --subnet-id subnet-0abcdef1234567890 \
    --description "my dual-stack network interface" \
    --ipv6-address-count 1 \
    --groups sg-1234567890abcdef0
```

Exemplo 2: criar uma interface de rede com endereços IP específicos

Use o seguinte comando create-network-interface.

```
aws ec2 create-network-interface \
    --subnet-id subnet-0abcdef1234567890 \
    --description "my dual-stack network interface" \
    --private-ip-address 10.251.50.12 \
    --ipv6-addresses 2001:db8::1234:5678:1.2.3.4 \
    --groups sg-1234567890abcdef0
```

Exemplo 3: criar uma interface de rede com uma contagem de endereços IP secundários

Use o seguinte comando create-network-interface. Neste exemplo, o Amazon EC2 escolhe o endereço IP primário e o endereço IP secundário.

```
aws ec2 create-network-interface \
    --subnet-id subnet-0abcdef1234567890 \
    --description "my network interface" \
    --secondary-private-ip-address-count 2 \
    --groups sg-1234567890abcdef0
```

Exemplo 4: criar uma interface de rede com um endereço IP secundário específico

Use o seguinte comando create-network-interface. Esse exemplo especifica um endereço IP primário e um endereço IP secundário.

```
aws ec2 create-network-interface \
    --subnet-id subnet-0abcdef1234567890 \
    --description "my network interface" \
    --private-ip-addresses PrivateIpAddress=10.0.1.30,Primary=true \
                           PrivateIpAddress=10.0.1.31,Primary=false
    --groups sg-1234567890abcdef0
```

PowerShell

Exemplo 1: criar uma interface de rede com endereços IP escolhidos pelo Amazon EC2

Use o cmdlet New-EC2NetworkInterface. Esse exemplo cria uma interface de rede com um endereço IPv4 público e um endereço IPv6 escolhido pelo Amazon EC2.

```
New-EC2NetworkInterface `
    -SubnetId subnet-0abcdef1234567890 `
    -Description "my dual-stack network interface" `
    -Ipv6AddressCount 1 `
    -Group sg-1234567890abcdef0
```

Exemplo 2: criar uma interface de rede com endereços IP específicos

Use o cmdlet New-EC2NetworkInterface.

```
New-EC2NetworkInterface `
    -SubnetId subnet-0abcdef1234567890 `
```

```
    -Description "my dual-stack network interface" `
    -PrivateIpAddress 10.251.50.12 `
    -Ipv6Address $ipv6addr `
    -Group sg-1234567890abcdef0
```

Defina os endereços IPv6 da seguinte maneira.

```
$ipv6addr = New-Object Amazon.EC2.Model.InstanceIpv6Address
$ipv6addr1.Ipv6Address = "2001:db8::1234:5678:1.2.3.4"
```

Exemplo 3: criar uma interface de rede com uma contagem de endereços IP secundários

Use o cmdlet New-EC2NetworkInterface. Neste exemplo, o Amazon EC2 escolhe o endereço IP primário e o endereço IP secundário.

```
New-EC2NetworkInterface `
    -SubnetId subnet-0abcdef1234567890 `
    -Description "my network interface" `
    -SecondaryPrivateIpAddressCount 2 `
    -Group sg-1234567890abcdef0
```

Exemplo 4: criar uma interface de rede com um endereço IP secundário específico

Use o cmdlet New-EC2NetworkInterface. Esse exemplo especifica um endereço IP primário e um endereço IP secundário.

```
New-EC2NetworkInterface `
    -SubnetId subnet-0abcdef1234567890 `
    -Description "my network interface" `
    -PrivateIpAddresses @($primary, $secondary) `
    -Group sg-1234567890abcdef0
```

Defina os endereços secundários da seguinte forma.

```
$primary = New-Object Amazon.EC2.Model.PrivateIpAddressSpecification
$primary.PrivateIpAddress = "10.0.1.30"
$primary.Primary = $true
$secondary = New-Object Amazon.EC2.Model.PrivateIpAddressSpecification
$secondary.PrivateIpAddress = "10.0.1.31"
$secondary.Primary = $false
```

Anexos de interface de rede para sua instância do EC2

É possível criar interfaces de rede para serem usadas por suas instâncias do EC2 como interfaces de rede primárias ou secundárias. É necessário anexar uma interface de rede a uma instância do EC2 se estiver na mesma zona de disponibilidade da interface de rede. O tipo de instância de uma instância determina quantas interfaces de rede você pode conectar à instância. Para obter mais informações, consulte the section called “Endereços IP por interface de rede”.

Considerações

- É possível 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).
- É possível desanexar as interfaces de rede secundárias quando a instância estiver sendo executada ou estiver parada. No entanto, não é possível desanexar a interface de rede primária.
- É possível desanexar uma interface de rede secundária de uma instância e anexá-la a outra instância.
- Ao executar uma instância usando a CLI, a API ou um SDK, é possível especificar a interface de rede primária e interfaces de rede adicionais. Observação: não será possível habilitar a atribuição automática de endereços IPv4 públicos se você adicionar uma interface de rede secundária durante a inicialização.
- 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.
- Você não pode anexar outra interface de rede a uma instância (por exemplo, uma configuração de agrupamento NIC) para aumentar ou dobrar a largura de banda da rede de ou para a instância dual-homed.
- Se você anexar várias interfaces de rede da mesma sub-rede a uma instância, poderá encontrar problemas de rede, como roteamento assimétrico. Se possível, adicione um endereço IPv4 privado secundário na interface de rede primária.

- Para instâncias do EC2 em uma sub-rede somente IPv6, se você anexar uma interface de rede secundária, o nome de host DNS privado da interface de rede secundária será resolvido como o endereço IPv6 primário na interface primária de rede.
- [Instâncias do Windows]: caso adicione várias interfaces de rede a uma instância, você deverá configurar as interfaces de rede para usar o roteamento estático.

Anexar interface de rede

É possível associar uma interface de rede a alguma instância na mesma zona de disponibilidade da interface de rede usando a página de Instâncias ou Interfaces de rede do console do Amazon EC2. Se preferir, você pode associar uma interface de rede existente ao iniciar instâncias.

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.

Console

Para anexar uma interface de rede usando a página Instâncias

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Marque a caixa de seleção da instância.
4. Escolha Actions (Ações), Networking (Redes), Attach network interface (Associar interface de rede).
5. Escolha uma VPC. A interface de rede pode residir na mesma VPC da sua instância ou em outra VPC de sua propriedade, desde que a interface de rede esteja na mesma zona de disponibilidade da instância. Isso permite que você crie instâncias de múltiplas hospedagens em VPCs com diferentes configurações de rede e segurança.
6. Selecione uma interface de rede. Se a instância suportar várias placas de rede, será possível escolher uma placa de rede.
7. Escolha Associar.

Para associar uma interface de rede usando a página Interfaces de rede

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

2. No painel de navegação, selecione Network Interfaces.
3. Marque a caixa de seleção para a interface de rede.
4. Clique em Actions (Ações) e em Attach (Associar).
5. Escolha uma instância. Se a instância suportar várias placas de rede, será possível escolher uma placa de rede.
6. Escolha Associar.

AWS CLI

Para anexar uma interface de rede

Use o seguinte comando attach-network-interface.

```
aws ec2 attach-network-interface \
    --network-interface-id eni-1234567890abcdef0 \
    --instance-id i-1234567890abcdef0 \
    --device-index 1
```

PowerShell

Para anexar uma interface de rede

Use o cmdlet Add-EC2NetworkInterface.

```
Add-EC2NetworkInterface `
    -NetworkInterfaceId eni-1234567890abcdef0 `
    -InstanceId i-1234567890abcdef0 `
    -DeviceIndex 1
```

Desanexar uma interface de rede

É possível separar uma interface de rede secundária associada a uma instância do EC2 a qualquer momento usando a página Instances (Instâncias) ou Network Interfaces (Interfaces de rede) do console do Amazon EC2.

Se você tentar separar uma interface de rede associada a um recurso de outro serviço, como um load balancer do Elastic Load Balancing, uma função do Lambda, um WorkSpace ou um gateway

NAT, você receberá um erro informando que você não tem permissão para acessar o recurso. Para localizar qual serviço criou o recurso anexado a uma interface de rede, verifique a descrição da interface de rede. Se você excluir o recurso, sua interface de rede será excluída.

Console

Para desanexar uma interface de rede usando a página Instâncias

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Marque a caixa de seleção da instância. Verifique a seção Network interfaces (Interfaces de rede) da guia Networking (Rede) para verificar se a interface de rede está conectada a uma instância como uma interface de rede secundária.
4. Escolha Actions (Ações), Networking (Redes), Detach network interface (Separar interface de rede).
5. Selecione a interface de rede e escolha Separar.

Para desanexar uma interface de rede usando a página Interfaces de rede

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Network Interfaces.
3. Marque a caixa de seleção para a interface de rede. Verifique a seção Instance details (Detalhes da instância) da guia Details (Detalhes) para verificar se a interface de rede está conectada a uma instância como uma interface de rede secundária.
4. Clique em Actions (Ações) e em Detach (Desanexar).
5. Quando a confirmação for solicitada, selecione Detach (Desanexar).
6. Se a interface de rede não conseguir se separar da instância, escolha Force detachment (Forçar desanexação), Enable (Ativar) e tente novamente. Recomendamos a desanexação forçada somente como último recurso. Forçar a separação pode impedir que você associe outra interface de rede no mesmo índice até reiniciar a instância. Isso também pode impedir que os metadados da instância reflitam que a interface de rede foi separada até que você reinicie a instância.

AWS CLI

Para desanexar uma interface de rede

Use o seguinte comando detach-network-interface.

```
aws ec2 detach-network-interface --attachment-id eni-attach-016c93267131892c9
```

PowerShell

Para desanexar uma interface de rede

Use o cmdlet Dismount-EC2NetworkInterface.

```
Dismount-EC2NetworkInterface -AttachmentId eni-attach-016c93267131892c9
```

Gerenciar os endereços IP para a interface de rede

É possível gerenciar os seguintes endereços IP para suas interfaces de rede:

- Endereços IP elásticos (um por endereço IPv4 privado)
- Endereços IPv4
- Endereços IPv6

Console

Para gerenciar os endereços IP 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. Marque a caixa de seleção para a interface de rede.
4. Para gerenciar os endereços IPv4 e IPv6, faça o seguinte:
    a. Clique em Actions (Ações) e em Manage IP addresses (Gerenciar endereços IP).
    b. Expanda a interface de rede.
    c. Para endereços IPv4, modifique os endereços IP conforme necessário. Para atribuir um endereço IPv4 adicional, selecione Atribuir novo endereço IP e especifique um endereço IPv4 do intervalo de sub-rede ou deixe que a AWS escolha um para você.
    d. (Pilha dupla ou somente IPv6) Em Endereços IPv6, edite os endereços IP conforme necessário. Para atribuir um endereço IPv6 adicional, selecione Atribuir novo endereço

IP e especifique um endereço IPv6 do intervalo de sub-rede ou deixe que a AWS escolha um para você.

e. Para atribuir ou cancelar a atribuição de um endereço IPv4 público a uma interface de rede, escolha Atribuir IP público automaticamente. Você pode habilitar ou desabilitar isso para qualquer interface de rede, mas isso afeta somente a interface de rede primária.

f. (Pilha dupla ou somente IPv6) Em Atribuir IP IPv6 primário, escolha Habilitar para atribuir um endereço IPv6 primário. O primeiro GUA associado à interface de rede é escolhido como o endereço IPv6 principal. Após atribuir um endereço IPv6 primário, você não pode alterá-lo. Esse endereço será o endereço IPv6 primário até que a instância seja encerrada ou a interface de rede seja desconectada.

g. Escolha Salvar.

5. Para associar um endereço IP elástico, faça o seguinte:

   a. Clique em Actions (Ações) e em Associate address (Associar endereço).

   b. Para Elastic IP address (Endereço IP elástico), selecione o endereço IP elástico.

   c. Para Private IPv4 address (Endereço IPv4 privado), selecione o endereço IPv4 privado a ser associado ao endereço IP elástico.

   d. (Opcional) Escolha Allow the Elastic IP address to be reassociated (Permitir que o endereço IP elástico seja reassociado) se a interface de rede estiver atualmente associada a outra instância ou interface de rede.

   e. Escolha Associate.

6. Para desassociar um endereço IP elástico, faça o seguinte:

   a. Escolha Actions e Disassociate address.

   b. Em Public IP address (Endereço IP público), selecione o endereço IP elástico.

   c. Escolha Disassociate (Desassociar).

AWS CLI

Para gerenciar os endereços IPv4

Use o seguinte comando assign-private-ip-addresses para atribuir um endereço IPv4.

```
aws ec2 assign-private-ip-addresses \
    --network-interface-id eni-1234567890abcdef0 \
    --private-ip-addresses 10.0.0.82
```

Use o seguinte comando unassign-private-ip-addresses para desatribuir um endereço IPv4.

```
aws ec2 unassign-private-ip-addresses \
    --network-interface-id eni-1234567890abcdef0 \
    --private-ip-addresses 10.0.0.82
```

Para gerenciar os endereços IPv6

Use o seguinte comando assign-ipv6-addresses para atribuir um endereço IPv6.

```
aws ec2 assign-ipv6-addresses \
    --network-interface-id eni-1234567890abcdef0 \
    --ipv6-addresses 2001:db8:1234:1a00:9691:9503:25ad:1761
```

Use o seguinte comando unassign-ipv6-addresses para desatribuir um endereço IPv6.

```
aws ec2 unassign-ipv6-addresses \
    --network-interface-id eni-1234567890abcdef0 \
    --ipv6-addresses 2001:db8:1234:1a00:9691:9503:25ad:1761
```

Para gerenciar o endereço IP elástico do endereço IPv4 privado primário

Use o seguinte comando associate-address para associar um endereço IP elástico ao endereço IPv4 privado primário.

```
aws ec2 associate-address \
    --allocation-id eipalloc-0b263919b6EXAMPLE \
    --network-interface-id eni-1234567890abcdef0
```

Use o seguinte comando disassociate-address para desassociar um endereço IP elástico do endereço IPv4 privado primário.

```
aws ec2 disassociate-address --association-id eipassoc-2bebb745a1EXAMPLE
```

PowerShell

Para gerenciar os endereços IPv4

Use o cmdlet Register-EC2PrivateIpAddress para atribuir um endereço IPv4.

```
Register-EC2PrivateIpAddress `
```

```
    -NetworkInterfaceId eni-1234567890abcdef0 `
    -PrivateIpAddress 10.0.0.82
```

Use o cmdlet Unregister-EC2PrivateIpAddress para desatribuir um endereço IPv4.

```
Unregister-EC2PrivateIpAddress `
    -NetworkInterfaceId eni-1234567890abcdef0 `
    -PrivateIpAddress 10.0.0.82
```

Para gerenciar os endereços IPv6

Use o cmdlet Register-EC2Ipv6AddressList para atribuir um endereço IPv6.

```
Register-EC2Ipv6AddressList `
    -NetworkInterfaceId eni-1234567890abcdef0 `
    -Ipv6Address 2001:db8:1234:1a00:9691:9503:25ad:1761
```

Use o cmdlet Unregister-EC2Ipv6AddressList para desatribuir um endereço IPv6.

```
Unregister-EC2Ipv6AddressList `
    -NetworkInterfaceId eni-1234567890abcdef0 `
    -Ipv6Address 2001:db8:1234:1a00:9691:9503:25ad:1761
```

Para gerenciar o endereço IP elástico do endereço IPv4 privado primário

Use o cmdlet Register-EC2Address para associar um endereço IP elástico ao endereço IPv4 privado primário.

```
Register-EC2Address `
    -NetworkInterfaceId eni-1234567890abcdef0 `
    -AllocationId eipalloc-0b263919b6EXAMPLE
```

Use o cmdlet Unregister-EC2Address para desassociar um endereço IP elástico do endereço IPv4 privado primário.

```
Unregister-EC2Address -AssociationId eipassoc-2bebb745a1EXAMPLE
```

Modificar atributos da interface de rede

É possível alterar os seguintes atributos de interface de rede:

- Descrição
- Grupos de segurança
- Excluir no encerramento
- Verificação de origem/destino
- Tempo limite de rastreamento de conexão ociosa

Considerações

Não é possível alterar os atributos de uma interface de rede gerenciada pelo solicitante.

Console

Para modificar atributos da 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. Marque a caixa de seleção para a interface de rede.
4. Para alterar a descrição, faça o seguinte:
   a. Clique em Actions (Ações) e em Change description (Alterar a descrição).
   b. Em Descrição, insira uma descrição.
   c. Escolha Salvar.
5. Para alterar os grupos de segurança, faça o seguinte:
   a. Clique em Actions (Ações) e em Change security groups (Alterar grupos de segurança).
   b. Em Grupos de segurança associados, adicione e remova grupos de segurança conforme necessário. O grupo de segurança e a interface de rede devem ser criados para a mesma VPC.
   c. Escolha Salvar.
6. Para alterar o comportamento de encerramento, faça o seguinte:
   a. Clique em Actions (Ações) e em Change termination behavior (Alterar comportamento de encerramento).
   b. Selecione ou desmarque Excluir ao encerrar, Habilitar.
   c. Escolha Salvar.

7. Para alterar a verificação de origem/destino, faça o seguinte:

   a. Clique em Actions (Ações), Change source/dest check (Alterar verificação de origem/destino).

   b. Selecione ou desmarque Verificação de origem/destino, Habilitar.

   c. Escolha Salvar.

8. Para alterar os tempos limite de rastreamento de conexão, faça o seguinte:

   a. Escolha Ações, Modificar tempo limite de rastreamento de conexão ociosa.

   b. Modifique os valores de tempo limite conforme necessário. Para obter mais informações, consulte Tempo limite de rastreamento de conexão ociosa.

      - Tempo limite para TCP estabelecido: tempo limite (em segundos) para conexões TCP ociosas em um estado estabelecido.
        - Mín: `60` segundos
        - Máx: `432000` segundos
        - Padrão: `350` segundos para tipos de instância Nitrov6, excluindo P6e-GB200. E `432000` segundos para outros tipos de instâncias, incluindo P6e-GB200.
        - Recomendado: menos de `432000` segundos
      - Tempo limite de UDP: tempo limite (em segundos) para fluxos UDP ociosos que só tiverem tráfego em uma única direção ou uma única transação de solicitação-resposta.
        - Mín: `30` segundos
        - Máx: `60` segundos
        - Padrão: `30` segundos
      - Tempo limite de fluxo UDP: tempo limite (em segundos) para fluxos UDP ociosos classificados como fluxos que tiveram mais de uma transação de solicitação-resposta.
        - Mín: `60` segundos
        - Máx: `180` segundos
        - Padrão: `180` segundos

   c. Escolha Salvar.

AWS CLI

Example Exemplo: modificar a descrição

Use o seguinte comando modify-network-interface-attribute.

```
aws ec2 modify-network-interface-attribute \
    --network-interface-id eni-1234567890abcdef0 \
    --description "my updated description"
```

Example Exemplo: modificar os grupos de segurança

Use o seguinte comando modify-network-interface-attribute.

```
aws ec2 modify-network-interface-attribute \
    --network-interface-id eni-1234567890abcdef0 \
    --groups sg-1234567890abcdef0
```

Example Exemplo: modificar o comportamento de encerramento

Use o seguinte comando modify-network-interface-attribute.

```
aws ec2 modify-network-interface-attribute \
    --network-interface-id eni-1234567890abcdef0 \
    --attachment AttachmentId=eni-attach-43348162abEXAMPLE,DeleteOnTermination=false
```

Example Exemplo: habilitar as verificações de origem/destino

Use o seguinte comando modify-network-interface-attribute.

```
aws ec2 modify-network-interface-attribute \
    --network-interface-id eni-1234567890abcdef0 \
    --source-dest-check
```

Example Exemplo: modificar o tempo limite de rastreamento de conexão ociosa

Use o seguinte comando modify-network-interface-attribute. Para obter mais informações, consulte Tempo limite de rastreamento de conexão ociosa.

```
aws ec2 modify-network-interface-attribute \
    --network-interface-id eni-1234567890abcdef0 \
```

```
    --connection-tracking-specification
 TcpEstablishedTimeout=172800,UdpStreamTimeout=90,UdpTimeout=60
```

PowerShell

Example Exemplo: modificar a descrição

Use o cmdlet Edit-EC2NetworkInterfaceAttribute.

```
Edit-EC2NetworkInterfaceAttribute `
    -NetworkInterfaceId eni-1234567890abcdef0 `
    -Description "my updated description"
```

Example Exemplo: modificar os grupos de segurança

Use o cmdlet Edit-EC2NetworkInterfaceAttribute.

```
Edit-EC2NetworkInterfaceAttribute `
    -NetworkInterfaceId eni-1234567890abcdef0 `
    -Group sg-1234567890abcdef0
```

Example Exemplo: modificar o comportamento de encerramento

Use o cmdlet Edit-EC2NetworkInterfaceAttribute.

```
Edit-EC2NetworkInterfaceAttribute `
    -NetworkInterfaceId eni-1234567890abcdef0 `
    -Attachment_AttachmentId eni-attach-43348162abEXAMPLE `
    -Attachment_DeleteOnTermination $false
```

Example Exemplo: habilitar as verificações de origem/destino

Use o cmdlet Edit-EC2NetworkInterfaceAttribute.

```
Edit-EC2NetworkInterfaceAttribute `
    -NetworkInterfaceId eni-1234567890abcdef0 `
    -SourceDestCheck $true
```

Example Exemplo: modificar os tempos limite de rastreamento de conexão ociosa

Use o cmdlet Edit-EC2NetworkInterfaceAttribute. Para obter mais informações, consulte Tempo limite de rastreamento de conexão ociosa.

```
Edit-EC2NetworkInterfaceAttribute `
    -NetworkInterfaceId eni-1234567890abcdef0 `
    -ConnectionTrackingSpecification_TcpEstablishedTimeout 172800 `
    -ConnectionTrackingSpecification_UdpStreamTimeout 90 `
    -ConnectionTrackingSpecification_UdpTimeout 60
```

Várias interfaces de rede para as instâncias do Amazon EC2

Anexar várias interfaces de rede a uma instância é útil quando você precisa do seguinte:

- Uma rede de gerenciamento.
- Dispositivos de rede e segurança.
- Instâncias dual-homed com workloads em diferentes sub-redes ou VPCs.
- Uma solução de baixo orçamento e alta disponibilidade.

Rede de gerenciamento

A visão geral a seguir descreve uma rede de gerenciamento criada usando várias interfaces de rede.

Critérios

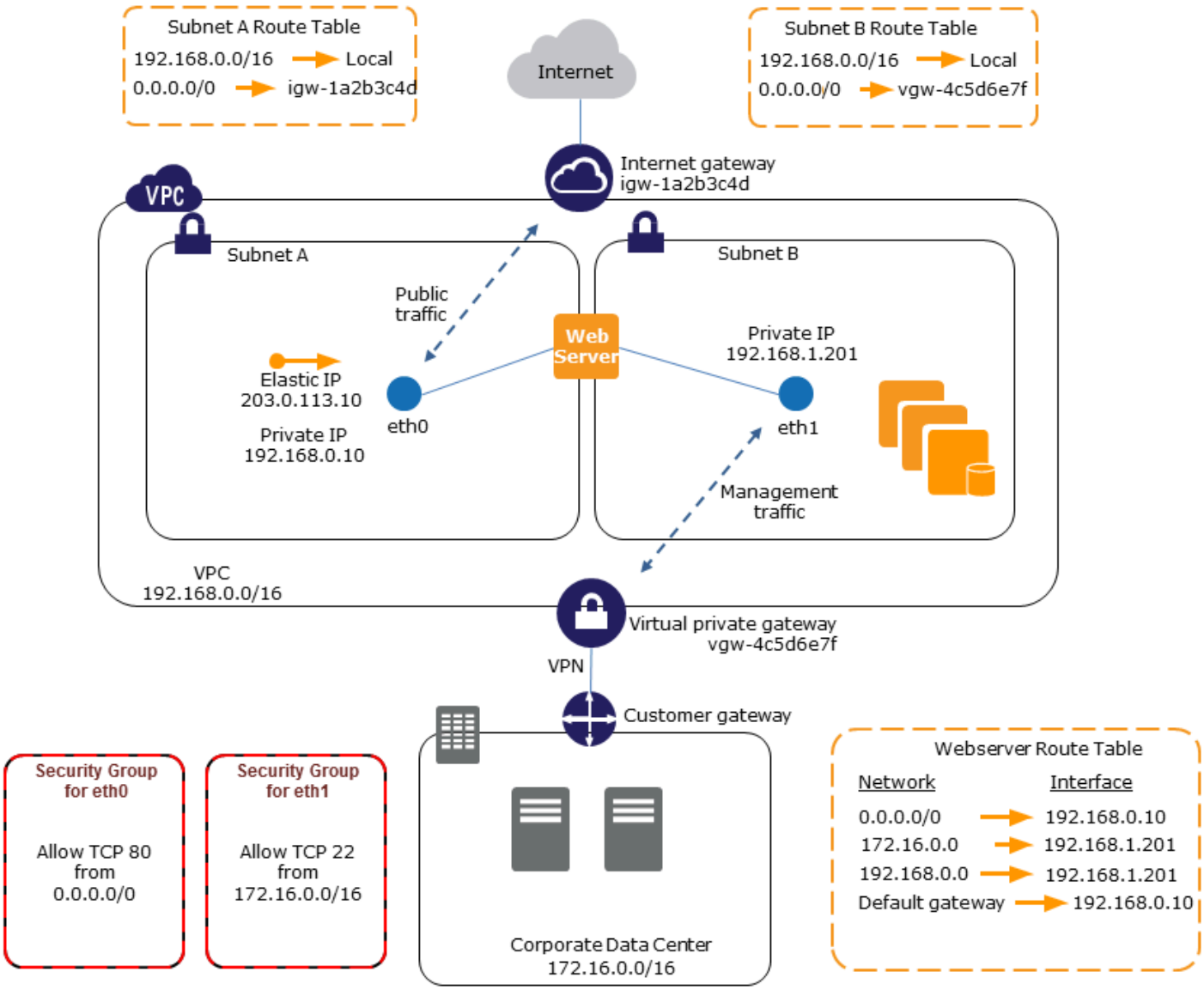
- A interface de rede primária na instância (por exemplo, eth0) lida com o tráfego público.
- A interface de rede secundária na instância (por exemplo, eth1) lida com o tráfego de gerenciamento de backend. Ela está conectada a uma sub-rede separada com controles de acesso mais restritivos e localizada na mesma zona de disponibilidade que a interface de rede primária.

Configurações

- A interface de rede primária, que pode ou não estar por trás de um balanceador de carga, tem um grupo de segurança associado que permite acesso ao servidor a partir da Internet. Por exemplo, permitir as portas TCP 80 e 443 de 0.0.0.0/0 ou do balanceador de carga.
- A interface de rede secundária tem um grupo de segurança associado que permite somente o acesso SSH, iniciado usando um dos seguintes locais:
  - Um intervalo permitido de endereços IP, dentro da VPC ou da Internet.
  - Uma sub-rede privada na mesma zona de disponibilidade que a interface de rede primária.

- Um gateway privado virtual.

> **Note**
>
> 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, é possível mover a interface e/ou o endereço IPv4 privado secundário para uma instância standby.



Dispositivos de rede e segurança

Algumas ferramentas de rede e segurança, como load balancers, servidores de tradução de endereço de rede (NAT) e servidores proxy preferem ser configurados com várias interfaces de rede. É possível criar e associar interfaces de rede secundárias às instâncias em uma VPC que executa esses tipos de aplicações e configurar interfaces adicionais com seus próprios endereços IP públicos e privados, grupos de segurança e verificação de origem/destino.

Instâncias dual-homed com workloads em diferentes sub-redes

É possível colocar uma interface de rede em cada um dos servidores Web que se conecta a uma rede mid-tier na qual reside o servidor de aplicações. O servidor de aplicações também pode ser dual-homed para uma rede backend (sub-rede) no servidor onde reside o banco de dados. Em vez de rotear pacotes de rede pelas instâncias dual-homed, cada instância dual-homed recebe e processa solicitações no front-end, inicia uma conexão ao backend e, então, envia solicitações aos servidores na rede backend.

Instâncias dual-homed com workloads em diferentes VPCs na mesma conta

É possível iniciar uma instância do EC2 em uma VPC e anexar uma ENI secundária de uma VPC diferente, desde que a interface de rede esteja na mesma zona de disponibilidade da instância. Isso permite que você crie instâncias de múltiplas hospedagens em VPCs com diferentes configurações de rede e segurança. Você não pode criar instâncias de múltiplas hospedagens em VPCs de contas diferentes da AWS.

É possível usar instâncias de múltiplas hospedagens em VPCs nos seguintes casos de uso:

- Superar sobreposições de CIDR entre duas VPCs que não podem ser emparelhadas: você pode aproveitar um CIDR secundário em uma VPC e permitir que uma instância se comunique em dois intervalos de IP não sobrepostos.
- Conectar várias VPCs em uma única conta: habilitar a comunicação entre recursos individuais que normalmente seriam separados pelos limites da VPC.

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, é possível 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.

Interfaces de rede gerenciadas pelo solicitante

Uma interface de rede gerenciada pelo solicitante é uma interface de rede que um AWS service (Serviço da AWS) cria na VPC em seu nome. A interface de rede está associada a um recurso de outro serviço, como uma instância de banco de dados do Amazon RDS, um gateway NAT ou um endpoint da VPC de interface de AWS PrivateLink.

Considerações

- É possível visualizar as interfaces de rede gerenciadas pelo solicitante em sua conta. É possível adicionar ou remover etiquetas, mas não pode alterar outras propriedades de uma interface de rede gerenciada pelo solicitante.
- Não é possível desvincular uma interface de rede gerenciada pelo solicitante.
- Ao excluir o recurso associado à interface de rede gerenciada pelo solicitante, o AWS service (Serviço da AWS) desvinculará e excluirá a interface de rede. Se o serviço desvinculou uma interface de rede, mas não a excluiu, será possível excluir a interface de rede desvinculada.

Console

Para visualizar interfaces de rede gerenciadas pelo solicitante

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Network & Security (Rede e segurança), Network Interfaces (Interfaces de rede).
3. Selecione o ID da interface de rede para abrir sua página de detalhes.
4. Estes são os principais campos que podem ser usados para determinar a finalidade da interface de rede:

   - Descrição: uma descrição fornecida pelo serviço da AWS que criou a interface. Por exemplo, "VPC Endpoint Interface vpce 089f2123488812123".

- Gerenciado pelo solicitante: indica se a interface de rede é gerenciada pela AWS.
- Requester ID (ID do solicitante): o alias ou ID da conta da AWS da entidade principal ou serviço que criou a interface de rede. Se você criou uma interface de rede, este campo exibirá o ID de sua Conta da AWS. Caso contrário, ele terá sido criado por outra entidade principal ou serviço.

AWS CLI

Para visualizar interfaces de rede gerenciadas pelo solicitante

Use o comando describe-network-interfaces como indicado a seguir.

```
aws ec2 describe-network-interfaces \
    --filters "Name=requester-managed,Values=true" \
    --query "NetworkInterfaces[*].[Description, InterfaceType]" \
    --output table
```

Veja a seguir um exemplo de saída que mostra os principais campos que é possível usar para determinar a finalidade da interface de rede: `Description` e `InterfaceType`.

```
-------------------------------------------------------------------------------
|                          DescribeNetworkInterfaces                          |
+-----------------------------------------------------+-------------------------+
|  VPC Endpoint Interface: vpce-0f00567fa8477a1e6     |  interface              |
|  VPC Endpoint Interface vpce-0d8ddce4be80e4474      |  interface              |
|  VPC Endpoint Interface vpce-078221a1e27d1ea5b      |  vpc_endpoint           |
|  Resource Gateway Interface rgw-0bba03f3d56060135   |  interface              |
|  VPC Endpoint Interface: vpce-0cc199f605eaeace7     |  interface              |
|  VPC Endpoint Interface vpce-019b90d6f16d4f958      |  interface              |
+-----------------------------------------------------+-------------------------+
```

PowerShell

Para visualizar interfaces de rede gerenciadas pelo solicitante

Use o cmdlet Get-EC2NetworkInterface como indicado a seguir.

```
Get-EC2NetworkInterface -Filter @{Name="requester-managed"; Values="true"} | Select
 Description, InterfaceType
```

Veja a seguir um exemplo de saída que mostra os principais campos que é possível usar para determinar a finalidade de uma interface de rede: `Description` e `InterfaceType`.

```
Description                                      InterfaceType
-----------                                      -------------
VPC Endpoint Interface: vpce-0f00567fa8477a1e6   interface
VPC Endpoint Interface vpce-0d8ddce4be80e4474    interface
VPC Endpoint Interface vpce-078221a1e27d1ea5b    vpc_endpoint
Resource Gateway Interface rgw-0bba03f3d56060135 interface
VPC Endpoint Interface: vpce-0cc199f605eaeace7   interface
VPC Endpoint Interface vpce-019b90d6f16d4f958    interface
```

Delegação de prefixo para interfaces de rede do Amazon EC2

É possível atribuir um intervalo de CIDR IPv4 ou IPv6 privado, automático ou manualmente, às suas interfaces de rede. Ao atribuir prefixos, você dimensiona e simplifica o gerenciamento de aplicações, incluindo aplicações de contêiner e rede que exigem vários endereços IP em uma instância. Para obter mais informações sobre endereços IPv4 e IPv6, consulte Endereçamento IP de instâncias do Amazon EC2.

As seguintes opções estão disponíveis:

- Atribuição automática: a AWS escolhe o prefixo e o atribui à sua interface de rede. Se a sub-rede da interface de rede tiver uma reserva de CIDR de sub-rede do tipo `prefix`, selecionaremos os prefixos da reserva de CIDR da sub-rede. Caso contrário, selecionaremos os prefixos do intervalo de CIDR da sub-rede.
- Atribuição manual: você especifica o prefixo e a AWS verifica se o prefixo ainda não está atribuído a outros recursos antes de atribuí-lo à interface de rede.

Atribuir prefixos apresenta os seguintes benefícios:

- Endereços IP aumentados em uma interface de rede — Quando você usa um prefixo, atribui um bloco de endereços IP em vez de endereços IP individuais. Isso aumenta o número de endereços IP para uma interface de rede.
- Gerenciamento simplificado da VPC para contêineres — em aplicações de contêiner, cada contêiner requer um endereço IP exclusivo. A atribuição de prefixos à instância simplifica o gerenciamento de suas VPCs, pois é possível iniciar e encerrar contêineres sem precisar chamar APIs do Amazon EC2 para atribuições de IP individuais.

Sumário

- Conceitos básicos
- Considerações
- Gerenciar prefixos para interfaces de rede
  - Atribuir prefixos durante a criação da interface de rede
  - Atribuir prefixos a uma interface de rede existente
  - Remover prefixos de suas interfaces de rede

Conceitos básicos

- É possível atribuir um prefixo a interfaces de rede novas ou existentes.
- Para usar prefixos, atribua um prefixo à interface de rede, depois anexe a interface de rede à instância e configure o sistema operacional.
- Quando você escolhe a opção para especificar um prefixo, o prefixo deve atender aos seguintes requisitos:
  - O prefixo IPv4 que é possível especificar é `/28`.
  - O prefixo IPv6 que é possível especificar é `/80`.
  - O prefixo está na sub-rede CIDR da interface de rede e não se sobrepõe a outros prefixos ou endereços IP atribuídos a recursos existentes na sub-rede.
- É possível atribuir um prefixo à interface de rede primária ou secundária.
- É possível atribuir um endereço IP elástico a uma interface de rede que tenha um prefixo atribuído a ela.
- Também é possível atribuir um endereço IP elástico à parte do endereço IP do prefixo atribuído.
- Um nome de host DNS privado (interno) é resolvido para o endereço IPv4 privado da instância.
- Atribuímos cada endereço IPv4 privado para uma interface de rede, incluindo os de prefixos, usando o seguinte formato:
  - `us-east-1`Região da

    ```
    ip-private-ipv4-address.ec2.internal
    ```

  - Todas as outras regiões

    ```
    ip-private-ipv4-address.region.compute.internal
    ```

Considerações

Leve o seguinte em consideração ao usar endpoints do :

- Interfaces de rede com prefixos são compatíveis com instâncias baseadas em Nitro.
- Os prefixos de interfaces de rede devem usar endereços IPv6 ou endereços IPv4 privados.
- O número máximo de endereços IP que podem ser atribuídos a uma interface de rede depende do tipo de instância. Todo prefixo que você atribui a uma interface de rede conta como um endereço IP. Por exemplo, uma instância `c5.large` tem um limite de `10` endereços IPv4 por interface de rede. Toda interface de rede para essa instância tem um endereço IPv4 primário. Se uma interface de rede não tiver endereços IPv4 secundários, será possível atribuir até nove prefixos à interface de rede. Para cada endereço IPv4 adicional que você atribuir a uma interface de rede, poderá atribuir um prefixo a menos à interface de rede. Para obter mais informações, consulte Máximo de endereços IP por interface de rede.
- Os prefixos são incluídos nas verificações de origem/destino.
- Configure seu sistema operacional para trabalhar com interfaces de rede com prefixos. Observe o seguinte:
  - Algumas AMIs do Amazon Linux contêm scripts adicionais instalados pela AWS, conhecidos como `ec2-net-utils`. Esses scripts opcionalmente automatizam a configuração das suas interfaces de rede. Eles são para uso somente no Amazon Linux.
  - Para contêineres, será possível usar uma Container Network Interface (CNI) para o plugin Kubernetes, ou `dockerd` se você usar o Docker para gerenciar seus contêineres.

Gerenciar prefixos para interfaces de rede

Ao atribuir prefixos a uma interface de rede, você pode escolher se deseja que atribuamos automaticamente os prefixos ou se deseja especificar prefixos personalizados. Se você nos permitir atribuir prefixos automaticamente e a sub-rede da interface de rede tiver uma reserva de CIDR de sub-rede do tipo `prefix`, selecionaremos os prefixos da reserva de CIDR da sub-rede. Caso contrário, selecionaremos os prefixos do intervalo de CIDR da sub-rede.

Tarefas

- Atribuir prefixos durante a criação da interface de rede
- Atribuir prefixos a uma interface de rede existente
- Remover prefixos de suas interfaces de rede

Atribuir prefixos durante a criação da interface de rede

É possível atribuir prefixos automáticos ou personalizados ao criar uma interface de rede.

Console

Para atribuir prefixos automáticos durante a criação da interface de rede

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Network Interfaces.
3. Clique em Create network interface (Criar interface de rede).
4. Insira uma descrição para a interface de rede, selecione a sub-rede na qual deseja criar a interface de rede e configure os endereços IPv4 e IPv6 privados.
5. Expanda Advanced settings (Configurações avançadas).
6. Para Delegação de prefixo IPv4, faça um dos seguintes:
   - Para atribuir automaticamente um prefixo IPv4, escolha Atribuir automaticamente. Para Número de prefixos IPv4, insira o número de prefixos a serem atribuídos.
   - Para atribuir um prefixo IPv4 específico, escolha Personalizar. Escolha Adicionar novo prefixo e insira o prefixo.
7. Para delegação de prefixo IPv6, faça um dos seguintes:
   - Para atribuir automaticamente um prefixo IPv6, escolha Atribuir automaticamente. Para Número de prefixos IPv6, insira o número de prefixos a serem atribuídos.
   - Para atribuir um prefixo IPv6 específico, escolha Personalizar. Escolha Adicionar novo prefixo e insira o prefixo.

   > **Note**
   >
   > Delegação de prefixo IPv6 aparece somente se a sub-rede selecionada estiver habilitada para IPv6.

8. Selecione os grupos de segurança a serem associados à interface de rede e atribua marcações de recursos, se necessário.
9. Clique em Criar interface de rede.

AWS CLI

Para atribuir prefixos IPv4 automáticos durante a criação da interface de rede

Use o comando create-network-interface e defina `--ipv4-prefix-count` como o número de prefixos IPv4 para a AWS atribuir. No exemplo a seguir, a AWS atribui um prefixo IPv4.

```
aws ec2 create-network-interface \
    --subnet-id subnet-047cfed18eEXAMPLE \
    --description "IPv4 automatic example" \
    --ipv4-prefix-count 1
```

Para atribuir prefixos IPv4 específicos durante a criação da interface de rede

Use o comando create-network-interface e defina `--ipv4-prefixes` como os prefixos. A AWS seleciona endereços IPv4 desse intervalo. No exemplo a seguir, o prefixo CIDR é 10.0.0.208/28.

```
aws ec2 create-network-interface \
    --subnet-id subnet-047cfed18eEXAMPLE \
    --description "IPv4 manual example" \
    --ipv4-prefixes Ipv4Prefix=10.0.0.208/28
```

Para atribuir prefixos IPv6 automáticos durante a criação da interface de rede

Use o comando create-network-interface e defina `--ipv6-prefix-count` como o número de prefixos IPv6 para a AWS atribuir. No exemplo a seguir, a AWS atribui um prefixo IPv6.

```
aws ec2 create-network-interface \
    --subnet-id subnet-047cfed18eEXAMPLE \
    --description "IPv6 automatic example" \
    --ipv6-prefix-count 1
```

Para atribuir prefixos IPv6 específicos durante a criação da interface de rede

Use o comando create-network-interface e defina `--ipv6-prefixes` como os prefixos. A AWS seleciona endereços IPv6 desse intervalo. No exemplo a seguir, o prefixo CIDR é 2600:1f13:fc2:a700:1768::/80.

```
aws ec2 create-network-interface \
    --subnet-id subnet-047cfed18eEXAMPLE \
    --description "IPv6 manual example" \
```

```
    --ipv6-prefixes Ipv6Prefix=2600:1f13:fc2:a700:1768::/80
```

PowerShell

Para atribuir prefixos IPv4 automáticos durante a criação da interface de rede

Use o cmdlet New-EC2NetworkInterface e defina `Ipv4PrefixCount` como o número de prefixos IPv4 para a AWS atribuir. No exemplo a seguir, a AWS atribui um prefixo IPv4.

```
New-EC2NetworkInterface `
    -SubnetId 'subnet-047cfed18eEXAMPLE' `
    -Description 'IPv4 automatic example' `
    -Ipv4PrefixCount 1
```

Para atribuir prefixos IPv4 específicos durante a criação da interface de rede

Use o cmdlet New-EC2NetworkInterface e defina `Ipv4Prefix` como os prefixos. A AWS seleciona endereços IPv4 desse intervalo. No exemplo a seguir, o prefixo CIDR é 10.0.0.208/28.

```
Import-Module AWS.Tools.EC2
New-EC2NetworkInterface `
    -SubnetId 'subnet-047cfed18eEXAMPLE' `
    -Description 'IPv4 manual example' `
    -Ipv4Prefix (New-Object `
        -TypeName Amazon.EC2.Model.Ipv4PrefixSpecificationRequest `
        -Property @{Ipv4Prefix = '10.0.0.208/28'})
```

Para atribuir prefixos IPv6 automáticos durante a criação da interface de rede

Use o cmdlet New-EC2NetworkInterface e defina `Ipv6PrefixCount` como o número de prefixos IPv6 para a AWS atribuir. No exemplo a seguir, a AWS atribui um prefixo IPv6.

```
New-EC2NetworkInterface `
    -SubnetId 'subnet-047cfed18eEXAMPLE' `
    -Description 'IPv6 automatic example' `
    -Ipv6PrefixCount 1
```

Para atribuir prefixos IPv6 específicos durante a criação da interface de rede

Use o cmdlet New-EC2NetworkInterface e defina `Ipv6Prefixes` como os prefixos. A AWS seleciona endereços IPv6 desse intervalo. No exemplo a seguir, o prefixo CIDR é 2600:1f13:fc2:a700:1768::/80.

```
Import-Module AWS.Tools.EC2
New-EC2NetworkInterface `
    -SubnetId 'subnet-047cfed18eEXAMPLE' `
    -Description 'IPv6 manual example' `
    -Ipv6Prefix (New-Object `
        -TypeName Amazon.EC2.Model.Ipv6PrefixSpecificationRequest `
        -Property @{Ipv6Prefix = '2600:1f13:fc2:a700:1768::/80'})
```

Atribuir prefixos a uma interface de rede existente

É possível atribuir prefixos automáticos ou personalizados a uma interface de rede existente.

Console

Para atribuir prefixos automáticos a uma interface de rede existente

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Network Interfaces.
3. Selecione a interface de rede à qual atribuir os prefixos e escolha Ações, Gerenciar prefixos.
4. Para Delegação de prefixo IPv4, faça um dos seguintes:
   - Para atribuir automaticamente um prefixo IPv4, escolha Atribuir automaticamente. Para Número de prefixos IPv4, insira o número de prefixos a serem atribuídos.
   - Para atribuir um prefixo IPv4 específico, escolha Personalizar. Escolha Adicionar novo prefixo e insira o prefixo.
5. Para delegação de prefixo IPv6, faça um dos seguintes:
   - Para atribuir automaticamente um prefixo IPv6, escolha Atribuir automaticamente. Para Número de prefixos IPv6, insira o número de prefixos a serem atribuídos.
   - Para atribuir um prefixo IPv6 específico, escolha Personalizar. Escolha Adicionar novo prefixo e insira o prefixo.

   > **Note**
   >
   > Delegação de prefixo IPv6 aparece somente se a sub-rede selecionada estiver habilitada para IPv6.

6. Escolha Salvar.

AWS CLI

Use o comando assign-ipv6-addresses para atribuir prefixos IPv6 e o comando assign-private-ip-addresses para atribuir prefixos IPv4 a interfaces de rede existentes.

Para atribuir prefixos IPv4 automáticos a uma interface de rede existente

Use o comando assign-private-ip-addresses e defina `--ipv4-prefix-count` como o número de prefixos IPv4 para a AWS atribuir. No exemplo a seguir, a AWS atribui um prefixo IPv4.

```
aws ec2 assign-private-ip-addresses \
    --network-interface-id eni-081fbb4095EXAMPLE \
    --ipv4-prefix-count 1
```

Para atribuir prefixos IPv4 específicos para uma interface de rede existente

Use o comando assign-private-ip-addresses e defina `--ipv4-prefixes` para o prefixo. A AWS seleciona endereços IPv4 desse intervalo. No exemplo a seguir, o prefixo CIDR é 10.0.0.208/28.

```
aws ec2 assign-private-ip-addresses \
    --network-interface-id eni-081fbb4095EXAMPLE \
    --ipv4-prefixes 10.0.0.208/28
```

Para atribuir prefixos IPv6 automáticos a uma interface de rede existente

Use o comando assign-ipv6-addresses e defina `--ipv6-prefix-count` como o número de prefixos IPv6 para a AWS atribuir. No exemplo a seguir, a AWS atribui um prefixo IPv6.

```
aws ec2 assign-ipv6-addresses \
    --network-interface-id eni-00d577338cEXAMPLE \
    --ipv6-prefix-count 1
```

Para atribuir prefixos IPv6 específicos para uma interface de rede existente

Usar o comando assign-ipv6-addresses e defina `--ipv6-prefixes`para o prefixo. A AWS seleciona endereços IPv6 desse intervalo. No exemplo a seguir, o prefixo CIDR é2600:1f13:fc2:a700:18bb::/80.

```
aws ec2 assign-ipv6-addresses \
    --network-interface-id eni-00d577338cEXAMPLE \
```

```
    --ipv6-prefixes 2600:1f13:fc2:a700:18bb::/80
```

PowerShell

Para atribuir prefixos IPv4 automáticos a uma interface de rede existente

Use o cmdlet Register-EC2PrivateIpAddress e defina `Ipv4PrefixCount` como o número de prefixos IPv4 para a AWS atribuir. No exemplo a seguir, a AWS atribui um prefixo IPv4.

```
Register-EC2PrivateIpAddress `
    -NetworkInterfaceId 'eni-00d577338cEXAMPLE' `
    -Ipv4PrefixCount 1
```

Para atribuir prefixos IPv4 específicos para uma interface de rede existente

Use o cmdlet Register-EC2PrivateIpAddress e defina `Ipv4Prefix` como o prefixo. A AWS seleciona endereços IPv4 desse intervalo. No exemplo a seguir, o prefixo CIDR é 10.0.0.208/28.

```
Register-EC2PrivateIpAddress `
    -NetworkInterfaceId 'eni-00d577338cEXAMPLE' `
    -Ipv4Prefix '10.0.0.208/28'
```

Para atribuir prefixos IPv6 automáticos a uma interface de rede existente

Use o cmdlet Register-EC2Ipv6AddressList e defina `Ipv6PrefixCount` como o número de prefixos IPv4 para a AWS atribuir. No exemplo a seguir, a AWS atribui um prefixo IPv6.

```
Register-EC2Ipv6AddressList `
    -NetworkInterfaceId 'eni-00d577338cEXAMPLE' `
    -Ipv6PrefixCount 1
```

Para atribuir prefixos IPv6 específicos para uma interface de rede existente

Use o cmdlet Register-EC2Ipv6AddressList e defina `Ipv6Prefix` como o prefixo. A AWS seleciona endereços IPv4 desse intervalo. No exemplo a seguir, o prefixo CIDR é 2600:1f13:fc2:a700:18bb::/80.

```
Register-EC2Ipv6AddressList `
    -NetworkInterfaceId 'eni-00d577338cEXAMPLE' `
    -Ipv6Prefix '2600:1f13:fc2:a700:18bb::/80'
```

Remover prefixos de suas interfaces de rede

É possível remover prefixos de uma interface de rede existente.

Console

Para remover os prefixos de uma interface de rede

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Network Interfaces.
3. Selecione a interface de rede.
4. Escolha Ações, Gerenciar prefixos.
5. Para Delegar prefixos IPv4, para remover prefixos específicos, escolha Cancelar atribuição ao lado dos prefixos a serem removidos. Para remover todos os prefixos, escolha Não atribuir.
6. Para Delegar prefixos IPv6, para remover prefixos específicos, escolha Cancelar atribuição ao lado dos prefixos a serem removidos. Para remover todos os prefixos, escolha Não atribuir.

> **Note**
>
> Delegação de prefixo IPv6 aparece somente se a sub-rede selecionada estiver habilitada para IPv6.

7. Escolha Salvar.

AWS CLI

É possível usar ounassign-ipv6-addressespara remover prefixos IPv6 e o comandounassign-private-ip-addressespara remover prefixos IPv4 de suas interfaces de rede existentes.

Para remover prefixos IPv4 de uma interface de rede

Use o comando unassign-private-ip-addresses e defina `--ipv4-prefix` como o CIDR de prefixo a ser removido.

```
aws ec2 unassign-private-ip-addresses \
```

```
    --network-interface-id eni-081fbb4095EXAMPLE \
    --ipv4-prefixes 10.0.0.176/28
```

Para remover prefixos IPv6 de uma interface de rede

Use o comando unassign-ipv6-addresses e defina `--ipv6-prefix` como o CIDR de prefixo a ser removido.

```
aws ec2 unassign-ipv6-addresses \
    --network-interface-id eni-00d577338cEXAMPLE \
    --ipv6-prefix 2600:1f13:fc2:a700:18bb::/80
```

PowerShell

Para remover prefixos IPv4 de uma interface de rede

Use o cmdlet Unregister-EC2PrivateIpAddress e defina `Ipv4Prefix` como o CIDR de prefixo a ser removido.

```
Unregister-EC2PrivateIpAddress `
    -NetworkInterfaceId 'eni-00d577338cEXAMPLE' `
    -Ipv4Prefix '10.0.0.208/28'
```

Para remover prefixos IPv6 de uma interface de rede

Use o cmdlet Unregister-EC2Ipv6AddressList e defina `Ipv6Prefix` como o CIDR de prefixo a ser removido.

```
Unregister-EC2Ipv6AddressList `
    -NetworkInterfaceId 'eni-00d577338cEXAMPLE' `
    -Ipv6Prefix '2600:1f13:fc2:a700:18bb::/80'
```

Excluir uma interface de rede

A exclusão de uma interface de rede libera todos os atributos associados com a interface e todos os endereços IP privados ou endereços IP elásticos a serem usados por outra instância.

Você não pode excluir uma interface de rede que esteja em uso. Primeiro, você devedesanexar a interface de rede.

Console

Excluir 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. Marque a caixa de seleção para a interface de rede e selecione Actions (Ações), Delete (Excluir).
4. Quando a confirmação for solicitada, escolha Excluir.

AWS CLI

Excluir uma interface de rede

Use o seguinte comando delete-network-interface.

```
aws ec2 delete-network-interface --network-interface-id eni-1234567890abcdef0
```

PowerShell

Excluir uma interface de rede

Use o cmdlet Remove-EC2NetworkInterface.

```
Remove-EC2NetworkInterface -NetworkInterfaceId eni-1234567890abcdef0
```

Largura de banda de rede de instâncias do Amazon EC2

As especificações de largura de banda da instância se aplicam tanto ao tráfego de entrada quanto de saída da instância. Por exemplo, se uma instância especificar até 10 Gbps de largura de banda, isso significa que ela tem até 10 Gbps de largura de banda para tráfego de entrada e, simultaneamente, até 10 Gbps para tráfego de saída. A largura de banda da rede disponível para uma instância do EC2 depende de vários fatores, como se segue.

Tráfego de vários fluxos

A largura de banda para tráfego de vários fluxos é limitada a 50% da largura de banda disponível para tráfego que passe por um gateway da Internet ou por um gateway local para instâncias com 32

ou mais vCPUs ou 5 Gbps, o que for maior. Para instâncias com menos de 32 vCPUs, a largura de banda é limitada a 5 Gbps.

Tráfego de fluxo único

A largura de banda para tráfego de fluxo único é limitada a 5 Gbps quando as instâncias não estão no mesmo grupo de posicionamento de cluster. Para reduzir a latência e aumentar a largura de banda de fluxo único, experimente uma dos seguintes opções:

- Use um grupo de posicionamento de cluster para conseguir uma largura de banda de até 10 Gbps para instâncias dentro do mesmo grupo de posicionamento.
- Configure vários caminhos entre dois endpoints para conseguir uma maior largura de banda usando Multipath TCP (MPTCP).
- Configure o ENA Express para as instâncias elegíeis na mesma zona de disponibilidade para conseguir até 25 Gbps entre essas instâncias.

> **Note**
>
> Um fluxo único é considerado um fluxo TCP ou UDP exclusivo de 5 tuplas. Para outros protocolos que seguem o cabeçalho IP, como `GRE` ou `IPsec`, a tupla 3 de IP de origem, de IP de destino e do próximo protocolo é usada para definir um fluxo.

Largura de banda disponível da instância

A largura de banda de rede disponível de uma instância depende do número de vCPUs que ela possui. Por exemplo, um`m5.8xlarge`tem 32 vCPUs e largura de banda de rede de 10 Gbps, e um`am5.16xlarge`tem 64 vCPUs e 20 Gbps de largura de banda de rede. As instâncias podem não atingir essa largura de banda, por exemplo, se excederem as permissões de rede no nível da instância, como pacote por segundo ou número de conexões controladas. A quantidade de largura de banda disponível que o tráfego pode utilizar depende do número de vCPUs e do destino. Por exemplo, uma instância `m5.16xlarge` tem 64 vCPUs, portanto, o tráfego para outra instância na região pode utilizar a largura de banda total disponível (20 Gbps). No entanto, o tráfego que passa por um gateway da Internet ou um gateway local pode utilizar apenas 50% da largura de banda disponível (10 Gbps).

Normalmente, instâncias com 16 vCPUs ou menos (tamanho `4xlarge` e inferiores) são documentadas como tendo “até” uma largura de banda especificada; por exemplo, “até 10 Gbps”.

Essas instâncias têm uma largura de banda de base. Para atender a demanda adicional, eles podem usar um mecanismo de crédito de E/S para explodir além da largura de banda de base. As instâncias podem usar largura de banda expansível por um tempo limitado, geralmente de 5 a 60 minutos, dependendo do tamanho da instância.

Uma instância recebe o número máximo de créditos de E/S de rede no lançamento. Se a instância esgotar seus créditos de E/S de rede, ela retornará à largura de banda da linha de base. Uma instância em execução ganha créditos de E/S de rede sempre que usa menos largura de banda de rede do que sua largura de banda de base. Uma instância interrompida não ganha créditos de E/S de rede. A expansão de instância é feita com base no melhor esforço, mesmo quando a instância tem créditos disponíveis, já que a largura de banda expansível é um recurso compartilhado.

Existem buckets de crédito de E/S de rede separados para o tráfego de entrada e de saída.

Performance de rede base e intermitente

O Guia de tipos de instância do Amazon EC2 descreve a performance de rede para cada tipo de instância, além de fornecer a largura de banda da rede de linha de base disponível para as instâncias que podem usar a largura de banda intermitente. Para saber mais, consulte:

- Network specifications: General purpose
- Network specifications: Compute optimized
- Network specifications: Memory optimized
- Network specifications: Storage optimized
- Network specifications: Accelerated computing
- Network specifications: High-performance computing
- Network specifications: Previous generation

Como alternativa, você pode usar uma ferramenta de linha de comandos para obter essas informações. O console do Amazon EC2 não exibe a largura de banda da rede de referência de um tipo de instância.

AWS CLI

É possível usar o comando describe-instance-types para exibir informações sobre um tipo de instância. O exemplo a seguir exibe as informações de performance de redes para todas as instâncias C5.

```
aws ec2 describe-instance-types \
    --filters "Name=instance-type,Values=c5.*" \
    --query "InstanceTypes[].[InstanceType, NetworkInfo.NetworkPerformance,
 NetworkInfo.NetworkCards[0].BaselineBandwidthInGbps] | sort_by(@,&[2])" \
    --output table
```

O seguinte é um exemplo de saída. Se sua saída não tiver a largura de linha de base, atualize para a versão mais recente do AWS CLI.

```
-----------------------------------------------
|           DescribeInstanceTypes             |
+--------------+--------------------+-------+
|  c5.large    |  Up to 10 Gigabit  |  0.75 |
|  c5.xlarge   |  Up to 10 Gigabit  |  1.25 |
|  c5.2xlarge  |  Up to 10 Gigabit  |  2.5  |
|  c5.4xlarge  |  Up to 10 Gigabit  |  5.0  |
|  c5.9xlarge  |  12 Gigabit        |  12.0 |
|  c5.12xlarge |  12 Gigabit        |  12.0 |
|  c5.18xlarge |  25 Gigabit        |  25.0 |
|  c5.24xlarge |  25 Gigabit        |  25.0 |
|  c5.metal    |  25 Gigabit        |  25.0 |
+--------------+--------------------+-------+
```

PowerShell

É possível usar o comando Get-EC2InstanceType do PowerShell para exibir informações sobre um tipo de instância. O exemplo a seguir exibe as informações de performance de redes para todas as instâncias C5.

```
Get-EC2InstanceType -Filter @{Name = "instance-type"; Values = "c5.*" } | `
    Select-Object `
    InstanceType,
    @{Name = 'NetworkPerformance'; Expression =
 {($_.Networkinfo.NetworkCards.NetworkPerformance)}},
    @{Name = 'BaselineBandwidthInGbps'; Expression =
 {($_.Networkinfo.NetworkCards.BaselineBandwidthInGbps)}} | `
Format-Table -AutoSize
```

O seguinte é um exemplo de saída.

```
InstanceType NetworkPerformance BaselineBandwidthInGbps
```

```
------------ ------------------ ----------------------
c5.4xlarge   Up to 10 Gigabit                    5.00
c5.xlarge    Up to 10 Gigabit                    1.25
c5.12xlarge  12 Gigabit                         12.00
c5.9xlarge   12 Gigabit                         12.00
c5.24xlarge  25 Gigabit                         25.00
c5.metal     25 Gigabit                         25.00
c5.2xlarge   Up to 10 Gigabit                    2.50
c5.large     Up to 10 Gigabit                    0.75
c5.18xlarge  25 Gigabit                         25.00
```

Configuração de ponderação de largura de banda de instâncias do EC2

Alguns tipos de instância oferecem suporte à ponderação de largura de banda configurável, na qual é possível selecionar uma ponderação de largura de banda de linha de base que favoreça o processamento da rede ou as operações do EBS. As configurações padrão da largura de banda de linha de base são determinadas pelo tipo de instância. É possível configurar a ponderação da largura de banda durante a inicialização ou modificar as configurações da instância com as preferências de ponderação a seguir:

- padrão: esta opção usa a configuração de largura de banda padrão para seu tipo de instância.
- vpc-1: esta opção aumenta a largura de banda de linha de base disponível para rede e diminui a largura de banda de linha de base para operações do EBS.
- ebs-1: esta opção aumenta a largura de banda de linha de base disponível para operações do EBS e diminui a largura de banda de linha de base para operações de rede.

Considerações sobre a ponderação de largura de banda

A seguir estão algumas considerações que podem afetar sua estratégia de ponderação de largura de banda.

- A definição de preferências de ponderação da largura de banda afeta somente as especificações de largura de banda. As especificações de pacotes de rede por segundo (PPS) e operações de entrada e saída por segundo (IOPS) do EBS não mudam.
- A especificação de largura de banda combinada entre a rede e o EBS não muda. Quando você seleciona uma configuração de ponderação de largura de banda, a largura de banda de linha de base disponível para a opção selecionada aumenta, e a largura de banda de linha de base para a opção restante é reduzida na mesma quantidade absoluta. Para todas as instâncias, exceto as

instâncias Flex, a largura de banda de pico disponível permanece a mesma para a opção que você selecionou e é reduzida para a opção restante. Para instâncias Flex até 4xlarge, a largura de banda de pico permanece inalterada. Para instâncias Flex 8xlarge e maiores, a largura de banda de pico aumenta na mesma proporção que a largura de banda básica.

- É importante entender como as mudanças na alocação de largura de banda podem afetar a performance de E/S do EBS. Para instâncias do EC2 que tenham configuração `vpc-1` (maior largura de banda de rede), é possível experimentar IOPS mais baixos para volumes do EBS se atingir o limite de largura de banda do EBS antes de atingir o limite de IOPS. Isso é mais perceptível com tamanhos maiores de E/S.

  Por exemplo, em um tipo de instância que normalmente oferece suporte a 240.000 IOPS com tamanho de E/S de 16 KiB, se você selecionar a ponderação `vpc-1`, isso poderá reduzir o IOPS alcançável devido ao limite ajustado de largura de banda da linha de base do EBS.

  Ao planejar sua workload, considere o tamanho e os padrões de E/S. Tamanhos menores de E/S têm menos probabilidade de serem afetados pelas limitações de largura de banda, enquanto tamanhos maiores de E/S ou workloads sequenciais podem sofrer mais impacto das mudanças na largura de banda. Sempre teste sua workload específica para garantir a performance ideal com a configuração escolhida.
- A especificação de largura de banda de vários fluxos de rede para tráfego que passa por um gateway da Internet ou por um gateway local é ajustada para 50% da largura de banda da linha de base da opção configurada ou para 5 Gbps, quando aplicável. Para obter mais informações, consulte Largura de banda de rede de instâncias do Amazon EC2.

  O exemplo a seguir é baseado em um tipo de instância que tem uma largura de banda de linha de base padrão de 40 Gbps e uma largura de banda de borda padrão de 20 Gbps. Se você escolher a ponderação de largura de banda `vpc-1` para essa instância, a largura de banda da linha de base ponderada mudará para 50 Gbps e a largura de banda da borda mudará para 25 Gbps.
- Esse atributo está disponível em todas as regiões comerciais, alinhado com a disponibilidade e o suporte de instâncias do EC2.
- Esse atributo não adiciona custo extra à sua instância EC2.

Tipos de instância com suporte para ponderação de largura de banda

Os tipos de instância nas seguintes famílias de instâncias suportam ponderação de largura de banda configurável.

- Uso geral: M8a, M8g, M8gd, M8i, M8id, M8i-flex
- Otimizadas para computação: C8a, C8g, C8gd, C8i, C8id, C8i-flex
- Otimizadas para memória: R8a, R8g, R8gd, R8i, R8id, R8i-flex, X8g, X8aedz, X8i

Verificar as configurações atuais de largura de banda

Para ver as configurações atuais de largura de banda da sua instância, selecione uma das guias para obter instruções.

Console

Para obter a configuração de largura de banda 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 que você deseja verificar na lista e navegue até a guia Rede. Sua configuração atual é exibida no campo Largura de banda configurada. O Amazon EC2 usará configurações padrão para seu tipo de instância se a largura de banda não estiver definida para um valor específico.

AWS CLI

Para obter a configuração de largura de banda de uma instância

Use o comando describe-instances.

```
aws ec2 describe-instances \
    --instance-ids i-1234567890abcdef0 \
    --query Reservations[].Instances[].NetworkPerformanceOptions.BandwidthWeighting
 \
    --output text
```

O seguinte é um exemplo de saída.

```
default
```

Este exemplo lista todas as instâncias que têm a preferência de ponderação de largura de banda definida como `vpc-1`, para maior largura de banda da rede.

```
aws ec2 describe-instances \
    --filters "Name=network-performance-options.bandwidth-weighting,Values=vpc-1" \
    --query Reservations[].Instances[].InstanceId \
    --output text
```

PowerShell

Para obter a configuração de largura de banda de uma instância

Use o cmdlet Get-EC2Instance.

```
(Get-EC2Instance `
    -
InstanceId i-1234567890abcdef0).Instances.NetworkPerformanceOptions.BandwidthWeighting.Value
```

O seguinte é um exemplo de saída.

```
default
```

Este exemplo lista todas as instâncias que têm a preferência de ponderação de largura de banda definida como `vpc-1`, para maior largura de banda da rede.

```
(Get-EC2Instance `
    -Filter @{Name="network-performance-options.bandwidth-
weighting";Values="vpc-1"}).Instances.InstanceId
```

Configurar a ponderação de largura de banda para a sua instância

É possível configurar a ponderação da largura de banda na execução, ou modificando as instâncias existentes a partir do console do EC2, de API/SDKs ou da CLI.

Configurar a ponderação da largura de banda ao executar uma instância

Para configurar as definições de largura de banda ao executar uma instância, selecione uma das guias para obter instruções.

Você também pode especificar a ponderação de largura de banda em um modelo de execução. Para criar um modelo de execução, consulte Criar um modelo de execução do Amazon EC2. O parâmetro

a ser definido está no mesmo local em que está para a execução de uma instância diretamente do console. Expanda a seção Detalhes avançados e defina a Configuração de largura de banda da instância.

Para iniciar uma instância com seu modelo de execução, consulte Executar instâncias do Ec2 usando um modelo de execução.

Console

Para inicializar uma instância com ponderação configurável de largura de banda

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione Iniciar instâncias. A página Executar uma instância se abrirá. Há várias outras maneiras de acessar a caixa de diálogo de inicialização, dependendo de sua preferência. Por exemplo, é possível executar uma instância diretamente de uma AMI ou do próprio painel do Amazon EC2.
4. A imagem de máquina da Amazon (AMI) a partir da qual você executa deve ser baseada na arquitetura `Arm`. Muitas imagens de Início rápido são compatíveis com as arquiteturas `x86` e `Arm`. Depois de escolher o sistema operacional da instância, selecione a opção `Arm` na lista Arquitetura.
5. O tipo de instância deve ser um dos Tipos de instâncias compatíveis para este recurso.
6. Ao expandir a seção Detalhes avançados, é possível rolar para baixo para encontrar as configurações de Configuração de largura de banda da instância. Selecione a opção de configuração de largura de banda para sua instância.
7. Defina todas as outras configurações da sua instância como faria normalmente e escolha Iniciar instância.

AWS CLI

Para inicializar uma instância com ponderação configurável de largura de banda

Use o comando run-instances com a opção a seguir para inicializar instâncias configuradas para maior ponderação da largura de banda da rede.

```
--network-performance-options BandwidthWeighting=vpc-1
```

Use o comando run-instances com a opção a seguir para inicializar instâncias configuradas para maior ponderação da largura de banda do EBS.

```
--network-performance-options BandwidthWeighting=ebs-1
```

PowerShell

Para inicializar uma instância com ponderação configurável de largura de banda

Use o cmdlet New-EC2Instance com o parâmetro a seguir para inicializar instâncias configuradas para maior ponderação da largura de banda da rede.

```
-NetworkPerformanceOptions_BandwidthWeighting vpc-1
```

Use o cmdlet New-EC2Instance com o parâmetro a seguir para inicializar instâncias configuradas para maior ponderação da largura de banda do EBC.

```
-NetworkPerformanceOptions_BandwidthWeighting ebs-1
```

Atualizar a ponderação da largura de banda para uma instância existente

Para atualizar a ponderação da largura de banda de uma instância existente, sua instância deve estar no estado `Stopped`.

Console

Para atualizar a ponderação de largura de banda

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância que você deseja atualizar na lista.
4. Antes de alterar a configuração da largura de banda, sua instância deve estar no estado `Stopped`. Se sua instância estiver em execução, selecione Interromper instância no menu Estado da instância.
5. Escolha Gerenciar largura de banda no menu Ações > Rede. Isso abrirá a caixa de diálogo Gerenciar largura de banda.

> **Note**
>
> Se seu tipo de instância não oferecer suporte à configuração para ponderação de largura de banda, esse item de menu será desabilitado.

6. Selecione a opção para atualizar sua instância e escolha Alterar para salvar suas configurações.

AWS CLI

Para atualizar a ponderação de largura de banda

Use o comando modify-instance-network-performance-options para configurar uma maior ponderação da largura de banda da rede para a instância especificada.

```
aws ec2 modify-instance-network-performance-options \
    --instance-id i-1234567890abcdef0 \
    --bandwidth-weighting=vpc-1
```

O exemplo a seguir configura uma maior ponderação da largura de banda de EBS para a instância especificada.

```
aws ec2 modify-instance-network-performance-options \
    --instance-id i-1234567890abcdef0 \
    --bandwidth-weighting=ebs-1
```

PowerShell

Para atualizar a ponderação de largura de banda

Use o cmdlet Edit-EC2InstanceNetworkPerformanceOption para configurar uma maior ponderação da largura de banda da rede para a instância especificada.

```
Edit-EC2InstanceNetworkPerformanceOption `
    -InstanceId i-1234567890abcdef0 `
    -BandwidthWeighting vpc-1
```

O exemplo a seguir configura uma maior ponderação da largura de banda de EBS para a instância especificada.

```
Edit-EC2InstanceNetworkPerformanceOption `
    -InstanceId i-1234567890abcdef0 `
    -BandwidthWeighting ebs-1
```

Performance de rede

A tabela a seguir mostra a performance de rede em Gbps, que pode ser alcançada com as configurações `default`, `vpc-1` e `ebs-1`.

Tipo de instância	**`default`** (Linha de base/expansão)	**`vpc-1`** (Linha de base/expansão)	**`ebs-1`** (Linha de base/expansão)
c8a.medium	0,52 / 12,5	0,65 / 12,5	0,438 / 10,0
c8a.large	0.937/12.5	1.172/12.5	0.774/10.0
c8a.xlarge	1.875/12.5	2.344/12.5	1.562/10.0
c8a.2xlarge	3.75/15.0	4.688/15.0	3.125/12.5
c8a.4xlarge	7.5/15.0	9.375/15.0	6.25/12.5
c8a.8xlarge	15.0	18.75	12,5
c8a.12xlarge	22.5	28.125	18.75
c8a.16xlarge	30.0	37.5	25.0
c8a.24xlarge	40.0	50.0	32.5
c8a.48xlarge	75.0	93,75	60.0
c8a.metal-24xl	40.0	50.0	32.5
c8a.metal-48xl	75.0	93,75	60.0
c8g.medium	0,52 / 12,5	0,65 / 12,5	0.441/10.0

Tipo de instância	**default** (Linha de base/expansão)	**vpc-1** (Linha de base/expansão)	**ebs-1** (Linha de base/expansão)
c8g.large	0.937/12.5	1.171/12.5	0.779/10.0
c8g.xlarge	1.875/12.5	2.344/12.5	1.562/10.0
c8g.2xlarge	3.75/15.0	4.688/15.0	3.125/12.5
c8g.4xlarge	7.5/15.0	9.375/15.0	6.25/12.5
c8g.8xlarge	15.0	18.75	12,5
c8g.12xlarge	22.5	28.125	18.75
c8g.16xlarge	30.0	37.5	25.0
c8g.24xlarge	40.0	50.0	32.5
c8g.48xlarge	50.0	62.5	40.0
c8g.metal-24xl	40.0	50.0	32.5
c8g.metal-48xl	50.0	62.5	40.0
c8gd.medium	0,52 / 12,5	0,65 / 12,5	0.441/10.0
c8gd.large	0.937/12.5	1.171/12.5	0.779/10.0
c8gd.xlarge	1.875/12.5	2.344/12.5	1.562/10.0
c8gd.2xlarge	3.75/15.0	4.688/15.0	3.125/12.5
c8gd.4xlarge	7.5/15.0	9.375/15.0	6.25/12.5
c8gd.8xlarge	15.0	18.75	12,5
c8gd.12xlarge	22.5	28.125	18.75

Tipo de instância	**default** (Linha de base/expansão)	**vpc-1** (Linha de base/expansão)	**ebs-1** (Linha de base/expansão)
c8gd.16xlarge	30.0	37.5	25.0
c8gd.24xlarge	40.0	50.0	32.5
c8gd.48xlarge	50.0	62.5	40.0
c8gd.metal-24xl	40.0	50.0	32.5
c8gd.metal-48xl	50.0	62.5	40.0
c8i.large	0.937/12.5	1.172/12.5	0.774/10.0
c8i.xlarge	1.875/12.5	2.344/12.5	1.562/10.0
c8i.2xlarge	3.75/15.0	4.688/15.0	3.125/12.5
c8i.4xlarge	7.5/15.0	9.375/15.0	6.25/12.5
c8i.8xlarge	15.0	18.75	12,5
c8i.12xlarge	22.5	28.125	18.75
c8i.16xlarge	30.0	37.5	25.0
c8i.24xlarge	40.0	50.0	32.5
c8i.32xlarge	50.0	62.5	40.0
c8i.48xlarge	75.0	93,75	60.0
c8i.96xlarge	100.0	125.0	80.0
c8i.metal-48xl	75.0	93,75	60.0
c8i.metal-96xl	100.0	125.0	80.0

Tipo de instância	**default** (Linha de base/expansão)	**vpc-1** (Linha de base/expansão)	**ebs-1** (Linha de base/expansão)
c8id.large	0.937/12.5	1.172/12.5	0.774/10.0
c8id.xlarge	1.875/12.5	2.344/12.5	1.562/10.0
c8id.2xlarge	3.75/15.0	4.688/15.0	3.125/12.5
c8id.4xlarge	7.5/15.0	9.375/15.0	6.25/12.5
c8id.8xlarge	15.0	18.75	12,5
c8id.12xlarge	22.5	28.125	18.75
c8id.16xlarge	30.0	37.5	25.0
c8id.24xlarge	40.0	50.0	32.5
c8id.32xlarge	50.0	62.5	40.0
c8id.48xlarge	75.0	93,75	60.0
c8id.96xlarge	100.0	125.0	80.0
c8id.metal-48xl	75.0	93,75	60.0
c8id.metal-96xl	100.0	125.0	80.0
c8i-flex.large	0.468/12.5	0.585/12.5	0.389/10.0
c8i-flex.xlarge	0.937/12.5	1.172/12.5	0.779/10.0
c8i-flex.2xlarge	1.875/15.0	2.344/15.0	1.562/12.5
c8i-flex.4xlarge	3.75/15.0	4.688/15.0	3.125/12.5
c8i-flex.8xlarge	7.5/15.0	9.375/18.75	6.25/12.5

Tipo de instância	**default** (Linha de base/expansão)	**vpc-1** (Linha de base/expansão)	**ebs-1** (Linha de base/expansão)
c8i-flex.12xlarge	11.25/22.5	14.063/28.125	9.375/18.75
c8i-flex.16xlarge	15.0/30.0	18.75/37.5	12.5/25.0
m8a.medium	0,52 / 12,5	0,65 / 12,5	0,438 / 10,0
m8a.large	0.937/12.5	1.172/12.5	0.774/10.0
m8a.xlarge	1.875/12.5	2.344/12.5	1.562/10.0
m8a.2xlarge	3.75/15.0	4.688/15.0	3.125/12.5
m8a.4xlarge	7.5/15.0	9.375/15.0	6.25/12.5
m8a.8xlarge	15.0	18.75	12,5
m8a.12xlarge	22.5	28.125	18.75
m8a.16xlarge	30.0	37.5	25.0
m8a.24xlarge	40.0	50.0	32.5
m8a.48xlarge	75.0	93,75	60.0
m8a.metal-24xl	40.0	50.0	32.5
m8a.metal-48xl	75.0	93,75	60.0
m8g.medium	0,52 / 12,5	0,65 / 12,5	0.441/10.0
m8g.large	0.937/12.5	1.171/12.5	0.779/10.0
m8g.xlarge	1.875/12.5	2.344/12.5	1.562/10.0
m8g.2xlarge	3.75/15.0	4.688/15.0	3.125/12.5

Tipo de instância	**default** (Linha de base/expansão)	**vpc-1** (Linha de base/expansão)	**ebs-1** (Linha de base/expansão)
m8g.4xlarge	7.5/15.0	9.375/15.0	6.25/12.5
m8g.8xlarge	15.0	18.75	12,5
m8g.12xlarge	22.5	28.125	18.75
m8g.16xlarge	30.0	37.5	25.0
m8g.24xlarge	40.0	50.0	32.5
m8g.48xlarge	50.0	62.5	40.0
m8g.metal-24xl	40.0	50.0	32.5
m8g.metal-48xl	50.0	62.5	40.0
m8gd.medium	0,52 / 12,5	0,65 / 12,5	0.441/10.0
m8gd.large	0.937/12.5	1.171/12.5	0.779/10.0
m8gd.xlarge	1.875/12.5	2.344/12.5	1.562/10.0
m8gd.2xlarge	3.75/15.0	4.688/15.0	3.125/12.5
m8gd.4xlarge	7.5/15.0	9.375/15.0	6.25/12.5
m8gd.8xlarge	15.0	18.75	12,5
m8gd.12xlarge	22.5	28.125	18.75
m8gd.16xlarge	30.0	37.5	25.0
m8gd.24xlarge	40.0	50.0	32.5
m8gd.48xlarge	50.0	62.5	40.0

Tipo de instância	**default** (Linha de base/expansão)	**vpc-1** (Linha de base/expansão)	**ebs-1** (Linha de base/expansão)
m8gd.metal-24xl	40.0	50.0	32.5
m8gd.metal-48xl	50.0	62.5	40.0
m8i.large	0.937/12.5	1.172/12.5	0.774/10.0
m8i.xlarge	1.875/12.5	2.344/12.5	1.562/10.0
m8i.2xlarge	3.75/15.0	4.688/15.0	3.125/12.5
m8i.4xlarge	7.5/15.0	9.375/15.0	6.25/12.5
m8i.8xlarge	15.0	18.75	12,5
m8i.12xlarge	22.5	28.125	18.75
m8i.16xlarge	30.0	37.5	25.0
m8i.24xlarge	40.0	50.0	32.5
m8i.32xlarge	50.0	62.5	40.0
m8i.48xlarge	75.0	93,75	60.0
m8i.96xlarge	100.0	125.0	80.0
m8i.metal-48xl	75.0	93,75	60.0
m8i.metal-96xl	100.0	125.0	80.0
m8id.large	0.937/12.5	1.172/12.5	0.774/10.0
m8id.xlarge	1.875/12.5	2.344/12.5	1.562/10.0
m8id.2xlarge	3.75/15.0	4.688/15.0	3.125/12.5

Tipo de instância	**default** (Linha de base/expansão)	**vpc-1** (Linha de base/expansão)	**ebs-1** (Linha de base/expansão)
m8id.4xlarge	7.5/15.0	9.375/15.0	6.25/12.5
m8id.8xlarge	15.0	18.75	12,5
m8id.12xlarge	22.5	28.125	18.75
m8id.16xlarge	30.0	37.5	25.0
m8id.24xlarge	40.0	50.0	32.5
m8id.32xlarge	50.0	62.5	40.0
m8id.48xlarge	75.0	93,75	60.0
m8id.96xlarge	100.0	125.0	80.0
m8id.metal-48xl	75.0	93,75	60.0
m8id.metal-96xl	100.0	125.0	80.0
m8i-flex.large	0.468/12.5	0.585/12.5	0.389/10.0
m8i-flex.xlarge	0.937/12.5	1.172/12.5	0.779/10.0
m8i-flex.2xlarge	1.875/15.0	2.344/15.0	1.562/12.5
m8i-flex.4xlarge	3.75/15.0	4.688/15.0	3.125/12.5
m8i-flex.8xlarge	7.5/15.0	9.375/18.75	6.25/12.5
m8i-flex.12xlarge	11.25/22.5	14.063/28.125	9.375/18.75
m8i-flex.16xlarge	15.0/30.0	18.75/37.5	12.5/25.0
r8a.medium	0,52 / 12,5	0,65 / 12,5	0,438 / 10,0

Tipo de instância	**default** (Linha de base/expansão)	**vpc-1** (Linha de base/expansão)	**ebs-1** (Linha de base/expansão)
r8a.large	0.937/12.5	1.172/12.5	0.774/10.0
r8a.xlarge	1.875/12.5	2.344/12.5	1.562/10.0
r8a.2xlarge	3.75/15.0	4.688/15.0	3.125/12.5
r8a.4xlarge	7.5/15.0	9.375/15.0	6.25/12.5
r8a.8xlarge	15.0	18.75	12,5
r8a.12xlarge	22.5	28.125	18.75
r8a.16xlarge	30.0	37.5	25.0
r8a.24xlarge	40.0	50.0	32.5
r8a.48xlarge	75.0	93,75	60.0
m8a.metal-24xl	40.0	50.0	32.5
m8a.metal-48xl	75.0	93,75	60.0
r8g.medium	0,52 / 12,5	0,65 / 12,5	0.441/10.0
r8g.large	0.937/12.5	1.171/12.5	0.779/10.0
r8g.xlarge	1.875/12.5	2.344/12.5	1.562/10.0
r8g.2xlarge	3.75/15.0	4.688/15.0	3.125/12.5
r8g.4xlarge	7.5/15.0	9.375/15.0	6.25/12.5
r8g.8xlarge	15.0	18.75	12,5
r8g.12xlarge	22.5	28.125	18.75

Tipo de instância	**default** (Linha de base/expansão)	**vpc-1** (Linha de base/expansão)	**ebs-1** (Linha de base/expansão)
r8g.16xlarge	30.0	37.5	25.0
r8g.24xlarge	40.0	50.0	32.5
r8g.48xlarge	50.0	62.5	40.0
r8g.metal-24xl	40.0	50.0	32.5
r8g.metal-48xl	50.0	62.5	40.0
r8gd.medium	0,52 / 12,5	0,65 / 12,5	0.441/10.0
r8gd.large	0.937/12.5	1.171/12.5	0.779/10.0
r8gd.xlarge	1.875/12.5	2.344/12.5	1.562/10.0
r8gd.2xlarge	3.75/15.0	4.688/15.0	3.125/12.5
r8gd.4xlarge	7.5/15.0	9.375/15.0	6.25/12.5
r8gd.8xlarge	15.0	18.75	12,5
r8gd.12xlarge	22.5	28.125	18.75
r8gd.16xlarge	30.0	37.5	25.0
r8gd.24xlarge	40.0	50.0	32.5
r8gd.48xlarge	50.0	62.5	40.0
r8gd.metal-24xl	40.0	50.0	32.5
r8gd.metal-48xl	50.0	62.5	40.0
r8i.large	0.937/12.5	1.172/12.5	0.774/10.0

Tipo de instância	**default** (Linha de base/expansão)	**vpc-1** (Linha de base/expansão)	**ebs-1** (Linha de base/expansão)
r8i.xlarge	1.875/12.5	2.344/12.5	1.562/10.0
r8i.2xlarge	3.75/15.0	4.688/15.0	3.125/12.5
r8i.4xlarge	7.5/15.0	9.375/15.0	6.25/12.5
r8i.8xlarge	15.0	18.75	12,5
r8i.12xlarge	22.5	28.125	18.75
r8i.16xlarge	30.0	37.5	25.0
r8i.24xlarge	40.0	50.0	32.5
r8i.32xlarge	50.0	62.5	40.0
r8i.48xlarge	75.0	93,75	60.0
r8i.96xlarge	100.0	125.0	80.0
r8i.metal-48xl	75.0	93,75	60.0
r8i.metal-96xl	100.0	125.0	80.0
r8id.large	0.937/12.5	1.172/12.5	0.774/10.0
r8id.xlarge	1.875/12.5	2.344/12.5	1.562/10.0
r8id.2xlarge	3.75/15.0	4.688/15.0	3.125/12.5
r8id.4xlarge	7.5/15.0	9.375/15.0	6.25/12.5
r8id.8xlarge	15.0	18.75	12,5
r8id.12xlarge	22.5	28.125	18.75

Tipo de instância	**default** (Linha de base/expansão)	**vpc-1** (Linha de base/expansão)	**ebs-1** (Linha de base/expansão)
r8id.16xlarge	30.0	37.5	25.0
r8id.24xlarge	40.0	50.0	32.5
r8id.32xlarge	50.0	62.5	40.0
r8id.48xlarge	75.0	93,75	60.0
r8id.96xlarge	100.0	125.0	80.0
r8id.metal-48xl	75.0	93,75	60.0
r8id.metal-96xl	100.0	125.0	80.0
r8i-flex.large	0.468/12.5	0.585/12.5	0.389/10.0
r8i-flex.xlarge	0.937/12.5	1.172/12.5	0.779/10.0
r8i-flex.2xlarge	1.875/15.0	2.344/15.0	1.562/12.5
r8i-flex.4xlarge	3.75/15.0	4.688/15.0	3.125/12.5
r8i-flex.8xlarge	7.5/15.0	9.375/18.75	6.25/12.5
r8i-flex.12xlarge	11.25/22.5	14.063/28.125	9.375/18.75
r8i-flex.16xlarge	15.0/30.0	18.75/37.5	12.5/25.0
x8g.medium	0,52 / 12,5	0,65 / 12,5	0.441/10.0
x8g.large	0.937/12.5	1.171/12.5	0.779/10.0
x8g.xlarge	1.875/12.5	2.344/12.5	1.562/10.0
x8g.2xlarge	3.75/15.0	4.688/15.0	3.125/12.5

Tipo de instância	**default** (Linha de base/expansão)	**vpc-1** (Linha de base/expansão)	**ebs-1** (Linha de base/expansão)
x8g.4xlarge	7.5/15.0	9.375/15.0	6.25/12.5
x8g.8xlarge	15.0	18.75	12,5
x8g.12xlarge	22.5	28.125	18.75
x8g.16xlarge	30.0	37.5	25.0
x8g.24xlarge	40.0	50.0	32.5
x8g.48xlarge	50.0	62.5	40.0
x8g.metal-24xl	40.0	50.0	32.5
x8g.metal-48xl	50.0	62.5	40.0
x8aedz.large	1,562 / 18,75	1,953 / 18,75	1,249 / 15,0
x8aedz.xlarge	3,125 / 18,75	3,907 / 18,75	2,5 / 15,0
x8aedz.3xlarge	9.375/18.75	11,719 / 18,75	7.5/15.0
x8aedz.6xlarge	18.75	23.438	15.0
x8aedz.12xlarge	37.5	46.875	30.0
x8aedz.24xlarge	75.0	93,75	60.0
x8aedz.metal-12xl	37.5	46.875	30.0
x8aedz.metal-24xl	75.0	93,75	60.0
x8i.large	0.937/12.5	1.172/12.5	0.774/10.0
x8i.xlarge	1.875/12.5	2.344/12.5	1.562/10.0

Tipo de instância	**`default`** (Linha de base/expansão)	**`vpc-1`** (Linha de base/expansão)	**`ebs-1`** (Linha de base/expansão)
x8i.2xlarge	3.75/15.0	4.688/15.0	3.125/12.5
x8i.4xlarge	7.5/15.0	9.375/15.0	6.25/12.5
x8i.8xlarge	15.0	18.75	12,5
x8i.12xlarge	22.5	28.125	18.75
x8i.16xlarge	30.0	37.5	25.0
x8i.24xlarge	40.0	50.0	32.5
x8i.32xlarge	50.0	62.5	40.0
x8i.48xlarge	75.0	93,75	60.0
x8i.64xlarge	80.0	100.0	62.5
x8i.96xlarge	100.0	125.0	80.0
x8i.metal-48xl	75.0	93,75	60.0
x8i.metal-96xl	100.0	125.0	80.0

Performance do Amazon EBS

A tabela a seguir mostra a performance do Amazon EBS em Gbps, que pode ser alcançada com as configurações `default`, `vpc-1` e `ebs-1`.

Tipo de instância	**default** (Linha de base/expansão)	**vpc-1** (Linha de base/expansão)	**ebs-1** (Linha de base/expansão)
c8a.medium	0,325 / 10,0	0,195 / 6,25	0,407 / 10,0
c8a.large	0.65/10.0	0.415/6.25	0.813/10.0
c8a.xlarge	1.25/10.0	0.781/6.25	1.563/10.0
c8a.2xlarge	2.5/10.0	1.562/6.25	3.125/10.0
c8a.4xlarge	5.0/10.0	3.125/6.25	6.25/10.0
c8a.8xlarge	10.0	6.25	12,5
c8a.12xlarge	15.0	9.375	18.75
c8a.16xlarge	20.0	12,5	25.0
c8a.24xlarge	30.0	20.0	37.5
c8a.48xlarge	60.0	41.25	75.0
c8a.metal-24xl	30.0	20.0	37.5
c8a.metal-48xl	60.0	41.25	75.0
c8g.medium	0.315/10.0	0.185/6.25	0.394/10.0
c8g.large	0.63/10.0	0.396/6.25	0.788/10.0
c8g.xlarge	1.25/10.0	0.781/6.25	1.563/10.0
c8g.2xlarge	2.5/10.0	1.562/6.25	3.125/10.0
c8g.4xlarge	5.0/10.0	3.125/6.25	6.25/10.0
c8g.8xlarge	10.0	6.25	12,5

Tipo de instância	**default** (Linha de base/expansão)	**vpc-1** (Linha de base/expansão)	**ebs-1** (Linha de base/expansão)
c8g.12xlarge	15.0	9.375	18.75
c8g.16xlarge	20.0	12,5	25.0
c8g.24xlarge	30.0	20.0	37.5
c8g.48xlarge	40.0	27.5	50.0
c8g.metal-24xl	30.0	20.0	37.5
c8g.metal-48xl	40.0	27.5	50.0
c8gd.medium	0.315/10.0	0.185/6.25	0.394/10.0
c8gd.large	0.63/10.0	0.396/6.25	0.788/10.0
c8gd.xlarge	1.25/10.0	0.781/6.25	1.563/10.0
c8gd.2xlarge	2.5/10.0	1.562/6.25	3.125/10.0
c8gd.4xlarge	5.0/10.0	3.125/6.25	6.25/10.0
c8gd.8xlarge	10.0	6.25	12,5
c8gd.12xlarge	15.0	9.375	18.75
c8gd.16xlarge	20.0	12,5	25.0
c8gd.24xlarge	30.0	20.0	37.5
c8gd.48xlarge	40.0	27.5	50.0
c8gd.metal-24xl	30.0	20.0	37.5
c8gd.metal-48xl	40.0	27.5	50.0

Tipo de instância	**default** (Linha de base/expansão)	**vpc-1** (Linha de base/expansão)	**ebs-1** (Linha de base/expansão)
c8i.large	0.65/10.0	0.415/6.25	0.813/10.0
c8i.xlarge	1.25/10.0	0.781/6.25	1.563/10.0
c8i.2xlarge	2.5/10.0	1.562/6.25	3.125/10.0
c8i.4xlarge	5.0/10.0	3.125/6.25	6.25/10.0
c8i.8xlarge	10.0	6.25	12,5
c8i.12xlarge	15.0	9.375	18.75
c8i.16xlarge	20.0	12,5	25.0
c8i.24xlarge	30.0	20.0	37.5
c8i.32xlarge	40.0	27.5	50.0
c8i.48xlarge	60.0	41.25	75.0
c8i.96xlarge	80.0	55.0	100.0
c8i.metal-48xl	60.0	41.25	75.0
c8i.metal-96xl	80.0	55.0	100.0
c8id.large	0.65/10.0	0.415/6.25	0.813/10.0
c8id.xlarge	1.25/10.0	0.781/6.25	1.563/10.0
c8id.2xlarge	2.5/10.0	1.562/6.25	3.125/10.0
c8id.4xlarge	5.0/10.0	3.125/6.25	6.25/10.0
c8id.8xlarge	10.0	6.25	12,5

Tipo de instância	**default** (Linha de base/expansão)	**vpc-1** (Linha de base/expansão)	**ebs-1** (Linha de base/expansão)
c8id.12xlarge	15.0	9.375	18.75
c8id.16xlarge	20.0	12,5	25.0
c8id.24xlarge	30.0	20.0	37.5
c8id.32xlarge	40.0	27.5	50.0
c8id.48xlarge	60.0	41.25	75.0
c8id.96xlarge	80.0	55.0	100.0
c8id.metal-48xl	60.0	41.25	75.0
c8id.metal-96xl	80.0	55.0	100.0
c8i-flex.large	0.315/10.0	0.198/6.25	0.394/10.0
c8i-flex.xlarge	0.63/10.0	0.395/6.25	0.788/10.0
c8i-flex.2xlarge	1.25/10.0	0.781/6.25	1.563/10.0
c8i-flex.4xlarge	2.5/10.0	1.562/6.25	3.125/10.0
c8i-flex.8xlarge	5.0/10.0	3.125/6.25	6.25/12.5
c8i-flex.12xlarge	7.5/15.0	4.687/9.375	9.375/18.75
c8i-flex.16xlarge	10.0/20.0	6.25/12.5	12.5/25.0
m8a.medium	0,325 / 10,0	0,195 / 6,25	0,407 / 10,0
m8a.large	0.65/10.0	0.415/6.25	0.813/10.0
m8a.xlarge	1.25/10.0	0.781/6.25	1.563/10.0

Tipo de instância	**default** (Linha de base/expansão)	**vpc-1** (Linha de base/expansão)	**ebs-1** (Linha de base/expansão)
m8a.2xlarge	2.5/10.0	1.562/6.25	3.125/10.0
m8a.4xlarge	5.0/10.0	3.125/6.25	6.25/10.0
m8a.8xlarge	10.0	6.25	12,5
m8a.12xlarge	15.0	9.375	18.75
m8a.16xlarge	20.0	12,5	25.0
m8a.24xlarge	30.0	20.0	37.5
m8a.48xlarge	60.0	41.25	75.0
m8a.metal-24xl	30.0	20.0	37.5
m8a.metal-48xl	60.0	41.25	75.0
m8g.medium	0.315/10.0	0.185/6.25	0.394/10.0
m8g.large	0.63/10.0	0.396/6.25	0.788/10.0
m8g.xlarge	1.25/10.0	0.781/6.25	1.563/10.0
m8g.2xlarge	2.5/10.0	1.562/6.25	3.125/10.0
m8g.4xlarge	5.0/10.0	3.125/6.25	6.25/10.0
m8g.8xlarge	10.0	6.25	12,5
m8g.12xlarge	15.0	9.375	18.75
m8g.16xlarge	20.0	12,5	25.0
m8g.24xlarge	30.0	20.0	37.5

Tipo de instância	**default** (Linha de base/expansão)	**vpc-1** (Linha de base/expansão)	**ebs-1** (Linha de base/expansão)
m8g.48xlarge	40.0	27.5	50.0
m8g.metal-24xl	30.0	20.0	37.5
m8g.metal-48xl	40.0	27.5	50.0
m8gd.medium	0.315/10.0	0.185/6.25	0.394/10.0
m8gd.large	0.63/10.0	0.396/6.25	0.788/10.0
m8gd.xlarge	1.25/10.0	0.781/6.25	1.563/10.0
m8gd.2xlarge	2.5/10.0	1.562/6.25	3.125/10.0
m8gd.4xlarge	5.0/10.0	3.125/6.25	6.25/10.0
m8gd.8xlarge	10.0	6.25	12,5
m8gd.12xlarge	15.0	9.375	18.75
m8gd.16xlarge	20.0	12,5	25.0
m8gd.24xlarge	30.0	20.0	37.5
m8gd.48xlarge	40.0	27.5	50.0
m8gd.metal-24xl	30.0	20.0	37.5
m8gd.metal-48xl	40.0	27.5	50.0
m8i.large	0.65/10.0	0.415/6.25	0.813/10.0
m8i.xlarge	1.25/10.0	0.781/6.25	1.563/10.0
m8i.2xlarge	2.5/10.0	1.562/6.25	3.125/10.0

Tipo de instância	**default** (Linha de base/expansão)	**vpc-1** (Linha de base/expansão)	**ebs-1** (Linha de base/expansão)
m8i.4xlarge	5.0/10.0	3.125/6.25	6.25/10.0
m8i.8xlarge	10.0	6.25	12,5
m8i.12xlarge	15.0	9.375	18.75
m8i.16xlarge	20.0	12,5	25.0
m8i.24xlarge	30.0	20.0	37.5
m8i.32xlarge	40.0	27.5	50.0
m8i.48xlarge	60.0	41.25	75.0
m8i.96xlarge	80.0	55.0	100.0
m8i.metal-48xl	60.0	41.25	75.0
m8i.metal-96xl	80.0	55.0	100.0
m8id.large	0.65/10.0	0.415/6.25	0.813/10.0
m8id.xlarge	1.25/10.0	0.781/6.25	1.563/10.0
m8id.2xlarge	2.5/10.0	1.562/6.25	3.125/10.0
m8id.4xlarge	5.0/10.0	3.125/6.25	6.25/10.0
m8id.8xlarge	10.0	6.25	12,5
m8id.12xlarge	15.0	9.375	18.75
m8id.16xlarge	20.0	12,5	25.0
m8id.24xlarge	30.0	20.0	37.5

Tipo de instância	**default** (Linha de base/expansão)	**vpc-1** (Linha de base/expansão)	**ebs-1** (Linha de base/expansão)
m8id.32xlarge	40.0	27.5	50.0
m8id.48xlarge	60.0	41.25	75.0
m8id.96xlarge	80.0	55.0	100.0
m8id.metal-48xl	60.0	41.25	75.0
m8id.metal-96xl	80.0	55.0	100.0
m8i-flex.large	0.315/10.0	0.198/6.25	0.394/10.0
m8i-flex.xlarge	0.63/10.0	0.395/6.25	0.788/10.0
m8i-flex.2xlarge	1.25/10.0	0.781/6.25	1.563/10.0
m8i-flex.4xlarge	2.5/10.0	1.562/6.25	3.125/10.0
m8i-flex.8xlarge	5.0/10.0	3.125/6.25	6.25/12.5
m8i-flex.12xlarge	7.5/15.0	4.687/9.375	9.375/18.75
m8i-flex.16xlarge	10.0/20.0	6.25/12.5	12.5/25.0
r8a.medium	0,325 / 10,0	0,195 / 6,25	0,407 / 10,0
r8a.large	0.65/10.0	0.415/6.25	0.813/10.0
r8a.xlarge	1.25/10.0	0.781/6.25	1.563/10.0
r8a.2xlarge	2.5/10.0	1.562/6.25	3.125/10.0
r8a.4xlarge	5.0/10.0	3.125/6.25	6.25/10.0
r8a.8xlarge	10.0	6.25	12,5

Tipo de instância	**default** (Linha de base/expansão)	**vpc-1** (Linha de base/expansão)	**ebs-1** (Linha de base/expansão)
r8a.12xlarge	15.0	9.375	18.75
r8a.16xlarge	20.0	12,5	25.0
r8a.24xlarge	30.0	20.0	37.5
r8a.48xlarge	60.0	41.25	75.0
m8a.metal-24xl	30.0	20.0	37.5
m8a.metal-48xl	60.0	41.25	75.0
r8g.medium	0.315/10.0	0.185/6.25	0.394/10.0
r8g.large	0.63/10.0	0.396/6.25	0.788/10.0
r8g.xlarge	1.25/10.0	0.781/6.25	1.563/10.0
r8g.2xlarge	2.5/10.0	1.562/6.25	3.125/10.0
r8g.4xlarge	5.0/10.0	3.125/6.25	6.25/10.0
r8g.8xlarge	10.0	6.25	12,5
r8g.12xlarge	15.0	9.375	18.75
r8g.16xlarge	20.0	12,5	25.0
r8g.24xlarge	30.0	20.0	37.5
r8g.48xlarge	40.0	27.5	50.0
r8g.metal-24xl	30.0	20.0	37.5
r8g.metal-48xl	40.0	27.5	50.0

Tipo de instância	**default** (Linha de base/expansão)	**vpc-1** (Linha de base/expansão)	**ebs-1** (Linha de base/expansão)
r8gd.medium	0.315/10.0	0.185/6.25	0.394/10.0
r8gd.large	0.63/10.0	0.396/6.25	0.788/10.0
r8gd.xlarge	1.25/10.0	0.781/6.25	1.563/10.0
r8gd.2xlarge	2.5/10.0	1.562/6.25	3.125/10.0
r8gd.4xlarge	5.0/10.0	3.125/6.25	6.25/10.0
r8gd.8xlarge	10.0	6.25	12,5
r8gd.12xlarge	15.0	9.375	18.75
r8gd.16xlarge	20.0	12,5	25.0
r8gd.24xlarge	30.0	20.0	37.5
r8gd.48xlarge	40.0	27.5	50.0
r8gd.metal-24xl	30.0	20.0	37.5
r8gd.metal-48xl	40.0	27.5	50.0
r8i.large	0.65/10.0	0.415/6.25	0.813/10.0
r8i.xlarge	1.25/10.0	0.781/6.25	1.563/10.0
r8i.2xlarge	2.5/10.0	1.562/6.25	3.125/10.0
r8i.4xlarge	5.0/10.0	3.125/6.25	6.25/10.0
r8i.8xlarge	10.0	6.25	12,5
r8i.12xlarge	15.0	9.375	18.75

Tipo de instância	**default** (Linha de base/expansão)	**vpc-1** (Linha de base/expansão)	**ebs-1** (Linha de base/expansão)
r8i.16xlarge	20.0	12,5	25.0
r8i.24xlarge	30.0	20.0	37.5
r8i.32xlarge	40.0	27.5	50.0
r8i.48xlarge	60.0	41.25	75.0
r8i.96xlarge	80.0	55.0	100.0
r8i.metal-48xl	60.0	41.25	75.0
r8i.metal-96xl	80.0	55.0	100.0
r8id.large	0.65/10.0	0.415/6.25	0.813/10.0
r8id.xlarge	1.25/10.0	0.781/6.25	1.563/10.0
r8id.2xlarge	2.5/10.0	1.562/6.25	3.125/10.0
r8id.4xlarge	5.0/10.0	3.125/6.25	6.25/10.0
r8id.8xlarge	10.0	6.25	12,5
r8id.12xlarge	15.0	9.375	18.75
r8id.16xlarge	20.0	12,5	25.0
r8id.24xlarge	30.0	20.0	37.5
r8id.32xlarge	40.0	27.5	50.0
r8id.48xlarge	60.0	41.25	75.0
r8id.96xlarge	80.0	55.0	100.0

Tipo de instância	**default** (Linha de base/expansão)	**vpc-1** (Linha de base/expansão)	**ebs-1** (Linha de base/expansão)
r8id.metal-48xl	60.0	41.25	75.0
r8id.metal-96xl	80.0	55.0	100.0
r8i-flex.large	0.315/10.0	0.198/6.25	0.394/10.0
r8i-flex.xlarge	0.63/10.0	0.395/6.25	0.788/10.0
r8i-flex.2xlarge	1.25/10.0	0.781/6.25	1.563/10.0
r8i-flex.4xlarge	2.5/10.0	1.562/6.25	3.125/10.0
r8i-flex.8xlarge	5.0/10.0	3.125/6.25	6.25/12.5
r8i-flex.12xlarge	7.5/15.0	4.687/9.375	9.375/18.75
r8i-flex.16xlarge	10.0/20.0	6.25/12.5	12.5/25.0
x8g.medium	0.315/10.0	0.185/6.25	0.394/10.0
x8g.large	0.63/10.0	0.396/6.25	0.788/10.0
x8g.xlarge	1.25/10.0	0.781/6.25	1.563/10.0
x8g.2xlarge	2.5/10.0	1.562/6.25	3.125/10.0
x8g.4xlarge	5.0/10.0	3.125/6.25	6.25/10.0
x8g.8xlarge	10.0	6.25	12,5
x8g.12xlarge	15.0	9.375	18.75
x8g.16xlarge	20.0	12,5	25.0
x8g.24xlarge	30.0	20.0	37.5

Tipo de instância	**default** (Linha de base/expansão)	**vpc-1** (Linha de base/expansão)	**ebs-1** (Linha de base/expansão)
x8g.48xlarge	40.0	27.5	50.0
x8g.metal-24xl	30.0	20.0	37.5
x8g.metal-48xl	40.0	27.5	50.0
x8aedz.large	1,25 / 15,0	0,859 / 10,312	1,563 / 15,0
x8aedz.xlarge	2,5 / 15,0	1,718 / 10,312	3,125 / 15,0
x8aedz.3xlarge	7.5/15.0	5,156 / 10,312	9.375/15.0
x8aedz.6xlarge	15.0	10.312	18.75
x8aedz.12xlarge	30.0	20.625	37.5
x8aedz.24xlarge	60.0	41.25	75.0
x8aedz.metal-12xl	30.0	20.625	37.5
x8aedz.metal-24xl	60.0	41.25	75.0
x8i.large	0.65/10.0	0.415/6.25	0.813/10.0
x8i.xlarge	1.25/10.0	0.781/6.25	1.563/10.0
x8i.2xlarge	2.5/10.0	1.562/6.25	3.125/10.0
x8i.4xlarge	5.0/10.0	3.125/6.25	6.25/10.0
x8i.8xlarge	10.0	6.25	12,5
x8i.12xlarge	15.0	9.375	18.75
x8i.16xlarge	20.0	12,5	25.0

Tipo de instância	**default** (Linha de base/expansão)	**vpc-1** (Linha de base/expansão)	**ebs-1** (Linha de base/expansão)
x8i.24xlarge	30.0	20.0	37.5
x8i.32xlarge	40.0	27.5	50.0
x8i.48xlarge	60.0	41.25	75.0
x8i.64xlarge	70.0	50.0	87.5
x8i.96xlarge	80.0	55.0	100.0
x8i.metal-48xl	60.0	41.25	75.0
x8i.metal-96xl	80.0	55.0	100.0

Monitorar largura de banda da instância

É possível usar métricas do CloudWatch para monitorar a largura de banda da instância e os pacotes enviados e recebidos. É possível usar as métricas de performance de rede fornecidas pelo driver Elastic Network Adapter (ENA) para monitorar quando o tráfego excede as permissões de rede definidas pelo Amazon EC2 no nível da instância.

É possível configurar se o Amazon EC2 envia dados de métrica para a instância ao CloudWatch usando períodos de um ou cinco minutos. É possível que as métricas de performance da rede mostrem que uma permissão foi excedida e os pacotes foram descartados enquanto as métricas da instância do CloudWatch não o fazem. Isso pode acontecer quando a instância tem um pico curto na demanda por recursos de rede (conhecido como micropico de tráfego), mas as métricas do CloudWatch não são detalhadas o suficiente para refletir esses picos de microssegundos.

Saiba mais

- Métricas de instância
- Melhor desempenho de rede

Redes aperfeiçoadas para instâncias do Amazon EC2

A rede avançada usa virtualização de E/S raiz (SR-IOV) para fornecer recursos de rede de alta performance em tipos de instâncias com suporte. A SR-IOV é um método de virtualização de dispositivos que fornece performance de E/S mais elevado e menor utilização de CPU em comparação com interfaces de redes virtualizadas tradicionais. A rede avançada fornece uma largura de banda maior, uma performance melhor de pacotes por segundo (PPS) e latências consistentemente menores entre instâncias. Não há nenhuma cobrança adicional pelo uso da rede avançada.

Para obter mais informações sobre a velocidade de rede compatível com cada tipo de instância, consulte Tipos de instância do Amazon EC2.

É possível habilitar redes avançadas usando um dos seguintes mecanismos:

Elastic Network Adapter (ENA)

O Elastic Network Adapter (ENA) oferece suporte a velocidades de rede de até 100 Gbps para tipos de instâncias compatíveis.

Todas as instâncias baseadas em Nitro usam o ENA para obter uma rede aprimorada. Além disso, as seguintes instâncias baseadas em Xen usam ENA: H1, I3, G3, `m4.16xlarge`, P2, P3, P3dn e R4.

Para obter mais informações, consulte Habilitar redes aperfeiçoadas com o ENA em instâncias do EC2.

Interface Intel 82599 Virtual Function (VF)

A interface Intel 82599 Virtual Function oferece suporte a velocidades de rede de até 10 Gbps para tipos de instâncias compatíveis.

Os seguintes tipos de instância usam a interface Intel 82599 VF para redes aprimoradas: C3, C4, D2, I2, M4 (excluindo o m4.16xlarge) e R3.

Para obter mais informações, consulte Habilitar redes aperfeiçoadas com a interface Intel 82599 VF.

Conteúdo

- Habilitar redes aperfeiçoadas com o ENA em instâncias do EC2
- Melhorar a performance da rede entre instâncias do EC2 com ENA Express

- Habilitar redes aperfeiçoadas com a interface Intel 82599 VF
- Monitorar o desempenho de rede de instâncias do EC2
- Aprimorar a latência de rede para instâncias do EC2 baseadas no Linux
- Considerações sobre o Nitro System para ajuste de performance
- Otimizar performance da rede em instâncias do Windows do EC2

Habilitar redes aperfeiçoadas com o ENA em instâncias do EC2

O Amazon EC2 oferece recursos de rede avançada pelo Elastic Network Adapter (ENA). Para usar a rede aperfeiçoada, é necessário usar uma AMI que inclua o driver do ENA necessário ou instalá-lo manualmente. Em seguida, habilite o suporte do ENA na instância.

Para revisar as notas de versão ou as instruções de instalação de um driver do ENA, consulte a guia que corresponde à plataforma do sistema operacional da instância.

Linux

É possível consultar a seguinte documentação no GitHub:

- Analise as notas de lançamento do driver do kernel do ENA do Linux no GitHub.
- Para ter uma visão geral do driver do kernel do ENA do Linux que inclui instruções de instalação, consulte Linux kernel driver for Elastic Network Adapter (ENA) family no GitHub.

Windows

É possível revisar a seguinte documentação na seção Gerenciar drivers de dispositivo deste guia:

- Rastrear os lançamentos da versão do driver do ENA do Windows.
- Instalar o driver do ENA em instâncias do Windows do EC2.

Para instâncias baseadas em Nitro, os recursos da rede aperfeiçoada variam de acordo com a versão do Nitro que o tipo de instância implementa.

Para analisar as especificações de rede da instância, escolha o link da família de instâncias para seu tipo de instância. Se você não tiver certeza quanto a qual família de instâncias é aplicável, consulte Convenções de nomenclatura no guia Tipos de instância do Amazon EC2.

- Network specifications for accelerated computing instances

- Network specifications for compute optimized instances
- Network specifications for general purpose instances
- Network specifications for high-performance computing instances
- Network specifications for memory optimized instances
- Network specifications for storage optimized instances

Conteúdo

- Pré-requisitos para redes aperfeiçoadas com o ENA
- Testar se a rede avançada está habilitada
- Habilitar redes avançadas na instância
- Filas do ENA
- Solucionar problemas do driver do kernel do ENA no Linux
- Solução de problemas do driver do Adaptador de Rede Elástica do Windows

Pré-requisitos para redes aperfeiçoadas com o ENA

Para se preparar para a rede avançada com o ENA, configure a instância da seguinte forma:

- Execute uma instância baseada em Nitro.
- Verifique se a instância tem conectividade com a Internet.
- Se houver dados importantes na instância que deseja preservar, você deverá fazer backup desses dados agora criando uma AMI na instância. A atualização do driver do kernel do ENA e a habilitação do atributo `enaSupport` podem renderizar instâncias incompatíveis ou sistemas operacionais inacessíveis. Se você tiver um backup recente, seus dados ainda serão retidos, caso isso ocorra.
- Instâncias do Linux: inicie a instância usando uma versão compatível do kernel do Linux e uma distribuição com suporte, para que as redes aperfeiçoadas do ENA sejam habilitadas automaticamente para a instância. Para obter mais informações, consulte Notas de release do driver ENA do kernel do Linux.
- Instâncias do Windows: se a instância estiver executando o Windows Server 2008 R2 SP1, verifique se ela tem a atualização de suporte à assinatura de código SHA-2.
- Use o AWS CloudShell no Console de gerenciamento da AWS ou instale e configure a AWS CLI ou o AWS Tools for Windows PowerShell em qualquer computador de sua escolha, de preferência

em seu desktop local ou notebook. Para obter mais informações sobre o ACM, consulte Acessar o Amazon EC2 ou o Guia do usuário do AWS CloudShell. A rede avançada não pode ser gerenciada no console do Amazon EC2.

Testar se a rede avançada está habilitada

É possível testar se as redes aperfeiçoadas estão habilitadas nas instâncias ou nas AMIs.

Atributo de instância

Verifique o valor do atributo de instância `enaSupport`.

AWS CLI

Use o comando describe-instances.

```
aws ec2 describe-instances \
    --instance-ids i-1234567890abcdef0 \
    --query "Reservations[].Instances[].EnaSupport"
```

Se a rede aprimorada estiver habilitada, a saída será a seguinte.

```
[
    true
]
```

PowerShell

Use o cmdlet Get-EC2Instance.

```
(Get-EC2Instance -InstanceId i-1234567890abcdef0).Instances.EnaSupport
```

Se a rede aprimorada estiver habilitada, a saída será a seguinte.

```
True
```

Atributo de imagem

Verifique o valor do atributo de imagem `enaSupport`.

AWS CLI

Use o comando describe-images.

```
aws ec2 describe-images \
    --image-id ami-0abcdef1234567890 \
    --query "Images[].EnaSupport"
```

Se a rede aprimorada estiver habilitada, a saída será a seguinte.

```
[
    true
]
```

PowerShell

Use o cmdlet Get-EC2Image.

```
(Get-EC2Image -ImageId ami-0abcdef1234567890).EnaSupport
```

Se a rede aprimorada estiver habilitada, a saída será a seguinte.

```
True
```

Driver da interface de rede do Linux

Use o comando a seguir para verificar se o driver do kernel do `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`. Se sua distribuição Linux oferecer suporte a nomes de rede previsíveis, o nome poderia ser algo como `ens5`. Para obter mais informações, expanda a seção para RHEL, SUSE e CentOS em Habilitar redes avançadas na instância.

No exemplo a seguir, o driver do kernel do `ena` não está carregado porque o driver listado é `vif`.

```
[ec2-user ~]$ ethtool -i eth0
driver: vif
version:
firmware-version:
bus-info: vif-0
supports-statistics: yes
supports-test: no
```

```
supports-eeprom-access: no
supports-register-dump: no
supports-priv-flags: no
```

Neste exemplo, o driver do kernel do `ena` está carregado e na versão mínima recomendada. Essa instância configurou a rede avançada corretamente.

```
[ec2-user ~]$ ethtool -i eth0
driver: ena
version: 1.5.0g
firmware-version:
expansion-rom-version:
bus-info: 0000:00:05.0
supports-statistics: yes
supports-test: no
supports-eeprom-access: no
supports-register-dump: no
supports-priv-flags: no
```

Habilitar redes avançadas na instância

O procedimento usado dependerá do sistema operacional da instância.

Amazon Linux

As AMIs do Amazon Linux incluem o driver do kernel necessário para redes aperfeiçoadas com o ENA instalado e o suporte para ENA habilitado. Portanto, se você executar uma instância com uma versão HVM do Amazon Linux em um tipo de instância compatível, a rede avançada já estará habilitada para a instância. Para obter mais informações, consulte Testar se a rede avançada está habilitada.

Ubuntu

As AMIs HVM mais recentes do Ubuntu incluem o driver do kernel necessário para redes aperfeiçoadas com o ENA instalado e o suporte para ENA habilitado. Portanto, se você executar uma instância com a AMI do HVM do Ubuntu mais recente em um tipo de instância compatível, a rede avançada já estará habilitada para a instância. Para obter mais informações, consulte Testar se a rede avançada está habilitada.

Se tiver executado a instância usando uma AMI mais antiga e ela ainda não tiver as redes avançadas habilitadas, será possível instalar o pacote do kernel `linux-aws` para obter os drivers de redes avançadas mais recentes e atualizar o atributo necessário.

Para instalar o pacote do kernel **`linux-aws`** (Ubuntu 16.04 ou posterior)

O Ubuntu 16.04 e o 18.04 são fornecidos com o kernel personalizado do Ubuntu (pacote do kernel `linux-aws`). Para usar um kernel diferente, entre em contato com o Suporte.

Para instalar o pacote do kernel **`linux-aws`** (Ubuntu Trusty 14.04)

1. Conecte-se à sua instância.
2. Atualize o cache de pacotes e os pacotes.

```
ubuntu:~$ sudo apt-get update && sudo apt-get upgrade -y linux-aws
```

> **Important**
>
> Se, durante o processo de atualização, for solicitada a instalação do `grub`, use o `/dev/xvda` para instalar o `grub` e, em seguida, escolha manter a versão atual do `/boot/grub/menu.lst`.

3. [Instância com EBS] A partir do computador local, interrompa a instância usando o console do Amazon EC2 ou um dos seguintes comandos: stop-instances (AWS CLI) ou Stop-EC2Instance (AWS Tools for Windows PowerShell).

   [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).
4. No computador local, ative o atributo de rede avançada usando um dos seguintes comandos:

   - modify-instance-attribute (AWS CLI)

     ```
     aws ec2 modify-instance-attribute --instance-id i-1234567890abcdef0 --ena-support
     ```

   - Edit-EC2InstanceAttribute (ferramentas para o Windows PowerShell)

     ```
     Edit-EC2InstanceAttribute -InstanceId i-1234567890abcdef0 -EnaSupport $true
     ```
5. (Opcional) Crie uma AMI na instância, conforme descrito em Criação de uma AMI baseada no Amazon EBS. A AMI herda o atributo de rede avançada `enaSupport` da instância. Portanto, é possível usar essa AMI para executar outra instância com a rede avançada habilitada por padrão.

6. A partir do computador local, inicie a instância usando o console do Amazon EC2 ou um dos seguintes comandos: start-instances (AWS CLI) ou Start-EC2Instance (AWS Tools for Windows PowerShell).

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 baseada no Amazon S3, habilitando o atributo de rede avançada ao registrar a AMI.

- register-image (AWS CLI)

```
aws ec2 register-image --ena-support ...
```

- Register-EC2Image (AWS Tools for Windows PowerShell)

```
Register-EC2Image -EnaSupport $true ...
```

RHEL, SUSE e CentOS

As AMIs mais recentes para Red Hat Enterprise Linux, SUSE Linux Enterprise Server e CentOS incluem o driver do kernel necessário para redes aperfeiçoadas com o ENA e o suporte para ENA habilitado. Portanto, se você executar uma instância com a AMI mais recente em um tipo de instância compatível, a rede aprimorada já estará habilitada para a instância. Para obter mais informações, consulte Testar se a rede avançada está habilitada.

O procedimento a seguir fornece as etapas gerais para habilitar a rede aprimorada em uma distribuição do Linux diferente do Amazon Linux AMI ou do Ubuntu. Para obter mais informações, como a sintaxe detalhada dos comandos, os locais dos arquivos ou o suporte para o pacote e a ferramenta, consulte a documentação da sua distribuição do Linux.

Para habilitar a rede avançada no Linux

1. Conecte-se à sua instância.
2. Clone o código-fonte do driver do kernel do ena na instância no GitHub em https://github.com/amzn/amzn-drivers. (Como o SUSE Linux Enterprise Server 12 SP2 e posterior incluem ENA 2.02 por padrão, não é necessário fazer download e compilar o driver ENA. Para o SUSE Linux

Enterprise Server 12 SP2 e posterior, é necessário registrar uma solicitação para adicionar a versão do driver que deseja ao kernel comercial).

```
git clone https://github.com/amzn/amzn-drivers
```

3. Compile e instale o driver do kernel do `ena` na instância. Essas etapas dependem da distribuição Linux. Para obter mais informações sobre a compilação do driver do kernel no Red Hat Enterprise Linux, consulte How do I install the latest ENS driver for enhanced network support on an Amazon EC2 instance that runs RHEL?
4. Execute o comando sudo depmod para atualizar as dependências do driver do kernel.
5. Atualize o `initramfs` na instância para garantir que o novo driver do kernel seja carregado no momento da inicialização. Por exemplo, se a distribuição oferecer suporte a dracut, será possível usar o comando a seguir.

```
dracut -f -v
```

6. Determine se o sistema usa nomes previsíveis de interface de rede por padrão. Os sistemas que usam as versões 197 ou superiores do systemd ou udev podem renomear dispositivos de Ethernet e não garantem que uma única interface de rede será nomeada `eth0`. Esse comportamento pode causar problemas para conexão à instância. Para mais informações e ver outras opções de configuração, consulte Nomes previsíveis de interface de rede no site freedesktop.org.

   a. É possível verificar as versões do systemd ou udev em sistemas baseados em RPM com o comando a seguir.

   ```
   rpm -qa | grep -e '^systemd-[0-9]\+\|^udev-[0-9]\+'
   systemd-208-11.el7_0.2.x86_64
   ```

   No exemplo do Red Hat Enterprise Linux 7 acima, a versão do systemd é a 208, portanto, os nomes previsíveis de interface de rede devem ser desativados.

   b. Desabilite nomes previsíveis de interface de rede adicionando a opção `net.ifnames=0` à linha `GRUB_CMDLINE_LINUX` no `/etc/default/grub`.

   ```
   sudo sed -i '/^GRUB\_CMDLINE\_LINUX/s/\"$/\ net\.ifnames\=0\"/' /etc/default/
   grub
   ```

   c. Recompile o arquivo de configuração do grub.

```
sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

7. [Instância com EBS] No computador local, interrompa a instância usando o console do Amazon EC2 ou um dos seguintes comandos: stop-instances (AWS CLI), Stop-EC2Instance (AWS Tools for Windows PowerShell).

   [Instância baseada em armazenamento de instâncias] Você não pode parar a instância para modificar o atributo. Em vez disso, siga este procedimento: Para habilitar as redes avançadas no Linux (instâncias compatíveis com o armazenamento de instância).

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 i-1234567890abcdef0 --ena-support
     ```

   - Edit-EC2InstanceAttribute (ferramentas para o Windows PowerShell)

     ```
     Edit-EC2InstanceAttribute -InstanceId i-1234567890abcdef0 -EnaSupport $true
     ```

9. (Opcional) Crie uma AMI na instância, conforme descrito em Criação de uma AMI baseada no Amazon EBS. A AMI herda o atributo de rede avançada `enaSupport` da instância. Portanto, é possível usar essa AMI para executar outra instância com a rede avançada habilitada por padrão.

   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. A partir do computador local, inicie a instância usando o console do Amazon EC2 ou um dos seguintes comandos: start-instances (AWS CLI) ou Start-EC2Instance (AWS Tools for Windows PowerShell).

11. (Opcional) Conecte-se à instância e verifique se o driver do kernel está instalado.

    Se não for possível conectar-se à instância depois de habilitar a rede avançada, consulte Solucionar problemas do driver do kernel do ENA no Linux.

Para habilitar as redes avançadas no Linux (instâncias compatíveis com o armazenamento de instância)

Siga o procedimento anterior até a etapa onde você para a instância. Crie uma nova AMI como descrito em Criação de uma AMI baseada no Amazon S3, habilitando o atributo de rede avançada ao registrar a AMI.

- register-image (AWS CLI)

```
aws ec2 register-image --ena-support ...
```

- Register-EC2Image (AWS Tools for Windows PowerShell)

```
Register-EC2Image -EnaSupport ...
```

Ubuntu com DKMS

Esse método é apenas para fins de teste e feedback. Não é destinado ao uso com implantações de produção. Para implantações de produção, consulte Ubuntu.

> **Important**
>
> O uso do DKMS anula o acordo de suporte da sua assinatura. Ele não deve ser usado para implantações de produção.

Para habilitar a rede avançada com o ENA no Ubuntu (instâncias com suporte do EBS)

1. Siga as etapas 1 e 2 em Ubuntu.
2. Instale os pacotes `build-essential` para compilar o driver do kernel e o pacote `dkms` para que o driver do kernel do `ena` seja recompilado sempre que o kernel for atualizado.

   ```
   ubuntu:~$ sudo apt-get install -y build-essential dkms
   ```

3. Clone a fonte do driver do kernel do `ena` na instância no 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 (é possível localizar o número da versão atual nas notas de release) do código-fonte ao nome do diretório. Por exemplo, a versão `1.0.0` é mostrada no exemplo a seguir.

```
ubuntu:~$ sudo mv amzn-drivers /usr/src/amzn-drivers-1.0.0
```

5. Crie o arquivo de configuração do DKMS com os valores a seguir substituindo a versão do `ena`.

   Criar o arquivo.

```
ubuntu:~$ sudo touch /usr/src/amzn-drivers-1.0.0/dkms.conf
```

   Edite 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 driver do kernel do `ena` na instância usando o DKMS.

   Adicione o driver do kernel ao DKMS.

```
ubuntu:~$ sudo dkms add -m amzn-drivers -v 1.0.0
```

   Crie o driver do kernel usando o comando dkms.

```
ubuntu:~$ sudo dkms build -m amzn-drivers -v 1.0.0
```

   Instale o driver do kernel usando dkms.

```
ubuntu:~$ sudo dkms install -m amzn-drivers -v 1.0.0
```

7. Reconstrua `initramfs` para que o driver do kernel correto seja carregado no momento da inicialização.

```
ubuntu:~$ sudo update-initramfs -u -k all
```

8. Verifique se o kernel do driver `ena` está instalado usando o comando modinfo ena em Testar se a rede avançada está habilitada.

```
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)
```

9. Passe para a etapa 3 em Ubuntu.

Habilitar redes avançadas no Windows

Se você executou a instância e ela ainda não tiver a rede avançada habilitada, você deverá fazer download e instalar o driver do adaptador de rede necessário na instância e, em seguida, definir o atributo `enaSupport` da instância para ativar a rede avançada.

Para habilitar a rede avançada

1. Conecte-se à instância e faça login como administrador local.
2. [Windows Server 2016 e 2019 apenas] Execute o seguinte script do PowerShell do EC2Launch para configurar a instância depois de instalar o driver.

```
PS C:\> C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeInstance.ps1 -
Schedule
```

3. Na instância, instale o driver da seguinte forma:
   a. Faça download do driver mais recente para a instância.
   b. Extraia o arquivo zip.
   c. Instale o driver executando o script `install.ps1` do PowerShell.

> **Note**
>
> Se você receber um erro de política de execução, defina a política como `Unrestricted` (por padrão, ela é definida como `Restricted` ou `RemoteSigned`). Em uma linha de comando, execute `Set-ExecutionPolicy -ExecutionPolicy Unrestricted` e, depois, execute o script `install.ps1` do PowerShell novamente.

4. No seu computador local, interrompa a instância usando o console do Amazon EC2 ou um dos comandos a seguir: stop-instances (AWS CLI) ou Stop-EC2Instance (AWS Tools for Windows PowerShell).
5. Ative o suporte ao ENA na instância da seguinte maneira:
   a. No computador local, verifique o atributo de suporte ao ENA da instância do EC2 em sua instância executando um dos seguinte comandos. Se o atributo não estiver habilitado, a saída será “[]” ou em branco. `EnaSupport` será definido como `false` por padrão.
      - describe-instances (AWS CLI)

```
aws ec2 describe-instances --instance-ids i-1234567890abcdef0 --query
 "Reservations[].Instances[].EnaSupport"
```

      - Get-EC2Instance (ferramentas para o Windows PowerShell)

```
(Get-EC2Instance -InstanceId i-1234567890abcdef0).Instances.EnaSupport
```

b. Para ativar o suporte ao ENA, execute um dos seguintes comandos:

- modify-instance-attribute (AWS CLI)

```
aws ec2 modify-instance-attribute --instance-id i-1234567890abcdef0 --ena-
support
```

- Edit-EC2InstanceAttribute (AWS Tools for Windows PowerShell)

```
Edit-EC2InstanceAttribute -InstanceId i-1234567890abcdef0 -EnaSupport $true
```

Se encontrar problemas ao reiniciar a instância, também é possível desativar o suporte ao ENA com um dos seguintes comandos:

- modify-instance-attribute (AWS CLI)

```
aws ec2 modify-instance-attribute --instance-id i-1234567890abcdef0 --no-ena-
support
```

- Edit-EC2InstanceAttribute (AWS Tools for Windows PowerShell)

```
Edit-EC2InstanceAttribute -InstanceId i-1234567890abcdef0 -EnaSupport $false
```

c. Verifique se o atributo foi definido como `true` usando describe-instances ou Get-EC2Instance conforme mostrado anteriormente. Você agora deve ver a seguinte saída:

```
[
 true
]
```

6. A partir do computador local, inicie a instância usando o console do Amazon EC2 ou um dos seguintes comandos: start-instances (AWS CLI) ou Start-EC2Instance (AWS Tools for Windows PowerShell).
7. Na instância, valide se o driver do ENA está instalado e ativado da seguinte maneira:

a. Clique com o botão direito do mouse no ícone de rede e escolha Abrir Central de Rede e Compartilhamento.

b. Escolha o adaptador de Ethernet (por exemplo, Ethernet 2).

c. Escolha Detalhes. Para Detalhes da conexão de rede, verifique se a Descrição é Amazon Elastic Network Adapter.

8. (Opcional) Crie uma AMI na instância. A AMI herda o atributo `enaSupport` da instância. Portanto, é possível usar essa AMI para executar outra instância com ENA ativado por padrão.

Filas do ENA

As filas do ENA são alocadas para as interfaces de rede com limites estáticos padrão com base no tipo e no tamanho da instância. Nos tipos de instância compatíveis, você pode alocar dinamicamente essas filas nas Interfaces de Rede Elástica (ENIs). Embora o número total de filas por instância dependa do tipo e do tamanho da instância, você pode configurar várias ENIs com filas de ENA até atingir o número máximo de filas da ENI e da instância.

A alocação flexível de filas do ENA otimiza a distribuição de recursos, permitindo a máxima utilização da vCPU. Workloads de alta performance de rede normalmente exigem várias filas do ENA. É possível ajustar a performance de rede e os pacotes por segundo (PPS) ajustando o número de filas de acordo com suas necessidades específicas de workload. Por exemplo, aplicações com uso intensivo de rede podem exigir mais filas em comparação com aplicações com uso intensivo de CPU.

Tópicos

- Instâncias compatíveis
- Modificar o número de filas

Instâncias compatíveis

As instâncias a seguir são compatíveis com a alocação dinâmica de várias filas do ENA.

Uso geral

Tipo de instância	Filas ENA padrão por interface	Máximo de filas ENA por interface	Máximo de filas ENA por instância
	M6i		
`m6i.large`	2	2	6

Tipo de instância	Filas ENA padrão por interface	Máximo de filas ENA por interface	Máximo de filas ENA por instância
m6i.xlarge	4	4	16
m6i.2xlarge	8	8	32
m6i.4xlarge	8	16	64
m6i.8xlarge	8	32	64
m6i.12xlarge	8	32	64
m6i.16xlarge	8	32	120
m6i.24xlarge	8	32	120
m6i.32xlarge	8	32	120
M6id			
m6id.large	2	2	6
m6id.xlarge	4	4	16
m6id.2xlarge	8	8	32
m6id.4xlarge	8	16	64
m6id.8xlarge	8	32	64
m6id.12xlarge	8	32	64
m6id.16xlarge	8	32	120
m6id.24xlarge	8	32	120
m6id.32xlarge	8	32	120
M6idn			

Tipo de instância	Filas ENA padrão por interface	Máximo de filas ENA por interface	Máximo de filas ENA por instância
m6idn.large	2	2	6
m6idn.xlarge	4	4	16
m6idn.2xlarge	8	8	32
m6idn.4xlarge	8	16	64
m6idn.8xlarge	16	32	128
m6idn.12xlarge	16	32	128
m6idn.16xlarge	16	32	240
m6idn.24xlarge	32	32	480
m6idn.32xlarge	32	32	512 *
	M6in		
m6in.large	2	2	6
m6in.xlarge	4	4	16
m6in.2xlarge	8	8	32
m6in.4xlarge	8	16	64
m6in.8xlarge	16	32	128
m6in.12xlarge	16	32	128
m6in.16xlarge	16	32	240
m6in.24xlarge	32	32	480
m6in.32xlarge	32	32	512 *

Tipo de instância	Filas ENA padrão por interface	Máximo de filas ENA por interface	Máximo de filas ENA por instância
M8a			
m8a.medium	1	1	3
m8a.large	2	2	6
m8a.xlarge	4	4	16
m8a.2xlarge	8	8	32
m8a.4xlarge	8	16	64
m8a.8xlarge	8	32	128
m8a.12xlarge	16	64	192
m8a.16xlarge	16	64	256
m8a.24xlarge	16	128	384
m8a.48xlarge	32	128	768
m8a.metal-24xl	16	128	384
m8a.metal-48xl	32	128	768
M8azn			
m8azn.medium	1	1	3
m8azn.large	2	2	8
m8azn.xlarge	4	4	16
m8azn.3xlarge	4	16	48
m8azn.6xlarge	8	32	96

Tipo de instância	Filas ENA padrão por interface	Máximo de filas ENA por interface	Máximo de filas ENA por instância
m8azn.12xlarge	8	64	192
m8azn.24xlarge	16	128	384
m8azn.metal-12xl	8	64	192
m8azn.metal-24xl	16	128	384
M8gb			
m8gb.medium	1	1	2
m8gb.large	2	2	6
m8gb.xlarge	4	4	16
m8gb.2xlarge	8	8	32
m8gb.4xlarge	8	16	64
m8gb.8xlarge	8	32	128
m8gb.12xlarge	16	64	192
m8gb.16xlarge	16	64	256
m8gb.24xlarge	16	128	384
m8gb.48xlarge	32	128	768 *
M8gn			
m8gn.medium	1	1	2
m8gn.large	2	2	6
m8gn.xlarge	4	4	16

Tipo de instância	Filas ENA padrão por interface	Máximo de filas ENA por interface	Máximo de filas ENA por instância
m8gn.2xlarge	8	8	32
m8gn.4xlarge	8	16	64
m8gn.8xlarge	8	32	128
m8gn.12xlarge	16	64	192
m8gn.16xlarge	16	64	256
m8gn.24xlarge	16	128	384
m8gn.48xlarge	32	128	768 *
M8i			
m8i.large	2	2	6
m8i.xlarge	4	4	16
m8i.2xlarge	8	8	32
m8i.4xlarge	8	16	64
m8i.8xlarge	8	32	128
m8i.12xlarge	16	64	192
m8i.16xlarge	16	64	256
m8i.24xlarge	16	128	384
m8i.32xlarge	16	128	512
m8i.48xlarge	32	128	768
m8i.96xlarge	32	128	1536

Tipo de instância	Filas ENA padrão por interface	Máximo de filas ENA por interface	Máximo de filas ENA por instância
m8i.metal-48xl	32	128	768
m8i.metal-96xl	32	128	1536
M8id			
m8id.large	2	2	6
m8id.xlarge	4	4	16
m8id.2xlarge	8	8	32
m8id.4xlarge	8	16	64
m8id.8xlarge	8	32	128
m8id.12xlarge	16	64	192
m8id.16xlarge	16	64	256
m8id.24xlarge	16	128	384
m8id.32xlarge	16	128	512
m8id.48xlarge	32	128	768
m8id.96xlarge	32	128	1536
m8id.metal-48xl	32	128	768
m8id.metal-96xl	32	128	1536
M8i-flex			
m8i-flex.large	1	1	3
m8i-flex.xlarge	2	2	8

Tipo de instância	Filas ENA padrão por interface	Máximo de filas ENA por interface	Máximo de filas ENA por instância
m8i-flex.2xlarge	4	4	16
m8i-flex.4xlarge	4	8	32
m8i-flex.8xlarge	4	16	64
m8i-flex.12xlarge	8	32	96
m8i-flex.16xlarge	8	32	128

> **Note**
>
> * Esses tipos de instância contam com várias placas de rede. Outros tipos de instância contam com uma única placa de rede. Para obter mais informações, consulte Placas de rede.

Otimizadas para computação

Tipo de instância	Filas ENA padrão por interface	Máximo de filas ENA por interface	Máximo de filas ENA por instância
	C6i		
c6i.large	2	2	6
c6i.xlarge	4	4	16
c6i.2xlarge	8	8	32
c6i.4xlarge	8	16	64
c6i.8xlarge	8	32	64
c6i.12xlarge	8	32	64

Tipo de instância	Filas ENA padrão por interface	Máximo de filas ENA por interface	Máximo de filas ENA por instância
c6i.16xlarge	8	32	120
c6i.24xlarge	8	32	120
c6i.32xlarge	8	32	120
C6id			
c6id.large	2	2	6
c6id.xlarge	4	4	16
c6id.2xlarge	8	8	32
c6id.4xlarge	8	16	64
c6id.8xlarge	8	32	64
c6id.12xlarge	8	32	64
c6id.16xlarge	8	32	120
c6id.24xlarge	8	32	120
c6id.32xlarge	8	32	120
C6in			
c6in.large	2	2	6
c6in.xlarge	4	4	16
c6in.2xlarge	8	8	32
c6in.4xlarge	8	16	64
c6in.8xlarge	16	32	128

Tipo de instância	Filas ENA padrão por interface	Máximo de filas ENA por interface	Máximo de filas ENA por instância
c6in.12xlarge	16	32	128
c6in.16xlarge	16	32	240
c6in.24xlarge	32	32	480
c6in.32xlarge	32	32	512 *
C8a			
c8a.medium	1	1	3
c8a.large	2	2	6
c8a.xlarge	4	4	16
c8a.2xlarge	8	8	32
c8a.4xlarge	8	16	64
c8a.8xlarge	8	32	128
c8a.12xlarge	16	64	192
c8a.16xlarge	16	64	256
c8a.24xlarge	16	128	384
c8a.48xlarge	32	128	768
c8a.metal-24xl	16	128	384
c8a.metal-48xl	32	128	768
C8gb			
c8gb.medium	1	1	2

Tipo de instância	Filas ENA padrão por interface	Máximo de filas ENA por interface	Máximo de filas ENA por instância
c8gb.large	2	2	6
c8gb.xlarge	4	4	16
c8gb.2xlarge	8	8	32
c8gb.4xlarge	8	16	64
c8gb.8xlarge	8	32	128
c8gb.12xlarge	16	64	192
c8gb.16xlarge	16	64	256
c8gb.24xlarge	16	128	384
c8gb.48xlarge	32	128	768 *
c8gb.metal-24xl	32	128	768
c8gb.metal-48xl	32	128	768 *
C8gn			
c8gn.medium	1	1	2
c8gn.large	2	2	6
c8gn.xlarge	4	4	16
c8gn.2xlarge	8	8	32
c8gn.4xlarge	8	16	64
c8gn.8xlarge	8	32	128
c8gn.12xlarge	16	64	192

Tipo de instância	Filas ENA padrão por interface	Máximo de filas ENA por interface	Máximo de filas ENA por instância
c8gn.16xlarge	16	64	256
c8gn.24xlarge	16	128	384
c8gn.48xlarge	32	128	768 *
c8gn.metal-24xl	32	128	768
c8gn.metal-48xl	32	128	768 *
C8i			
c8i.large	2	2	6
c8i.xlarge	4	4	16
c8i.2xlarge	8	8	32
c8i.4xlarge	8	16	64
c8i.8xlarge	8	32	128
c8i.12xlarge	16	64	192
c8i.16xlarge	16	64	256
c8i.24xlarge	16	128	384
c8i.32xlarge	16	128	512
c8i.48xlarge	32	128	768
c8i.96xlarge	32	128	1536
c8i.metal-48xl	32	128	768
c8i.metal-96xl	32	128	1536

Tipo de instância	Filas ENA padrão por interface	Máximo de filas ENA por interface	Máximo de filas ENA por instância
C8id			
c8id.large	2	2	6
c8id.xlarge	4	4	16
c8id.2xlarge	8	8	32
c8id.4xlarge	8	16	64
c8id.8xlarge	8	32	128
c8id.12xlarge	16	64	192
c8id.16xlarge	16	64	256
c8id.24xlarge	16	128	384
c8id.32xlarge	16	128	512
c8id.48xlarge	32	128	768
c8id.96xlarge	32	128	1536
c8id.metal-48xl	32	128	768
c8id.metal-96xl	32	128	1536
C8i-flex			
c8i-flex.large	1	1	3
c8i-flex.xlarge	2	2	8
c8i-flex.2xlarge	4	4	16
c8i-flex.4xlarge	4	8	32

Tipo de instância	Filas ENA padrão por interface	Máximo de filas ENA por interface	Máximo de filas ENA por instância
c8i-flex.8xlarge	4	16	64
c8i-flex.12xlarge	8	32	96
c8i-flex.16xlarge	8	32	128

> **Note**
>
> * Esses tipos de instância contam com várias placas de rede. Outros tipos de instância contam com uma única placa de rede. Para obter mais informações, consulte Placas de rede.

Otimizado para memória

Tipo de instância	Filas ENA padrão por interface	Máximo de filas ENA por interface	Máximo de filas ENA por instância
	R6i		
r6i.large	2	2	6
r6i.xlarge	4	4	16
r6i.2xlarge	8	8	32
r6i.4xlarge	8	16	64
r6i.8xlarge	8	32	64
r6i.12xlarge	8	32	64
r6i.16xlarge	8	32	120
r6i.24xlarge	8	32	120

Tipo de instância	Filas ENA padrão por interface	Máximo de filas ENA por interface	Máximo de filas ENA por instância
r6i.32xlarge	8	32	120
R6id			
r6id.large	2	2	6
r6id.xlarge	4	4	16
r6id.2xlarge	8	8	32
r6id.4xlarge	8	16	64
r6id.8xlarge	8	32	64
r6id.12xlarge	8	32	64
r6id.16xlarge	8	32	120
r6id.24xlarge	8	32	120
r6id.32xlarge	8	32	120
R6idn			
r6idn.large	2	2	6
r6idn.xlarge	4	4	16
r6idn.2xlarge	8	8	32
r6idn.4xlarge	8	16	64
r6idn.8xlarge	16	32	128
r6idn.12xlarge	16	32	128
r6idn.16xlarge	16	32	240

Tipo de instância	Filas ENA padrão por interface	Máximo de filas ENA por interface	Máximo de filas ENA por instância
r6idn.24xlarge	32	32	480
r6idn.32xlarge	32	32	512 *
	R6in		
r6in.large	2	2	6
r6in.xlarge	4	4	16
r6in.2xlarge	8	8	32
r6in.4xlarge	8	16	64
r6in.8xlarge	16	32	128
r6in.12xlarge	16	32	128
r6in.16xlarge	16	32	240
r6in.24xlarge	32	32	480
r6in.32xlarge	32	32	512 *
	R8a		
r8a.medium	1	1	3
r8a.large	2	2	6
r8a.xlarge	4	4	16
r8a.2xlarge	8	8	32
r8a.4xlarge	8	16	64
r8a.8xlarge	8	32	128

Tipo de instância	Filas ENA padrão por interface	Máximo de filas ENA por interface	Máximo de filas ENA por instância
r8a.12xlarge	16	64	192
r8a.16xlarge	16	64	256
r8a.24xlarge	16	128	384
r8a.48xlarge	32	128	768
r8a.metal-24xl	16	128	384
r8a.metal-48xl	32	128	768
R8gb			
r8gb.medium	1	1	2
r8gb.large	2	2	6
r8gb.xlarge	4	4	16
r8gb.2xlarge	8	8	32
r8gb.4xlarge	8	16	64
r8gb.8xlarge	8	32	128
r8gb.12xlarge	16	64	192
r8gb.16xlarge	16	64	256
r8gb.24xlarge	16	128	384
r8gb.48xlarge	32	128	768 *
r8gb.metal-24xl	32	128	768
r8gb.metal-48xl	32	128	768 *

Tipo de instância	Filas ENA padrão por interface	Máximo de filas ENA por interface	Máximo de filas ENA por instância
	R8gn		
r8gn.medium	1	1	2
r8gn.large	2	2	6
r8gn.xlarge	4	4	16
r8gn.2xlarge	8	8	32
r8gn.4xlarge	8	16	64
r8gn.8xlarge	8	32	128
r8gn.12xlarge	16	64	192
r8gn.16xlarge	16	64	256
r8gn.24xlarge	16	128	384
r8gn.48xlarge	32	128	768 *
r8gn.metal-24xl	32	128	768
r8gn.metal-48xl	32	128	768 *
	R8i		
r8i.large	2	2	6
r8i.xlarge	4	4	16
r8i.2xlarge	8	8	32
r8i.4xlarge	8	16	64
r8i.8xlarge	8	32	128

Tipo de instância	Filas ENA padrão por interface	Máximo de filas ENA por interface	Máximo de filas ENA por instância
r8i.12xlarge	16	64	192
r8i.16xlarge	16	64	256
r8i.24xlarge	16	128	384
r8i.32xlarge	16	128	512
r8i.48xlarge	32	128	768
r8i.96xlarge	32	128	1536
r8i.metal-48xl	32	128	768
r8i.metal-96xl	32	128	1536
R8id			
r8id.large	2	2	6
r8id.xlarge	4	4	16
r8id.2xlarge	8	8	32
r8id.4xlarge	8	16	64
r8id.8xlarge	8	32	128
r8id.12xlarge	16	64	192
r8id.16xlarge	16	64	256
r8id.24xlarge	16	128	384
r8id.32xlarge	16	128	512
r8id.48xlarge	32	128	768

Tipo de instância	Filas ENA padrão por interface	Máximo de filas ENA por interface	Máximo de filas ENA por instância
r8id.96xlarge	32	128	1536
r8id.metal-48xl	32	128	768
r8id.metal-96xl	32	128	1536
R8i-flex			
r8i-flex.large	1	1	3
r8i-flex.xlarge	2	2	8
r8i-flex.2xlarge	4	4	16
r8i-flex.4xlarge	4	8	32
r8i-flex.8xlarge	4	16	64
r8i-flex.12xlarge	8	32	96
r8i-flex.16xlarge	8	32	128
X8aedz			
x8aedz.large	2	2	8
x8aedz.xlarge	4	4	16
x8aedz.3xlarge	4	16	48
x8aedz.6xlarge	8	32	96
x8aedz.12xlarge	8	64	192
x8aedz.24xlarge	16	128	384
x8aedz.metal-12xl	8	64	192

Tipo de instância	Filas ENA padrão por interface	Máximo de filas ENA por interface	Máximo de filas ENA por instância
x8aedz.metal-24xl	16	128	384
	X8i		
x8i.large	2	2	6
x8i.xlarge	4	4	16
x8i.2xlarge	8	8	32
x8i.4xlarge	8	16	64
x8i.8xlarge	8	32	128
x8i.12xlarge	16	64	192
x8i.16xlarge	16	64	256
x8i.24xlarge	16	128	384
x8i.32xlarge	16	128	512
x8i.48xlarge	32	128	768
x8i.64xlarge	32	128	1024
x8i.96xlarge	32	128	1536
x8i.metal-48xl	32	128	768
x8i.metal-96xl	32	128	1536

Note

* Esses tipos de instância contam com várias placas de rede. Outros tipos de instância contam com uma única placa de rede. Para obter mais informações, consulte Placas de rede.

Modificar o número de filas

É possível modificar o número de filas do ENA usando o Console de gerenciamento da AWS ou a AWS CLI. No Console de gerenciamento da AWS, a configuração de filas do ENA está disponível em toda configuração de Interface de rede.

Para modificar o número de filas do ENA usando a AWS CLI, use um dos comandos a seguir. Antes de modificar o número de filas, use o comando a seguir para verificar o número atual de filas.

```
aws ec2 describe-instances --instance-id i-1234567890abcdef0
```

> **Note**
>
> - É necessário parar a instância antes de modificar o número de filas do ENA.
> - O valor das filas do ENA deve ser uma potência de 2, como, 1, 2, 4, 8, 16, 32 etc.
> - O número de filas alocadas para uma única ENI não pode exceder o número de vCPUs disponíveis na instância.

`attach-network-interface`

No exemplo a seguir, 32 filas do ENA estão configuradas em uma ENI.

```
aws ec2 attach-network-interface \
  --network-interface-id eni-001aa1bb223cdd4e4 \
  --instance-id i-1234567890abcdef0 \
  --device-index 1 \
  --ena-queue-count 32
```

`run-instances`

No exemplo a seguir, 2 filas do ENA são configuradas em cada uma das 3 ENIs.

```
aws ec2 run-instances \
  --image-id ami-12ab3c30 \
  --instance-type c6i.large \
  --min-count 1 \
  --max-count 1 \
```

```
  --network-interfaces \
    "[{\"DeviceIndex\":0,\"SubnetId\":\"subnet-123456789012a345a\",\"EnaQueueCount
\":2},
      {\"DeviceIndex\":1,\"SubnetId\":\"subnet-123456789012a345a\",\"EnaQueueCount
\":2},
      {\"DeviceIndex\":2,\"SubnetId\":\"subnet-123456789012a345a\",\"EnaQueueCount
\":2}]"
```

modify-network-interface-attribute

No exemplo a seguir, 32 filas do ENA estão configuradas em uma ENI.

```
aws ec2 modify-network-interface-attribute \
--network-interface-id eni-1234567890abcdef0 \
--attachment AttachmentId=eni-attach-12345678,EnaQueueCount=32
```

No exemplo a seguir, a contagem do ENA é redefinida com o valor padrão.

```
aws ec2 modify-network-interface-attribute \
--network-interface-id eni-1234567890abcdef0 \
--attachment AttachmentId=eni-attach-12345678,DefaultEnaQueueCount=true
```

Solucionar problemas do driver do kernel do ENA no Linux

O Elastic Network Adapter (ENA) é projetado para melhorar a integridade do sistema operacional e reduzir as possibilidades de interrupção de longo prazo por conta de comportamento inesperado de hardware e/ou falhas. A arquitetura do ENA mantém falhas do dispositivo ou do driver o mais transparentes possível para o sistema. Este tópico fornece informações de solução de problemas para o ENA.

Caso você não consiga se conectar à sua instância, comece com a seção Solucionar problemas de conectividade.

Se você experimentar degradação de performance após migrar para um tipo de instância de sexta geração, consulte o artigo What do I need to do before I migrate my EC2 instance to a sixth generation instance to make sure that I get maximum network performance?

Se você for capaz de se conectar à sua instância, pode coletar informações de diagnóstico usando os mecanismos de detecção e recuperação de falhas, cobertos nas seções posteriores deste tópico.

Tópicos

- Solucionar problemas de conectividade
- Mecanismo de keep-alive
- Registre o tempo limite de leitura
- Statistics
- Logs de erro do driver no syslog
- Notificações de configuração abaixo do ideal

Solucionar problemas de conectividade

Se você perder a conectividade ao habilitar a rede avançada, o módulo `ena` talvez seja incompatível com o kernel atualmente em execução na sua instância. Isso pode acontecer se você instalar o módulo para uma versão específica do kernel (sem dkms ou com um arquivo dkms.conf configurado indevidamente) e o kernel da instância for atualizado. Se o kernel da instância que estiver carregado no momento da inicialização não tiver o módulo `ena` corretamente instalado, sua instância não reconhecerá o adaptador de rede e sua instância ficará inacessível.

Se você habilitar a rede avançada para uma instância de PV ou AMI, isso também poderá tornar a instância inatingível.

.Se sua instância tornar-se inacessível após habilitar a rede avançada com ENA, é possível 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, o comando stop-instances (AWS CLI) ou o cmdlet Stop-EC2Instance (AWS Tools for PowerShell).
2. No seu computador local, desabilite o atributo de rede avançada usando o comando modify-instance-attribute com a opção `--no-ena-support` ou o cmdlet Edit-EC2InstanceAttribute com o parâmetro `-EnaSupport $false`.
3. No computador local, inicie a instância usando o console do Amazon EC2, o comandos start-instances ou o cmdlet Start-EC2Instance.
4. (Opcional) Conecte-se à sua instância e tente reinstalar o módulo `ena` com a versão atual do kernel seguindo as etapas em Habilitar redes aperfeiçoadas com o ENA em instâncias do EC2.

Para desabilitar a rede avançada com o ENA (instâncias com suporte do armazenamento de instâncias)

1. Crie uma nova AMI conforme descrito em Criação de uma AMI baseada no Amazon S3.
2. Ao registrar a AMI, certifique-se de incluir a opção `--no-ena-support` no comando stop-instances (AWS CLI) ou o parâmetro `-EnaSupport $false` no cmdlet Register-EC2Image.

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.

Exemplo do procedimento de redefinição:

```
[18509.800135] ena 0000:00:07.0 eth1: Keep alive watchdog timeout. // The watchdog
 process initiates a reset
[18509.815244] ena 0000:00:07.0 eth1: Trigger reset is on
[18509.825589] ena 0000:00:07.0 eth1: tx_timeout: 0 // The driver logs the current
 statistics
[18509.834253] ena 0000:00:07.0 eth1: io_suspend: 0
[18509.842674] ena 0000:00:07.0 eth1: io_resume: 0
[18509.850275] ena 0000:00:07.0 eth1: wd_expired: 1
[18509.857855] ena 0000:00:07.0 eth1: interface_up: 1
[18509.865415] ena 0000:00:07.0 eth1: interface_down: 0
[18509.873468] ena 0000:00:07.0 eth1: admin_q_pause: 0
```

```
[18509.881075] ena 0000:00:07.0 eth1: queue_0_tx_cnt: 0
[18509.888629] ena 0000:00:07.0 eth1: queue_0_tx_bytes: 0
[18509.895286] ena 0000:00:07.0 eth1: queue_0_tx_queue_stop: 0
.......
........
[18511.280972] ena 0000:00:07.0 eth1: free uncompleted tx skb qid 3 idx 0x7 // At the
 end of the down process, the driver discards incomplete packets.
[18511.420112] [ENA_COM: ena_com_validate_version] ena device version: 0.10 //The
 driver begins its up process
[18511.420119] [ENA_COM: ena_com_validate_version] ena controller version: 0.0.1
 implementation version 1
[18511.420127] [ENA_COM: ena_com_admin_init] ena_defs : Version:[b9692e8] Build date
 [Wed Apr  6 09:54:21 IDT 2016]
[18512.252108] ena 0000:00:07.0: Device watchdog is Enabled
[18512.674877] ena 0000:00:07.0: irq 46 for MSI/MSI-X
[18512.674933] ena 0000:00:07.0: irq 47 for MSI/MSI-X
[18512.674990] ena 0000:00:07.0: irq 48 for MSI/MSI-X
[18512.675037] ena 0000:00:07.0: irq 49 for MSI/MSI-X
[18512.675085] ena 0000:00:07.0: irq 50 for MSI/MSI-X
[18512.675141] ena 0000:00:07.0: irq 51 for MSI/MSI-X
[18512.675188] ena 0000:00:07.0: irq 52 for MSI/MSI-X
[18512.675233] ena 0000:00:07.0: irq 53 for MSI/MSI-X
[18512.675279] ena 0000:00:07.0: irq 54 for MSI/MSI-X
[18512.772641] [ENA_COM: ena_com_set_hash_function] Feature 10 isn't supported
[18512.772647] [ENA_COM: ena_com_set_hash_ctrl] Feature 18 isn't supported
[18512.775945] ena 0000:00:07.0: Device reset completed successfully // The reset
 process is complete
```

Registre o tempo limite de leitura

A arquitetura de ENA sugere um uso específico limitado de operações de leitura de E/S (MMIO) mapeadas de memória. Os registros de MMIO são acessados pelo driver do dispositivo ENA somente durante o procedimento de inicialização.

Se os logs do driver (disponíveis na saída do dmesg) indicarem falhas nas operações de leitura, isso pode ser causado por um driver incompatível ou incorretamente compilado, um dispositivo de hardware ocupado ou falha de hardware.

As entradas intermitentes do log que indicam falhas nas operações de leitura não devem ser consideradas um problema; o driver fará novas tentativas nesse caso. Contudo, uma sequência de entradas de log contendo falhas de leitura indica problema de driver ou de hardware.

Abaixo está um exemplo de entrada de log do driver indicando falha na operação de leitura devido a um tempo limite:

```
[ 47.113698] [ENA_COM: ena_com_reg_bar_read32] reading reg failed for timeout.
 expected: req id[1] offset[88] actual: req id[57006] offset[0]
[ 47.333715] [ENA_COM: ena_com_reg_bar_read32] reading reg failed for timeout.
 expected: req id[2] offset[8] actual: req id[57007] offset[0]
[ 47.346221] [ENA_COM: ena_com_dev_reset] Reg read32 timeout occurred
```

Statistics

Se você tiver problemas de latência ou de performance de rede insuficiente, recupere as estatísticas dos dispositivos e examine-as. Essas estatísticas podem ser obtidas usando ethtool, como mostrado abaixo:

```
[ec2-user ~]$ ethtool -S ethN
NIC statistics:
 tx_timeout: 0
 suspend: 0
 resume: 0
 wd_expired: 0
 interface_up: 1
 interface_down: 0
 admin_q_pause: 0
 bw_in_allowance_exceeded: 0
 bw_out_allowance_exceeded: 0
 pps_allowance_exceeded: 0
 conntrack_allowance_available: 450878
 conntrack_allowance_exceeded: 0
 linklocal_allowance_exceeded: 0
 queue_0_tx_cnt: 4329
 queue_0_tx_bytes: 1075749
 queue_0_tx_queue_stop: 0
 ...
```

Os parâmetros de saída de comando a seguir estão descritos abaixo:

`tx_timeout`: *N*

O número de vezes que o watchdog Netdev foi ativado.

`suspend`: *N*

O número de vezes que o driver realizou uma operação de suspensão.

`resume`: *N*

O número de vezes que o driver realizou uma operação de retomada.

`wd_expired`: *N*

O número de vezes que o driver não recebeu o evento de keep-alive nos três segundos anteriores.

`interface_up`: *N*

O número de vezes que a interface do ENA foi ativada.

`interface_down`: *N*

O número de vezes que a interface do ENA foi desativada.

`admin_q_pause`: *N*

O número de vezes que a fila do administrador não foi encontrada em um estado de execução.

`bw_in_allowance_exceeded`: *N*

Número de pacotes na fila ou descartados porque a largura de banda agregada de entrada excedeu o máximo para a instância.

`bw_out_allowance_exceeded`: *N*

Número de pacotes na fila ou descartados porque a largura de banda agregada de saída excedeu o máximo para a instância.

`pps_allowance_exceeded`: *N*

Número de pacotes na fila ou descartados porque o PPS bidirecional excedeu o máximo para a instância.*

`conntrack_allowance_available`: *N*

O número de conexões rastreadas que podem ser estabelecidas pela instância antes de atingir a cota de conexões rastreadas desse tipo de instância. Disponível somente para instâncias baseadas em Nitro. Não é compatível com instâncias do FreeBSD ou ambientes DPDK.

`conntrack_allowance_exceeded`: *N*

Número de pacotes descartados porque o monitoramento da conexão excedeu o máximo para a instância e não foi possível estabelecer novas conexões. Isso pode resultar em perda de pacotes para tráfego indo para a instância ou vindo da instância

`linklocal_allowance_exceeded`: *N*

Número de pacotes descartados porque o PPS do tráfego para os serviços de proxy local excedeu o máximo para a interface da rede. Isso afeta o tráfego para o serviço Amazon DNS, o serviço de metadados de instância e o Serviço de Sincronização Temporal da Amazon, mas não afeta o tráfego para resolvedores personalizados de DNS.

`queue_`*N*`_tx_cnt`: *N*

O número de pacotes transmitidos para essa fila.

`queue_`*N*`_tx_bytes`: *N*

O número de bytes transmitidos para essa fila.

`queue_`*N*`_tx_queue_stop`: *N*

O número de vezes em que a fila *N* estava cheia e interrompida.

`queue_`*N*`_tx_queue_wakeup`: *N*

O número de vezes que a fila *N* foi retomada depois de ser interrompida.

`queue_`*N*`_tx_dma_mapping_err`: *N*

Contagem de erro de acesso da memória direta. Se esse valor não for 0, isso indica recursos de sistema baixos.

`queue_`*N*`_tx_linearize`: *N*

O número de vezes que a linearização de SKB foi tentada para essa fila.

`queue_`*N*`_tx_linearize_failed`: *N*

O número de vezes que a linearização de SKB apresentou falha para essa fila.

`queue_`*N*`_tx_napi_comp`: *N*

O número de vezes que o manipulador `napi` chamou `napi_complete` para essa fila.

`queue_`*N*`_tx_tx_poll`: *N*

O número de vezes que o manipulador `napi` foi programado para essa fila.

`queue_N_tx_doorbells`: *N*

O número de campainhas de transmissão para essa fila.

`queue_N_tx_prepare_ctx_err`: *N*

O número de vezes que `ena_com_prepare_tx` apresentou falha para essa fila.

`queue_N_tx_bad_req_id`: *N*

`req_id` inválido para essa fila. O `req_id` válido é zero, menos `queue_size`, menos 1.

`queue_N_tx_llq_buffer_copy`: *N*

O número de pacotes cujo tamanho dos cabeçalhos é maior do que a entrada llq para essa fila.

`queue_N_tx_missed_tx`: *N*

O número de pacotes deixados sem conclusão para essa fila.

`queue_N_tx_unmask_interrupt`: *N*

O número de vezes que a interrupção tx foi desmascarada para essa fila.

`queue_N_rx_cnt`: *N*

O número de pacotes recebidos para essa fila.

`queue_N_rx_bytes`: *N*

O número de bytes recebidos para essa fila.

`queue_N_rx_rx_copybreak_pkt`: *N*

O número de vezes que a fila rx recebeu um pacote menor que o tamanho do pacote de rx_copybreak para essa fila.

`queue_N_rx_csum_good`: *N*

O número de vezes que a fila rx recebeu um pacote em que a soma de verificação foi verificada e estava correta para essa fila.

`queue_N_rx_refil_partial`: *N*

O número de vezes que o driver não teve sucesso ao reabastecer a parte vazia da fila rx com buffers para essa fila. Se esse valor não for zero, isso indica recursos de memória baixa.

`queue_N_rx_bad_csum`: *N*

O número de vezes que a fila `rx` teve uma soma de verificação errada para a fila (somente se o descarregamento da soma de verificação for compatível).

`queue_N_rx_page_alloc_fail`: *N*

O número de vezes que a alocação de página apresentou falha para essa fila. Se esse valor não for zero, isso indica recursos de memória baixa.

`queue_N_rx_skb_alloc_fail`: *N*

O número de vezes que a alocação de SKB apresentou falha para essa fila. Se esse valor não for zero, isso indica recursos de sistema baixos.

`queue_N_rx_dma_mapping_err`: *N*

Contagem de erro de acesso da memória direta. Se esse valor não for 0, isso indica recursos de sistema baixos.

`queue_N_rx_bad_desc_num`: *N*

Excesso de buffers por pacote. Se o valor não for 0, isso indica o uso de buffers muito pequenos.

`queue_N_rx_bad_req_id`: *N*

O req_id para essa fila não é válido. O req_id válido é de [0, queue_size - 1].

`queue_N_rx_empty_rx_ring`: *N*

O número de vezes que a fila rx estava vazia para essa fila.

`queue_N_rx_csum_unchecked`: *N*

O número de vezes que a fila rx recebeu um pacote cuja soma de verificação não foi verificada para essa fila.

`queue_N_rx_xdp_aborted`: *N*

O número de vezes que um pacote XDP foi classificado como XDP_ABORT.

`queue_N_rx_xdp_drop`: *N*

O número de vezes que um pacote XDP foi classificado como XDP_DROP.

`queue_N_rx_xdp_pass`: *N*

O número de vezes que um pacote XDP foi classificado como XDP_PASS.

`queue_N_rx_xdp_tx`: *N*

O número de vezes que um pacote XDP foi classificado como XDP_TX.

`queue_N_rx_xdp_invalid`: *N*

O número de vezes que o código de retorno XDP para o pacote não foi válido.

`queue_N_rx_xdp_redirect: N`

O número de vezes que um pacote XDP foi classificado como XDP_REDIRECT.

`queue_N_xdp_tx_cnt: N`

O número de pacotes transmitidos para essa fila.

`queue_N_xdp_tx_bytes: N`

O número de bytes transmitidos para essa fila.

`queue_N_xdp_tx_queue_stop: N`

O número de vezes que essa fila estava cheia e interrompida.

`queue_N_xdp_tx_queue_wakeup: N`

O número de vezes que essa fila foi retomada depois de ser interrompida.

`queue_N_xdp_tx_dma_mapping_err: N`

Contagem de erro de acesso da memória direta. Se esse valor não for 0, isso indica recursos de sistema baixos.

`queue_N_xdp_tx_linearize: N`

O número de vezes que a linearização de buffer XDP foi tentada para essa fila.

`queue_N_xdp_tx_linearize_failed: N`

O número de vezes que a linearização do buffer XDP apresentou falha para essa fila.

`queue_N_xdp_tx_napi_comp: N`

O número de vezes que o manipulador napi chamou napi_complete para essa fila.

`queue_N_xdp_tx_tx_poll: N`

O número de vezes que o manipulador napi foi programado para essa fila.

`queue_N_xdp_tx_doorbells: N`

O número de campainhas de transmissão para essa fila.

`queue_N_xdp_tx_prepare_ctx_err: N`

O número de vezes que ena_com_prepare_tx apresentou falha para essa fila. Esse valor sempre deve ser zero; caso contrário, consulte os logs do driver.

`queue_N_xdp_tx_bad_req_id: N`

O req_id para essa fila não é válido. O req_id válido é de [0, queue_size - 1].

`queue_N_xdp_tx_llq_buffer_copy: N`

O número de pacotes que tiveram seus cabeçalhos copiados usando a cópia do buffer llq para essa fila.

`queue_N_xdp_tx_missed_tx: N`

O número de vezes que uma entrada de fila tx perdeu um timeout de conclusão para essa fila.

`queue_N_xdp_tx_unmask_interrupt: N`

O número de vezes que a interrupção tx foi desmascarada para essa fila.

`ena_admin_q_aborted_cmd: N`

O número de comandos de administrador que foram abortados. Isso normalmente acontece durante o procedimento de autorrecuperação.

`ena_admin_q_submitted_cmd: N`

O número de campainhas da fila do administrador.

`ena_admin_q_completed_cmd: N`

O número de conclusões da fila do administrador.

`ena_admin_q_out_of_space: N`

O número de vezes que o driver tentou enviar o novo comando de administrador, mas a fila estava cheia.

`ena_admin_q_no_completion: N`

O número de vezes o driver não obteve a conclusão de um administrador para um comando.

Logs de erro do driver no syslog

O driver do ENA grava mensagens de log para syslog durante a inicialização do sistema. É possível 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 alguns 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.

falha em alocar buffer para a fila rx

Esse é um erro recuperável e indica que pode ter havido um problema de pressão de memória quando o erro ocorreu.

Não há suporte para o recurso *X*

O recurso mencionado não é compatível com o Elastic Network Adapter. Os valores possíveis para *X* incluem:

- 10: a configuração da função RSS Hash não é compatível com este dispositivo.
- 12: a configuração da tabela RSS Indirection não é compatível com este dispositivo.
- 18: a configuração de RSS Hash Input não é compatível com este dispositivo.
- 20: a moderação de interrupção não é compatível para este dispositivo.
- 27: o driver Adaptador de Rede Elástica 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.

Notificações de configuração abaixo do ideal

O dispositivo ENA detecta configurações abaixo do ideal no driver, as quais podem ser alteradas. O dispositivo notifica o driver ENA e registra um aviso no console. O exemplo a seguir mostra o formato da mensagem de aviso.

```
Sub-optimal configuration notification code: 1. Refer to AWS ENA documentation for
 additional details and mitigation options.
```

A lista a seguir mostra detalhes do código de notificação e as ações recomendadas para descobertas de configurações abaixo do ideal.

- Código 1: não é recomendado utilizar o ENA Express com configuração de LLQ amplo

  A ENI do ENA Express está configurada com LLQ amplo. Essa configuração está abaixo do ideal e pode afetar a performance do ENA Express. Recomendamos desabilitar as configurações de LLQ amplo ao usar ENIs do ENA Express conforme mostrado a seguir.

  ```
  sudo rmmod ena && sudo modprobe ena force_large_llq_header=0
  ```

  Para obter mais informações sobre a configuração ideal do ENA Express consulte Melhorar a performance da rede entre instâncias do EC2 com ENA Express.

- Código 2: não é recomendado usar a ENI do ENA Express com profundidade de fila Tx abaixo do ideal

  A ENI do ENA Express está configurada com profundidade de fila Tx abaixo do ideal. Essa configuração pode afetar a performance do ENA Express. Recomendamos aumentar todas as filas Tx para o valor máximo para a interface de rede quando você usar ENIs do ENA Express como a seguir.

  É possível pode executar os seguintes comandos ethtool para ajustar o tamanho do LLQ
  Para saber mais sobre como controlar, consultar e habilitar o LLQ amplo, consulte o tópico Enfileiramento de baixa latência grande (Large LLQ) da documentação do driver do kernel Linux para ENA no Repositório de drivers da Amazon no GitHub.

  ```
  ethtool -g interface
  ```

  Defina suas filas Tx para a profundidade máxima:

  ```
  ethtool -G interface tx depth
  ```

  Para obter mais informações sobre a configuração ideal do ENA Express consulte Melhorar a performance da rede entre instâncias do EC2 com ENA Express.

- Código 3: ENA com tamanho de LLQ normal e tráfego de pacotes Tx excede o tamanho máximo aceito pelo cabeçalho

  Por padrão, o LLQ do ENA oferece suporte a cabeçalhos de pacote Tx com até 96 bytes de tamanho. Se o tamanho do cabeçalho do pacote for maior que 96 bytes, o pacote será descartado. Para mitigar esse problema, recomendamos habilitar o LLQ amplo, o que aumenta o tamanho máximo do cabeçalho do pacote Tx para 224 bytes.

  No entanto, quando você ativa o LLQ amplo, o tamanho máximo do anel Tx é reduzido de 1000 para 512 entradas. O LLQ amplo é habilitado por padrão para todos os tipos de instância Nitro v4 e posteriores.

  - Os tipos de instância Nitro v4 têm um tamanho de anel Tx de LLQ amplo máximo padrão de 512 entradas, que não pode ser alterado.
  - Os tipos de instância Nitro v5 têm um tamanho de anel Tx de LLQ amplo padrão de 512 entradas, o qual pode ser alterado para até 1000 entradas.

É possível pode executar os seguintes comandos ethtool para ajustar o tamanho do LLQ
Para saber mais sobre como controlar, consultar e habilitar o LLQ amplo, consulte o tópico Enfileiramento de baixa latência grande (Large LLQ) da documentação do driver do kernel Linux para ENA no Repositório de drivers da Amazon no GitHub.

Encontre a profundidade máxima para suas filas Tx:

```
ethtool -g interface
```

Defina suas filas Tx para a profundidade máxima:

```
ethtool -G interface tx depth
```

Solução de problemas do driver do Adaptador de Rede Elástica do Windows

O Elastic Network Adapter (ENA) é projetado para melhorar a integridade do sistema operacional e reduzir as possibilidades de interrupção na operação da sua instância de Windows por conta de comportamento inesperado de hardware ou falhas. A arquitetura do ENA mantém falhas do dispositivo ou do driver o mais transparentes possível para o sistema operacional.

Colete informações de diagnóstico sobre a instância

As etapas para abrir as ferramentas do sistema operacional (SO) Windows variam, dependendo da versão do sistema operacional instalada na instância. Nas seções a seguir, usamos a caixa de diálogo Run (Executar) para abrir as ferramentas, o que funciona da mesma forma em todas as versões do sistema operacional. No entanto, é possível acessar essas ferramentas usando qualquer método que preferir.

Acesse a caixa de diálogo Run (Executar)

- Usando a combinação de teclas do logo do Windows: `Windows + R`
- Usando a barra de pesquisa:
  - Insira `run` na barra de pesquisa.
  - Selecione a aplicação Run (Executar) a partir dos resultados da pesquisa.

Algumas etapas exigem que o menu de contexto acesse propriedades ou ações sensíveis ao contexto. Há várias maneiras de fazer isso, dependendo da versão do sistema operacional e do hardware.

Acesse o menu de contexto

- Usando o mouse: clique com o botão direito do mouse em um item para abrir seu menu de contexto.
- Usando o teclado:
  - Dependendo da versão do sistema operacional, use `Shift` + `F10`, ou `Ctrl` + `Shift` + `F10`.
  - Se você tiver a tecla de contexto no teclado (três linhas horizontais em uma caixa), selecione o item desejado e pressione a tecla de contexto.

Se você puder se conectar à instância, use as técnicas a seguir para coletar informações de diagnóstico para solução de problemas.

Verifique o status do dispositivo ENA

Para verificar o status do driver ENAdo Windows usando o Gerenciador de dispositivos do Windows, siga estas etapas:

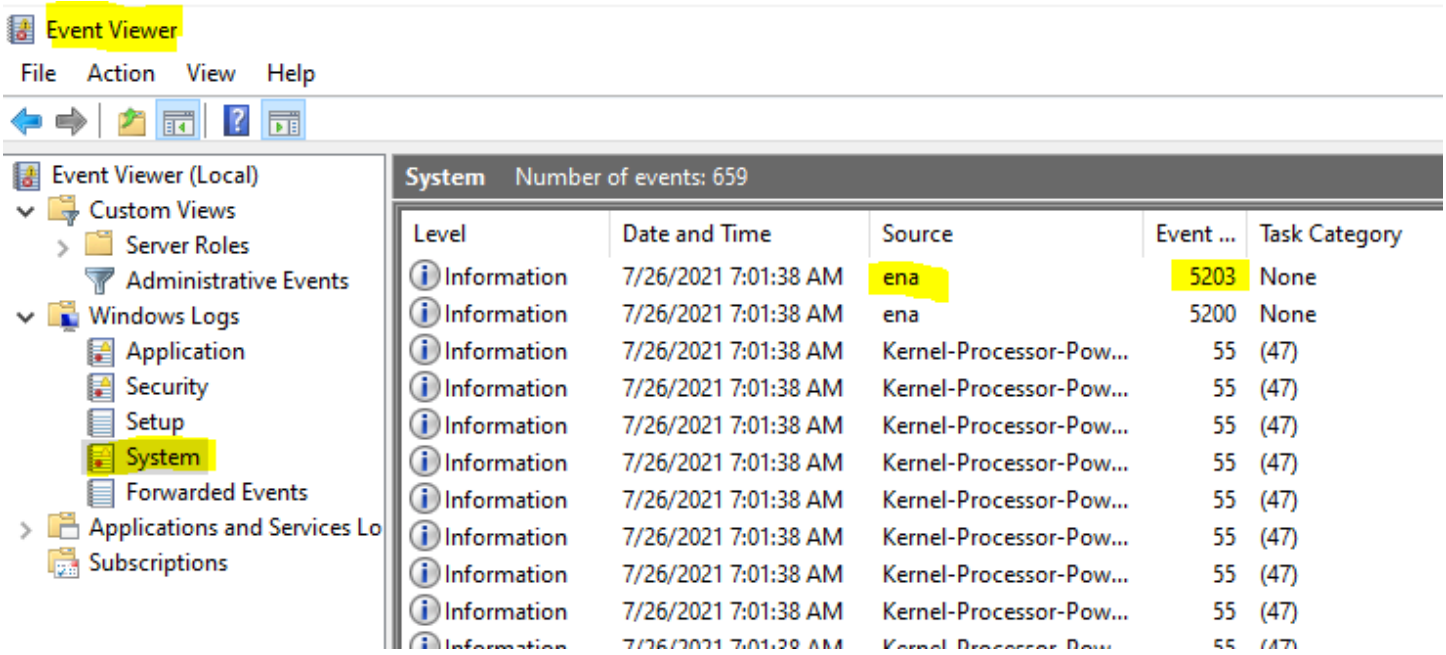
1. Abra a caixa de diálogo Run (Executar) usando um dos métodos descritos na seção anterior.
2. Para abrir o Gerenciador de dispositivos do Windows, insira `devmgmt.msc` na caixa Run (Executar).
3. Escolha OK. Isso abre a janela Gerenciador de dispositivos.
4. Selecione a seta à esquerda de Network adapters (Adaptadores de rede) para expandir a lista.
5. Escolha o nome ou abra o menu de contexto para Amazon Elastic Network Adapter (Adaptador do Amazon Elastic Network) e, depois, escolha Properties (Propriedades). Isso abre a caixa de diálogo Propriedades do Adaptador de Rede Elástica da Amazon.
6. Verifique se a mensagem na guia Geral sinaliza "Este dispositivo está funcionando corretamente".

Investigue mensagens de evento do driver

Para revisar os logs de eventos do driver ENA do Windows usando o Visualizador de eventos do Windows, siga estas etapas:

1. Abra a caixa de diálogo Run (Executar) usando um dos métodos descritos na seção anterior.
2. Para abrir o Visualizador de eventos do Windows, insira `eventvwr.msc` na caixa Run (Executar).
3. Escolha OK. Isso abrirá a janela Event Viewer (Visualizador de eventos).
4. Expanda o menu Windows Logs (Logs do Windows) e, em seguida, escolha System (Sistema).
5. Em Actions (Ações), no painel superior direito, escolha Filter Current Log (Filtrar log atual). Isso exibe a caixa de diálogo de filtragem.
6. Na caixa Event sources (Origens de eventos), insira `ena`. Isso limita os resultados a eventos gerados pelo driver ENA do Windows.
7. Escolha OK. Isso mostra os resultados do log de eventos filtrados nas seções de detalhes da janela.
8. Para examinar os detalhes, selecione uma mensagem de evento na lista.

O exemplo a seguir mostra um evento de driver ENA na lista de eventos do sistema do Visualizador de eventos do Windows:



Resumo da mensagem do evento

A tabela a seguir mostra as mensagens de evento geradas pelo driver ENA do Windows.

Entrada

ID do evento	Descrição do evento do driver ENA	Tipo
5001	Hardware is out of resources (O hardware está sem recursos)	Erro
5002	Adapter has detected a hardware error (O adaptador detectou um erro de hardware)	Erro
5005	Adapter has timed out on NDIS operation that did not complete in a timely manner (O adaptador expirou o tempo limite na operação do NDIS que não foi concluída em tempo hábil)	Erro
5032	Adapter has failed to reset the device (Falha do adaptador ao redefinir o dispositivo)	Erro
5200	Adapter has been initialized (O adaptador foi inicializado)	Informativo
5201	Adapter has been halted (O adaptador foi interrompido)	Informativo
5202	Adapter has been paused (O adaptador foi pausado)	Informativo
5203	Adapter has been restarted (O adaptador foi reiniciado)	Informativo

ID do evento	Descrição do evento do driver ENA	Tipo
5204	Adapter has been shut down (O adaptador foi desligado)	Informativo
5205	Adapter has been reset (O adaptador foi redefinido)	Erro
5206	Adapter has been surprise removed (O adaptador foi removido de surpresa)	Erro
5208	Adapter initialization routine has failed (A rotina de inicializ ação do adaptador falhou)	Erro
5210	Adapter has encountered and successfully recovered an internal issue (O adaptador encontrou problema interno e recuperou com êxito)	Erro

Analise as métricas de performance

O driver ENA do Windows publica métricas de performance de rede de instâncias onde elas estão habilitadas. É possível exibir e habilitar métricas na instância usando a aplicação nativa Monitor de performance. Para obter mais informações sobre as métricas que o driver ENA do Windows produz, consulte Monitorar o desempenho de rede de instâncias do EC2.

Em casos em que as métricas do ENA estão habilitadas e o agente do Amazon CloudWatch está instalado, o CloudWatch coleta as métricas associadas aos contadores no Monitor de performance do Windows, bem como algumas métricas avançadas para o ENA. Essas métricas são coletadas além das métricas habilitadas por padrão em instâncias do EC2. Para obter mais informações sobre as métricas, consulte Métricas coletadas pelo agente CloudWatch no Guia do usuário do Amazon CloudWatch.

> **Note**
>
> As métricas de performance estão disponíveis para as versões 2.4.0 e posteriores do driver ENA (também para a versão 2.2.3). O driver ENA versão 2.2.4 foi revertido devido à possível degradação da performance nas instâncias do EC2 de sexta geração. Recomendamos que você atualize para a versão atual do driver para garantir que tenha as últimas atualizações.

Algumas maneiras como usar métricas de performance são:

- Solucionar problemas de performance de instâncias.
- Escolher o tamanho certo de instância para um workload.
- Planejar atividades de escalabilidade proativamente.
- Fazer benchmark em aplicações para determinar se elas maximizam a performance disponível em uma instância.

Taxa de atualização

Por padrão, o driver atualiza métricas usando um intervalo de 1 segundo. No entanto, a aplicação que recupera as métricas pode usar um intervalo diferente para sondagem. É possível alterar o intervalo de atualização no Gerenciador de dispositivos, usando as propriedades avançadas do driver.

Para alterar o intervalo de atualização de métricas para o driver ENA do Windows, siga estas etapas:

1. Abra a caixa de diálogo Run (Executar) usando um dos métodos descritos na seção anterior.
2. Para abrir o Gerenciador de dispositivos do Windows, insira `devmgmt.msc` na caixa Run (Executar).
3. Escolha OK. Isso abre a janela Gerenciador de dispositivos.
4. Selecione a seta à esquerda de Network adapters (Adaptadores de rede) para expandir a lista.
5. Escolha o nome ou abra o menu de contexto para Amazon Elastic Network Adapter (Adaptador do Amazon Elastic Network) e, depois, escolha Properties (Propriedades). Isso abre a caixa de diálogo Propriedades do Adaptador de Rede Elástica da Amazon.
6. Abra a guia Advanced (Avançado) na janela suspensa.
7. Na lista Property (Propriedade), escolha Metrics Refresh Interval (Intervalo de atualização das métricas) para alterar o valor.

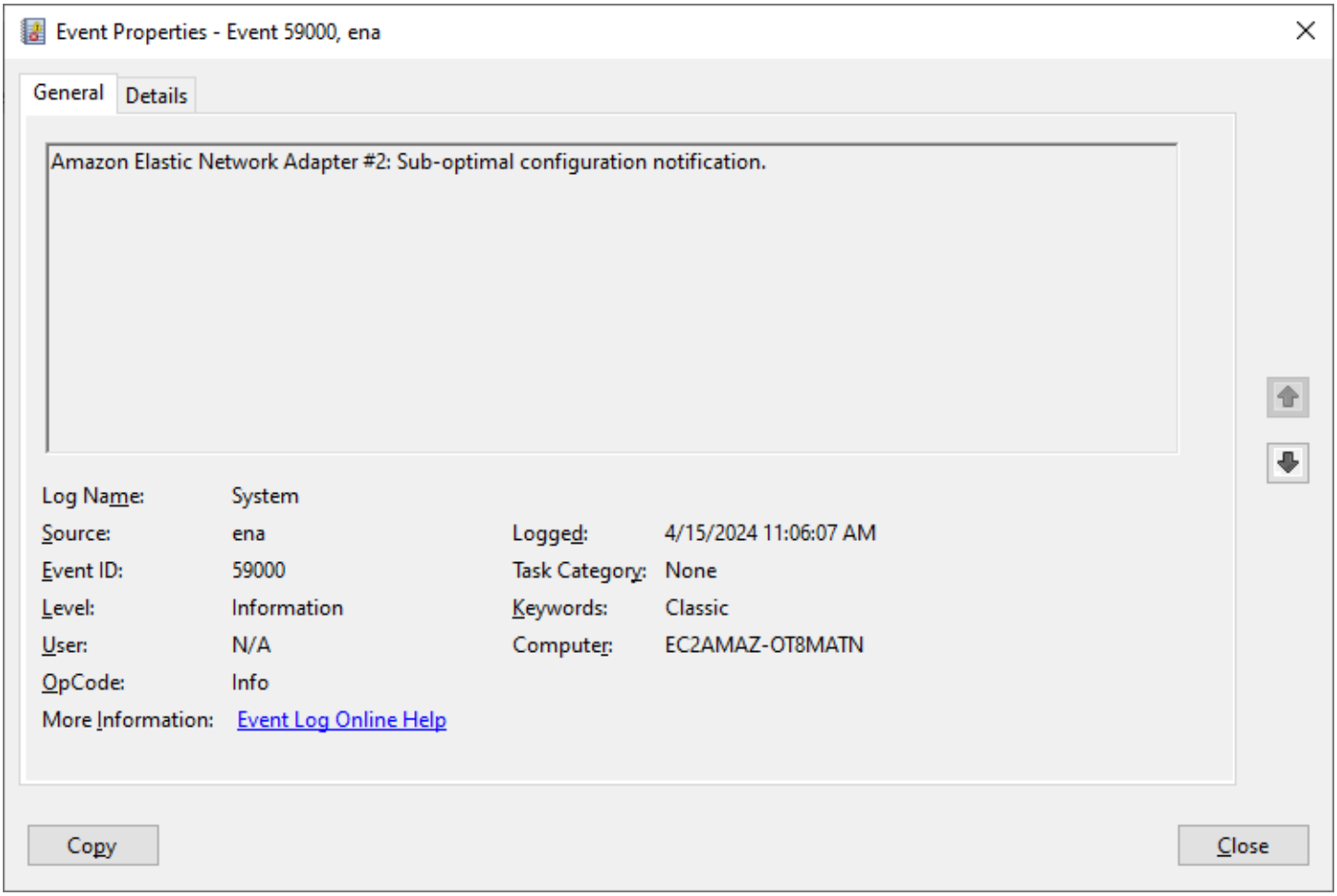
8. Quando tiver concluído, escolha OK.

Investigar notificações de configuração aquém do ideal

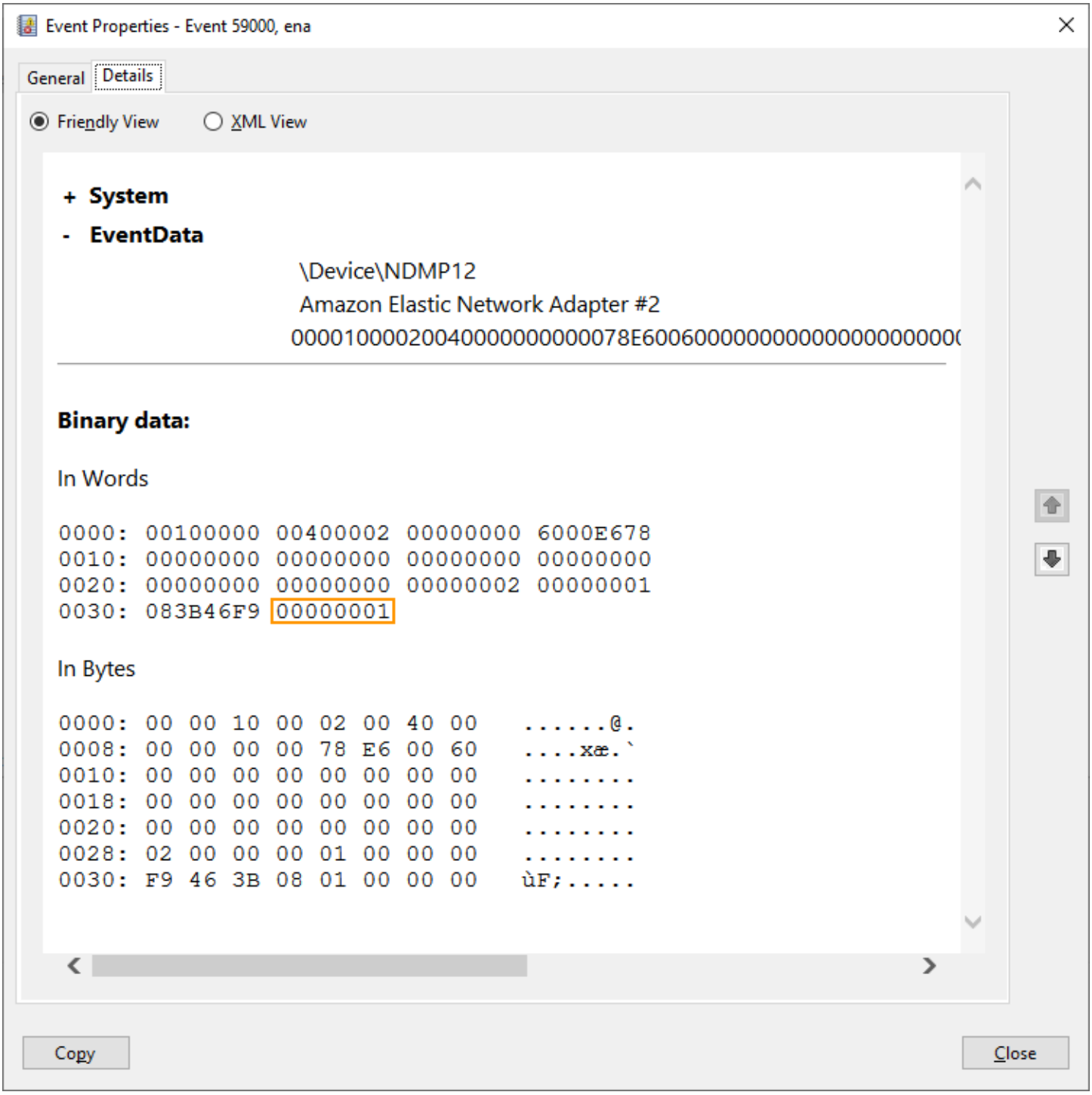
O dispositivo ENA detecta configurações abaixo do ideal no driver, as quais podem ser alteradas. O dispositivo notifica o driver do ENA e registra uma notificação de evento. Para revisar os eventos de configuração aquém do ideal no Visualizador de Eventos do Windows

1. Abra a caixa de diálogo Run (Executar) usando um dos métodos descritos na seção anterior.
2. Para abrir o Visualizador de eventos do Windows, insira `eventvwr.msc` na caixa Run (Executar).
3. Escolha OK. Isso abrirá a janela Event Viewer (Visualizador de eventos).
4. Expanda o menu Windows Logs (Logs do Windows) e, em seguida, escolha System (Sistema).
5. Em Actions (Ações), no painel superior direito, escolha Filter Current Log (Filtrar log atual). Isso exibe a caixa de diálogo de filtragem.
6. Na caixa Event sources (Origens de eventos), insira `ena`. Isso limita os resultados a eventos gerados pelo driver ENA do Windows.
7. Escolha OK. Isso mostra os resultados do log de eventos filtrados nas seções de detalhes da janela.

Os eventos com o ID `5900`0 notificam você sobre descobertas de configuração aquém do ideal. Clique com o botão direito do mouse em um evento e escolha Propriedades do evento para abrir uma visualização detalhada ou selecione Painel de visualização no menu Visualizar para ver os mesmos detalhes.



Abra a guia Detalhes para ver o código do evento. Na seção Dados binários: em palavras, a última palavra é o código.



A lista a seguir mostra detalhes do código de notificação e as ações recomendadas para descobertas de configurações abaixo do ideal.

- Código **1**: não é recomendado utilizar o ENA Express com configuração de LLQ amplo

A ENI do ENA Express está configurada com LLQ amplo. Essa configuração está abaixo do ideal e pode afetar a performance do ENA Express. Recomendamos desabilitar as configurações de LLQ amplo ao usar ENIs do ENA Express conforme mostrado a seguir.

1. Para abrir o Gerenciador de dispositivos do Windows, insira `devmgmt.msc` na caixa Run (Executar).
2. Escolha OK. Isso abre a janela Gerenciador de dispositivos.
3. Selecione a seta à esquerda de Network adapters (Adaptadores de rede) para expandir a lista.
4. Abra as propriedades de dispositivo para o `Amazon Elastic Network Adapter`.
5. Ali, abra a guia Avançado para fazer as alterações.
6. Selecione a propriedade Política de tamanho de cabeçalho de LLQ e defina seu valor como `Normal (128 Bytes)`.
7. Escolha OK para salvar as alterações.

- Código **2**: ENI do ENA Express com profundidade de fila Tx abaixo do ideal não é recomendada

  A ENI do ENA Express está configurada com profundidade de fila Tx abaixo do ideal. Essa configuração pode afetar a performance do ENA Express. Recomendamos aumentar todas as filas Tx para o valor máximo para a interface de rede quando você usar ENIs do ENA Express como a seguir.

  Siga estas etapas para aumentar as filas de Tx para a profundidade máxima:

  1. Para abrir o Gerenciador de dispositivos do Windows, insira `devmgmt.msc` na caixa Run (Executar).
  2. Escolha OK. Isso abre a janela Gerenciador de dispositivos.
  3. Selecione a seta à esquerda de Network adapters (Adaptadores de rede) para expandir a lista.
  4. Abra as propriedades de dispositivo para o `Amazon Elastic Network Adapter`.
  5. Ali, abra a guia Avançado para fazer as alterações.
  6. Selecione a propriedade Buffers de transmissão e defina seu valor como o máximo permitido.
  7. Escolha OK para salvar as alterações.

Redefinição do adaptador ENA

O processo de redefinição é iniciado quando o driver ENA do Windows detecta um erro em um adaptador e marca o adaptador como não íntegro. O driver não pode redefinir a si mesmo,

portanto, depende do sistema operacional verificar o status da integridade do adaptador e chamar o identificador de redefinição para o driver ENA do Windows. O processo de redefinição pode resultar em um breve período de tempo em que ocorre perda de tráfego. No entanto, as conexões TCP devem ser capazes de se recuperar.

O adaptador ENA também pode solicitar indiretamente um procedimento de redefinição do dispositivo, ao não enviar uma notificação de manutenção de atividade. Por exemplo, se o adaptador ENA atingir um estado desconhecido depois de carregar uma configuração irrecuperável, poderá parar de enviar notificações de keep-alive.

Causas comuns para redefinição do adaptador ENA

- Mensagens de keep-alive estão ausentes

  O dispositivo ENA posta eventos de keep-alive em uma taxa fixa (geralmente uma vez por segundo). O driver ENA do Windows implanta um mecanismo de watchdog, que verifica a presença dessas mensagens keep-alive. Se detectar uma ou mais novas mensagens desde a última vez que foi verificada, ele registra um resultado de êxito. Caso contrário, o driver conclui que o dispositivo sofreu uma falha e inicia uma sequência de redefinição.
- Os pacotes estão presos em filas de transmissão

  O adaptador ENA verifica se os pacotes estão fluindo pelas filas de transmissão conforme esperado. O driver ENA do Windows detecta se os pacotes estão ficando presos e inicia uma sequência de redefinição caso estejam.
- Tempo limite de leitura para registros de E/S mapeados da memória (MMIO)

  Para limitar as operações de leitura de E/S mapeadas de memória (MMIO), o driver ENA do Windows acessa os registros do MMIO somente durante os processos de inicialização e redefinição. Se o driver detectar um tempo limite, ele executará uma das seguintes ações, dependendo do processo em execução:
  - Se um tempo limite for detectado durante a inicialização, ele falhará no fluxo, o que resulta na exibição de um ponto de exclamação amarelo pelo adaptador ENA no Gerenciador de dispositivos do Windows.
  - Se um tempo limite for detectado durante a reinicialização, ele falhará no fluxo. O sistema operacional inicia uma remoção surpresa do adaptador ENA e o recupera parando e iniciando o adaptador que foi removido. Para obter mais informações sobre a remoção surpresa de uma placa de interface de rede (NIC), consulte Como lidar com a remoção surpresa de uma NIC na documentação Desenvolvedor de hardware do Microsoft Windows.

Cenários de solução de problemas

Os cenários a seguir podem ajudar a solucionar problemas que possam ocorrer com o driver ENA do Windows. Recomendamos que você comece atualizando seu driver ENA, se você não tiver a versão mais recente. Para encontrar o driver mais recente para a versão do sistema operacional Windows, consulte Rastrear os lançamentos da versão do driver do ENA do Windows.

Versão inesperada do driver ENA instalada

Descrição

Depois de seguir as etapas para instalar uma versão específica do driver ENA, o gerenciador de dispositivos do Windows mostra que o Windows instalou uma versão diferente do driver ENA.

Causa

Quando você executa a instalação de um pacote de driver, o Windows classifica todos os pacotes de drivers válidos para determinado dispositivo no armazenamento de drivers local antes da execução. Em seguida, ele seleciona o pacote com o menor valor de classificação como a melhor correspondência. Isso pode ser diferente do pacote que você pretendia instalar. Para obter mais informações sobre o processo de seleção do pacote de driver de dispositivo, consulte Como o Windows seleciona um pacote de driver para um dispositivo no site de documentação da Microsoft.

Solução

Para garantir que o Windows instale a versão do pacote de driver escolhida, você pode remover pacotes de drivers de classificação inferior do armazenamento de drivers com a ferramenta de linha de comando PnPUtil.

Siga estas etapas para atualizar o driver ENA:

1. Conecte-se à instância e faça login como administrador local.
2. Abra a janela de propriedades do Gerenciador de dispositivos, conforme descrito na seção Verifique o status do dispositivo ENA. Isso abre a guia Geral da janela Propriedades do Adaptador de Rede Elástica da Amazon.
3. Abra a guia Driver.
4. Escolha Update Driver (Atualizar driver). Isso abre a caixa de diálogo Atualizar software do driver: Adaptador de Rede Elástica da Amazon.
    a. Na seção Como deseja pesquisar o software de driver?, escolha Procurar software de driver no computador.

b. Na página Procurar software de driver no computador, escolha Permitir escolher em uma lista de drivers de dispositivo em meu computador, localizado abaixo da barra de pesquisa.

c. Na página Selecionar o driver do dispositivo que você deseja instalar para este hardware, escolha Ter disco....

d. Na janela Instalar do disco, escolha Procurar..., próximo à localização na lista suspensa.

e. Navegue até o local em que você fez o download do pacote de driver ENA de destino. Selecione o arquivo denominado `ena.inf` e escolha Abrir.

f. Para iniciar a instalação, escolha OK e, em seguida, escolha Avançar.

5. Se o instalador não reinicializar automaticamente sua instância, execute o cmdlet Restart-Computer do PowerShell.

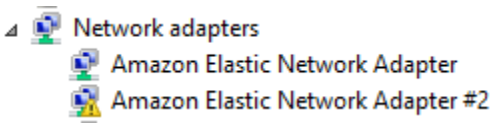
```
PS C:\> Restart-Computer
```

Aviso de dispositivo para driver ENA

Descrição

O ícone do adaptador ENA na seção Network adapters (Adaptadores de rede) do Gerenciador de dispositivos exibe um sinal de aviso (um triângulo amarelo com um ponto de exclamação dentro).

O exemplo a seguir mostra um adaptador ENA com o ícone de aviso no Gerenciador de dispositivos do Windows:



Causa

Esse aviso de dispositivo geralmente é causado por problemas de ambiente, o que pode exigir mais pesquisas, e muitas vezes exige um processo de eliminação para determinar a causa subjacente. Para obter uma lista completa de erros do dispositivo, consulte Mensagens de erro do Gerenciador de dispositivos na documentação da Microsoft.

Solução

A solução para este aviso de dispositivo depende da causa raiz. O processo de eliminação descrito aqui inclui algumas etapas básicas para ajudar a identificar e resolver os problemas mais comuns

que podem ter uma solução simples. É necessária uma análise de causa raiz adicional quando essas etapas não resolvem o problema.

Siga estas etapas para ajudar a identificar e resolver problemas comuns:

1. Interrompa e inicie o dispositivo.

   Abra a janela de propriedades do Gerenciador de dispositivos, conforme descrito na seção Verifique o status do dispositivo ENA. Isso abre a guia General (Geral) da janela Amazon Elastic Network Adapter Properties (Propriedades do adaptador do Amazon Elastic Network), onde Device status (Status do dispositivo) exibe o código de erro e uma mensagem curta.

   a. Abra a guia Driver.
   b. Selecione Disable Device (Desabilitar dispositivo) e responda Yes (Sim) para a mensagem de aviso exibida.
   c. Selecione Enable Device (Habilitar dispositivo).
2. Interrompa e inicie a instância do EC2

   Se o adaptador ainda mostrar o ícone de aviso no Gerenciador de dispositivos, a próxima etapa é interromper e iniciar a instância do EC2. Isso reinicia a instância em hardware diferente na maioria dos casos.
3. Investigue possível problema de recursos da instância

   Se você interrompeu e iniciou sua instância do EC2 e o problema persistir, isso pode indicar um problema de recurso na instância, como memória insuficiente.

Tempo limite de conexão com redefinição do adaptador (códigos de erro 5007, 5205)

Descrição

O Visualizador de eventos do Windows mostra o tempo limite do adaptador e os eventos de redefinição que ocorrem em combinação para adaptadores ENA. As mensagens são semelhantes aos exemplos a seguir:

- ID do evento 5007: adaptador do Amazon Elastic Network: Timed out during an operation (Tempo limite durante uma operação).
- ID do evento 5205: adaptador do Amazon Elastic Network Adapter: Adapter reset has been started (A redefinição do adaptador foi iniciada).

As redefinições do adaptador causam interrupção mínima no tráfego. Mesmo quando há várias redefinições, seria incomum que elas causem qualquer interrupção grave da rede.

Causa

Essa sequência de eventos indica que o driver ENA Windows iniciou uma redefinição para um adaptador ENA que não respondeu. No entanto, o mecanismo que o driver do dispositivo usa para detectar esse problema está sujeito a falsos positivos resultantes da falta de CPU 0.

Solução

Se essa combinação de erros ocorrer com frequência, verifique suas alocações de recursos para ver onde os ajustes podem ser úteis.

1. Abra a caixa de diálogo Run (Executar) usando um dos métodos descritos na seção anterior.
2. Para abrir o Monitor de recursos do Windows, insira `resmon` na caixa Run (Executar).
3. Escolha OK. Isso abre a janela do Monitor de recursos.
4. Abra a guia CPU. Gráficos de uso por CPU são mostrados ao longo do lado direito da janela Monitor de recursos.
5. Verifique os níveis de uso da CPU 0 para ver se eles estão muito altos.

Recomendamos que você configure o RSS para excluir a CPU 0 para o adaptador ENA em tipos de instância maiores (mais de 16 vCPU). Para tipos de instância menores, a configuração do RSS pode melhorar a experiência, mas devido ao menor número de núcleos disponíveis, o teste é necessário para garantir que a restrição dos núcleos da CPU não impacte negativamente a performance.

Use o comando Set-NetAdapterRss para configurar o RSS para seu adaptador ENA, conforme mostrado no exemplo a seguir.

```
Set-NetAdapterRss -name (Get-NetAdapter | Where-Object {$_.InterfaceDescription -like
 "*Elastic*"}).Name -Baseprocessorgroup 0 -BaseProcessorNumber 1
```

A migração para uma infra-estrutura de instância de sexta geração afeta a performance ou a anexação

Descrição

Se você migrar para uma instância do EC2 de sexta geração, poderá ter uma performance reduzida ou falhas de anexação do ENA se não tiver atualizado a versão do driver do ENA Windows.

Causa

Os tipos de instância do EC2 de sexta geração exigem a seguinte versão mínima do driver ENA para Windows, com base no sistema operacional da instância.

Versão mínima

Versão Windows Server	Versão do driver ENA
Windows Server 2008 R2	2.2.3 ou 2.4.0
Windows Server 2012 e posterior	2.2.3 e posterior
Estação de trabalho Windows	2.2.3 e posterior

Solução

Antes de fazer o upgrade para uma instância do EC2 de sexta geração, certifique-se de que a AMI a partir da qual você iniciar tenha os drivers compatíveis com base no sistema operacional da instância, como mostrado na tabela anterior. Para obter mais informações, consulte What do I need to do before migrating my EC2 instance to a sixth generation instance to make sure that I get maximum network performance? no AWS re:Post Knowledge Center.

Performance abaixo da ideal para a interface de rede elástica (ENI)

Descrição

A interface ENA não está funcionando conforme o esperado.

Causa

A análise de causa raiz para problemas de performance é um processo de eliminação. Existem muitas variáveis envolvidas para se nomear uma causa comum.

Solução

A primeira etapa na análise da causa raiz é revisar as informações de diagnóstico da instância que não está funcionando conforme o esperado, para determinar se há erros que podem estar causando

o problema. Para obter mais informações, consulte a seção Colete informações de diagnóstico sobre a instância.

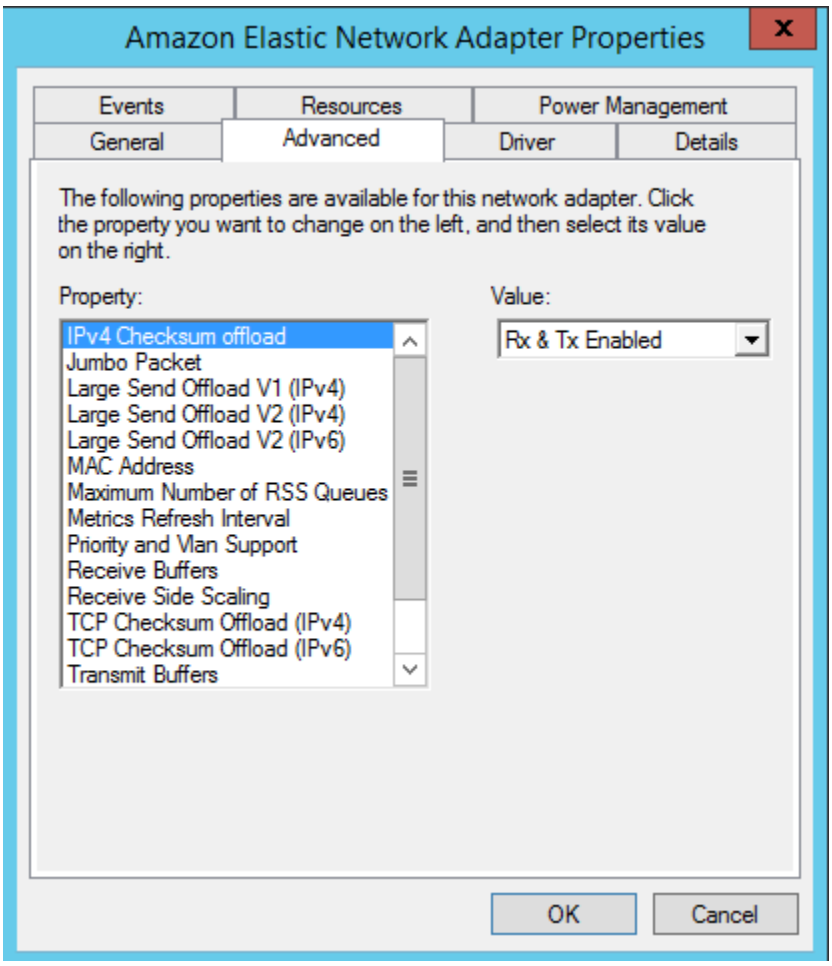
Para obter a máxima performance da rede em instâncias com redes avançadas, pode ser necessário modificar a configuração do sistema operacional padrão. Outras otimizações, como ativar o descarregamento de soma de verificação e a habilitação do RSS, por exemplo, já estão em vigor por padrão em AMIs oficiais do Windows. Para outras otimizações que você pode aplicar ao adaptador ENA, consulte os ajustes de performance mostrados em Ajustes de performance do adaptador ENA.

Recomendamos que você prossiga com cautela e limite os ajustes de propriedade do dispositivo àqueles listados nesta seção ou a alterações específicas recomendadas pela equipe de suporte da AWS.

Para alterar as propriedades do adaptador ENA, siga estas etapas:

1. Abra a caixa de diálogo Run (Executar) usando um dos métodos descritos na seção anterior.
2. Para abrir o Gerenciador de dispositivos do Windows, insira `devmgmt.msc` na caixa Run (Executar).
3. Escolha OK. Isso abre a janela Gerenciador de dispositivos.
4. Selecione a seta à esquerda de Network adapters (Adaptadores de rede) para expandir a lista.
5. Escolha o nome ou abra o menu de contexto para Amazon Elastic Network Adapter (Adaptador do Amazon Elastic Network) e, depois, escolha Properties (Propriedades). Isso abre a caixa de diálogo Propriedades do Adaptador de Rede Elástica da Amazon.
6. Para fazer suas alterações, abra a guia Avançado.
7. Quando concluir, escolha OK para salvar suas alterações.

O exemplo a seguir mostra uma propriedade do adaptador ENA Gerenciador de dispositivos do Windows.



Ajustes de performance do adaptador ENA

A tabela a seguir inclui propriedades que podem ser ajustadas para melhorar a performance da interface ENA.

Entrada

Propriedade	Descrição	Valor padrão	Ajuste
Buffers de recebimento	Controla o número de entradas nas filas de recebimento do software.	1024	Pode ser aumentado até um máximo de 8192.
Receive Side Scaling (RSS)	Habilita a distribuição eficiente do	Habilitada	É possível espalhar a carga em vários

Propriedade	Descrição	Valor padrão	Ajuste
	processamento de recebimento de rede em várias CPUs em sistemas multiproc essadores.		processadores. Para saber mais, consulte Otimizar performance da rede em instâncias do Windows do EC2.

Propriedade	Descrição	Valor padrão	Ajuste
Número máximo de filas de RSS	Define o número máximo de filas de RSS permitidas quando RSS está habilitado.	32	O número de filas de RSS é determinado durante a inicialização do driver e inclui as seguintes limitações (entre outras): • Limite de fila de RSS definido por esta propriedade • Limites de instância (contagem de vCPU) • Limites de geração de hardware (até oito filas de RSS no ENAv1 e até 32 filas de RSS no ENAv2) É possível definir o valor de 1 a 32, dependendo dos limites de geração de instância e hardware. Para saber mais, consulte Otimizar performance da rede em instâncias do Windows do EC2.

Propriedade	Descrição	Valor padrão	Ajuste
Pacote jumbo	Permite o uso de frames jumbo ethernet (mais de 1500 bytes de carga útil).	Desabilitado (isso limita a carga útil a 1500 bytes ou menos)	O valor pode ser configurado para `9015`, o que se traduz em 9001 bytes de carga útil. Essa é a carga útil máxima para frames ethernet jumbo. Consulte Considerações sobre o uso de frames ethernet jumbo.

Considerações sobre o uso de frames ethernet jumbo

Os frames jumbo permitem mais de 1500 bytes de dados ao aumentar o tamanho da carga útil por pacote, o que aumenta o percentual do pacotes que não configura sobrecarga. São necessários menos pacotes para enviar a mesma quantidade de dados usáveis. No entanto, o tráfego é limitado a um MTU máximo de 1500 nos seguintes casos:

- Tráfego fora de uma determinada região da AWS para EC2 Classic.
- Tráfego fora de uma única VPC
- Tráfego em uma conexão de emparelhamento de VPC entre regiões
- Tráfego através de ligações de VPN
- Tráfego em um gateway de Internet

> **Note**
>
> Pacotes com mais de 1500 bytes são fragmentados. Se você tiver o sinalizador `Don't Fragment` definido no cabeçalho IP, esses pacotes são descartados.
> Os frames jumbo devem ser usados com cuidado para o tráfego voltado para Internet ou qualquer tráfego que saia de uma VPC. Os pacotes são fragmentados por sistemas

intermediários, que retarda o tráfego. Para usar frames jumbo dentro de uma VPC sem afetar o tráfego de saída que está saindo da VPC, tente uma das seguintes opções:

- Configure o tamanho da MTU por rota.
- Use várias interfaces de rede com diferentes tamanhos de MTU e rotas diferentes.

Casos de uso recomendados para frames jumbo

Frames jumbo podem ser úteis para tráfego dentro de e entre VPCs. Recomendamos usar frames jumbo para os seguintes casos de uso:

- Para instâncias posicionadas em um grupo de posicionamento de cluster, os frames jumbo ajudam a alcançar a throughput máxima de rede possível. Para ter mais informações, consulte Grupos de posicionamento para as instâncias do Amazon EC2.
- É possível usar quadros jumbo para tráfego entre suas VPCs e suas redes on-premises por meio do Direct Connect. Para obter mais informações sobre o uso de Direct Connect e a verificação da capacidade de frames jumbo, consulte MTU para interfaces virtuais privadas ou interfaces virtuais de trânsito no Guia do usuário do Direct Connect.
- Para obter mais informações sobre tamanhos de MTU compatíveis com gateways de trânsito, consulte Cotas para seus gateways de trânsito em Gateways de trânsito da Amazon VPC.

Melhorar a performance da rede entre instâncias do EC2 com ENA Express

O ENA Express conta com a tecnologia AWS Scalable Reliable Datagram (SRD). SRD é um protocolo de transporte de rede de alta performance que usa roteamento dinâmico para aumentar o throughput e minimizar a latência final. Com o ENA Express, é possível estabelecer a comunicação entre duas instâncias do EC2 na mesma zona de disponibilidade.

Benefícios do ENA Express

- Aumenta a largura de banda máxima que um fluxo único pode usar de 5 Gbps para até 25 Gbps dentro da zona de disponibilidade, respeitando o limite agregado da instância.
- Reduz a latência final do tráfego de rede entre instâncias do EC2, especialmente durante períodos de grande carga na rede.
- Detecta e evita caminhos de rede congestionados.

- Executa algumas tarefas diretamente na camada da rede, como a reordenação de pacotes na extremidade receptora e a maioria das retransmissões necessárias. Isso libera a camada de aplicação para outros trabalhos.

> **Note**
>
> - Se a aplicação enviar ou receber um grande volume de pacotes por segundo e precisar otimizar a latência a maioria das vezes, especialmente durante períodos em que não há congestionamento na rede, o Redes avançadas pode ser mais adequado para a sua rede.
> - O tráfego ENA Express não pode ser enviado numa Zona Local.

Depois que você habilita o ENA Express para a conexão da interface de rede em uma instância, a instância remetente inicia a comunicação com a instância destinatária, e o SRD detecta se o ENA Express está funcionando tanto na instância remetente quanto na instância destinatária. Se o ENA Express estiver operando, a comunicação poderá usar transmissão SRD. Se o ENA Express não estiver operando, a comunicação retornará para a transmissão por ENA padrão.

Durante períodos em que o tráfego de rede é leve, você pode notar um ligeiro aumento na latência de pacote (dezenas de microssegundos) quando o pacote usa o ENA Express. Durante esses períodos, as aplicações que priorizam características específicas de performance de rede podem se beneficiar do ENA Express da seguinte forma:

- Os processos podem se beneficiar do aumento da largura de banda máxima de fluxo único, de 5 Gbps para até 25 Gbps, dentro da zona de disponibilidade, respeitando o limite agregado da instância. Por exemplo, se um tipo de instância específico for compatível com até 12,5 Gbps, a largura de banda de um único fluxo também será limitada a 12,5 Gbps.
- Processos mais longos devem ter uma latência de cauda reduzida durante períodos de congestionamento da rede.
- Os processos podem se beneficiar de uma distribuição mais suave e padrão dos tempos de resposta da rede.

Tópicos

- Como o ENA Express funciona
- Tipos de instâncias compatíveis com o ENA Express

- Pré-requisitos para instâncias Linux
- Ajustar a performance das configurações do ENA Express em instâncias do Linux
- Revisar as configurações do ENA Express para instâncias do EC2
- Definir as configurações do ENA Express para instâncias do EC2

Como o ENA Express funciona

O ENA Express conta com a tecnologia AWS Scalable Reliable Datagram (SRD). O mecanismo distribui pacotes para cada fluxo de rede em diferentes caminhos de rede da AWS e ajusta dinamicamente a distribuição quando detecta sinais de congestionamento. Ele também gerencia a reordenação de pacotes na extremidade receptora.

Para garantir que o ENA Express possa gerenciar o tráfego de rede conforme previsto, as instâncias de envio e recebimento e a comunicação entre elas devem atender a todos os seguintes requisitos:

- Os tipos de instâncias de envio e de recebimento são compatíveis. Para obter mais informações, consulte a tabela Tipos de instâncias compatíveis com o ENA Express.
- As instâncias de envio e de recebimento devem ter o ENA Express configurado. Se houver diferenças na configuração, você pode se deparar com situações em que o tráfego use a transmissão ENA padrão. O cenário a seguir mostra o que pode acontecer.

  Cenário: diferenças na configuração

Instância	ENA Express habilitado	O UDP usa o ENA Express
Instância 1	Sim	Sim
Instância 2	Sim	Não

  Nesse caso, o tráfego TCP entre as duas instâncias pode usar o ENA Express, pois ambas as instâncias o habilitaram. No entanto, como uma das instâncias não usa o ENA Express para tráfego UDP, a comunicação entre essas duas instâncias por UDP usa a transmissão ENA padrão.
- As instâncias de envio e recebimento devem ser executadas na mesma zona de disponibilidade.
- O caminho da rede entre as instâncias não deve incluir caixas de middleware. No momento, o ENA Express não é compatível com caixas de middleware.

- (Somente para instâncias do Linux) Para utilizar todo o potencial da largura de banda, use a versão 2.2.9 ou versões posteriores do driver.
- (Somente para instâncias do Linux) Para produzir métricas, use a versão 2.8 ou versões posteriores do driver.

Se algum requisito não for atendido, as instâncias usarão o protocolo TCP/UDP padrão, mas sem o SRD para comunicação.

Para garantir que o driver de rede da instância esteja configurado para performance ideal, analise as melhores práticas recomendadas para drivers do ENA. Essas práticas recomendadas também se aplicam ao ENA Express. Para obter mais informações, consulte ENA Linux Driver Best Practices and Performance Optimization Guide (Guia de Práticas Recomendadas e Otimização de Performance do Driver) no GitHub.

> **Note**
>
> O Amazon EC2 se refere à relação entre uma instância e uma interface de rede que está anexada a ela como um anexo. As configurações do ENA Express se aplicam ao anexo. Se a interface de rede for separada da instância, o anexo deixará de existir e as configurações do ENA Express aplicadas a ele não estarão mais em vigor. O mesmo acontece quando uma instância é encerrada, mesmo que a interface de rede permaneça.

Depois de habilitar o ENA Express para os anexos de interface de rede na instância de envio e na instância de recebimento, é possível usar as métricas do ENA Express para ajudar a garantir que as instâncias aproveitem ao máximo as melhorias de performance que a tecnologia SRD oferece. Para obter mais informações sobre as métricas do ENA Express, consulte Métricas do ENA Express.

Tipos de instâncias compatíveis com o ENA Express

Os tipos de instância a seguir são compatíveis com o ENA Express.

General purpose

Tipo de instância	Arquitetura
`m6a.12xlarge`	x86_64

Tipo de instância	Arquitetura
m6a.16xlarge	x86_64
m6a.24xlarge	x86_64
m6a.32xlarge	x86_64
m6a.48xlarge	x86_64
m6a.metal	x86_64
m6i.8xlarge	x86_64
m6i.12xlarge	x86_64
m6i.16xlarge	x86_64
m6i.24xlarge	x86_64
m6i.32xlarge	x86_64
m6i.metal	x86_64
m6id.8xlarge	x86_64
m6id.12xlarge	x86_64
m6id.16xlarge	x86_64
m6id.24xlarge	x86_64
m6id.32xlarge	x86_64
m6id.metal	x86_64
m6idn.8xlarge	x86_64
m6idn.12xlarge	x86_64
m6idn.16xlarge	x86_64

Tipo de instância	Arquitetura
m6idn.24xlarge	x86_64
m6idn.32xlarge	x86_64
m6idn.metal	x86_64
m6in.8xlarge	x86_64
m6in.12xlarge	x86_64
m6in.16xlarge	x86_64
m6in.24xlarge	x86_64
m6in.32xlarge	x86_64
m6in.metal	x86_64
m7a.12xlarge	x86_64
m7a.16xlarge	x86_64
m7a.24xlarge	x86_64
m7a.32xlarge	x86_64
m7a.48xlarge	x86_64
m7a.metal-48xl	x86_64
m7g.12xlarge	arm64
m7g.16xlarge	arm64
m7g.metal	arm64
m7gd.12xlarge	arm64
m7gd.16xlarge	arm64

Tipo de instância	Arquitetura
m7gd.metal	arm64
m7i.12xlarge	x86_64
m7i.16xlarge	x86_64
m7i.24xlarge	x86_64
m7i.48xlarge	x86_64
m7i.metal-24xl	x86_64
m7i.metal-48xl	x86_64
m8a.16xlarge	x86_64
m8a.24xlarge	x86_64
m8a.48xlarge	x86_64
m8a.metal-24xl	x86_64
m8a.metal-48xl	x86_64
m8azn.12xlarge	x86_64
m8azn.24xlarge	x86_64
m8azn.metal-12xl	x86_64
m8azn.metal-24xl	x86_64
m8g.12xlarge	arm64
m8g.16xlarge	arm64
m8g.24xlarge	arm64
m8g.48xlarge	arm64

Tipo de instância	Arquitetura
m8g.metal-24xl	arm64
m8g.metal-48xl	arm64
m8gb.8xlarge	arm64
m8gb.12xlarge	arm64
m8gb.16xlarge	arm64
m8gb.24xlarge	arm64
m8gb.48xlarge	arm64
m8gd.12xlarge	arm64
m8gd.16xlarge	arm64
m8gd.24xlarge	arm64
m8gd.48xlarge	arm64
m8gd.metal-24xl	arm64
m8gd.metal-48xl	arm64
m8gn.8xlarge	arm64
m8gn.12xlarge	arm64
m8gn.16xlarge	arm64
m8gn.24xlarge	arm64
m8gn.48xlarge	arm64
m8i.24xlarge	x86_64
m8i.32xlarge	x86_64

Tipo de instância	Arquitetura
m8i.48xlarge	x86_64
m8i.96xlarge	x86_64
m8i.metal-48xl	x86_64
m8i.metal-96xl	x86_64
m8id.24xlarge	x86_64
m8id.32xlarge	x86_64
m8id.48xlarge	x86_64
m8id.96xlarge	x86_64
m8id.metal-48xl	x86_64
m8id.metal-96xl	x86_64

Compute optimized

Tipo de instância	Arquitetura
c6a.12xlarge	x86_64
c6a.16xlarge	x86_64
c6a.24xlarge	x86_64
c6a.32xlarge	x86_64
c6a.48xlarge	x86_64
c6a.metal	x86_64
c6gn.4xlarge	arm64

Tipo de instância	Arquitetura
c6gn.8xlarge	arm64
c6gn.12xlarge	arm64
c6gn.16xlarge	arm64
c6i.8xlarge	x86_64
c6i.12xlarge	x86_64
c6i.16xlarge	x86_64
c6i.24xlarge	x86_64
c6i.32xlarge	x86_64
c6i.metal	x86_64
c6id.8xlarge	x86_64
c6id.12xlarge	x86_64
c6id.16xlarge	x86_64
c6id.24xlarge	x86_64
c6id.32xlarge	x86_64
c6id.metal	x86_64
c6in.8xlarge	x86_64
c6in.12xlarge	x86_64
c6in.16xlarge	x86_64
c6in.24xlarge	x86_64
c6in.32xlarge	x86_64

Tipo de instância	Arquitetura
c6in.metal	x86_64
c7a.12xlarge	x86_64
c7a.16xlarge	x86_64
c7a.24xlarge	x86_64
c7a.32xlarge	x86_64
c7a.48xlarge	x86_64
c7a.metal-48xl	x86_64
c7g.12xlarge	arm64
c7g.16xlarge	arm64
c7g.metal	arm64
c7gd.12xlarge	arm64
c7gd.16xlarge	arm64
c7gd.metal	arm64
c7gn.4xlarge	arm64
c7gn.8xlarge	arm64
c7gn.12xlarge	arm64
c7gn.16xlarge	arm64
c7gn.metal	arm64
c7i.12xlarge	x86_64
c7i.16xlarge	x86_64

Tipo de instância	Arquitetura
c7i.24xlarge	x86_64
c7i.48xlarge	x86_64
c7i.metal-24xl	x86_64
c7i.metal-48xl	x86_64
c8a.16xlarge	x86_64
c8a.24xlarge	x86_64
c8a.48xlarge	x86_64
c8a.metal-24xl	x86_64
c8a.metal-48xl	x86_64
c8g.12xlarge	arm64
c8g.16xlarge	arm64
c8g.24xlarge	arm64
c8g.48xlarge	arm64
c8g.metal-24xl	arm64
c8g.metal-48xl	arm64
c8gb.8xlarge	arm64
c8gb.12xlarge	arm64
c8gb.16xlarge	arm64
c8gb.24xlarge	arm64
c8gb.48xlarge	arm64

Tipo de instância	Arquitetura
c8gb.metal-24xl	arm64
c8gb.metal-48xl	arm64
c8gd.12xlarge	arm64
c8gd.16xlarge	arm64
c8gd.24xlarge	arm64
c8gd.48xlarge	arm64
c8gd.metal-24xl	arm64
c8gd.metal-48xl	arm64
c8gn.8xlarge	arm64
c8gn.12xlarge	arm64
c8gn.16xlarge	arm64
c8gn.24xlarge	arm64
c8gn.48xlarge	arm64
c8gn.metal-24xl	arm64
c8gn.metal-48xl	arm64
c8i.24xlarge	x86_64
c8i.32xlarge	x86_64
c8i.48xlarge	x86_64
c8i.96xlarge	x86_64
c8i.metal-48xl	x86_64

Tipo de instância	Arquitetura
c8i.metal-96xl	x86_64
c8id.24xlarge	x86_64
c8id.32xlarge	x86_64
c8id.48xlarge	x86_64
c8id.96xlarge	x86_64
c8id.metal-48xl	x86_64
c8id.metal-96xl	x86_64

Memory optimized

Tipo de instância	Arquitetura
r6a.12xlarge	x86_64
r6a.16xlarge	x86_64
r6a.24xlarge	x86_64
r6a.32xlarge	x86_64
r6a.48xlarge	x86_64
r6a.metal	x86_64
r6i.8xlarge	x86_64
r6i.12xlarge	x86_64
r6i.16xlarge	x86_64
r6i.24xlarge	x86_64

Tipo de instância	Arquitetura
r6i.32xlarge	x86_64
r6i.metal	x86_64
r6id.8xlarge	x86_64
r6id.12xlarge	x86_64
r6id.16xlarge	x86_64
r6id.24xlarge	x86_64
r6id.32xlarge	x86_64
r6id.metal	x86_64
r6idn.8xlarge	x86_64
r6idn.12xlarge	x86_64
r6idn.16xlarge	x86_64
r6idn.24xlarge	x86_64
r6idn.32xlarge	x86_64
r6idn.metal	x86_64
r6in.8xlarge	x86_64
r6in.12xlarge	x86_64
r6in.16xlarge	x86_64
r6in.24xlarge	x86_64
r6in.32xlarge	x86_64
r6in.metal	x86_64

Tipo de instância	Arquitetura
r7a.12xlarge	x86_64
r7a.16xlarge	x86_64
r7a.24xlarge	x86_64
r7a.32xlarge	x86_64
r7a.48xlarge	x86_64
r7a.metal-48xl	x86_64
r7g.12xlarge	arm64
r7g.16xlarge	arm64
r7g.metal	arm64
r7gd.12xlarge	arm64
r7gd.16xlarge	arm64
r7gd.metal	arm64
r7i.12xlarge	x86_64
r7i.16xlarge	x86_64
r7i.24xlarge	x86_64
r7i.48xlarge	x86_64
r7i.metal-24xl	x86_64
r7i.metal-48xl	x86_64
r7iz.8xlarge	x86_64
r7iz.12xlarge	x86_64

Tipo de instância	Arquitetura
r7iz.16xlarge	x86_64
r7iz.32xlarge	x86_64
r7iz.metal-16xl	x86_64
r7iz.metal-32xl	x86_64
r8a.16xlarge	x86_64
r8a.24xlarge	x86_64
r8a.48xlarge	x86_64
r8a.metal-24xl	x86_64
r8a.metal-48xl	x86_64
r8g.12xlarge	arm64
r8g.16xlarge	arm64
r8g.24xlarge	arm64
r8g.48xlarge	arm64
r8g.metal-24xl	arm64
r8g.metal-48xl	arm64
r8gb.8xlarge	arm64
r8gb.12xlarge	arm64
r8gb.16xlarge	arm64
r8gb.24xlarge	arm64
r8gb.48xlarge	arm64

Tipo de instância	Arquitetura
r8gb.metal-24xl	arm64
r8gb.metal-48xl	arm64
r8gd.12xlarge	arm64
r8gd.16xlarge	arm64
r8gd.24xlarge	arm64
r8gd.48xlarge	arm64
r8gd.metal-24xl	arm64
r8gd.metal-48xl	arm64
r8gn.8xlarge	arm64
r8gn.12xlarge	arm64
r8gn.16xlarge	arm64
r8gn.24xlarge	arm64
r8gn.48xlarge	arm64
r8gn.metal-24xl	arm64
r8gn.metal-48xl	arm64
r8i.24xlarge	x86_64
r8i.32xlarge	x86_64
r8i.48xlarge	x86_64
r8i.96xlarge	x86_64
r8i.metal-48xl	x86_64

Tipo de instância	Arquitetura
r8i.metal-96xl	x86_64
r8id.24xlarge	x86_64
r8id.32xlarge	x86_64
r8id.48xlarge	x86_64
r8id.96xlarge	x86_64
r8id.metal-48xl	x86_64
r8id.metal-96xl	x86_64
u7i-6tb.112xlarge	x86_64
u7i-8tb.112xlarge	x86_64
u7i-12tb.224xlarge	x86_64
u7in-16tb.224xlarge	x86_64
u7in-24tb.224xlarge	x86_64
u7in-32tb.224xlarge	x86_64
u7inh-32tb.480xlarge	x86_64
x2idn.16xlarge	x86_64
x2idn.24xlarge	x86_64
x2idn.32xlarge	x86_64
x2idn.metal	x86_64
x2iedn.8xlarge	x86_64
x2iedn.16xlarge	x86_64

Tipo de instância	Arquitetura
x2iedn.24xlarge	x86_64
x2iedn.32xlarge	x86_64
x2iedn.metal	x86_64
x8g.12xlarge	arm64
x8g.16xlarge	arm64
x8g.24xlarge	arm64
x8g.48xlarge	arm64
x8g.metal-24xl	arm64
x8g.metal-48xl	arm64
x8aedz.24xlarge	x86_64
x8aedz.metal-24xl	x86_64
x8i.24xlarge	x86_64
x8i.32xlarge	x86_64
x8i.48xlarge	x86_64
x8i.64xlarge	x86_64
x8i.96xlarge	x86_64
x8i.metal-48xl	x86_64
x8i.metal-96xl	x86_64

Accelerated computing

Tipo de instância	Arquitetura
g6.48xlarge	x86_64
g6e.12xlarge	x86_64
g6e.24xlarge	x86_64
g6e.48xlarge	x86_64
g7e.12xlarge	x86_64
g7e.24xlarge	x86_64
g7e.48xlarge	x86_64
p5.4xlarge	x86_64
p5.48xlarge	x86_64
p5e.48xlarge	x86_64
p5en.48xlarge	x86_64
p6-b200.48xlarge	x86_64
p6-b300.48xlarge	x86_64

Storage optimized

Tipo de instância	Arquitetura
i4g.4xlarge	arm64
i4g.8xlarge	arm64
i4g.16xlarge	arm64

Tipo de instância	Arquitetura
i4i.8xlarge	x86_64
i4i.12xlarge	x86_64
i4i.16xlarge	x86_64
i4i.24xlarge	x86_64
i4i.32xlarge	x86_64
i4i.metal	x86_64
i7i.12xlarge	x86_64
i7i.16xlarge	x86_64
i7i.24xlarge	x86_64
i7i.48xlarge	x86_64
i7i.metal-24xl	x86_64
i7i.metal-48xl	x86_64
i7ie.12xlarge	x86_64
i7ie.18xlarge	x86_64
i7ie.24xlarge	x86_64
i7ie.48xlarge	x86_64
i7ie.metal-24xl	x86_64
i7ie.metal-48xl	x86_64
i8g.12xlarge	arm64
i8g.16xlarge	arm64

Tipo de instância	Arquitetura
i8g.24xlarge	arm64
i8g.48xlarge	arm64
i8g.metal-24xl	arm64
i8ge.12xlarge	arm64
i8ge.18xlarge	arm64
i8ge.24xlarge	arm64
i8ge.48xlarge	arm64
i8ge.metal-24xl	arm64
i8ge.metal-48xl	arm64
im4gn.4xlarge	arm64
im4gn.8xlarge	arm64
im4gn.16xlarge	arm64

Pré-requisitos para instâncias Linux

Para garantir que o ENA Express possa operar de forma eficaz, atualize as configurações da instância do Linux, como mostrado a seguir.

- Se sua instância usar frames jumbo, execute o comando a seguir para definir a unidade máxima de transmissão (MTU) como 8900.

```
[ec2-user ~]$ sudo ip link set dev eth0 mtu 8900
```

- Aumente o tamanho do anel do receptor (Rx), da seguinte forma:

```
[ec2-user ~]$ ethtool -G device rx 8192
```

- Para maximizar a largura de banda do ENA Express, configure seus limites de fila TCP da seguinte forma:

  1. Defina o limite de fila pequena do TCP para 1 MB ou mais. Isso aumenta a quantidade de dados enfileirados para transmissão em um soquete.

     ```
     sudo sh -c 'echo 1048576 > /proc/sys/net/ipv4/tcp_limit_output_bytes'
     ```

  2. Desabilite os limites da fila de bytes no enésimo dispositivo se eles estiverem habilitados para sua distribuição Linux. Fazer isso aumenta os dados enfileirados para transmissão para a fila do dispositivo.

     ```
     sudo sh -c 'for txq in /sys/class/net/eth0/queues/tx-*; do echo max > ${txq}/
     byte_queue_limits/limit_min; done'
     ```

     > **Note**
     >
     > O driver do ENA para a distribuição Amazon Linux desabilita os limites da fila de bytes por padrão.

Ajustar a performance das configurações do ENA Express em instâncias do Linux

Para verificar a configuração da sua instância Linux a fim de extrair a performance ideal do ENA Express, é possível executar o seguinte script que está disponível no repositório do Amazon GitHub:

https://github.com/amzn/amzn-ec2-ena-utilities/blob/main/ena-express/check-ena-express-settings.sh

O script executa uma série de testes e sugere as alterações de configuração recomendadas e necessárias.

Revisar as configurações do ENA Express para instâncias do EC2

É possível verificar as configurações do ENA Express por instância ou por interface de rede. Para atualizar as configurações do ENA Express, consulte the section called “Definir configurações da instância”.

Console

Para visualizar as configurações do ENA Express para 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 (Interfaces de rede).
3. Selecione uma interface de rede para ver os detalhes dessa instância. É possível escolher o link Network interface ID (ID da interface de rede) para abrir a página de detalhes ou pode marcar a caixa de seleção no lado esquerdo da lista para ver os detalhes no painel de detalhes na parte inferior da página.
4. Na seção Anexo da interface de rede na guia Detalhes ou na página de detalhes, revise as configurações de ENA Express e ENA Express UDP.

Para visualizar as configurações do ENA Express para uma instância

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação à esquerda, selecione Instâncias.
3. Selecione uma instância para ver os detalhes dessa instância. É possível escolher o link Instance ID (ID da instância) para abrir a página de detalhes ou pode marcar a caixa de seleção no lado esquerdo da lista para ver os detalhes no painel de detalhes na parte inferior da página.
4. Na seção Network interfaces (Interfaces de rede) na guia Networking (Rede), role para a direita para revisar as configurações do ENA Express e do UDP do ENA Express.

AWS CLI

Para obter as configurações do ENA Express para uma instância

Use o comando describe-instances. Esse exemplo de comando retorna uma lista de configurações do ENA Express para as interfaces de rede associadas a cada uma das instâncias em execução especificadas pelo parâmetro `--instance-ids`.

```
aws ec2 describe-instances \
    --instance-ids i-1234567890abcdef0 i-0598c7d356eba48d7 \
    --query 'Reservations[*].Instances[*].[InstanceId,
 NetworkInterfaces[*].Attachment.EnaSrdSpecification]'
```

O seguinte é um exemplo de saída.

```
[
    [
        [
            "i-1234567890abcdef0",
            [
                {
                    "EnaSrdEnabled": true,
                    "EnaSrdUdpSpecification": {
                        "EnaSrdUdpEnabled": false
                    }
                }
            ]
        ]
    ],
    [
        [
            "i-0598c7d356eba48d7",
            [
            {
                    "EnaSrdEnabled": true,
                    "EnaSrdUdpSpecification": {
                        "EnaSrdUdpEnabled": false
                    }
                }
            ]
        ]
    ]
]
```

Para obter as configurações do ENA Express para uma interface de rede

Use o comando describe-network-interfaces.

```
aws ec2 describe-network-interfaces \
    --network-interface-ids eni-1234567890abcdef0 \
    --query NetworkInterfaces[].[NetworkInterfaceId,Attachment.EnaSrdSpecification]
```

O seguinte é um exemplo de saída.

```
[
    [
```

```
        "eni-1234567890abcdef0",
        {
            "EnaSrdEnabled": true,
            "EnaSrdUdpSpecification": {
                "EnaSrdUdpEnabled": false
            }
        }
    ]
]
```

PowerShell

Para obter as configurações do ENA Express para uma interface de rede

Use o cmdlet Get-EC2NetworkInterface.

```
Get-EC2NetworkInterface `
    -NetworkInterfaceId eni-1234567890abcdef0 | `
Select-Object `
    Association,
    NetworkInterfaceId,
    OwnerId,
    @{Name = 'AttachTime'; Expression = { $_.Attachment.AttachTime } },
    @{Name = 'AttachmentId'; Expression = { $_.Attachment.AttachmentId } },
    @{Name = 'DeleteOnTermination'; Expression =
 { $_.Attachment.DeleteOnTermination } },
    @{Name = 'NetworkCardIndex'; Expression = { $_.Attachment.NetworkCardIndex } },
    @{Name = 'InstanceId'; Expression = { $_.Attachment.InstanceId } },
    @{Name = 'InstanceOwnerId'; Expression = { $_.Attachment.InstanceOwnerId } },
    @{Name = 'Status'; Expression = { $_.Attachment.Status } },
    @{Name = 'EnaSrdEnabled'; Expression =
 { $_.Attachment.EnaSrdSpecification.EnaSrdEnabled } },
    @{Name = 'EnaSrdUdpEnabled'; Expression =
 { $_.Attachment.EnaSrdSpecification.EnaSrdUdpSpecification.EnaSrdUdpEnabled } }
```

O seguinte é um exemplo de saída.

```
Association         :
NetworkInterfaceId  : eni-0d1234e5f6a78901b
OwnerId             : 111122223333
AttachTime          : 6/11/2022 1:13:11 AM
AttachmentId        : eni-attach-0d1234e5f6a78901b
DeleteOnTermination : True
```

```
NetworkCardIndex    : 0
InstanceId          : i-1234567890abcdef0
InstanceOwnerId     : 111122223333
Status              : attached
EnaSrdEnabled       : True
EnaSrdUdpEnabled    : False
```

Definir as configurações do ENA Express para instâncias do EC2

É possível configurar o ENA Express para os tipos de instância do EC2 compatíveis sem precisar instalar qualquer software adicional. Para obter mais informações, consulte the section called “Tipos de instâncias compatíveis com o ENA Express”.

Console

Para gerenciar o ENA Express para 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 (Interfaces de rede).
3. Selecione uma interface de rede que é anexada a uma instância. É possível escolher o link Network interface ID (ID da interface de rede) para abrir a página de detalhes ou pode marcar a caixa de seleção no lado esquerdo da lista.
4. Escolha Manage ENA Express (Gerenciar o ENA Express) no menu Action (Ação) no canto superior direito da página. Isso abre a caixa de diálogo Manage ENA Express (Gerenciar o ENA Express), com o ID da interface de rede selecionado e as configurações atuais exibidas.

   Se a interface de rede selecionada não estiver anexada a uma instância, essa ação não aparecerá no menu.
5. Para usar o ENA Express, marque a caixa de seleção Habilitar.
6. Quando o ENA Express está habilitado, você pode definir as configurações de UDP. Para usar o UDP do ENA Express, marque a caixa de seleção Habilitar.
7. Para salvar suas configurações, escolha Save (Salvar).

Para gerenciar o ENA Express para uma instância

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação à esquerda, selecione Instâncias.

3. Selecione a instância que você quer gerenciar. É possível escolher o link Instance ID (ID da instância) para abrir a página de detalhes ou pode marcar a caixa de seleção no lado esquerdo da lista.
4. Selecione a Network interface (Interface de rede) a ser configurada para sua instância.
5. Escolha Manage ENA Express (Gerenciar o ENA Express) no menu Action (Ação) no canto superior direito da página.
6. Para configurar o ENA Express para uma interface de rede anexada à instância, selecione-a na lista Network interface (Interface de rede).
7. Para usar o ENA Express no anexo de interface de rede selecionado, marque a caixa de seleção Habilitar.
8. Quando o ENA Express está habilitado, você pode definir as configurações de UDP. Para usar o UDP do ENA Express, marque a caixa de seleção Habilitar.
9. Para salvar suas configurações, escolha Save (Salvar).

Para configurar o ENA Express ao anexar 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 (Interfaces de rede).
3. Selecione uma interface que não esteja anexada a uma instância (o Status é Available [Disponível]). É possível escolher o link Network interface ID (ID da interface de rede) para abrir a página de detalhes ou pode marcar a caixa de seleção no lado esquerdo da lista.
4. Selecione a Instance (Instância) à qual você vai anexar.
5. Para usar o ENA Express depois de anexar a interface de rede à instância, marque a caixa de seleção Habilitar.
6. Quando o ENA Express está habilitado, você pode definir as configurações de UDP. Para usar o UDP do ENA Express, marque a caixa de seleção Habilitar.
7. Para anexar a interface de rede à instância e salvar as configurações do ENA Express, escolha Attach (Anexar).

AWS CLI

Para configurar o ENA Express ao anexar uma interface de rede

Utilize o comando attach-network-interface, conforme mostrado nos exemplos a seguir.

Exemplo 1: usar o ENA Express para tráfego TCP, mas não para tráfego UDP

Este exemplo configura `EnaSrdEnabled` como `true` e permite que `EnaSrdUdpEnabled` use `false` como padrão.

```
aws ec2 attach-network-interface \
    --network-interface-id eni-1234567890abcdef0 \
    --instance-id i-1234567890abcdef0 \
    --device-index 1 \
    --ena-srd-specification 'EnaSrdEnabled=true'
```

Exemplo 2: usar o ENA Express para tráfego TCP e tráfego UDP

Este exemplo configura `EnaSrdEnabled` e `EnaSrdUdpEnabled` como `true`.

```
aws ec2 attach-network-interface \
    --network-interface-id eni-1234567890abcdef0 \
    --instance-id i-1234567890abcdef0 \
    --device-index 1 \
    --ena-srd-specification
 'EnaSrdEnabled=true,EnaSrdUdpSpecification={EnaSrdUdpEnabled=true}'
```

Para atualizar as configurações do ENA Express para um anexo da interface de rede

Utilize o comando modify-network-interface-attribute, conforme mostrado nos exemplos a seguir.

Exemplo 1: usar o ENA Express para tráfego TCP, mas não para tráfego UDP

Este exemplo configura `EnaSrdEnabled` como `true` e permitirá que `EnaSrdUdpEnabled` use `false` como padrão se ele nunca tiver sido definido antes.

```
aws ec2 modify-network-interface-attribute \
    --network-interface-id eni-1234567890abcdef0 \
    --ena-srd-specification 'EnaSrdEnabled=true'
```

Exemplo 2: usar o ENA Express para tráfego TCP e tráfego UDP

Este exemplo configura `EnaSrdEnabled` e `EnaSrdUdpEnabled` como `true`.

```
aws ec2 modify-network-interface-attribute \
```

```
    --network-interface-id eni-1234567890abcdef0 \
    --ena-srd-specification
 'EnaSrdEnabled=true,EnaSrdUdpSpecification={EnaSrdUdpEnabled=true}'
```

Exemplo 3: parar de usar o ENA Express para tráfego UDP

Este exemplo configura `EnaSrdUdpEnabled` como `false`.

```
aws ec2 modify-network-interface-attribute \
    --network-interface-id eni-1234567890abcdef0 \
    --ena-srd-specification 'EnaSrdUdpSpecification={EnaSrdUdpEnabled=false}'
```

PowerShell

Para configurar o ENA Express ao anexar uma interface de rede

Utilize o cmdlet Add-EC2NetworkInterface, conforme mostrado nos exemplos a seguir.

Exemplo 1: usar o ENA Express para tráfego TCP, mas não para tráfego UDP

Este exemplo configura `EnaSrdEnabled` como `true` e permite que `EnaSrdUdpEnabled` use `false` como padrão.

```
Add-EC2NetworkInterface `
    -NetworkInterfaceId eni-1234567890abcdef0 `
    -InstanceId i-1234567890abcdef0 `
    -DeviceIndex 1 `
    -EnaSrdSpecification_EnaSrdEnabled $true
```

Exemplo 2: usar o ENA Express para tráfego TCP e tráfego UDP

Este exemplo configura `EnaSrdEnabled` e `EnaSrdUdpEnabled` como `true`.

```
Add-EC2NetworkInterface `
    -NetworkInterfaceId eni-1234567890abcdef0 `
    -InstanceId i-1234567890abcdef0 `
    -DeviceIndex 1 `
    -EnaSrdSpecification_EnaSrdEnabled $true `
    -EnaSrdUdpSpecification_EnaSrdUdpEnabled $true
```

Para configurar o ENA Express para o anexo da interface de rede

Utilize o cmdlet Edit-EC2NetworkInterfaceAttribute, conforme mostrado nos exemplos a seguir.

Exemplo 1: usar o ENA Express para tráfego TCP, mas não para tráfego UDP

Este exemplo configura `EnaSrdEnabled` como `true` e permitirá que `EnaSrdUdpEnabled` use `false` como padrão se ele nunca tiver sido definido antes.

```
Edit-EC2NetworkInterfaceAttribute `
    -NetworkInterfaceId eni-1234567890abcdef0 `
    -EnaSrdSpecification_EnaSrdEnabled $true ;
Get-EC2NetworkInterface -NetworkInterfaceId eni-0123f4567890a1b23 | `
Select-Object `
    NetworkInterfaceId,
    @{Name = 'EnaSrdEnabled'; Expression =
 { $_.Attachment.EnaSrdSpecification.EnaSrdEnabled }},
    @{Name = 'EnaSrdUdpEnabled'; Expression =
 { $_.Attachment.EnaSrdSpecification.EnaSrdUdpSpecification.EnaSrdUdpEnabled }} | `
Format-List
```

Exemplo 2: usar o ENA Express para tráfego TCP e tráfego UDP

Este exemplo configura `EnaSrdEnabled` e `EnaSrdUdpEnabled` como `true`.

```
Edit-EC2NetworkInterfaceAttribute `
    -NetworkInterfaceId eni-1234567890abcdef0 `
    -EnaSrdSpecification_EnaSrdEnabled $true `
    -EnaSrdSpecification_EnaSrdUdpSpecification_EnaSrdUdpEnabled $true ;
Get-EC2NetworkInterface -NetworkInterfaceId eni-1234567890abcdef0 | `
Select-Object `
    NetworkInterfaceId,
    @{Name = 'EnaSrdEnabled'; Expression =
 { $_.Attachment.EnaSrdSpecification.EnaSrdEnabled }},
    @{Name = 'EnaSrdUdpEnabled'; Expression =
 { $_.Attachment.EnaSrdSpecification.EnaSrdUdpSpecification.EnaSrdUdpEnabled }} | `
Format-List
```

Exemplo 3: parar de usar o ENA Express para tráfego UDP

Este exemplo configura `EnaSrdUdpEnabled` como `false`.

```
Edit-EC2NetworkInterfaceAttribute `
    -NetworkInterfaceId eni-0123f4567890a1b23 `
    -EnaSrdSpecification_EnaSrdUdpSpecification_EnaSrdUdpEnabled $false ;
```

```
Get-EC2NetworkInterface -NetworkInterfaceId eni-0123f4567890a1b23 | `
Select-Object `
    NetworkInterfaceId,
    @{Name = 'EnaSrdEnabled'; Expression =
 { $_.Attachment.EnaSrdSpecification.EnaSrdEnabled }},
    @{Name = 'EnaSrdUdpEnabled'; Expression =
 { $_.Attachment.EnaSrdSpecification.EnaSrdUdpSpecification.EnaSrdUdpEnabled }} | `
Format-List
```

Configuração do ENA Express na inicialização

É possível usar um dos métodos a seguir para configurar o ENA Express diretamente quando iniciar uma instância. Os links especificados encaminham você para as instruções do Console de gerenciamento da AWS para esses métodos.

- Assistente de inicialização de instâncias: é possível configurar o ENA Express na inicialização com o assistente de inicialização de instâncias. Para obter mais informações, consulte Configuração avançada de rede nas Configurações de rede para o assistente de inicialização de instâncias.
- Modelo de inicialização: é possível configurar o ENA Express na inicialização ao usar um modelo de inicialização. Para obter mais informações, consulte a página Criar um modelo de execução do Amazon EC2 e, em seguida, expanda a seção Configurações de rede e revise a Configuração de rede avançada.

Habilitar redes aperfeiçoadas com a interface Intel 82599 VF

Para instâncias baseadas em Xen, a interface Intel 82599 Virtual Function (VF) fornece recursos de redes aperfeiçoadas. A interface usa o driver Intel `ixgbevf`.

As guias a seguir mostram como verificar o driver do adaptador de rede instalado no sistema operacional da instância.

Linux

Driver da interface de rede do Linux

Use o comando a seguir para verificar se o módulo está sendo usado em uma interface específica, substituindo o nome da interface que você deseja verificar. Se estiver usando uma única interface (padrão), ela será `eth0`. Se o sistema operacional oferecer suporte a nomes de rede previsíveis, esse poderá ser um nome como `ens5`.

No exemplo acima, o módulo `ixgbevf` não está carregado porque o driver listado é `vif`.

```
[ec2-user ~]$ ethtool -i eth0
driver: vif
version:
firmware-version:
bus-info: vif-0
supports-statistics: yes
supports-test: no
supports-eeprom-access: no
supports-register-dump: no
supports-priv-flags: no
```

Nesse exemplo, o módulo `ixgbevf` está carregado. Essa instância configurou a rede avançada corretamente.

```
[ec2-user ~]$ ethtool -i eth0
driver: ixgbevf
version: 4.0.3
firmware-version: N/A
bus-info: 0000:00:03.0
supports-statistics: yes
supports-test: yes
supports-eeprom-access: no
supports-register-dump: yes
supports-priv-flags: no
```

Windows

Adaptador de rede do Windows

Para verificar se o driver está instalado, conecte-se à instância e abra o Gerenciador de dispositivos. Você deve ver `Intel(R) 82599 Virtual Function` listado em Adaptadores de rede.

Conteúdo

- Preparar a instância para redes aperfeiçoadas
- Testar se a rede avançada está habilitada
- Habilitar redes avançadas na instância
- Solucionar problemas de conectividade

Preparar a instância para redes aperfeiçoadas

Para se preparar para a rede avançada com a interface Intel 82599 VF, configure a instância da seguinte forma:

- Verifique se o tipo de instância é um dos seguintes: C3, C4, D2, I2, M4 (excetom4.16xlarge) e R3.
- Verifique se a instância tem conectividade com a Internet.
- Se houver dados importantes na instância que deseja preservar, você deverá fazer backup desses dados agora criando uma AMI na instância. A atualização de kernels e módulos de kernel e a habilitação do atributo `sriovNetSupport` podem renderizar instâncias incompatíveis ou sistemas operacionais inacessíveis. Se você tiver um backup recente, seus dados ainda serão retidos, caso isso ocorra.
- Instâncias do Linux: inicie a instância usando uma AMI de HVM com a versão 2.6.32 ou com versões posteriores do kernel do Linux. As AMIs HVM do Amazon Linux mais recentes têm os módulos necessários para a rede avançada instalada e também têm os atributos necessários definidos. Portanto, se você executar uma instância compatível com redes avançadas com Amazon EBS que usa uma AMI de HVM do Amazon Linux, a rede avançada já estará habilitada para a instância.

  > **Warning**
  >
  > A rede avançada é compatível apenas com instâncias de HVM. A habilitação da rede avançada com uma instância PV pode torná-la inacessível. A configuração desse atributo sem o módulo ou a versão do módulo adequados também pode tornar a instância inacessível.

- Instâncias do Windows: inicie a instância usando uma AMI de HVM de 64 bits. Não é possível habilitar as redes aperfeiçoadas no Windows Server 2008. A rede avançada já está habilitada para AMIs do Windows Server 2012 R2 e do Windows Server 2016 e posterior. O Windows Server 2012 R2 inclui o driver 1.0.15.3 da Intel e recomendamos atualizar esse driver para a versão mais recente usando o utilitário Pnputil.exe.
- Use o AWS CloudShell do Console de gerenciamento da AWS ou instale e configure a AWS CLI ou o AWS Tools for Windows PowerShell em qualquer computador que desejar, de preferência em seu desktop ou notebook local. Para obter mais informações sobre o ACM, consulte Acessar o Amazon EC2 ou o Guia do usuário do AWS CloudShell. A rede avançada não pode ser gerenciada no console do Amazon EC2.

Testar se a rede avançada está habilitada

Verifique se o atributo `sriovNetSupport` está definido na instância ou na imagem.

AWS CLI

Para verificar o atributo de instância (sriovNetSupport)

Use o seguinte comando describe-instance-attribute: Se o atributo estiver definido, o valor será `simple`.

```
aws ec2 describe-instance-attribute \
    --instance-id i-1234567890abcdef0 \
    --attribute sriovNetSupport
```

Para verificar o atributo de imagem (sriovNetSupport)

Use o seguinte comando describe-images: Se o atributo estiver definido, o valor será `simple`.

```
aws ec2 describe-images \
    --image-id ami-0abcdef1234567890 \
    --query "Images[].SriovNetSupport"
```

PowerShell

Para verificar o atributo de instância (sriovNetSupport)

Use o cmdlet Get-EC2InstanceAttribute. Se o atributo estiver definido, o valor será `simple`.

```
Get-EC2InstanceAttribute `
    -InstanceId i-1234567890abcdef0 `
    -Attribute sriovNetSupport
```

Para verificar o atributo de imagem (sriovNetSupport)

Use o seguinte comando describe-images: Se o atributo estiver definido, o valor será `simple`.

```
(Get-EC2Image -ImageId ami-0abcdef1234567890).SriovNetSupport
```

Habilitar redes avançadas na instância

O procedimento usado dependerá do sistema operacional da instância.

> **Warning**
>
> Não há nenhuma maneira de desabilitar o atributo de rede avançada depois de ele ser habilitado.

Amazon Linux

As AMIs de HVM do Amazon Linux têm o módulo `ixgbevf` necessário para a rede avançada instalado e também têm o atributo necessário `sriovNetSupport` definido. Portanto, se você executar um tipo de instância que use uma AMI de HVM do Amazon Linux, a rede avançada já estará habilitada para a instância. Para obter mais informações, consulte Testar se a rede avançada está habilitada.

Se você executou a instância usando uma AMI do Amazon Linux mais antiga e ela ainda não tiver a rede avançada habilitada, use o seguinte procedimento para habilitar a rede avançada.

Para habilitar a rede avançada

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 `ixgbevf`:

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

3. A partir do computador local, reinicialize sua instância usando o console do Amazon EC2 ou um dos comandos a seguir: reboot-instances (AWS CLI) ou Restart-EC2Instance (AWS Tools for Windows PowerShell).
4. Conecte-se à instância novamente e verifique se o módulo `ixgbevf` está instalado e na versão mínima recomendada usando o comando modinfo ixgbevf em Testar se a rede avançada está habilitada.
5. [Instância com EBS] A partir do computador local, interrompa a instância usando o console do Amazon EC2 ou um dos seguintes comandos: stop-instances (AWS CLI) ou Stop-EC2Instance (AWS Tools for Windows PowerShell).

   [Instância baseada em armazenamento de instâncias] Você não pode parar a instância para modificar o atributo. Em vez disso, pule o próximo procedimento.
6. No computador local, ative o atributo de rede avançada usando um dos seguintes comandos:

AWS CLI

Use o comando modify-instance-attribute da seguinte forma.

```
aws ec2 modify-instance-attribute \
    --instance-id i-1234567890abcdef0 \
    --sriov-net-support simple
```

PowerShell

Use o cmdlet Edit-EC2InstanceAttribute conforme mostrado a seguir.

```
Edit-EC2InstanceAttribute `
    -InstanceId i-1234567890abcdef0 `
    -SriovNetSupport "simple"
```

7. (Opcional) Crie uma AMI na instância, conforme descrito em Criação de uma AMI baseada no Amazon EBS. A AMI herda o atributo da rede avançada da instância. Portanto, é possível usar essa AMI para executar outra instância com a rede avançada habilitada por padrão.
8. A partir do computador local, inicie a instância usando o console do Amazon EC2 ou um dos seguintes comandos: start-instances (AWS CLI) ou Start-EC2Instance (AWS Tools for Windows PowerShell).
9. Conecte-se à instância e verifique se o módulo `ixgbevf` está instalado e carregado na interface de rede usando o comando ethtool -i eth***n*** em Testar se a rede avançada está habilitada.

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 baseada no Amazon S3, habilitando o atributo de rede avançada ao registrar a AMI.

AWS CLI

Use o comando register-image da seguinte forma.

```
aws ec2 register-image --sriov-net-support simple ...
```

PowerShell

Use Register-EC2Image da seguinte forma:

```
Register-EC2Image -SriovNetSupport "simple" ...
```

Ubuntu

Antes de começar, o verifica se a rede avançada já está habilitada 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`.

Outras distribuições do Linux

Antes de começar, o verifica se a rede avançada já está habilitada em sua instância. As AMIs do HVM Quick Start mais recentes incluem os drivers necessários para rede avançada, portanto, você não precisa executar etapas adicionais.

O procedimento a seguir fornece as etapas gerais se precisar habilitar a rede avançada com a interface Intel 82599 VF em uma distribuição do Linux diferente do Amazon Linux ou do Ubuntu. Para

obter mais informações, como a sintaxe detalhada dos comandos, os locais dos arquivos ou suporte para o pacote e a ferramenta, consulte a documentação específica à sua distribuição do Linux.

Para habilitar a rede avançada no Linux

1. Conecte-se à sua instância.
2. Faça download da fonte para o módulo `ixgbevf` na instância do Sourceforge em https://sourceforge.net/projects/e1000/files/ixgbevf%20stable/.

   Versões do `ixgbevf` anteriores à 2.16.4, incluindo a versão 2.14.2, não são compiladas adequadamente em algumas distribuições do Linux, incluindo certas versões do Ubuntu.
3. Compile e instale o módulo `ixgbevf` na instância.

   > ⚠ Warning
   >
   > Se você compilar o módulo `ixgbevf` para o kernel atual e, depois, atualizar o kernel sem recompilar o driver para o novo kernel, o sistema poderá reverter o módulo `ixgbevf` específico à distribuição na próxima reinicialização. Isso poderá tornar o sistema inacessível se a versão específica à distribuição for incompatível com a rede avançada.
4. Execute o comando sudo depmod para atualizar as dependências do módulo.
5. Atualize o `initramfs` na instância para garantir que o novo módulo seja carregado na hora da inicialização.
6. Determine se o sistema usa nomes previsíveis de interface de rede por padrão. Os sistemas que usam as versões 197 ou superiores do systemd ou udev podem renomear dispositivos de Ethernet e não garantem que uma única interface de rede será nomeada `eth0`. Esse comportamento pode causar problemas para conexão à instância. Para mais informações e ver outras opções de configuração, consulte Nomes previsíveis de interface de rede no site freedesktop.org.

   a. É possível 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] A partir do computador local, interrompa a instância usando o console do Amazon EC2 ou um dos seguintes comandos: stop-instances (AWS CLI) ou Stop-EC2Instance (AWS Tools for Windows PowerShell).

   [Instância baseada em armazenamento de instâncias] Você não pode parar a instância para modificar o atributo. Em vez disso, pule o próximo procedimento.

8. No computador local, ative o atributo de rede avançada usando um dos seguintes comandos:

   AWS CLI

   Use o comando modify-instance-attribute da seguinte forma.

   ```
   aws ec2 modify-instance-attribute \
       --instance-id i-1234567890abcdef0 -\
       -sriov-net-support simple
   ```

   PowerShell

   Use o cmdlet Edit-EC2InstanceAttribute conforme mostrado a seguir.

   ```
   Edit-EC2InstanceAttribute `
       -InstanceId i-1234567890abcdef0 `
       -SriovNetSupport "simple"
   ```

9. (Opcional) Crie uma AMI na instância, conforme descrito em Criação de uma AMI baseada no Amazon EBS. A AMI herda o atributo da rede avançada da instância. Portanto, é possível usar essa AMI para executar outra instância com a rede avançada habilitada por padrão.

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. A partir do computador local, inicie a instância usando o console do Amazon EC2 ou um dos seguintes comandos: start-instances (AWS CLI) ou Start-EC2Instance (AWS Tools for Windows PowerShell).
11. (Opcional) Conecte-se à instância e verifique se o módulo está instalado.

Para habilitar as redes avançadas (instâncias compatíveis com o armazenamento de instância)

Siga o procedimento anterior até a etapa onde você para a instância. Crie uma nova AMI como descrito em Criação de uma AMI baseada no Amazon S3, habilitando o atributo de rede avançada ao registrar a AMI.

AWS CLI

Use o comando register-image da seguinte forma.

```
aws ec2 register-image --sriov-net-support simple ...
```

PowerShell

Use Register-EC2Image da seguinte forma:

```
Register-EC2Image -SriovNetSupport "simple" ...
```

Windows

Se você executou a instância e ela ainda não tiver a rede avançada habilitada, você deverá fazer download e instalar o driver do adaptador de rede necessário na instância e, em seguida, definir o atributo `sriovNetSupport` da instância para ativar a rede avançada. Você só pode habilitar esse atributo em tipos de instâncias compatíveis. Para obter mais informações, consulte Redes aperfeiçoadas para instâncias do Amazon EC2.

> **Important**
>
> Para ver as atualizações de driver mais recentes nas AMIs do Windows, consulte o histórico de versões da AMI do Windows na Referência da AMI do AWS Windows.

Para habilitar a rede avançada

1. Conecte-se à instância e faça login como administrador local.
2. [Windows Server 2016 e posterior] Execute o seguinte script PowerShell do EC2 Launch para configurar a instância depois de instalar o driver.

```
PS C:\> C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeInstance.ps1 -
Schedule
```

> **Important**
>
> A senha do administrador será redefinida quando você habilitar o script de inicialização do EC2 da instância. É possível modificar o arquivo de configuração para desabilitar a redefinição da senha do administrador especificando-a nas configurações das tarefas de inicialização.

3. Na instância, faça download do driver do adaptador de rede da Intel para seu sistema operacional:

   - Windows Server 2022

     Visite a página de download e faça download do `Wired_driver_version_x64.zip`.
   - Windows Server 2019, inclusive para a versão de servidor 1809 e posterior*

     Visite a página de download e faça download do `Wired_driver_version_x64.zip`.
   - Windows Server 2016, inclusive para a versão de servidor 1803 e anterior*

     Visite a página de download e faça download do `Wired_driver_version_x64.zip`.
   - Windows Server 2012 R2

     Visite a página de download e faça download do `Wired_driver_version_x64.zip`.
   - Windows Server 2012

Visite a página de download e faça download do `Wired_driver_version_x64.zip`.

- Windows Server 2008 R2

  Visite a página de download e faça download do `PROWinx64Legacy.exe`.

*As versões de servidor 1803 e anteriores, bem como a 1809 e posterior, não são especificamente abordadas nas páginas de Drivers e Software da Intel.

4. Instale o driver do adaptador de rede da Intel para seu sistema operacional:

   - Windows Server 2008 R2

     1. Na pasta Downloads, localize o arquivo `PROWinx64Legacy.exe` e renomeie-o como `PROWinx64Legacy.zip`.
     2. Extraia o conteúdo do arquivo `PROWinx64Legacy.zip`.
     3. Abra a linha de comando, navegue até a pasta com os arquivos extraídos e execute o comando a seguir a fim de usar o utilitário `pnputil` para adicionar e instalar o arquivo INF no armazenamento de drivers.

     ```
     C:\> pnputil -a PROXGB\Winx64\NDIS62\vxn62x64.inf
     ```

   - Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2 e Windows Server 2012

     1. Na pasta Downloads, extraia o conteúdo do arquivo `Wired_driver_version_x64.zip`.
     2. Abra a linha de comando, navegue até a pasta com os arquivos extraídos e execute os comandos a seguir a fim de usar o utilitário `pnputil` para adicionar e instalar o arquivo INF no armazenamento de drivers.

        - Windows Server 2022

        ```
        pnputil -i -a PROXGB\Winx64\NDIS68\vxn68x64.inf
        ```

        - Windows Server 2019

        ```
        pnputil -i -a PROXGB\Winx64\NDIS68\vxn68x64.inf
        ```

        - Windows Server 2016

        ```
        pnputil -i -a PROXGB\Winx64\NDIS65\vxn65x64.inf
        ```

- Windows Server 2012 R2

```
pnputil -i -a PROXGB\Winx64\NDIS64\vxn64x64.inf
```

- Windows Server 2012

```
pnputil -i -a PROXGB\Winx64\NDIS63\vxn63x64.inf
```

5. No computador local, ative o atributo de rede avançada usando um dos seguintes comandos:

   AWS CLI

   Use o comando modify-instance-attribute da seguinte forma.

```
aws ec2 modify-instance-attribute \
    --instance-id i-1234567890abcdef0 \
    --sriov-net-support simple
```

   PowerShell

   Use o cmdlet Edit-EC2InstanceAttribute conforme mostrado a seguir.

```
Edit-EC2InstanceAttribute `
    -InstanceId i-1234567890abcdef0 `
    -SriovNetSupport "simple"
```

6. (Opcional) Crie uma AMI na instância, conforme descrito em Criação de uma AMI baseada no Amazon EBS. A AMI herda o atributo da rede avançada da instância. Portanto, é possível usar essa AMI para executar outra instância com a rede avançada habilitada por padrão.
7. A partir do computador local, inicie a instância usando o console do Amazon EC2 ou um dos seguintes comandos: start-instances (AWS CLI) ou Start-EC2Instance (AWS Tools for Windows PowerShell).

Solucionar problemas de conectividade

Se você perder a conectividade ao habilitar a rede avançada, o módulo `ixgbevf` talvez seja incompatível com o kernel. Tente instalar a versão do módulo `ixgbevf` incluída com a distribuição do Linux para a instância.

Se você habilitar a rede avançada para uma instância de PV ou de AMI, poderá tornar a instância inatingível.

Para obter mais informações, consulte Como faço para ativar e configurar a rede aprimorada em minhas instâncias do EC2?

Monitorar o desempenho de rede de instâncias do EC2

O driver Elastic Network Adapter (ENA) publica métricas de performance de rede com base nas instâncias em que elas estão habilitadas. É possível usar essas métricas para solucionar problemas de performance da instância, escolher o tamanho certo da instância para uma workload, planejar atividades de dimensionamento proativamente e comparar aplicações para determinar se eles maximizam a performance disponível em uma instância.

O Amazon EC2 define os máximos de rede no nível da instância para garantir uma experiência de rede de alta qualidade, incluindo performance consistente da rede entre tamanhos de instância. A AWS fornece máximos para o seguinte em cada instância:

- Capacidade de largura de banda: cada instância do EC2 tem uma largura de banda máxima para tráfego agregado de entrada e saída, com base no tipo e no tamanho da instância. Algumas instâncias usam um mecanismo de crédito de E/S para alocar a largura de banda da rede com base na utilização média da largura de banda. O Amazon EC2 também tem largura de banda máxima para o tráfego da Direct Connect e da Internet. Para obter mais informações, consulte Largura de banda de rede de instâncias do Amazon EC2.
- Performance de pacote por segundo (PPS): cada instância do EC2 tem uma performance máxima de PPS, com base no tipo e no tamanho da instância.
- Conexões rastreadas: o grupo de segurança rastreia cada conexão estabelecida para garantir que os pacotes de retorno sejam entregues como esperado. Há um número máximo de conexões que podem ser rastreadas por instância. Para obter mais informações, consulte Rastreamento de conexão de grupo de segurança do Amazon EC2.
- Acesso ao serviço de link local: o Amazon EC2 fornece um PPS máximo por interface de rede para o tráfego de serviços de proxy local, como o serviço Amazon DNS, o serviço de metadados de instância e o Serviço de Sincronização Temporal da Amazon.

Quando o tráfego de rede de uma instância excede um máximo, a AWS formata o tráfego que excede o máximo ao enfileirar e eliminar pacotes de rede. É possível monitorar quando o tráfego

excede um máximo usando as métricas de performance de rede. Essas métricas informam sobre o impacto no tráfego da rede e possíveis problemas de performance da rede, em tempo real.

Conteúdo

- Requisitos
- Métricas para o driver ENA
- Exibir as métricas de performance de rede para sua instância do
- Métricas do ENA Express
- Métricas de performance de rede com o driver DPDK para ENA
- Métricas em instâncias que executam o FreeBSD

Requisitos

Instâncias do Linux

- Instale o driver ENA versão 2.2.10 ou posterior. Para verificar a versão instalada, use o comando ethtool. No exemplo a seguir, a versão atende ao requisito mínimo.

  ```
  [ec2-user ~]$ ethtool -i eth0 | grep version
  version: 2.2.10
  ```

  Para atualizar seu driver ENA, consulte Redes avançadas.
- Para importar essas métricas para o Amazon CloudWatch, instale o agente CloudWatch. Para obter mais informações, consulte Coletar métricas de performance de rede no Guia do usuário do Amazon CloudWatch.
- Para oferecer suporte à métrica `conntrack_allowance_available`, instale a versão 2.8.1 ou anterior do driver do ENA.
- Para substituir o limite de PPS de fragmento de saída de 1024, instale o driver do ENA versão 2.13.3 ou posterior.

Instâncias do Windows

- Instalar o driver ENA versão 2.2.2 ou posterior. Para verificar a versão instalada, use o Gerenciador de dispositivos da seguinte forma.

  1. Abra o Gerenciador de dispositivos executando `devmgmt.msc`.

2. Expanda Network Adapters (Adaptadores de rede).
3. Escolha Amazon Elastic Network Adapter , Properties (Propriedades).
4. Na guia Driver, localize Driver Version (Versão do driver).

Para atualizar seu driver ENA, consulte Redes avançadas.

- Para importar essas métricas para o Amazon CloudWatch, instale o agente CloudWatch. Para obter mais informações, consulte Coletar métricas avançadas de rede no Guia do usuário do Amazon CloudWatch.

Métricas para o driver ENA

O driver ENA entrega as seguintes métricas para a instância em tempo real. Elas fornecem o número cumulativo de pacotes na fila ou descartados em cada interface de rede desde a última restauração do driver.

Métrica	Descrição	Com suporte para
`bw_in_allowance_exceeded`	Número de pacotes na fila ou descartados porque a largura de banda agregada de entrada excedeu o máximo para a instância.	Todos os tipos de instâncias
`bw_out_allowance_exceeded`	Número de pacotes na fila ou descartados porque a largura de banda agregada de saída excedeu o máximo para a instância.	Todos os tipos de instâncias
`conntrack_allowance_exceeded`	Número de pacotes descartados porque o monitoramento da conexão excedeu o máximo para a instância e não foi possível estabelecer novas conexões. Isso pode resultar em perda de	Todos os tipos de instâncias

Métrica	Descrição	Com suporte para
	pacotes para tráfego indo para a instância ou vindo da instância	
`conntrack_allowance_available`	O número de conexões rastreadas que podem ser estabelecidas pela instância antes de atingir a cota de conexões rastreadas desse tipo de instância.	Somente instâncias baseadas em Nitro
`linklocal_allowance_exceeded`	Número de pacotes descartados porque o PPS do tráfego para os serviços de proxy local excedeu o máximo para a interface da rede. Isso afeta o tráfego para o serviço Amazon DNS, o serviço de metadados de instância e o Serviço de Sincronização Temporal da Amazon, mas não afeta o tráfego para resolvedores personalizados de DNS.	Todos os tipos de instâncias
`pps_allowance_exceeded`	Número de pacotes na fila ou descartados porque o PPS bidirecional excedeu o máximo para a instância.*	Todos os tipos de instâncias

* Dependendo da configuração do modo proxy de fragmento para o driver do ENA Linux v2.13.3 ou posterior, esse limite também pode incluir descartes de fragmentos de saída que excedem 1024 PPS para a interface de rede. Se o modo de proxy de fragmento estiver habilitado para o driver Linux, as quedas de fragmento de saída ignoram o limite de 1024 PPS normalmente aplicável e são contadas dentro das permissões de PPS padrão. O modo proxy de fragmento está desabilitado por padrão.

Exibir as métricas de performance de rede para sua instância do

O procedimento usado dependerá do sistema operacional da instância.

Instâncias do Linux

É possível publicar métricas em suas ferramentas favoritas para visualizar os dados das métricas. Por exemplo, é possível publicar as métricas em Amazon CloudWatch usando o agente CloudWatch. O agente permite que você selecione métricas individuais e controle a publicação.

Também é possível usar o ethtool para recuperar as métricas para cada interface de rede, como eth0, conforme mostrado a seguir.

```
[ec2-user ~]$ ethtool -S eth0
     bw_in_allowance_exceeded: 0
     bw_out_allowance_exceeded: 0
     pps_allowance_exceeded: 0
     conntrack_allowance_exceeded: 0
     linklocal_allowance_exceeded: 0
     conntrack_allowance_available: 136812
```

Instâncias do Windows

É possível visualizar as métricas usando qualquer consumidor de contadores de performance do Windows. Os dados podem ser analisados de acordo com o manifesto EnaperfCounters. Esse é um arquivo XML que define o provedor do contador de performance e seus countersets.

Para instalar o manifesto

Se você executou a instância usando uma AMI que contém o driver ENA 2.2.2 ou posterior ou usou o script de instalação no pacote de driver para o driver ENA 2.2.2, o manifesto já está instalado. Para instalar o manifesto manualmente, use as seguintes etapas:

1. Remova o manifesto existente usando o seguinte comando:

   ```
   unlodctr /m:EnaPerfCounters.man
   ```

2. Copie o arquivo manifesto `EnaPerfCounters.man` do pacote de instalação do driver para `%SystemRoot%\System32\drivers`.
3. Instale o novo manifesto usando o seguinte comando:

   ```
   lodctr /m:EnaPerfCounters.man
   ```

Para visualizar métricas usando o monitor de desempenho

1. Abra o Monitor de performance.
2. Pressione Ctrl+N para adicionar novos contadores.
3. Escolha ENA Packets Shaping (Modelagem de pacotes de ENA na lista.
4. Selecione as instâncias a serem monitoradas e escolha Add (Adicionar).
5. Escolha OK.

Métricas do ENA Express

O ENA Express conta com a tecnologia AWS Scalable Reliable Datagram (SRD). SRD é um protocolo de transporte de rede de alta performance que usa roteamento dinâmico para aumentar o throughput e minimizar a latência final. Se você tiver habilitado o ENA Express para as anexos de interface de rede na instância de envio e na instância de recebimento, poderá usar as métricas do ENA Express para ajudar a garantir que as instâncias aproveitem ao máximo as melhorias de desempenho que a tecnologia SRD oferece. Por exemplo:

- Avalie os recursos para garantir que tenham capacidade suficiente para estabelecer mais conexões por SRD.
- Identifique onde existem potenciais problemas que impedem que pacotes de saída elegíveis usem o SRD.
- Calcule a porcentagem de tráfego de saída que usa SRD para a instância.
- Calcule a porcentagem de tráfego de entrada que usa SRD para a instância.

> **Note**
>
> Para produzir métricas, use a versão 2.8 ou superior do driver.

Para ver uma lista de métricas para instâncias do Linux filtradas para o ENA Express, execute o comando ethtool a seguir para a interface de rede (mostrado aqui como `eth0`). Anote o valor da métrica `ena_srd_mode`.

```
[ec2-user ~]$ ethtool -S eth0 | grep ena_srd
NIC statistics:
```

```
ena_srd_mode: 1
ena_srd_tx_pkts: 0
ena_srd_eligible_tx_pkts: 0
ena_srd_rx_pkts: 0
ena_srd_resource_utilization: 0
```

As métricas a seguir estão disponíveis para todas as instâncias que têm o ENA Express habilitado.

ena_srd_mode

Descreve quais recursos do ENA Express estão habilitados. Os valores são os seguintes:

- `0` = ENA Express desativado, UDP desativado
- `1` = ENA Express ativado, UDP desativado
- `2` = ENA Express desativado, UDP ativado

> **Note**
>
> Isso só acontece quando o ENA Express foi originalmente habilitado e o UDP foi configurado para usá-lo. O valor anterior é retido para tráfego UDP.

- `3` = ENA Express ativado, UDP ativado

ena_srd_eligible_tx_pkts

O número de redes é o seguinte:

- Os tipos de instâncias de envio e de recebimento são compatíveis. Para obter mais informações, consulte a tabela Tipos de instâncias compatíveis com o ENA Express.
- As instâncias de envio e de recebimento devem ter o ENA Express configurado.
- As instâncias de envio e recebimento devem ser executadas na mesma zona de disponibilidade.
- O caminho da rede entre as instâncias não deve incluir caixas de middleware. No momento, o ENA Express não é compatível com caixas de middleware.

> **Note**
>
> A métrica de elegibilidade do ENA Express abrange os requisitos de origem e destino e a rede entre os dois endpoints. Pacotes elegíveis ainda podem ser desqualificados depois de já terem sido contados. Por exemplo, se um pacote elegível estiver acima do limite da

unidade de transmissão máxima (MTU), ele retornará para a transmissão ENA padrão, embora o pacote ainda apareça como elegível no contador.

ena_srd_tx_pkts

O número de pacotes de SRD transmitidos em um determinado período.

ena_srd_rx_pkts

O número de pacotes de SRD recebidos em um determinado período.

ena_srd_resource_utilization

A porcentagem da utilização da memória máxima permitida para conexões por SRD simultâneas que a instância consumiu.

Para confirmar se a transmissão de pacotes está usando SRD, você pode comparar o número de pacotes elegíveis (métrica `ena_srd_eligible_tx_pkts`) com o número de pacotes por SRD transmitidos (métrica `ena_srd_tx_pkts`) durante um determinado período.

Tráfego de saída (pacotes de saída)

Para garantir que o tráfego de saída use SRD conforme esperado, compare o número de pacotes elegíveis para SRD (`ena_srd_eligible_tx_pkts`) com o número de pacotes SRD enviados (`ena_srd_tx_pkts`) em um determinado período.

Diferenças significativas entre o número de pacotes elegíveis e o número de pacotes SRD enviados geralmente são causadas por problemas de utilização de recursos. Quando a placa de rede anexada à instância esgota seus recursos máximos ou seus pacotes estão acima do limite de MTU, os pacotes elegíveis não podem ser transmitidos por SRD e devem retornar à transmissão ENA padrão. Os pacotes também podem apresentar essa diferença durante as migrações em tempo real ou as atualizações de servidores em tempo real. É necessária uma avaliação adicional para determinar a causa raiz.

Note

Você pode ignorar pequenas diferenças ocasionais entre o número de pacotes elegíveis e o número de pacotes SRD. Isso pode acontecer quando a instância estabelece uma conexão com outra instância para tráfego SRD, por exemplo.

Para descobrir qual porcentagem do tráfego total de saída em um determinado período usa SRD, compare o número de pacotes SRD enviados (`ena_srd_tx_pkts`) com o número total de pacotes enviados para a instância (`NetworkPacketOut`) durante esse período.

Tráfego de entrada (pacotes recebidos)

Para descobrir qual porcentagem do tráfego de entrada usa SRD, compare o número de pacotes SRD recebidos (`ena_srd_rx_pkts`) em um determinado período com o número total de pacotes recebidos para a instância (`NetworkPacketIn`) durante esse período.

Utilização de recursos

A utilização de recursos é baseada no número de conexões SRD simultâneas que uma única instância pode manter em um determinado momento. A métrica de utilização de recursos (`ena_srd_resource_utilization`) monitora a utilização atual da instância. À medida que a utilização se aproxima de 100%, você pode esperar problemas de performance. O ENA Express deixa de usar SRD e volta à transmissão ENA padrão, e a possibilidade de pacotes descartados aumenta. A alta utilização de recursos é um sinal de que está na hora de aumentar a escala da instância horizontalmente para melhorar a performance da rede.

> **Note**
>
> Quando o tráfego de rede de uma instância excede um máximo, a AWS formata o tráfego que excede o máximo ao enfileirar e eliminar pacotes de rede.

Persistência

As métricas de saída e entrada são cumulativas enquanto o ENA Express está habilitado para a instância. As métricas deixarão de ser acumulativas se o ENA Express for desativado, mas persistirão enquanto a instância ainda estiver em execução. As métricas serão redefinidas se a instância for reinicializada ou encerrada ou se a interface de rede for desconectada da instância.

Métricas de performance de rede com o driver DPDK para ENA

O driver ENA versão 2.2.0 e posterior oferece suporte a relatórios de métricas de rede. O DPDK 20.11 inclui o driver ENA 2.2.0 e é a primeira versão do DPDK a suportar esse recurso.

O driver DPDK v25.03 ou posterior oferece suporte ao modo de proxy de fragmento. Se o modo de proxy de fragmento estiver habilitado para o driver DPDK, os descartes de fragmentos de saída

ignoram o limite de 1024 PPS normalmente aplicável e são contados dentro das permissões de PPS padrão. O modo proxy de fragmento está desabilitado por padrão.

É possível usar uma aplicação de exemplo para visualizar estatísticas DPDK. Para iniciar uma versão interativa da aplicação de exemplo, execute o seguinte comando.

```
./app/dpdk-testpmd -- -i
```

Dentro desta sessão interativa, é possível inserir um comando para recuperar dados estatísticos estendidos para uma porta. O comando de exemplo a seguir recupera as estatísticas da porta 0.

```
show port xstats 0
```

Veja a seguir um exemplo de uma sessão interativa com a aplicação de exemplo DPDK.

```
[root@ip-192.0.2.0 build]# ./app/dpdk-testpmd -- -i
        EAL: Detected 4 lcore(s)
        EAL: Detected 1 NUMA nodes
        EAL: Multi-process socket /var/run/dpdk/rte/mp_socket
        EAL: Selected IOVA mode 'PA'
        EAL: Probing VFIO support...
        EAL:   Invalid NUMA socket, default to 0
        EAL:   Invalid NUMA socket, default to 0
        EAL: Probe PCI driver: net_ena (1d0f:ec20) device: 0000:00:06.0
(socket 0)
        EAL: No legacy callbacks, legacy socket not created
        Interactive-mode selected

        Port 0: link state change event
        testpmd: create a new mbuf pool <mb_pool_0>: n=171456,
size=2176, socket=0
        testpmd: preferred mempool ops selected: ring_mp_mc

        Warning! port-topology=paired and odd forward ports number, the
last port will pair with itself.

        Configuring Port 0 (socket 0)
        Port 0: 02:C7:17:A2:60:B1
        Checking link statuses...
        Done
        Error during enabling promiscuous mode for port 0: Operation
not supported - ignore
```

```
testpmd> show port xstats 0
###### NIC extended statistics for port 0
rx_good_packets: 0
tx_good_packets: 0
rx_good_bytes: 0
tx_good_bytes: 0
rx_missed_errors: 0
rx_errors: 0
tx_errors: 0
rx_mbuf_allocation_errors: 0
rx_q0_packets: 0
rx_q0_bytes: 0
rx_q0_errors: 0
tx_q0_packets: 0
tx_q0_bytes: 0
wd_expired: 0
dev_start: 1
dev_stop: 0
tx_drops: 0
bw_in_allowance_exceeded: 0
bw_out_allowance_exceeded: 0
pps_allowance_exceeded: 0
conntrack_allowance_exceeded: 0
linklocal_allowance_exceeded: 0
rx_q0_cnt: 0
rx_q0_bytes: 0
rx_q0_refill_partial: 0
rx_q0_bad_csum: 0
rx_q0_mbuf_alloc_fail: 0
rx_q0_bad_desc_num: 0
rx_q0_bad_req_id: 0
tx_q0_cnt: 0
tx_q0_bytes: 0
tx_q0_prepare_ctx_err: 0
tx_q0_linearize: 0
tx_q0_linearize_failed: 0
tx_q0_tx_poll: 0
tx_q0_doorbells: 0
tx_q0_bad_req_id: 0
tx_q0_available_desc: 1023
testpmd>
```

Para obter mais informações sobre a aplicação de exemplo e usá-lo para recuperar dados estatísticos estendidos, consulte Guia do usuário da aplicação Testpmd na documentação do DPDK.

Métricas em instâncias que executam o FreeBSD

A partir da versão 2.3.0, o driver ENA FreeBSD suporta a coleta de métricas de performance de rede em instâncias que executam o FreeBSD. Para habilitar a coleção de métricas do FreeBSD, insira o seguinte comando e defina o *intervalo* como um valor entre 1 e 3.600. Isso especifica com que frequência, em segundos, serão coletadas métricas do FreeBSD.

```
sysctl dev.ena.network_interface.eni_metrics.sample_interval=interval
```

Por exemplo, o comando a seguir define o driver para coletar métricas do FreeBSD na interface de rede 1 a cada 10 segundos:

```
sysctl dev.ena.1.eni_metrics.sample_interval=10
```

Para desativar a coleta de métricas do FreeBSD, é possível executar o comando anterior e especificar `0` como o *intervalo*.

Depois de habilitar a coleta de métricas do FreeBSD, é possível recuperar o conjunto mais recente de métricas coletadas ao executar o comando apresentado a seguir.

```
sysctl dev.ena.network_interface.eni_metrics
```

Aprimorar a latência de rede para instâncias do EC2 baseadas no Linux

A latência de rede corresponde à quantidade de tempo que um pacote de dados demora para se deslocar da origem até o destino. As aplicações que enviam dados pela rede dependem de respostas em tempo hábil para fornecer uma experiência positiva ao usuário. A alta latência de rede pode acarretar diversos problemas, como os seguintes:

- Tempos de carregamento lentos para páginas da Web.
- Atraso na transmissão de vídeo.
- Dificuldade de acesso aos recursos online.

Esta seção descreve as etapas que podem ser seguidas para aprimorar a latência de rede em instâncias do Amazon EC2 executadas em Linux. Para obter a latência ideal, siga estas etapas

para definir as configurações de sua instância, kernel e driver ENA. Para obter orientação de configurações adicionais, consulte o Guia de práticas recomendadas e otimização de performance para o driver ENA do Linux no GitHub.

> **Note**
>
> As etapas e configurações podem variar um pouco, dependendo do hardware de rede específico, da AMI da qual você executou a instância e do caso de uso da aplicação. Antes de realizar qualquer alteração, teste e monitore minuciosamente a performance da rede para garantir que esteja obtendo os resultados desejados.

Reduzir o número de saltos de rede para pacotes de dados

Cada salto que um pacote de dados tem ao se mover de um roteador para outro aumenta a latência da rede. Normalmente, o tráfego passa por diversos saltos para chegar ao seu destino. Há duas maneiras de reduzir os saltos de rede para as instâncias do Amazon EC2, conforme apresentado a seguir:

- Grupo com posicionamento em cluster: ao especificar um grupo com posicionamento em cluster, o Amazon EC2 executa instâncias que estão com grande proximidade umas das outras, fisicamente na mesma zona de disponibilidade (AZ) comempacotamento mais restrito. A proximidade física das instâncias no grupo permite que elas aproveitem a conectividade de alta velocidade, resultando em baixa latência e alta throughput de fluxo único.
- Host dedicado: um host dedicado é um servidor físico dedicado para seu uso. Com um host dedicado, é possível executar as instâncias no mesmo servidor físico. A comunicação entre instâncias executada no mesmo host dedicado pode ocorrer sem nenhum salto extra de rede.

Como a configuração do kernel do Linux afeta a latência

A configuração do kernel do Linux pode aumentar ou diminuir a latência da rede. Para atingir suas metas de otimização de latência, é importante ajustar a configuração do kernel do Linux de acordo com os requisitos específicos de sua workload.

Existem várias opções de configuração para o kernel do Linux que podem ajudar a diminuir a latência da rede. As opções mais impactantes são as seguintes.

- Ativação do modo de pesquisa ocupada: o modo de pesquisa ocupada reduz a latência no caminho de recebimento da rede. Ao ativar o modo de pesquisa ocupada, o código da camada de soquete pode pesquisar diretamente a fila de recebimento de um dispositivo de rede. A desvantagem de uma sondagem ocupada é o maior uso da CPU no host, resultante da sondagem de novos dados em um ciclo restrito. Há duas configurações globais que controlam o número de microssegundos para aguardar os pacotes para todas as interfaces.

  `busy_read`

  Um tempo limite de sondagem ocupada de baixa latência para leituras de soquete. Ele controla o número de microssegundos a aguardar para camada de soquete ler os pacotes na fila de dispositivos. Para habilitar o recurso globalmente com o comando sysctl, a organização Linux Kernel recomenda um valor de 50 microssegundos. Para obter mais informações, consulte busy_read no Guia do usuário e do administrador do kernel doo Linux.

  ```
  [ec2-user ~]$ sudo sysctl -w net.core.busy_read=50
  ```

  `busy_poll`

  Um tempo limite de sondagem ocupada de baixa latência para sondagem e seleção. Isso controla o número de microssegundos a aguardar por eventos. O valor recomendado está entre 50-100 microssegundos, dependendo do número de soquetes que você estiver sondando. Quanto mais soquetes você adicionar, maior deve ser o número.

  ```
  [ec2-user ~]$ sudo sysctl -w net.core.busy_poll=50
  ```

- Configuração dos estados de energia da CPU (C-states): os C-states controlam os níveis de suspensão em que um núcleo pode entrar quando está inativo. Você pode desejar controlar os C-states para ajustar o sistema em relação à latência versus performance. Em estados C mais profundos, a CPU está essencialmente “adormecida” e não poderá responder às solicitações até acordar e fazer a transição de volta ao estado ativo. 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. É possível configurar o sistema para que ele não use estados C mais profundos. No entanto, embora essa configuração

reduza a latência de reação do processador, ela também reduz o espaço disponível para outros núcleos para o Turbo Boost.

Para reduzir a latência de reação do processador, é possível limitar mais profundamente os C-states. Para obter mais informações, consulte High performance and low latency by limiting deeper C-states no Amazon Linux 2 User Guide.

Moderação de interrupção

O driver de rede ENA possibilita a comunicação entre uma instância e uma rede. O driver processa os pacotes de rede e os repassa à pilha de rede ou ao cartão Nitro. Quando um pacote de rede chega, o cartão Nitro gera uma interrupção para a CPU notificar o software sobre um evento.

Interromper

Uma interrupção é um sinal que um dispositivo ou aplicação envia ao processador. A interrupção informa ao processador que ocorreu um evento ou que foi atendida uma condição que requer atenção imediata. As interrupções podem lidar com tarefas urgentes, como receber dados de uma interface de rede, lidar com eventos de hardware ou atender a solicitações de outros dispositivos.

Moderação de interrupção

A moderação de interrupções é uma técnica que reduz o número de interrupções que um dispositivo gera agregando ou atrasando-as. O objetivo da moderação de interrupções é melhorar o desempenho do sistema, reduzindo a sobrecarga associada ao tratamento de um grande número de interrupções. Interrupções demais aumentam o uso da CPU, afetando negativamente a throughput, enquanto poucas interrupções aumentam a latência.

Moderação dinâmico de interrupções

A moderação dinâmica de interrupções é uma forma aprimorada de moderação de interrupção que ajusta dinamicamente a taxa de interrupções com base nos padrões atuais de carga e tráfego do sistema. O objetivo é encontrar um equilíbrio entre reduzir a sobrecarga de interrupções e os pacotes por segundo, ou a largura de banda.

> **Note**
>
> A moderação dinâmica de interrupções é habilitada por padrão em algumas AMIs (mas pode ser habilitada ou desabilitada em todas as AMIs).

Para minimizar a latência da rede, pode ser necessário desabilitar a moderação de interrupções. No entanto, isso também pode aumentar a sobrecarga do processamento de interrupção. É importante descobrir o balanceamento adequado entre reduzir a latência e minimizar a sobrecarga. Os comandos `ethtool` podem ajudar você a configurar a moderação de interrupção. Por padrão, `rx-usecs` está definido como `20` e `tx-usecs` está definido como `64`.

Para obter a configuração de modificação de interrupção atual, use o comando a seguir.

```
[ec2-user ~]$ ethtool -c interface | egrep "rx-usecs:|tx-usecs:|Adaptive RX"
Adaptive RX: on  TX: off
rx-usecs: 20
tx-usecs: 64
```

Para desativar a modificação de interrupções, use o comando a seguir.

```
[ec2-user ~]$ sudo ethtool -C interface adaptive-rx off rx-usecs 0 tx-usecs 0
```

Considerações sobre o Nitro System para ajuste de performance

O Sistema Nitro é uma coleção de hardware e componentes de software desenvolvidos pela AWS que permitem alta performance, alta disponibilidade e alta segurança. O Nitro System fornece funcionalidades semelhantes às funcionalidades do bare metal que eliminam a sobrecarga de virtualização e são compatíveis com workloads que requerem acesso total ao hardware de host. Para obter informações mais detalhadas, consulte AWS Nitro System.

Todos os tipos de instância do EC2 da geração atual executam o processamento de pacotes de rede em cartões Nitro do EC2. Este tópico aborda a manipulação de pacotes de alto nível no cartão Nitro, os aspectos conhecidos da arquitetura e da configuração de rede que afetam a performance da manipulação de pacotes e as ações você pode executar para atingir a performance máxima para as instâncias baseadas no Nitro.

Os cartões Nitro lidam com todas as interfaces de entrada e saída (E/S), como aquelas necessárias para as nuvens privadas virtuais (VPCs). Para todos os componentes que enviam ou recebem informações pela rede, os cartões Nitro atuam como um dispositivo de computação independente para o tráfego de E/S que é fisicamente separado da placa principal do sistema na qual as workloads do cliente são executadas.

Fluxo de pacotes de rede em cartões Nitro

As instâncias do EC2 desenvolvidas no Nitro System têm funcionalidades de aceleração de hardware que facilitam um processamento de pacotes mais rápido, conforme medido pelas taxas de throughput de pacotes por segundo (PPS). Quando um cartão Nitro executa a avaliação inicial para um novo fluxo, ele salva informações semelhantes para todos os pacotes no fluxo, como os grupos de segurança, as listas de controle de acesso e as entradas da tabela de rotas. Ao processar pacotes adicionais para o mesmo fluxo, ele pode usar as informações salvas para reduzir a sobrecarga desses pacotes.

A taxa de conexão é medida pela métrica de conexões por segundo (CPS). Cada nova conexão requer uma sobrecarga de processamento adicional que deve ser considerada nas estimativas de capacidade para a workload. É importante considerar as métricas de CPS e de PPS ao projetar as workloads.

Como uma conexão é estabelecida

Quando uma conexão é estabelecida entre uma instância baseada no Nitro e outro endpoint, o cartão Nitro avalia o fluxo completo do primeiro pacote enviado ou recebido entre os dois endpoints. Em geral não é necessária uma reavaliação completa para pacotes subsequentes do mesmo fluxo. No entanto, existem exceções. Para obter mais informações sobre as exceções, consulte Pacotes que não usam a aceleração de hardware.

As propriedades apresentadas a seguir definem os dois endpoints e o fluxo de pacotes entre eles. Essas cinco propriedades em conjunto são conhecidas como um fluxo de cinco tuplas.

- IP de origem
- Porta de origem
- IP de destino
- Porta de destino
- Protocolo de comunicação

A direção do fluxo de pacotes é conhecida como ingress (entrada) e egress (saída). As descrições de alto nível apresentadas a seguir resumem o fluxo de pacotes de rede de ponta a ponta.

- Ingress: quando um cartão Nitro lida com um pacote de rede de entrada, ele avalia o pacote em relação a regras de firewall com estado e a listas de controle de acesso. Ele rastreia a conexão,

realiza a medição dela e executa outras ações, conforme aplicável. Em seguida, ele encaminha o pacote ao destino na CPU de host.

- Egress: quando um cartão Nitro lida com um pacote de rede de saída, ele procura o destino da interface remota, avalia diversas funções da VPC, aplica limites de taxa e executa outras ações aplicáveis. Em seguida, ele encaminha o pacote para o destino do próximo salto na rede.

Projetar sua rede para desempenho ideal

Para aproveitar as funcionalidades de performance do Nitro System, é necessário compreender quais são as suas necessidades de processamento de rede e como elas afetam a workload dos seus recursos do Nitro. Em seguida, será possível realizar um projeto para obtenção de uma performance ideal para seu cenário de rede. As definições de infraestrutura, design e configuração da workload da aplicação podem afetar o processamento de pacotes e as taxas de conexão. Por exemplo, se a aplicação tiver uma alta taxa de estabelecimento de conexão, como um serviço de DNS, um firewall ou um roteador virtual, ela terá menos oportunidades de aproveitar a aceleração de hardware que ocorre somente após o estabelecimento da conexão.

É possível definir as configurações da aplicação e da infraestrutura para simplificar as workloads e aprimorar a performance da rede. No entanto, nem todos os pacotes que estão qualificados para a aceleração. O Nitro System utiliza todo o fluxo de rede para novas conexões e para pacotes que não estão qualificados para a aceleração.

O restante desta seção se concentrará nas considerações de projeto para a aplicação e para a infraestrutura com a finalidade de ajudar a garantir que os pacotes fluam dentro do caminho com aceleração, tanto quanto possível.

Considerações de projeto de rede para o Nitro System

Ao configurar o tráfego de rede para a instância, existem muitos aspectos a serem considerados que podem afetar a performance de PPS. Depois que um fluxo é estabelecido, a maioria dos pacotes que entram ou saem regularmente está qualificado para a aceleração. No entanto, existem exceções para garantir que os projetos de infraestrutura e os fluxos de pacotes continuem atendendo aos padrões dos protocolos.

Para obter a melhor performance do cartão Nitro, é necessário considerar com atenção os prós e os contras dos detalhes de configuração apresentados a seguir para a infraestrutura e para as aplicações.

Considerações sobre infraestrutura

A configuração da infraestrutura pode afetar o fluxo de pacotes e a eficiência do processamento. A lista apresentada a seguir inclui algumas considerações importantes.

Configuração da interface de rede com assimetria

Os grupos de segurança usam o rastreamento de conexão para rastrear informações sobre o tráfego que flui de e para a instância. O roteamento assimétrico, em que o tráfego entra em uma instância por meio de uma interface de rede e sai por meio de uma interface de rede diferente, pode reduzir a performance máxima que uma instância poderá alcançar se os fluxos forem rastreados. Para obter mais informações sobre o rastreamento de conexões para grupos de segurança, conexões não rastreadas e conexões rastreadas automaticamente, consulte Rastreamento de conexão de grupo de segurança do Amazon EC2.

Drivers de rede

Os drivers de rede são atualizados e lançados regularmente. A performance poderá ser significativamente prejudicada se os drivers estiverem desatualizados. Mantenha os drivers atualizados para garantir que você tenha os patches mais recentes e possa aproveitar as vantagens fornecidas pelos aprimoramentos de performance, como o recurso de caminho com aceleração que está disponível somente para a última geração de drivers. Os drivers anteriores não são compatíveis com o recurso de caminho com aceleração.

Para aproveitar o recurso de caminho com aceleração, recomendamos instalar o driver do ENA mais recente nas instâncias.

Instâncias do Linux: driver do ENA para o Linux na versão 2.2.9 ou em versões posteriores. Para instalar ou atualizar o driver do ENA para Linux usando o repositório Amazon Drivers no GitHub, consulte a seção Driver compilation do arquivo “leia-me”.

Instâncias do Windows: driver do ENA para o Windows na versão 2.0.0 ou em versões posteriores. Para instalar ou atualizar o driver do ENA para o Windows, consulte Instalar o driver do ENA em instâncias do Windows do EC2.

Distância entre os endpoints

Uma conexão entre duas instâncias na mesma zona de disponibilidade pode processar mais pacotes por segundo do que uma conexão entre regiões, como resultado do janelamento de TCP na camada da aplicação, que define quantos dados podem estar em trânsito a qualquer momento. As longas distâncias entre as instâncias aumentam a latência e diminuem o número de pacotes que os endpoints podem processar.

Limite de fila de bytes (BQL)

O BQL é um recurso que limita o número de bytes passados para a placa Nitro para reduzir o enfileiramento. O BQL é desabilitado por padrão nos drivers do ENA, nos sistemas operacionais Amazon Linux e na maioria das distribuições Linux. Se o BQL e a substituição do proxy de fragmento estiverem habilitados, isso pode resultar em limitações de desempenho, restringindo o número de bytes passados para o Nitro antes que todos os fragmentos sejam processados.

Considerações sobre o projeto da aplicação

Existem aspectos do projeto e da configuração da aplicação que podem afetar a eficiência do processamento. A lista apresentada a seguir inclui algumas considerações importantes.

Tamanho do pacote

Os pacotes com tamanhos maiores podem aumentar o throughput para os dados que uma instância pode enviar e receber na rede. O Amazon EC2 é compatível com jumbo frames de 9001 bytes, mas outros serviços podem impor limites diferentes. Os pacotes com tamanhos menores podem aumentar a taxa de processamento de pacotes, mas podem reduzir a largura de banda máxima alcançada quando o número de pacotes excede as permissões de PPS.

Se o tamanho de um pacote exceder a Unidade Máxima de Transmissão (MTU) de um salto de rede, um roteador ao longo do caminho poderá fragmentá-lo. Os fragmentos de pacotes resultantes são considerados exceções e são normalmente processados na taxa padrão (não acelerada). Isso pode causar variações na performance. No entanto, você pode substituir o comportamento padrão para pacotes fragmentados de saída com a configuração do modo de proxy de fragmentos. Para obter mais informações, consulte Maximização da performance da rede no Nitro System. Recomendamos avaliar a topologia ao configurar a MTU.

Compensações de protocolo

Os protocolos confiáveis, como o TCP, têm mais sobrecarga do que os protocolos não confiáveis, como o UDP. A menor sobrecarga e o processamento de rede simplificado para o protocolo de transporte UDP podem resultar em uma taxa de PPS mais alta, mas às custas da entrega confiável de pacotes. Se a entrega confiável de pacotes não for crítica para a aplicação, o protocolo UDP pode ser uma boa opção.

Microexpansão

A Microexpansão ocorre quando o tráfego excede as permissões durante breves períodos de tempo, em vez de ser distribuído uniformemente. Isso costuma acontecer em uma escala de microssegundos.

Por exemplo, suponhamos que você tenha uma instância que pode enviar até 10 Gbps e a aplicação envie 10 Gb completos em meio segundo. Essa microexpansão excede o permitido durante a primeira metade do segundo e não deixa nada para o restante da segunda. Mesmo que você tenha enviado 10 Gb no período de um segundo, as permissões na primeira metade do segundo podem resultar em pacotes enfileirados ou descartados.

É possível usar um programador de rede, como o Traffic Control do Linux, para ajudar no controle do throughput e evitar provocar pacotes enfileirados ou descartados como resultado de uma microexpansão.

Número de fluxos

Um único fluxo é limitado a 5 Gbps, a menos que esteja em um grupo de posicionamento de cluster que oferece suporte para até 10 Gbps ou que use o ENA Express, que oferece suporte para até 25 Gbps.

Da mesma forma que um cartão Nitro pode processar mais pacotes em vários fluxos, em vez de usar um único fluxo. Para atingir a taxa máxima de processamento de pacotes por instância, recomendamos, no mínimo, cem fluxos em instâncias com largura de banda agregada de 100 Gbps ou superior. À medida que as funcionalidades agregadas de largura de banda aumentam, o número de fluxos necessários para atingir as taxas de processamento máximas também aumenta. A avaliação comparativa ajudará você a definir qual configuração é necessária para atingir as taxas máximas em sua rede.

Filas do Adaptador de Rede Elástica (ENA)

O ENA (Elastic Network Adapter) usa várias filas de recepção (Rx) e transmissão (Tx) (filas do ENA) para melhorar a performance e a escalabilidade de rede nas instâncias do EC2. Essas filas gerenciam eficientemente o tráfego de rede balanceando a carga de dados enviados e recebidos entre as filas disponíveis.

Para obter mais informações, consulte the section called “Filas do ENA”.

Sobrecarga no processamento de recursos

Os recursos, como o Espelhamento de Tráfego e o ENA Express, podem adicionar mais sobrecarga de processamento, o que pode reduzir a performance absoluta do processamento

de pacotes. É possível limitar o uso de recursos ou desativá-los para aumentar as taxas de processamento de pacotes.

Rastreamento de conexão para manutenção do estado

Os grupos de segurança usam o rastreamento de conexão para armazenar as informações sobre o tráfego de entrada e de saída da instância. O rastreamento de conexão aplica regras a cada fluxo de tráfego de rede individual para determinar se o tráfego será permitido ou negado. O cartão Nitro usa o rastreamento de fluxo para realizar a manutenção do estado para o fluxo. À medida que mais regras do grupo de segurança são aplicadas, mais trabalho é necessário para avaliar o fluxo.

> **Note**
>
> Não são todos os fluxos de tráfego de rede que são rastreados. Se uma regra do grupo de segurança estiver configurada com Conexões não rastreadas, nenhum trabalho adicional será necessário, exceto para conexões que são rastreadas automaticamente a fim de garantir o roteamento simétrico quando houver vários caminhos de resposta válidos.

Pacotes que não usam a aceleração de hardware

Não são todos os pacotes que podem aproveitar a aceleração de hardware. O tratamento dessas exceções envolve alguma sobrecarga de processamento necessária para garantir a integridade dos fluxos de rede. Os fluxos de rede devem atender aos padrões de protocolo com confiabilidade, estar em conformidade com as alterações no projeto da VPC e rotear pacotes somente para destinos permitidos. No entanto, a sobrecarga reduz a performance.

Fragmentos de pacote

Conforme mencionado em Considerações da aplicação, os fragmentos de pacotes resultantes de pacotes que excedem a MTU da rede são tratados normalmente como exceções e não podem aproveitar a aceleração de hardware. Entretanto, é possível contornar as limitações do fragmento de saída com o modo de proxy de fragmento, dependendo da versão do driver. Para obter mais informações, consulte as ações que podem ser tomadas na seção Maximização da performance da rede no Nitro System.

Conexões ociosas

Quando uma conexão não tiver atividade por um período, mesmo que não tenha atingido o tempo limite, o sistema pode deixar de priorizá-la. Assim, se os dados forem recebidos depois que a conexão deixar de ser priorizada, o sistema precisará tratá-los como uma exceção para se reconectar.

Para gerenciar as conexões, é possível usar tempos limite de rastreamento de conexão para fechar as conexões ociosas. Além disso, é possível usar a opção keep-alive do TCP para manter as conexões ociosas abertas. Para obter mais informações, consulte Tempo limite de rastreamento de conexão ociosa.

Mutação da VPC

As atualizações em grupos de segurança, tabelas de rotas e listas de controle de acesso precisam ser avaliadas novamente no caminho de processamento para garantir que as entradas de rota e as regras do grupo de segurança ainda sejam aplicadas conforme o esperado.

Fluxos ICMP

O Internet Control Message Protocol (ICMP) é um protocolo de camada de rede que os dispositivos de rede usam para diagnosticar problemas de comunicação de rede. Esses pacotes sempre usam o fluxo completo.

Fluxos assimétricos de L2

O NitroV3 e as plataformas anteriores não usam aceleração de hardware para tráfego entre duas ENIs na mesma sub-rede quando uma ENI está usando o roteador de gateway padrão e a outra não. As plataformas NitroV4 e posteriores utilizam aceleração de hardware nesse cenário. Para obter uma melhor performance na plataforma NitroV3 ou anteriores, certifique-se de que o roteador de gateway padrão usado seja o mesmo em ambas as ENIs ou que essas ENIs estejam em sub-redes diferentes.

Maximização da performance da rede no Nitro System

Você pode maximizar a performance da rede no sistema Nitro ajustando as configurações de rede.

Tópicos

- Considerações
- Ajustar a performance de PPS

- Configurar a alocação da fila ENA
- Monitoramento da performance em instâncias do Linux

Considerações

Antes de tomar qualquer decisão em relação ao projeto ou ajustar quaisquer configurações de rede na instância, recomendamos que você siga etapas apresentadas a seguir para obter o melhor resultado:

1. Compreenda os prós e os contras das ações que você pode executar para aprimorar a performance ao analisar as Considerações de projeto de rede para o Nitro System.

   Para obter mais considerações e as práticas recomendadas para a configuração da instância no Linux, consulte ENA Linux Driver Best Practices and Performance Optimization Guide no GitHub.
2. Faça uma avaliação comparativa das workloads com a contagem máxima de fluxo ativo para definir uma referência para a performance da aplicação. Com uma referência para a performance, é possível testar variações nas configurações ou no projeto da aplicação para compreender quais considerações terão maior impacto, sobretudo se você planeja aumentar a escala verticalmente ou aumentar a escala horizontalmente.

Ajustar a performance de PPS

A seguinte lista contém ações que podem ser executadas para ajustar a performance de PPS, conforme as necessidades do sistema.

- Reduzir a distância física entre duas instâncias. Quando as instâncias de envio e de recebimento estão localizadas na mesma zona de disponibilidade ou usam grupos de posicionamento de cluster, é possível reduzir o número de saltos que um pacote precisa realizar para se deslocar de um endpoint para outro.
- Usar Conexões não rastreadas.
- Usar o protocolo UDP para o tráfego de rede.
- Para instâncias do EC2 com largura de banda agregada de 100 Gbps ou mais, distribuir a workload em cem ou mais fluxos individuais para distribuir o trabalho uniformemente pelo cartão Nitro.
- Para superar o limite de PPS do fragmento de saída nas instâncias do EC2, você pode habilitar o modo de proxy de fragmento (dependendo da versão do driver). Essa configuração permite que

pacotes fragmentados sejam avaliados no caminho de processamento, superando, assim, o limite de PPS de saída de 1024. Ao carregar o driver, execute um dos seguintes comandos para habilitar ou desabilitar o modo proxy de fragmento:

Habilitar o modo proxy de fragmento

```
sudo insmod ena.ko enable_frag_bypass=1
```

Desabilitar o modo proxy de fragmento

```
sudo insmod ena.ko enable_frag_bypass=0
```

Configurar a alocação da fila ENA

Nos tipos de instância compatíveis, você pode alocar dinamicamente essas filas nas Interfaces de Rede Elástica (ENIs). A alocação flexível de filas do ENA otimiza a distribuição de recursos, permitindo a máxima utilização da vCPU. Workloads de alta performance de rede normalmente exigem várias filas do ENA. Para obter mais informações, consulte Filas do ENA.

Monitoramento da performance em instâncias do Linux

É possível usar métricas do plug-in Ethtool em instâncias do Linux para monitorar indicadores de performance de rede de instâncias, como a largura de banda, a taxa de pacotes e o rastreamento de conexão. Para obter mais informações, consulte Monitorar o desempenho de rede de instâncias do EC2.

Otimizar performance da rede em instâncias do Windows do EC2

Para obter a máxima performance da rede nas instâncias do Windows com redes aperfeiçoadas, pode ser necessário modificar a configuração padrão do sistema operacional. Recomendamos as seguintes alterações de configuração para aplicações que exigem alta performance de rede. Outras otimizações (como ativar o descarregamento de soma de verificação e habilitar RSS, por exemplo) já estão configuradas nas AMIs oficiais do Windows.

> **Note**
>
> O descarregamento do TCP chimney deve ser desabilitado na maioria dos casos de uso e se tornou obsoleto a partir do Windows Server 2016.

Além dessas otimizações do sistema operacional, você também deve considerar a unidade de transmissão máxima (MTU - maximum transmission unit) de seu tráfego de rede e ajustá-la de acordo com sua workload e arquitetura de rede. Para obter mais informações, consulte Unidade de transmissão máxima (MTU) de rede para a instância do EC2.

A AWS mede regularmente as latências médias de ida e volta entre instâncias iniciadas em um grupo de posicionamento de cluster de 50 us e latência final de 200 us no percentil 99,9. Se suas aplicações exigirem baixas latências de forma consistente, recomendamos usar a versão mais recente dos drivers ENA em instâncias de performance fixa criadas no sistema Nitro.

Configurar a afinidade de CPU do Receive Side Scaling

O Receive Side Scaling (RSS) é usado para distribuir a carga da CPU do tráfego de rede em vários processadores. Por padrão, as AMIs oficiais do Amazon Windows são configuradas com RSS ativado. Interfaces de rede elástica do ENA fornecem até oito filas RSS. Com a definição de afinidade de CPU para filas RSS, bem como para outros processos do sistema, é possível distribuir a carga de CPU pelos sistemas com vários núcleos, permitindo que mais tráfego de rede seja processado. Em tipos de instância com mais de 16 vCPUs, recomendamos que você use o cmdlet `Set-NetAdapterRSS` do PowerShell, que exclui manualmente o processador de inicialização (processador lógico 0 e 1 quando o hyper-threading está ativado) da configuração de RSS para todas as interfaces de rede elástica, para evitar a contenção com vários componentes do sistema.

O Windows reconhece o hyper-thread e garante que as filas RSS de uma única placa de interface de rede (NIC) sejam sempre colocadas em diferentes núcleos físicos. Portanto, a menos que o hyper-threading esteja desabilitado, para evitar completamente a contenção com outras NICs, propague a configuração RSS de cada NIC entre um intervalo de 16 processadores lógicos. O cmdlet `Set-NetAdapterRss` permite que você defina o intervalo por NIC de processadores lógicos válidos definindo os valores de BaseProcessorGroup, BaseProcessorNumber, MaxProcessingGroup, MaxProcessorNumber e NumaNode (opcional). Se não houver núcleos físicos suficientes para eliminar completamente a contenção entre NICs, minimize os intervalos de sobreposição ou reduza o número de processadores lógicos nos intervalos de interface de rede elástica, dependendo da workload esperada da interface (ou seja, uma interface de rede administrativa de baixo volume talvez não precise de tantas filas RSS atribuídas). Além disso, como observado anteriormente, diversos componentes devem ser executados na CPU 0 e, por isso, recomendamos a exclusão em todas as configurações RSS quando houver vCPUs suficientes disponíveis.

Por exemplo, quando existem três interfaces de rede elástica em uma instância de 72 vCPUs com dois nós NUMA com o hyper-threading habilitado, os comandos a seguir distribuem a carga de rede entre as duas CPUs sem sobreposição e impedem completamente o uso do núcleo 0.

```
Set-NetAdapterRss -Name NIC1 -BaseProcessorGroup 0 -BaseProcessorNumber 2 -
MaxProcessorNumber 16
Set-NetAdapterRss -Name NIC2 -BaseProcessorGroup 1 -BaseProcessorNumber 0 -
MaxProcessorNumber 14
Set-NetAdapterRss -Name NIC3 -BaseProcessorGroup 1 -BaseProcessorNumber 16 -
MaxProcessorNumber 30
```

Observe que essas configurações são persistentes para cada adaptador de rede. Se uma instância for redimensionada para outra com um número diferente de vCPUs, você deverá reavaliar a configuração de RSS para cada interface de rede elástica habilitada. A documentação completa da Microsoft para o cmdlet pode ser encontrada aqui: Set-NetAdapterRss.

Observação especial para workloads SQL: também recomendamos que você revise suas configurações de afinidade de thread de E/S com sua configuração RSS da interface de rede elástica para minimizar a contenção de E/S e de rede para as mesmas CPUs. Consulte Configuração do servidor: máscara de afinidade.

Elastic Fabric Adapter para workloads de IA/ML e HPC no Amazon EC2

Um Elastic Fabric Adapter (EFA) é um dispositivo de rede que pode ser conectado à sua instância do Amazon EC2 para acelerar aplicações de Inteligência Artificial (IA), Machine Learning (ML) e Computação de Alta Performance (HPC). O EFA permite atingir a performance da aplicação de um cluster cluster de IA/ML ou HPC on-premises, com a escalabilidade, a flexibilidade e a elasticidade fornecidas pela Nuvem AWS.

O EFA fornece latência mais baixa e mais consistente e maior throughput que o transporte de TCP tradicionalmente usado em sistemas HPC baseados em nuvem. Esse recurso aprimora a performance da comunicação entre instâncias, que é essencial para o dimensionamento de aplicações de IA/ML e HPC. Ele é otimizado para funcionar na infraestrutura de rede da AWS existente e pode ser dimensionado dependendo dos requisitos da aplicação.

O EFA é integrado à Libfabric 1.7.0 e posteriores, é compatível com a Nvidia Collective Communications Library (NCCL) para aplicações de IA e ML, com a Open MPI 4.1 e posteriores, e com a Intel MPI 2019 Update 5 e posteriores para aplicações de HPC.

O EFA oferece suporte para gravação com tecnologia RDMA (Remote Direct Memory Access) na maioria dos tipos de instância compatíveis com a versão 4 ou com versões posteriores do Nitro. A

leitura com tecnologia RDMA é compatível com todas as instâncias com a versão 4 ou com versões posteriores do Nitro. Para obter mais informações, consulte Tipos de instâncias compatíveis.

Conteúdo

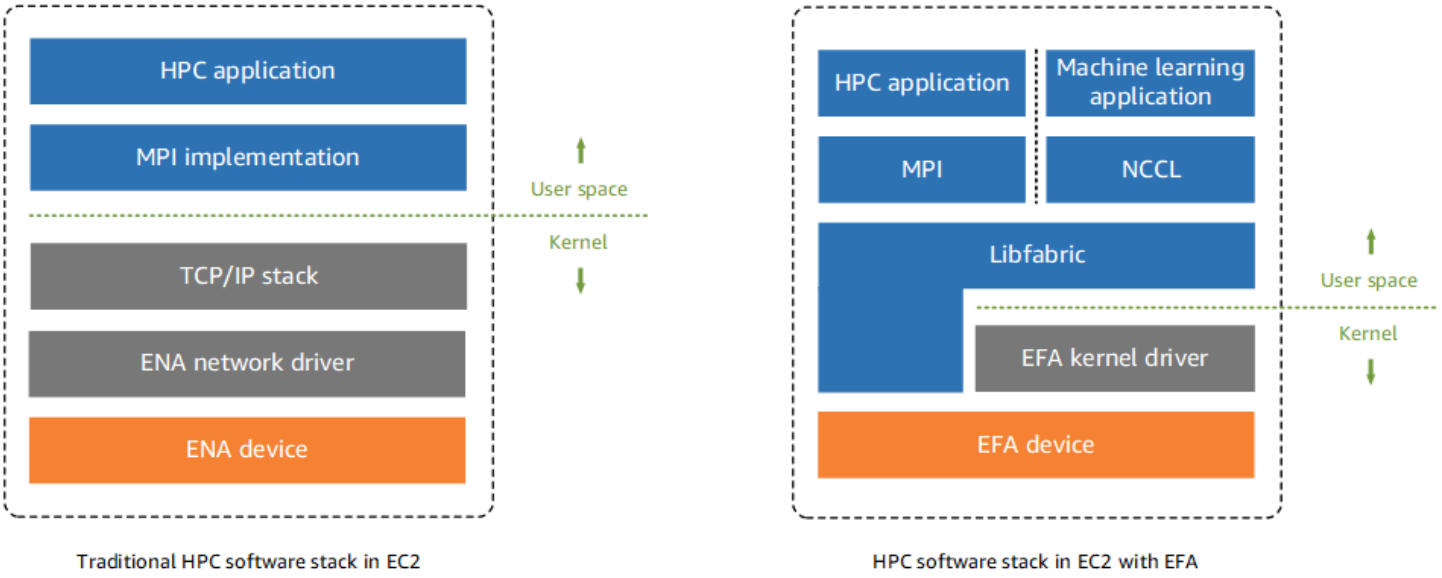
- Conceitos básicos de EFA
- Interfaces e bibliotecas compatíveis
- Tipos de instâncias compatíveis
- Sistemas operacionais compatíveis
- Limitações de EFA
- Preços do EFA
- Conceitos básicos do EFA e MPI para workloads de HPC no Amazon EC2
- Conceitos básicos do EFA e NCCL para workloads de ML no Amazon EC2
- Maximize a largura de banda da rede em instâncias do Amazon EC2 com várias placas de rede
- Criar e anexar um Elastic Fabric Adapter a uma instância do Amazon EC2
- Desanexar e excluir um EFA de uma instância do Amazon EC2
- Monitorar um Elastic Fabric Adapter no Amazon EC2
- Verificar o instalador EFA usando uma soma de verificação
- Observações sobre o Elastic Fabric Adapter

Conceitos básicos de EFA

Um dispositivo EFA pode ser conectado a uma instância EC2 de duas formas:

1. Usando uma interface EFA tradicional, também chamada de EFA com ENA, que cria um dispositivo EFA e um dispositivo ENA.
2. Usando uma interface exclusiva do EFA, que cria apenas o dispositivo do EFA.

O dispositivo EFA fornece recursos como desvio de sistema operacional integrado e controle de congestionamento mediante o protocolo Scalable Reliable Datagram (SRD). Os atributos do dispositivo EFA permitem uma funcionalidade de transporte confiável e de baixa latência que permite que a interface EFA forneça melhor performance de aplicações de HPC e ML no Amazon EC2. Já o dispositivo ENA oferece uma rede IP tradicional.



Tradicionalmente, as aplicações de IA/ML usam NCCL e as aplicações de HPC usam a Message Passing Interface (MPI) para estabelecer a interface com o transporte de rede do sistema. Na Nuvem AWS, isso significa que as aplicações fazem interface com NCCL ou MPI, que usa a pilha TCP/IP do sistema operacional e o driver de dispositivo ENA para habilitar a comunicação de rede entre as instâncias.

Com uma interface tradicional EFA (EFA com ENA) ou somente EFA, as aplicações de IA/ML usam NCCL e as aplicações de HPC usam MPI, para interagir diretamente com a API Libfabric. A API Libfabric ignora o kernel do sistema operacional e se comunica diretamente com o dispositivo EFA para colocar pacotes na rede. Isso reduz a sobrecarga e permite que as aplicações de IA/ML e HPC sejam executadas com mais eficiência.

> **Note**
>
> O Libfabric é um componente central do framework OpenFabrics Interfaces (OFI), que define e exporta a API do espaço do usuário do OFI. Para obter mais informações, consulte o site Libfabric OpenFabrics.

Diferenças entre as interfaces de rede ENA, EFA e somente EFA

O Amazon EC2 fornece dois tipos de interfaces de rede:

- As interfaces ENA fornecem todos os atributos tradicionais de rede IP e roteamento necessários para oferecer suporte à rede IP para uma VPC. Para mais informações, consulte Habilitar redes aperfeiçoadas com o ENA em instâncias do EC2.
- As interfaces EFA (EFA com ENA) fornecem o dispositivo ENA para rede IP e o dispositivo EFA para comunicação de baixa latência e alto throughput.
- As interfaces exclusivamente EFA são compatíveis apenas com os recursos do dispositivo EFA, sem o dispositivo ENA para redes IP tradicionais.

A tabela a seguir apresenta uma comparação das interfaces de rede ENA, EFA e exclusivamente EFA.

	ENA	EFA (EFA com ENA)	Exclusivamente EFA
Compatível com a funcionalidade de rede IP	Sim	Sim	Não
Podem ser atribuídos endereços IPv4 ou IPv6	Sim	Sim	Não
Pode ser usado como interface de rede primária, por exemplo	Sim	Sim	Não
Conta para o limite de anexos de ENI da instância	Sim	Sim	Sim

	ENA	EFA (EFA com ENA)	Exclusiva mente EFA
Compatível com o tipo de instância	Compatível com todos os tipos de instâncias baseadas em Nitro	Tipos de instâncias compatíveis	Tipos de instâncias compatíveis
Nomeação de parâmetro nas APIs do EC2	`interface`	`efa`	`efa-only`
Nomeação de campo no console do EC2	Nenhuma seleção	EFA com ENA	Exclusiva mente EFA

Interfaces e bibliotecas compatíveis

Os EFAs oferecem suporte às seguintes interfaces e bibliotecas:

- Open MPI 4.1 e posteriores
- Intel MPI 2019 Update 5 e posteriores
- NVIDIA Collective Communications Library (NCCL) 2.4.2 e posterior
- AWS Neuron SDK versão 2.3 e posterior

Tipos de instâncias compatíveis

Todos os tipos de instância a seguir oferecem suporte para EFA. Além disso, as tabelas indicam o suporte a leitura e gravação RDMA para os tipos de instâncias.

Nitro v6

Tipo de instância	Suporte para a leitura com tecnologia RDMA	Suporte para a gravação com tecnologia RDMA
Finalidade geral		
m8a.48xlarge	Yes	Yes
m8a.metal-48xl	Yes	Yes
m8azn.24xlarge	Yes	Yes
m8azn.metal-24xl	Yes	Yes
m8gb.16xlarge	Yes	Yes
m8gb.24xlarge	Yes	Yes
m8gb.48xlarge	Yes	Yes
m8gn.16xlarge	Yes	Yes
m8gn.24xlarge	Yes	Yes
m8gn.48xlarge	Yes	Yes
m8i.48xlarge	Yes	Yes
m8i.96xlarge	Yes	Yes
m8i.metal-48xl	Yes	Yes
m8i.metal-96xl	Yes	Yes
m8id.48xlarge	Yes	Yes
m8id.96xlarge	Yes	Yes
m8id.metal-48xl	Yes	Yes
m8id.metal-96xl	Yes	Yes

Tipo de instância	Suporte para a leitura com tecnologia RDMA	Suporte para a gravação com tecnologia RDMA
Otimizadas para computação		
c8a.48xlarge	Yes	Yes
c8a.metal-48xl	Yes	Yes
c8gb.16xlarge	Yes	Yes
c8gb.24xlarge	Yes	Yes
c8gb.48xlarge	Yes	Yes
c8gb.metal-24xl	Yes	Yes
c8gb.metal-48xl	Yes	Yes
c8gn.16xlarge	Yes	Yes
c8gn.24xlarge	Yes	Yes
c8gn.48xlarge	Yes	Yes
c8gn.metal-24xl	Yes	Yes
c8gn.metal-48xl	Yes	Yes
c8i.48xlarge	Yes	Yes
c8i.96xlarge	Yes	Yes
c8i.metal-48xl	Yes	Yes
c8i.metal-96xl	Yes	Yes
c8id.48xlarge	Yes	Yes
c8id.96xlarge	Yes	Yes
c8id.metal-48xl	Yes	Yes

Tipo de instância	Suporte para a leitura com tecnologia RDMA	Suporte para a gravação com tecnologia RDMA
c8id.metal-96xl	Yes	Yes
Otimizadas para memória		
r8a.48xlarge	Yes	Yes
r8a.metal-48xl	Yes	Yes
r8gb.16xlarge	Yes	Yes
r8gb.24xlarge	Yes	Yes
r8gb.48xlarge	Yes	Yes
r8gb.metal-24xl	Yes	Yes
r8gb.metal-48xl	Yes	Yes
r8gn.16xlarge	Yes	Yes
r8gn.24xlarge	Yes	Yes
r8gn.48xlarge	Yes	Yes
r8gn.metal-24xl	Yes	Yes
r8gn.metal-48xl	Yes	Yes
r8i.48xlarge	Yes	Yes
r8i.96xlarge	Yes	Yes
r8i.metal-48xl	Yes	Yes
r8i.metal-96xl	Yes	Yes
r8id.48xlarge	Yes	Yes
r8id.96xlarge	Yes	Yes

Tipo de instância	Suporte para a leitura com tecnologia RDMA	Suporte para a gravação com tecnologia RDMA
r8id.metal-48xl	Yes	Yes
r8id.metal-96xl	Yes	Yes
x8aedz.24xlarge	Yes	Yes
x8aedz.metal-24xl	Yes	Yes
x8i.48xlarge	Yes	Yes
x8i.64xlarge	Yes	Yes
x8i.96xlarge	Yes	Yes
x8i.metal-48xl	Yes	Yes
x8i.metal-96xl	Yes	Yes
Otimizada para armazenamento		
i8ge.48xlarge	Yes	No
i8ge.metal-48xl	Yes	No
Computação acelerada		
g7e.8xlarge	Yes	Yes
g7e.12xlarge	Yes	Yes
g7e.24xlarge	Yes	Yes
g7e.48xlarge	Yes	Yes
p6-b200.48xlarge	Yes	Yes
p6-b300.48xlarge	Yes	Yes
Computação de alta performance		

Tipo de instância	Suporte para a leitura com tecnologia RDMA	Suporte para a gravação com tecnologia RDMA
hpc8a.96xlarge	Yes	Yes

Nitro v5

Tipo de instância	Suporte para a leitura com tecnologia RDMA	Suporte para a gravação com tecnologia RDMA
Finalidade geral		
m8g.24xlarge	Yes	No
m8g.48xlarge	Yes	No
m8g.metal-24xl	Yes	No
m8g.metal-48xl	Yes	No
m8gd.24xlarge	No	No
m8gd.48xlarge	No	No
m8gd.metal-24xl	No	No
m8gd.metal-48xl	No	No
Otimizadas para computação		
c7gn.16xlarge	Yes	No
c7gn.metal	Yes	No
c8g.24xlarge	Yes	No
c8g.48xlarge	Yes	No
c8g.metal-24xl	Yes	No
c8g.metal-48xl	Yes	No

Tipo de instância	Suporte para a leitura com tecnologia RDMA	Suporte para a gravação com tecnologia RDMA
c8gd.24xlarge	No	No
c8gd.48xlarge	No	No
c8gd.metal-24xl	No	No
c8gd.metal-48xl	No	No
Otimizadas para memória		
r8g.24xlarge	No	No
r8g.48xlarge	No	No
r8g.metal-24xl	No	No
r8g.metal-48xl	No	No
r8gd.24xlarge	No	No
r8gd.48xlarge	No	No
r8gd.metal-24xl	No	No
r8gd.metal-48xl	No	No
x8g.24xlarge	No	No
x8g.48xlarge	No	No
x8g.metal-24xl	No	No
x8g.metal-48xl	No	No
Otimizada para armazenamento		
i7ie.48xlarge	Yes	No
i7ie.metal-48xl	Yes	No

Tipo de instância	Suporte para a leitura com tecnologia RDMA	Suporte para a gravação com tecnologia RDMA
i8g.48xlarge	No	No
Computação acelerada		
p5en.48xlarge	Yes	Yes
p6e-gb200.36xlarge	Yes	Yes
trn2.3xlarge	Yes	Yes
trn2.48xlarge	Yes	Yes
trn2u.48xlarge	Yes	Yes
Computação de alta performance		
hpc7g.4xlarge	Yes	No
hpc7g.8xlarge	Yes	No
hpc7g.16xlarge	Yes	No

Nitro v4

Tipo de instância	Suporte para a leitura com tecnologia RDMA	Suporte para a gravação com tecnologia RDMA
Finalidade geral		
m6a.48xlarge	Yes	Yes
m6a.metal	Yes	Yes
m6i.32xlarge	Yes	Yes
m6i.metal	Yes	Yes
m6id.32xlarge	Yes	Yes

Tipo de instância	Suporte para a leitura com tecnologia RDMA	Suporte para a gravação com tecnologia RDMA
m6id.metal	Yes	Yes
m6idn.32xlarge	Yes	Yes
m6idn.metal	Yes	Yes
m6in.32xlarge	Yes	Yes
m6in.metal	Yes	Yes
m7a.48xlarge	Yes	No
m7a.metal-48xl	Yes	No
m7g.16xlarge	Yes	No
m7g.metal	Yes	No
m7gd.16xlarge	Yes	No
m7gd.metal	Yes	No
m7i.48xlarge	Yes	No
m7i.metal-48xl	Yes	No
Otimizadas para computação		
c6a.48xlarge	Yes	Yes
c6a.metal	Yes	Yes
c6gn.16xlarge	Yes	Yes
c6i.32xlarge	Yes	Yes
c6i.metal	Yes	Yes
c6id.32xlarge	Yes	Yes

Tipo de instância	Suporte para a leitura com tecnologia RDMA	Suporte para a gravação com tecnologia RDMA
c6id.metal	Yes	Yes
c6in.32xlarge	Yes	Yes
c6in.metal	Yes	Yes
c7a.48xlarge	Yes	No
c7a.metal-48xl	Yes	No
c7g.16xlarge	Yes	Yes
c7g.metal	Yes	Yes
c7gd.16xlarge	Yes	No
c7gd.metal	Yes	No
c7i.48xlarge	Yes	No
c7i.metal-48xl	Yes	No
Otimizadas para memória		
r6a.48xlarge	Yes	Yes
r6a.metal	Yes	Yes
r6i.32xlarge	Yes	Yes
r6i.metal	Yes	Yes
r6id.32xlarge	Yes	Yes
r6id.metal	Yes	Yes
r6idn.32xlarge	Yes	Yes
r6idn.metal	Yes	Yes

Tipo de instância	Suporte para a leitura com tecnologia RDMA	Suporte para a gravação com tecnologia RDMA
r6in.32xlarge	Yes	Yes
r6in.metal	Yes	Yes
r7a.48xlarge	No	No
r7a.metal-48xl	No	No
r7g.16xlarge	No	No
r7g.metal	No	No
r7gd.16xlarge	No	No
r7gd.metal	No	No
r7i.48xlarge	No	No
r7i.metal-48xl	No	No
r7iz.32xlarge	No	No
r7iz.metal-32xl	No	No
u7i-6tb.112xlarge	Yes	Yes
u7i-8tb.112xlarge	Yes	Yes
u7i-12tb.224xlarge	Yes	Yes
u7in-16tb.224xlarge	Yes	Yes
u7in-24tb.224xlarge	Yes	Yes
u7in-32tb.224xlarge	Yes	Yes
u7inh-32tb.480xlarge	Yes	Yes
x2idn.32xlarge	Yes	Yes

Tipo de instância	Suporte para a leitura com tecnologia RDMA	Suporte para a gravação com tecnologia RDMA
x2idn.metal	Yes	Yes
x2iedn.32xlarge	Yes	Yes
x2iedn.metal	Yes	Yes
Otimizada para armazenamento		
i4g.16xlarge	Yes	Yes
i4i.32xlarge	Yes	Yes
i4i.metal	Yes	Yes
i7i.24xlarge	Yes	No
i7i.48xlarge	Yes	No
i7i.metal-48xl	Yes	No
im4gn.16xlarge	Yes	Yes
Computação acelerada		
f2.48xlarge	Yes	Yes
g6.8xlarge	Yes	Yes
g6.12xlarge	Yes	Yes
g6.16xlarge	Yes	Yes
g6.24xlarge	Yes	Yes
g6.48xlarge	Yes	Yes
g6e.8xlarge	Yes	Yes
g6e.12xlarge	Yes	Yes

Tipo de instância	Suporte para a leitura com tecnologia RDMA	Suporte para a gravação com tecnologia RDMA
g6e.16xlarge	Yes	Yes
g6e.24xlarge	Yes	Yes
g6e.48xlarge	Yes	Yes
gr6.8xlarge	Yes	Yes
p5.4xlarge	Yes	Yes
p5.48xlarge	Yes	Yes
p5e.48xlarge	Yes	Yes
trn1.32xlarge	Yes	Yes
trn1n.32xlarge	Yes	Yes
Computação de alta performance		
hpc6a.48xlarge	Yes	Yes
hpc6id.32xlarge	Yes	Yes
hpc7a.12xlarge	Yes	No
hpc7a.24xlarge	Yes	No
hpc7a.48xlarge	Yes	No
hpc7a.96xlarge	Yes	No

Nitro v3

Tipo de instância	Suporte para a leitura com tecnologia RDMA	Suporte para a gravação com tecnologia RDMA
Finalidade geral		

Tipo de instância	Suporte para a leitura com tecnologia RDMA	Suporte para a gravação com tecnologia RDMA
m5dn.24xlarge	No	No
m5dn.metal	No	No
m5n.24xlarge	No	No
m5n.metal	No	No
m5zn.12xlarge	No	No
m5zn.metal	No	No
Otimizadas para computação		
c5n.9xlarge	No	No
c5n.18xlarge	No	No
c5n.metal	No	No
Otimizadas para memória		
r5dn.24xlarge	No	No
r5dn.metal	No	No
r5n.24xlarge	No	No
r5n.metal	No	No
x2iezn.12xlarge	No	No
x2iezn.metal	No	No
Otimizada para armazenamento		
i3en.12xlarge	No	No
i3en.24xlarge	No	No

Tipo de instância	Suporte para a leitura com tecnologia RDMA	Suporte para a gravação com tecnologia RDMA
i3en.metal	No	No
Computação acelerada		
dl1.24xlarge	Yes	No
dl2q.24xlarge	No	No
g4dn.8xlarge	No	No
g4dn.12xlarge	No	No
g4dn.16xlarge	No	No
g4dn.metal	No	No
g5.8xlarge	No	No
g5.12xlarge	No	No
g5.16xlarge	No	No
g5.24xlarge	No	No
g5.48xlarge	No	No
inf1.24xlarge	No	No
p3dn.24xlarge	No	No
p4d.24xlarge	Yes	No
p4de.24xlarge	Yes	No
vt1.24xlarge	No	No
Geração anterior		
p3dn.24xlarge	No	No

Para ver os tipos de instância disponíveis com suporte a EFAs em uma região específica

Os tipos de instância disponíveis variam de acordo com a região. Para ver os tipos de instâncias disponíveis com suporte a EFAs em uma região, use o comando describe-instance-types com o parâmetro `--region`. Inclua o parâmetro `--filters` para definir o escopo dos resultados para os tipos de instância com suporte a EFA e o parâmetro `--query` para definir o escopo da saída para o valor de `InstanceType`.

```
aws ec2 describe-instance-types \
    --region us-east-1  \
    --filters Name=network-info.efa-supported,Values=true \
    --query "InstanceTypes[*].[InstanceType]"  \
    --output text | sort
```

Sistemas operacionais compatíveis

O suporte ao sistema operacional varia dependendo do tipo de processador. A tabela a seguir mostra os sistemas operacionais compatíveis.

Sistema operacional	Tipos de instância Intel/AMD (**x86_64**)	Tipos de instância AWS Graviton (**arm64**)
Amazon Linux 2023	✓	✓
Amazon Linux 2	✓	✓
RHEL 8 e 9	✓	✓
Debian 11, 12 e 13	✓	✓
Rocky Linux 8 e 9	✓	✓
Ubuntu 22.04 e 24.04	✓	✓

Sistema operacional	Tipos de instância Intel/AMD (**x86_64**)	Tipos de instância AWS Graviton (**arm64**)
SUSE Linux Enterprise 15 SP2 e posterior	✓	✓
OpenSUSE Leap 15.5 e posterior	✓	

> **Note**
>
> Alguns dos sistemas operacionais listados podem não ser compatíveis com a Intel MPI. Se você estiver usando a Intel MPI, consulte a documentação da Intel MPI para verificar a compatibilidade com seu sistema operacional.

Limitações de EFA

Os EFAs têm as seguintes limitações:

- A gravação com a tecnologia RDMA não é compatível com todos os tipos de instância. Para obter mais informações, consulte Tipos de instâncias compatíveis.
- Atualmente, o tráfego[1] EFA entre instâncias P4d/P4de/DL1 e outros tipos de instância não é compatível.
- Os tipos de instância compatíveis com várias placas de rede podem ser configurados com um EFA por placa de rede. Todos os outros tipos de instância compatíveis oferecem suporte a apenas um EFA por instância.
- Instâncias dedicadas `c7g.16xlarge`, `m7g.16xlarge` e `r7g.16xlarge` e hosts dedicados não são compatíveis quando um EFA está anexado.
- O tráfego[1] EFA não pode cruzar zonas de disponibilidade ou VPCs. Isso não se aplica ao tráfego IP normal do dispositivo ENA de uma interface EFA.
- O tráfego[1] EFA não é roteável. O tráfego IP normal do dispositivo ENA de uma interface EFA permanece roteável.
- EFA não é compatível com o AWS Outposts.

- O dispositivo EFA de uma interface EFA (EFA com ENA) é compatível com instâncias do Windows somente para aplicações AWS Cloud Digital Interface baseadas no Kit de Desenvolvimento de Software (AWS CDI SDK). Ao anexar uma interface EFA (EFA com ENA) a uma instância do Windows para aplicações não baseadas no SDK do CDI, ela funcionará como uma interface ENA, sem os recursos adicionais do dispositivo EFA. A interface exclusiva do EFA não é compatível com aplicações AWS CDI baseadas em Windows ou Linux. Para obter mais informações, consulte o Guia do Usuário do AWS Cloud Digital Interface Kit de Desenvolvimento de Software (AWS CDI SDK).

[1] O tráfego EFA se refere ao tráfego transmitido pelo dispositivo EFA de uma interface EFA (EFA com ENA) ou exclusivamente EFA.

Preços do EFA

O EFA está disponível como um recurso de rede opcional do Amazon EC2 que pode ser habilitado em qualquer instância compatível sem nenhum custo adicional.

Conceitos básicos do EFA e MPI para workloads de HPC no Amazon EC2

Este tutorial ajuda a executar um cluster de instância habilitado para MPI e EFA para workloads de HPC.

> **Note**
>
> As instâncias `u7i-12tb.224xlarge`, `u7in-16tb.224xlarge`, `u7in-24tb.224xlarge` e `u7in-32tb.224xlarge` podem executar até 128 processos MPI paralelos com o Open MPI ou até 256 processos MPI paralelos com o Intel MPI.

Tarefas

- Etapa 1: Preparar um grupo de segurança habilitado para EFA
- Etapa 2: Iniciar uma instância temporária
- Etapa 3: Instalar o software EFA
- Etapa 4: (opcional) habilitar o Open MPI 5
- Etapa 5: (opcional) instalar o Intel MPI
- Etapa 6: desabilitar a proteção ptrace
- Etapa 7. Confirmar instalação

- Etapa 8: instalar a aplicação de HPC
- Etapa 9: criar uma AMI habilitada para EFA
- Etapa 10: executar instâncias habilitadas para EFA em um grupo de posicionamento de cluster
- Etapa 11: Encerrar a instância temporária
- Etapa 12: habilitar SSH sem senha

Etapa 1: Preparar um grupo de segurança habilitado para EFA

Um EFA requer um grupo de segurança que permita todo o tráfego de entrada e saída do grupo de segurança e para ele próprio. O procedimento a seguir cria um grupo de segurança que permite todo o tráfego de entrada e saída de e para si mesmo e que permite tráfego SSH de entrada de qualquer endereço IPv4 para conectividade SSH.

> **Important**
>
> Esse grupo de segurança deve ser usado apenas para fins de teste. Para seus ambientes de produção, recomendamos que você crie uma regra SSH de entrada que permita o tráfego somente do endereço IP do qual você está se conectando, como o endereço IP do seu computador ou uma variedade de endereços IP na sua rede local.

Para outros cenários, consulte Regras de grupo de segurança para diferentes casos de uso.

Para criar um grupo de segurança habilitado para EFA

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Security Groups (Grupos de segurança) e, em seguida, Create Security Group (Criar grupo de segurança).
3. Na janela Security group (Grupo de segurança), faça o seguinte:
   a. Em Security group name (Nome do grupo de segurança), insira um nome descritivo para o grupo de segurança, como `EFA-enabled security group`.
   b. (Opcional) Em Description (Descrição), insira uma breve descrição do grupo de segurança.
   c. Em VPC, selecione a VPC na qual você pretende executar suas instâncias habilitadas para EFA.
   d. Escolha Criar grupo de segurança.

4. Selecione o grupo de segurança que você criou e, na guia Details (Detalhes), copie o Security group (Grupo de segurança).
5. Com o grupo de segurança ainda selecionado, escolha Actions (Ações), Edit inbound rules (Editar regras de entrada), e faça o seguinte:
   a. Escolha Adicionar regra.
   b. Para Tipo, escolha Todo o tráfego.
   c. Para Source type (Tipo de origem), escolha Custom (Personalizado) e cole o ID do grupo de segurança que você copiou no campo.
   d. Escolha Adicionar regra.
   e. Para Tipo, escolha SSH.
   f. Para Source type (Tipo de origem), escolha Anywhere-IPv4 (IPv4 em qualquer lugar).
   g. Selecione Salvar regras.
6. Na lista, selecione o grupo de segurança e escolha Actions (Ações), Edit outbound rules (Editar regras de saída), e faça o seguinte:
   a. Escolha Adicionar regra.
   b. Para Tipo, escolha Todo o tráfego.
   c. Para Destination (Destino), escolha Custom (Personalizado) e cole o ID do grupo de segurança que você copiou no campo.
   d. Selecione Salvar regras.

Etapa 2: Iniciar uma instância temporária

Execute uma instância temporária que é possível usar para instalar e configurar os componentes do software EFA. Você usa essa instância para criar um AMI habilitado para EFA a partir do qual é possível executar suas instâncias habilitadas para EFA.

Para executar uma instância temporária

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Instances (Instâncias) e, depois, escolha Launch Instances (Iniciar instâncias) para abrir o novo assistente de inicialização de instância.

3. (Opcional) Na seção Name and tags (Nome e etiquetas), forneça um nome para a instância, como `EFA-instance`. O nome é atribuído à instância como uma etiqueta de recurso (`Name=`*`EFA-instance`*).
4. Na seção Application and OS Images (Imagens de aplicação e sistema operacional), selecione uma AMI para um dos sistemas operacionais compatíveis.
5. Na seção Instance type (Tipo de instância), selecione um tipo de instância compatível.
6. Na seção Key pair (Par de chaves), selecione o par de chaves a ser usado na instância.
7. Na seção Network settings (Configurações da rede), escolha Edit (Editar) e faça o seguinte:

   a. Em Subnet (Sub-rede), escolha a sub-rede na qual deseja iniciar a instância. Se você não selecionar uma sub-rede, não será possível habilitar a instância para o EFA.

   b. Para Firewall (security groups) (Firewall/grupos de segurança), escolha Select existing security group (Selecione grupo de segurança existente) e, em seguida, selecione o grupo de segurança que você criou na etapa anterior.

   c. Expanda a seção Configuração de rede avançada.

      Para Interface de rede 1, selecione Índice da placa de rede = 0, Índice do dispositivo = 0 e Tipo de interface = EFA com ENA.

      (Opcional) Caso esteja usando um tipo de instância com várias placas, como `p4d.24xlarge` ou `p5.48xlarge`, para cada interface de rede adicional necessária, selecione Adicionar interface de rede, em Índice da placa de rede selecione o próximo índice não utilizado e, em seguida, selecione Índice do dispositivo = 1 e Tipo de interface = EFA com ENA ou exclusivamente EFA.
8. Na seção Storage (Armazenamento), configure os volumes conforme necessário.
9. No painel Summary (Resumo) painel, escolha Launch instance (Iniciar instância).

> **Note**
>
> Considere exigir o uso do IMDSv2 para a instância temporária, bem como para a AMI que você criará na Etapa 9, a menos que já tenha definido o IMDSv2 como padrão para a conta. Para obter mais informações sobre as etapas da configuração do IMDSv2, consulte Configurar opções de metadados da instância para novas instâncias.

Etapa 3: Instalar o software EFA

Instale o kernel habilitado para EFA, drivers EFA, Libfabric e pilha Open MPI que é necessário para oferecer compatibilidade com EFA em sua instância temporária.

As etapas diferem dependendo de como você planeja usar o EFA com Open MPI, com Intel MPI ou com Open MPI e Intel MPI.

> **Note**
>
> Alguns dos sistemas operacionais podem não ser compatíveis com a Intel MPI. Se você estiver usando a Intel MPI, consulte a documentação da Intel MPI para verificar a compatibilidade com seu sistema operacional.

Como instalar o software EFA

1. Conecte à instância que você iniciou. Para obter mais informações, consulte Conectar-se à instância do Linux usando SSH.
2. Para garantir que todos os pacotes de software estejam atualizados, execute uma atualização rápida de software em sua instância. esse processo pode demorar alguns minutos.
   - Amazon Linux 2023, Amazon Linux 2, RHEL 8/9, Rocky Linux 8/9

     ```
     $ sudo yum update -y
     ```

   - Ubuntu e Debian

     ```
     $ sudo apt-get update && sudo apt-get upgrade -y
     ```

   - SUSE Linux Enterprise

     ```
     $ sudo zypper update -y
     ```

3. Reinicialize a instância e reconecte-se a ela.
4. Faça download dos arquivos de instalação do software do EFA. Os arquivos de instalação do software são empacotados em um arquivo compactado tarball (`.tar.gz`). Para fazer download da última versão estável, use o seguinte comando:

Também é possível obter a versão mais recente substituindo o número da versão por `latest` no comando acima.

```
$ curl -O https://efa-installer.amazonaws.com/aws-efa-installer-1.47.0.tar.gz
```

5. (Opcional) Verifique a autenticidade e a integridade do arquivo do EFA tarball (`.tar.gz`).

   Recomendamos que você faça isso para verificar a identidade do fornecedor do software e para verificar se a aplicação não foi alterada ou corrompida desde que foi publicada. Se você não deseja verificar o arquivo tarball, ignore esta etapa.

   > **Note**
   >
   > Como alternativa, se você preferir verificar o arquivo tarball usando uma soma de verificação MD5 ou SHA256, consulte Verificar o instalador EFA usando uma soma de verificação.

   a. Faça download da chave GPG pública e importe-a para seu pen-drive.

   ```
   $ wget https://efa-installer.amazonaws.com/aws-efa-installer.key && gpg --
   import aws-efa-installer.key
   ```

   O comando deve retornar um valor de chave. Anote o valor da chave, pois ele será necessário na próxima etapa.

   b. Verifique a impressão digital da chave GPG. Execute o seguinte comando e especifique o valor de chave da etapa anterior.

   ```
   $ gpg --fingerprint key_value
   ```

   O comando deve retornar uma impressão digital idêntica a `4E90 91BC BB97 A96B 26B1 5E59 A054 80B1 DD2D 3CCC`. Se a impressão digital não corresponder, não execute o script de instalação do EFA e entre em contato com o Suporte.

   c. Faça download do arquivo de assinatura e verifique a assinatura do arquivo tarball EFA.

   ```
   $ wget https://efa-installer.amazonaws.com/aws-efa-installer-1.47.0.tar.gz.sig
    && gpg --verify ./aws-efa-installer-1.47.0.tar.gz.sig
   ```

Veja a seguir um exemplo de saída.

```
gpg: Signature made Wed 29 Jul 2020 12:50:13 AM UTC using RSA key ID DD2D3CCC
gpg: Good signature from "Amazon EC2 EFA <ec2-efa-maintainers@amazon.com>"
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the owner.
Primary key fingerprint: 4E90 91BC BB97 A96B 26B1  5E59 A054 80B1 DD2D 3CCC
```

Se o resultado incluir `Good signature` e a impressão digital corresponder à impressão digital retornada na etapa anterior, passe para a próxima etapa. Caso contrário, não execute o script de instalação do EFA e entre em contato com o Suporte.

6. Extraia os arquivos do arquivo compactado `.tar.gz` e navegue para o diretório extraído.

```
$ tar -xf aws-efa-installer-1.47.0.tar.gz && cd aws-efa-installer
```

7. Instale o software EFA. Dependendo de seu caso de uso, faça o seguinte.

> **Note**
>
> O EFA não oferece suporte ao NVIDIA GPUDirect com o SUSE Linux. Caso esteja usando SUSE Linux, você deverá especificar também a opção `--skip-kmod` para impedir a instalação do kmod. Por padrão, o SUSE Linux não permite módulos fora da árvore do kernel.

Open MPI and Intel MPI

Se planeja usar o EFA com Open MPI e Intel MPI, é necessário instalar o software EFA com Libfabric e Open MPI e concluir a Etapa 5: instalar o Intel MPI.

Para instalar o software EFA com Libfabric e Open MPI, execute o comando a seguir.

> **Note**
>
> A partir do EFA 1.30.0, tanto a Open MPI 4.1 quanto a Open MPI 5 são instaladas por padrão. Opcionalmente, você pode especificar a versão do Open MPI que deseja instalar. Para instalar apenas a Open MPI 4.1, inclua `--mpi=openmpi4`. Para

instalar somente o Open MPI 5, inclua `--mpi=openmpi5`. Para instalar os dois, omita a opção `--mpi`.

```
$ sudo ./efa_installer.sh -y
```

O Libfabric está instalado em `/opt/amazon/efa`. A Open MPI 4.1 é instalada em `/opt/amazon/openmpi`. O Open MPI 5 está instalado em `/opt/amazon/openmpi5`.

Open MPI only

Se planeja usar o EFA somente com Open MPI, é necessário instalar o software EFA com Libfabric e Open MPI, podendo ignorar a Etapa 5: instalar o Intel MPI. Para instalar o software EFA com Libfabric e Open MPI, execute o comando a seguir.

> **Note**
>
> A partir do EFA 1.30.0, tanto a Open MPI 4.1 quanto a Open MPI 5 são instaladas por padrão. Opcionalmente, você pode especificar a versão do Open MPI que deseja instalar. Para instalar apenas a Open MPI 4.1, inclua `--mpi=openmpi4`. Para instalar somente o Open MPI 5, inclua `--mpi=openmpi5`. Para instalar os dois, omita a opção `--mpi`.

```
$ sudo ./efa_installer.sh -y
```

O Libfabric está instalado em `/opt/amazon/efa`. A Open MPI 4.1 é instalada em `/opt/amazon/openmpi`. O Open MPI 5 está instalado em `/opt/amazon/openmpi5`.

Intel MPI only

Se você pretende usar o EFA somente com Intel MPI, instale o software EFA sem Libfabric e Open MPI. Nesse caso, o Intel MPI usa o Libfabric incorporado. Se você optar por fazer isso, deverá concluir a Etapa 5: instalar o Intel MPI.

Para instalar o software EFA sem Libfabric e Open MPI, execute o comando a seguir.

```
$ sudo ./efa_installer.sh -y --minimal
```

8. Se o instalador do EFA solicitar que você reinicialize a instância, faça-o e, em seguida, reconecte-se à instância. Caso contrário, faça logout da instância e faça login novamente para concluir a instalação.
9. Exclua o tarball descompactado e o tarball propriamente dito. Caso contrário, eles serão incluídos na AMI habilitada para EFA criada, aumentando seu tamanho.

Etapa 4: (opcional) habilitar o Open MPI 5

> **Note**
>
> Execute esta etapa somente se planeja usar o Open MPI 5.

A partir do EFA 1.30.0, tanto a Open MPI 4.1 quanto a Open MPI 5 são instaladas por padrão. Como alternativa, você pode escolher instalar apenas a Open MPI 4.1 ou a Open MPI 5.

Se você optou por instalar o Open MPI 5 na Etapa 3: instalar o software EFA e pretende usá-lo, execute as etapas a seguir para habilitá-lo.

Para habilitar o Open MPI 5

1. Adicione o Open MPI 5 à variável de ambiente PATH.

   ```
   $ module load openmpi5
   ```

2. Verifique se o Open MPI 5 está habilitado para uso.

   ```
   $ which mpicc
   ```

   O comando deve retornar o diretório de instalação do Open MPI 5: `/opt/amazon/openmpi5`.

3. (Opcional) Para garantir que o Open MPI 5 seja adicionado à variável de ambiente PATH sempre que a instância for iniciada, faça o seguinte:

   bash shell

   Adicione `module load openmpi5` a `/home/`*`username`*`/.bashrc` e `/home/`*`username`*`/.bash_profile`.

csh and tcsh shells

Adicione `module load openmpi5` a `/home/username/.cshrc`.

Se você precisar remover o Open MPI 5 da variável de ambiente PATH, execute o comando a seguir e remova o comando dos scripts de inicialização do shell.

```
$ module unload openmpi5
```

Etapa 5: (opcional) instalar o Intel MPI

> **Important**
>
> Execute esta etapa se planejar usar a Intel MPI. Se você planejar usa apenas Open MPI, ignore esta etapa.

A Intel MPI exige uma instalação adicional e a configuração de uma variável de ambiente.

Pré-requisito

Verifique se o usuário que executa as etapas a seguir tem permissões de sudo.

Para instalar a Intel MPI

1. Para baixar o script de instalação do Intel MPI, faça o seguinte
   a. Visite o site da Intel.
   b. Na seção da página da Web Intel MPI Library (Biblioteca Intel MPI), escolha o link para o instalador Intel MPI Library for Linux (Biblioteca MPI Intel para Linux) Offline.
2. Execute o script de instalação que você baixou na etapa anterior.

   ```
   $ sudo bash installation_script_name.sh
   ```
3. No instalador, escolha Accept & install (Aceitar e instalar).
4. Leia o Intel Improvement Program (Programa de melhoria da Intel), escolha a opção apropriada e, em seguida, escolha Begin Installation (Começar a instalação).
5. Quando a instalação terminar, escolha Fechar.

6. Por padrão, o Intel MPI usa o Libfabric integrado (interno). É possível configurar o Intel MPI para usar o Libfabric que acompanha o instalador do EFA. Normalmente, o instalador do EFA acompanha uma versão mais recente do Libfabric que o Intel MPI. Em alguns casos, o Libfabric que acompanha o instalador do EFA tem mais performance do que o Intel MPI. Para configurar o Intel MPI para usar o Libfabric que acompanha o instalador do EFA, siga um destes procedimentos, conforme o shell.

   bash shells

   Adicione a instrução a seguir a /home/*username*/.bashrc e /home/*username*/.bash_profile.

   ```
   export I_MPI_OFI_LIBRARY_INTERNAL=0
   ```

   csh and tcsh shells

   Adicione a instrução a seguir a /home/*username*/.cshrc.

   ```
   setenv I_MPI_OFI_LIBRARY_INTERNAL 0
   ```

7. Adicione o comando source a seguir ao script shell para obter o script `vars.sh` do diretório de instalação para configurar o ambiente do compilador sempre que a instância for iniciada. Dependendo de seu shell, faça o seguinte.

   bash shells

   Adicione a instrução a seguir a /home/*username*/.bashrc e /home/*username*/.bash_profile.

   ```
   source /opt/intel/oneapi/mpi/latest/env/vars.sh
   ```

   csh and tcsh shells

   Adicione a instrução a seguir a /home/*username*/.cshrc.

   ```
   source /opt/intel/oneapi/mpi/latest/env/vars.csh
   ```

8. Por padrão, se o EFA não estiver disponível devido a uma configuração incorreta, o Intel MPI assumirá como padrão a pilha de rede TCP/IP, podendo resultar em uma performance mais

lenta da aplicação. É possível evitar isso definindo `I_MPI_OFI_PROVIDER` como `efa`. Isso fará com que o Intel MPI apresente o seguinte erro, se o EFA não estiver disponível:

```
Abort (XXXXXX) on node 0 (rank 0 in comm 0): Fatal error in PMPI_Init: OtherMPI
 error,
MPIR_Init_thread (XXX).......:
MPID_Init (XXXX).............:
MPIDI_OFI_mpi_init_hook (XXXX):
open_fabric (XXXX)...........:
find_provider (XXXX).........:
OFI fi_getinfo() failed (ofi_init.c:2684:find_provider:
```

Dependendo de seu shell, faça o seguinte.

bash shells

Adicione a instrução a seguir a /home/*username*/.bashrc e /home/*username*/.bash_profile.

```
export I_MPI_OFI_PROVIDER=efa
```

csh and tcsh shells

Adicione a instrução a seguir a /home/*username*/.cshrc.

```
setenv I_MPI_OFI_PROVIDER efa
```

9. Por padrão, o Intel MPI não imprime informações de depuração. É possível especificar diferentes níveis de detalhamento para controlar as informações de depuração. Os valores possíveis (organizados em ordem pela quantidade de detalhes que fornecem) são: `0` (padrão), `1`, `2`, `3`, `4`, `5`. O nível `1` e superiores imprimem `libfabric version` e `libfabric provider`. Use `libfabric version` para verificar se o Intel MPI está usando o Libfabric interno ou o Libfabric que acompanha o instalador do EFA. Se estiver usando o Libfabric interno, a versão terá o sufixo `impi`. Use `libfabric provider` para verificar se o Intel MPI está usando o EFA ou a rede TCP/IP. Se estiver usando o EFA, o valor será `efa`. Se estiver usando TCP/IP, o valor será `tcp;ofi_rxm`.

   Para habilitar as informações de depuração, siga um destes procedimentos, conforme seu shell.

bash shells

Adicione a instrução a seguir a /home/*username*/.bashrc e /home/*username*/.bash_profile.

```
export I_MPI_DEBUG=value
```

csh and tcsh shells

Adicione a instrução a seguir a /home/*username*/.cshrc.

```
setenv I_MPI_DEBUG value
```

10. Por padrão, o Intel MPI usa a memória compartilhada do sistema operacional (shm) para comunicação intranós e usa Libfabric (ofi) somente para comunicação entre nós. Em geral, essa configuração fornece a melhor performance. Porém, em alguns casos, a malha Intel MPI shm pode fazer com que certas aplicações travem por tempo indeterminado.

    Para resolver esse problema, você pode forçar o Intel MPI a usar o Libfabric para comunicação intranós e entre nós. Para isso, faça o seguinte, de acordo com seu shell.

    bash shells

    Adicione a instrução a seguir a /home/*username*/.bashrc e /home/*username*/.bash_profile.

    ```
    export I_MPI_FABRICS=ofi
    ```

    csh and tcsh shells

    Adicione a instrução a seguir a /home/*username*/.cshrc.

    ```
    setenv I_MPI_FABRICS ofi
    ```

> **Note**
>
> O provedor de Libfabric do EFA usa a memória compartilhada do sistema operacional para comunicação intranós. Isso significa que a configuração `I_MPI_FABRICS` em `ofi` fornece uma performance semelhante à configuração `shm:ofi`.

11. Saia da instância e faça login novamente.

Se você não usar mais a Intel MPI, remova as variáveis de ambiente dos scripts shell de startup.

Etapa 6: desabilitar a proteção ptrace

Para melhorar a performance da aplicação HPC, o Libfabric usa a memória local da instância para comunicações entre processos quando os processos estão sendo executados na mesma instância.

O recurso de memória compartilhada usa CMA (Cross Memory Attach), que não é compatível com a proteção ptrace. Se estiver usando uma distribuição Linux que tenha a proteção ptrace habilitada por padrão, como o Ubuntu, desabilite-a. Se a sua distribuição Linux não tiver a proteção ptrace habilitada por padrão, ignore esta etapa.

Como desabilitar a proteção ptrace

Execute um destes procedimentos:

- Para desabilitar temporariamente a proteção ptrace para fins de teste, execute o seguinte comando.

```
$ sudo sysctl -w kernel.yama.ptrace_scope=0
```

- Para desabilitar permanentemente a proteção ptrace, adicione `kernel.yama.ptrace_scope = 0` a `/etc/sysctl.d/10-ptrace.conf` e reinicialize a instância.

Etapa 7. Confirmar instalação

Confirmar uma instalação bem-sucedida

1. Para confirmar se a Intel MPI foi instalada com êxito, execute o seguinte comando:

```
$ which mpicc
```

- Para Open MPI, o caminho retornado deve incluir `/opt/amazon/`.
- Para Intel MPI, o caminho retornado deve incluir `/opt/intel/`. Se o resultado esperado não for exibido, verifique se o script `vars.sh` da Intel MPI foi usado como origem.

2. Para confirmar se os componentes de software EFA e o Libfabric foram instalados com êxito, execute o comando a seguir.

```
$ fi_info -p efa -t FI_EP_RDM
```

O comando deve retornar informações sobre as interfaces EFA Libfabric. O exemplo a seguir mostra a saída do comando.

```
provider: efa
    fabric: EFA-fe80::94:3dff:fe89:1b70
    domain: efa_0-rdm
    version: 2.0
    type: FI_EP_RDM
    protocol: FI_PROTO_EFA
```

Etapa 8: instalar a aplicação de HPC

Instale a aplicação HPC na instância temporária. O procedimento de instalação varia dependendo da aplicação HPC específica. Para obter mais informações, consulte Manage software on your AL2 instance no Amazon Linux 2 User Guide.

> **Note**
>
> Pode ser necessário consultar a documentação da aplicação de HPC para obter instruções de instalação.

Etapa 9: criar uma AMI habilitada para EFA

Depois de instalar os componentes de software necessários, crie uma AMI que possa ser reutilizada para executar suas instâncias habilitadas para o EFA.

Para criar uma AMI a partir de sua instância temporária

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância, escolha Actions (Ações), Image (Imagem), Create image (Criar imagem).
4. Em Create image (Criar imagem), faça o seguinte:
   a. Em Image name (Nome da imagem), insira um nome descritivo para a AMI.
   b. (Opcional) Em Image description (Descrição da imagem), informe a descrição do propósito da AMI.
   c. Escolha Create Image (Criar imagem).
5. No painel de navegação, selecione AMIs.
6. Encontre a AMI que você criou na lista. Aguarde até que o status mude de `pending` para `available` antes de continuar para a próxima etapa.

Etapa 10: executar instâncias habilitadas para EFA em um grupo de posicionamento de cluster

Execute as instâncias habilitadas para EFA em um placement group de cluster usando a AMI habilitada para EFA criada na Etapa 7 e o grupo de segurança habilitado para EFA criado na Etapa 1.

> **Note**
>
> - Não é um requisito absoluto executar suas instâncias habilitadas para EFA em um placement group de cluster. No entanto, recomendamos a execução de suas instâncias habilitadas para EFA em um grupo de posicionamento de cluster ao executar as instâncias em um grupo de baixa latência em uma única zona de disponibilidade.
> - Para garantir que a capacidade esteja disponível à medida que escala as instâncias do cluster, é possível criar uma reserva de capacidade para o grupo de posicionamento de cluster. Para obter mais informações, consulte Usar reservas de capacidade em grupos de posicionamento de cluster.

Como iniciar uma instância

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Instances (Instâncias) e, depois, escolha Launch Instances (Iniciar instâncias) para abrir o novo assistente de inicialização de instância.
3. (Opcional) Na seção Name and tags (Nome e etiquetas), forneça um nome para a instância, como `EFA-instance`. O nome é atribuído à instância como uma etiqueta de recurso (`Name=EFA-instance`).
4. Na seção Application and OS Images (Imagens de aplicações e SO), selecione My AMIs (Minhas AMIs) e, em seguida, selecione a AMI que você criou na etapa anterior.
5. Na seção Instance type (Tipo de instância), selecione um tipo de instância compatível.
6. Na seção Key pair (Par de chaves), selecione o par de chaves a ser usado na instância.
7. Na seção Network settings (Configurações da rede), escolha Edit (Editar) e faça o seguinte:

   a. Em Subnet (Sub-rede), escolha a sub-rede na qual deseja iniciar a instância. Se você não selecionar uma sub-rede, não será possível habilitar a instância para o EFA.

   b. Para Firewall (security groups) (Firewall/grupos de segurança), escolha Select existing security group (Selecione grupo de segurança existente) e, em seguida, selecione o grupo de segurança que você criou na etapa anterior.

   c. Expanda a seção Configuração de rede avançada.

      Para Interface de rede 1, selecione Índice da placa de rede = 0, Índice do dispositivo = 0 e Tipo de interface = EFA com ENA.

      (Opcional) Caso esteja usando um tipo de instância com várias placas, como `p4d.24xlarge` ou `p5.48xlarge`, para cada interface de rede adicional necessária, selecione Adicionar interface de rede, em Índice da placa de rede, selecione o próximo índice não utilizado e, em seguida, selecione Índice do dispositivo = 1 e Tipo de interface = EFA com ENA ou exclusivamente EFA.
8. (Opcional) Na seção Storage (Armazenamento), configure os volumes conforme necessário.
9. Na seção Advanced details (Detalhes avançados), para Placement group name (Nome do grupo de posicionamento), selecione o grupo de posicionamento de cluster no qual iniciar as instâncias. Caso precise criar um novo grupo de posicionamento de cluster, escolha Create new placement group (Criar novo grupo de posicionamento).

10. No painel Summary (Resumo) à direita, em Number of instances (Número de instâncias), insira o número de instâncias habilitadas para EFA que você deseja iniciar e escolha Launch instance (Iniciar instância).

Etapa 11: Encerrar a instância temporária

Neste ponto, você não precisa mais da instância que iniciou na Etapa 2. É possível encerrar a instância para não incorrer mais em cobranças desnecessárias.

Para encerrar a instância temporária

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância temporária, escolha Ações, selecione Estado da instância, Encerrar (excluir) instância.
4. Quando a confirmação for solicitada, escolha Encerrar (excluir).

Etapa 12: habilitar SSH sem senha

Para permitir que suas aplicações sejam executadas em todas as instâncias do cluster, é necessário habilitar o acesso SSH sem senha do nó líder para os nós membros. O nó líder é a instância a partir da qual você executa suas aplicações. As instâncias restantes no cluster são os nós membros.

Para habilitar SSH sem senha entre as instâncias no cluster

1. Selecione uma instância no cluster como o nó líder e conecte-se a ela.
2. Desabilite `strictHostKeyChecking` e habilite `ForwardAgent` no nó líder. Abra o `~/.ssh/config` usando o editor de texto de sua preferência e adicione o seguinte.

```
Host *
    ForwardAgent yes
Host *
    StrictHostKeyChecking no
```

3. Gere um par de chaves RSA.

```
$ ssh-keygen -t rsa -N "" -f ~/.ssh/id_rsa
```

O par de chaves é criado no diretório do `$HOME/.ssh/`.

4. Altere as permissões da chave privada no nó líder.

```
$ chmod 600 ~/.ssh/id_rsa
chmod 600 ~/.ssh/config
```

5. Abra `~/.ssh/id_rsa.pub` usando seu editor de texto preferido e copie a chave.
6. Para cada nó de membro no cluster, faça o seguinte:

   a. Conecte-se à instância.

   b. Abra `~/.ssh/authorized_keys` usando o editor de texto de sua preferência e adicione a chave pública que você copiou anteriormente.

7. Para testar se o SSH sem senha está funcionando como esperado, conecte-se ao seu nó líder e execute o comando a seguir.

```
$ ssh member_node_private_ip
```

   É necessário se conectar ao nó membro sem receber uma solicitação para inserir uma chave ou senha.

Conceitos básicos do EFA e NCCL para workloads de ML no Amazon EC2

A Nvidia Collective Communications Library (NCCL) é uma biblioteca de rotinas de comunicação coletiva padrão para várias GPUs em um único nó ou em vários nós. A NCCL pode ser usada com o EFA, o Libfabric e a MPI para oferecer suporte a várias workloads de machine learning. Para obter mais informações, consulte o site da NCCL.

Requisitos

- Somente os tipos de instância da série P são compatíveis. Para obter mais informações, consulte Instâncias com computação acelerada do Amazon EC2.
- Apenas as AMIs básicas do Amazon Linux 2023, Amazon Linux 2, Ubuntu 24.04 e Ubuntu 22.04 são compatíveis.
- Somente a NCCL 2.4.2 e posterior são compatíveis com EFA.

Para obter mais informações sobre como executar workloads de machine learning com EFA e NCCL usando um AMIs de deep learning da AWS, consulte Usando o EFA no DLAMI no Guia do desenvolvedor do AMIs de deep learning da AWS.

Etapas

- Etapa 1: Preparar um grupo de segurança habilitado para EFA
- Etapa 2: Iniciar uma instância temporária
- Etapa 3: Instalar drivers de GPU Nvidia, o toolkit Nvidia CUDA e o cuDNN
- Etapa 4: instalar o GDRCopy
- Etapa 5: instalar o software EFA
- Etapa 6: instalar NCCL
- Etapa 7: Instalar os testes da NCCL
- Etapa 8: Testar a configuração do EFA e da NCCL
- Etapa 9: Instalar as aplicações de machine learning
- Etapa 10: Criar um EFA e uma AMI habilitada para NCCL
- Etapa 11: Encerrar a instância temporária
- Etapa 12: Iniciar instâncias habilitadas para EFA e para NCCL em um grupo de posicionamento de cluster
- Etapa 13: Habilitar SSH sem senha

Etapa 1: Preparar um grupo de segurança habilitado para EFA

Um EFA requer um grupo de segurança que permita todo o tráfego de entrada e saída do grupo de segurança e para ele próprio. O procedimento a seguir cria um grupo de segurança que permite todo o tráfego de entrada e saída de e para si mesmo e que permite tráfego SSH de entrada de qualquer endereço IPv4 para conectividade SSH.

> **Important**
>
> Esse grupo de segurança deve ser usado apenas para fins de teste. Para seus ambientes de produção, recomendamos que você crie uma regra SSH de entrada que permita o tráfego somente do endereço IP do qual você está se conectando, como o endereço IP do seu computador ou uma variedade de endereços IP na sua rede local.

Para outros cenários, consulte Regras de grupo de segurança para diferentes casos de uso.

Para criar um grupo de segurança habilitado para EFA

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Security Groups (Grupos de segurança) e, em seguida, Create Security Group (Criar grupo de segurança).
3. Na janela Security group (Grupo de segurança), faça o seguinte:
   a. Em Security group name (Nome do grupo de segurança), insira um nome descritivo para o grupo de segurança, como `EFA-enabled security group`.
   b. (Opcional) Em Description (Descrição), insira uma breve descrição do grupo de segurança.
   c. Em VPC, selecione a VPC na qual você pretende executar suas instâncias habilitadas para EFA.
   d. Escolha Criar grupo de segurança.
4. Selecione o grupo de segurança que você criou e, na guia Details (Detalhes), copie o Security group (Grupo de segurança).
5. Com o grupo de segurança ainda selecionado, escolha Actions (Ações), Edit inbound rules (Editar regras de entrada), e faça o seguinte:
   a. Escolha Adicionar regra.
   b. Para Tipo, escolha Todo o tráfego.
   c. Para Source type (Tipo de origem), escolha Custom (Personalizado) e cole o ID do grupo de segurança que você copiou no campo.
   d. Escolha Adicionar regra.
   e. Para Tipo, escolha SSH.
   f. Para Source type (Tipo de origem), escolha Anywhere-IPv4 (IPv4 em qualquer lugar).
   g. Selecione Salvar regras.
6. Na lista, selecione o grupo de segurança e escolha Actions (Ações), Edit outbound rules (Editar regras de saída), e faça o seguinte:
   a. Escolha Adicionar regra.
   b. Para Tipo, escolha Todo o tráfego.
   c. Para Destination (Destino), escolha Custom (Personalizado) e cole o ID do grupo de segurança que você copiou no campo.

d. Selecione Salvar regras.

Etapa 2: Iniciar uma instância temporária

Execute uma instância temporária que é possível usar para instalar e configurar os componentes do software EFA. Você usa essa instância para criar um AMI habilitado para EFA a partir do qual é possível executar suas instâncias habilitadas para EFA.

Para executar uma instância temporária

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Instances (Instâncias) e, depois, escolha Launch Instances (Iniciar instâncias) para abrir o novo assistente de inicialização de instância.
3. (Opcional) Na seção Name and tags (Nome e etiquetas), forneça um nome para a instância, como `EFA-instance`. O nome é atribuído à instância como uma etiqueta de recurso (`Name=`*`EFA-instance`*).
4. Na seção Application and OS Images (Imagens de aplicação e sistema operacional), selecione uma AMI para um dos sistemas operacionais compatíveis.
5. Na seção Instance type (Tipo de instância), selecione um tipo de instância compatível.
6. Na seção Key pair (Par de chaves), selecione o par de chaves a ser usado na instância.
7. Na seção Network settings (Configurações da rede), escolha Edit (Editar) e faça o seguinte:

   a. Em Subnet (Sub-rede), escolha a sub-rede na qual deseja iniciar a instância. Se você não selecionar uma sub-rede, não será possível habilitar a instância para o EFA.

   b. Para Firewall (security groups) (Firewall/grupos de segurança), escolha Select existing security group (Selecione grupo de segurança existente) e, em seguida, selecione o grupo de segurança que você criou na etapa anterior.

   c. Expanda a seção Configuração de rede avançada.

      Para Interface de rede 1, selecione Índice da placa de rede = 0, Índice do dispositivo = 0 e Tipo de interface = EFA com ENA.

      (Opcional) Se você estiver usando um tipo de instância com várias placas, como **`p4d.24xlarge`** ou**`p5.48xlarge`**, para cada interface de rede adicional necessária, escolha Adicionar interface de rede, em Índice da placa de rede, selecione o próximo índice

não utilizado e, em seguida, selecione Índice do dispositivo = 1 e Tipo de interface = EFA com ENA ou somente EFA..

8. Na seção Storage (Armazenamento), configure os volumes conforme necessário.

> **Note**
>
> É necessário provisionar um armazenamento adicional de 10 a 20 GiB para o Toolkit Nvidia CUDA. Se você não provisionar armazenamento suficiente, você receberá uma mensagem de erro `insufficient disk space` ao tentar instalar os drivers Nvidia e o Toolkit CUDA.

9. No painel Summary (Resumo) painel, escolha Launch instance (Iniciar instância).

Etapa 3: Instalar drivers de GPU Nvidia, o toolkit Nvidia CUDA e o cuDNN

Amazon Linux 2023 and Amazon Linux 2

Para instalar os drivers de GPU Nvidia, o toolkit Nvidia CUDA e o cuDNN

1. Para garantir que todos os pacotes de software estejam atualizados, execute uma atualização rápida de software em sua instância.

```
$ sudo yum upgrade -y && sudo reboot
```

   Reconecte-se à sua instância depois de reinicializá-la.

2. Instale os utilitários necessários para instalar os drivers de GPU Nvidia e o toolkit Nvidia CUDA.

```
$ sudo yum groupinstall 'Development Tools' -y
```

3. Desabilite os drivers de código aberto `nouveau`.

   a. Instale os utilitários necessários e o pacote de cabeçalhos kernel para a versão do kernel que está sendo executada.

```
$ sudo yum install -y wget kernel-devel-$(uname -r) kernel-headers-$(uname -r)
```

b. Adicione nouveau ao arquivo de lista de negação /etc/modprobe.d/blacklist.conf .

```
$ cat << EOF | sudo tee --append /etc/modprobe.d/blacklist.conf
blacklist vga16fb
blacklist nouveau
blacklist rivafb
blacklist nvidiafb
blacklist rivatv
EOF
```

c. Anexe GRUB_CMDLINE_LINUX="rdblacklist=nouveau" ao arquivo grub e recompile a configuração do Grub.

```
$ echo 'GRUB_CMDLINE_LINUX="rdblacklist=nouveau"' | sudo tee -a /etc/
default/grub \
&& sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

4. Reinicialize a instância e reconecte-se a ela.
5. Prepare os repositórios necessários

a. Ative o repositório EPEL e defina a distribuição como rhel7.

```
$ sudo amazon-linux-extras install epel \
&& distribution='rhel7'
```

b. Configure o repositório de rede CUDA e atualize o cache do repositório.

```
$ ARCH=$( /bin/arch ) \
&& sudo yum-config-manager --add-repo http://developer.download.nvidia.com/
compute/cuda/repos/$distribution/${ARCH}/cuda-$distribution.repo \
&& sudo yum clean expire-cache
```

c. (Somente kernel versão 5.10) Execute estas etapas somente se você estiver usando o Amazon Linux 2 com o kernel versão 5.10. Se você estiver usando o Amazon Linux 2 com o kernel versão 4.12, ignore estas etapas. Para verificar a versão do kernel, execute uname -r.

i. Crie o arquivo de configuração do driver Nvidia chamado /etc/dkms/nvidia.conf.

```
$ sudo mkdir -p /etc/dkms \
&& echo "MAKE[0]=\"'make' -j2 module SYSSRC=\${kernel_source_dir}
 IGNORE_XEN_PRESENCE=1 IGNORE_PREEMPT_RT_PRESENCE=1 IGNORE_CC_MISMATCH=1
 CC=/usr/bin/gcc10-gcc\"" | sudo tee /etc/dkms/nvidia.conf
```

ii. (`p4d.24xlarge` e `p5.48xlarge` somente) Copie o arquivo de configuração do driver NVIDIA.

```
$ sudo cp /etc/dkms/nvidia.conf /etc/dkms/nvidia-open.conf
```

6. Instale os drivers de GPU Nvidia, o toolkit Nvidia CUDA e o cuDNN.

```
$ sudo yum clean all \
&& sudo yum -y install nvidia-driver-latest-dkms \
&& sudo yum -y install cuda-drivers-fabricmanager cuda libcudnn8-devel
```

7. Reinicialize a instância e reconecte-se a ela.

8. (`p4d.24xlarge` e `p5.48xlarge` somente) Inicie o serviço NVIDIA Fabric Manager e verifique se ele será iniciado automaticamente quando a instância for iniciada. O Nvidia Fabric Manager é necessário para o gerenciamento do NV Switch.

```
$ sudo systemctl enable nvidia-fabricmanager && sudo systemctl start nvidia-
fabricmanager
```

9. Certifique-se de que os caminhos do CUDA sejam definidos cada vez que a instância for executada.

   - Em shells bash, adicione as seguintes instruções a `/home/`*`username`*`/.bashrc` e `/home/`*`username`*`/.bash_profile`.

     ```
     export PATH=/usr/local/cuda/bin:$PATH
     export LD_LIBRARY_PATH=/usr/local/cuda/lib64:/usr/local/cuda/extras/CUPTI/
     lib64:$LD_LIBRARY_PATH
     ```

   - Em shells tcsh, adicione as seguintes instruções a `/home/`*`username`*`/.cshrc`.

     ```
     setenv PATH=/usr/local/cuda/bin:$PATH
     setenv LD_LIBRARY_PATH=/usr/local/cuda/lib64:/usr/local/cuda/extras/CUPTI/
     lib64:$LD_LIBRARY_PATH
     ```

10. Para verificar se os drivers de GPU Nvidia estão funcionando, execute o comando a seguir.

```
$ nvidia-smi -q | head
```

O comando deve retornar informações sobre os as GPUs Nvidia, sobre os drivers de GPU Nvidia e sobre o toolkit Nvidia CUDA.

Ubuntu 24.04 and Ubuntu 22.04

Para instalar os drivers de GPU Nvidia, o toolkit Nvidia CUDA e o cuDNN

1. Para garantir que todos os pacotes de software estejam atualizados, execute uma atualização rápida de software em sua instância.

```
$ sudo apt-get update && sudo apt-get upgrade -y
```

2. Instale os utilitários necessários para instalar os drivers de GPU Nvidia e o toolkit Nvidia CUDA.

```
$ sudo apt-get update && sudo apt-get install build-essential -y
```

3. Para usar o driver de GPU Nvidia, é necessário primeiro desabilitar os drivers de código aberto `nouveau`.

   a. Instale os utilitários necessários e o pacote de cabeçalhos kernel para a versão do kernel que está sendo executada.

```
$ sudo apt-get install -y gcc make linux-headers-$(uname -r)
```

   b. Adicione `nouveau` ao arquivo de lista de negação `/etc/modprobe.d/blacklist.conf` .

```
$ cat << EOF | sudo tee --append /etc/modprobe.d/blacklist.conf
blacklist vga16fb
blacklist nouveau
blacklist rivafb
blacklist nvidiafb
blacklist rivatv
EOF
```

c. Abra o `/etc/default/grub` usando o editor de texto de sua preferência e adicione o seguinte.

```
GRUB_CMDLINE_LINUX="rdblacklist=nouveau"
```

d. Recompile a configuração do Grub.

```
$ sudo update-grub
```

4. Reinicialize a instância e reconecte-se a ela.
5. Adicione o repositório CUDA e instale os drivers de GPU Nvidia, o toolkit Nvidia CUDA e o cuDNN.

   - `p3dn.24xlarge`

```
$ sudo apt-key adv --fetch-keys http://developer.download.nvidia.com/compute/
machine-learning/repos/ubuntu2004/x86_64/7fa2af80.pub \
&& wget -O /tmp/deeplearning.deb http://developer.download.nvidia.com/compute/
machine-learning/repos/ubuntu2004/x86_64/nvidia-machine-learning-repo-
ubuntu2004_1.0.0-1_amd64.deb \
&& sudo dpkg -i /tmp/deeplearning.deb \
&& wget -O /tmp/cuda.pin https://developer.download.nvidia.com/compute/cuda/
repos/ubuntu2004/x86_64/cuda-ubuntu2004.pin \
&& sudo mv /tmp/cuda.pin /etc/apt/preferences.d/cuda-repository-pin-600 \
&& sudo apt-key adv --fetch-keys https://developer.download.nvidia.com/
compute/cuda/repos/ubuntu2004/x86_64/3bf863cc.pub \
&& sudo add-apt-repository 'deb http://developer.download.nvidia.com/compute/
cuda/repos/ubuntu2004/x86_64/ /' \
&& sudo apt update \
&& sudo apt install nvidia-dkms-535 \
&& sudo apt install -o Dpkg::Options::='--force-overwrite' cuda-drivers-535
 cuda-toolkit-12-3 libcudnn8 libcudnn8-dev -y
```

   - `p4d.24xlarge` e da `p5.48xlarge`

```
$ sudo apt-key adv --fetch-keys http://developer.download.nvidia.com/compute/
machine-learning/repos/ubuntu2004/x86_64/7fa2af80.pub \
&& wget -O /tmp/deeplearning.deb http://developer.download.nvidia.com/compute/
machine-learning/repos/ubuntu2004/x86_64/nvidia-machine-learning-repo-
ubuntu2004_1.0.0-1_amd64.deb \
&& sudo dpkg -i /tmp/deeplearning.deb \
```

```
&& wget -O /tmp/cuda.pin https://developer.download.nvidia.com/compute/cuda/
repos/ubuntu2004/x86_64/cuda-ubuntu2004.pin \
&& sudo mv /tmp/cuda.pin /etc/apt/preferences.d/cuda-repository-pin-600 \
&& sudo apt-key adv --fetch-keys https://developer.download.nvidia.com/
compute/cuda/repos/ubuntu2004/x86_64/3bf863cc.pub \
&& sudo add-apt-repository 'deb http://developer.download.nvidia.com/compute/
cuda/repos/ubuntu2004/x86_64/ /' \
&& sudo apt update \
&& sudo apt install nvidia-kernel-open-535 \
&& sudo apt install -o Dpkg::Options::='--force-overwrite' cuda-drivers-535
 cuda-toolkit-12-3 libcudnn8 libcudnn8-dev -y
```

6. Reinicialize a instância e reconecte-se a ela.
7. (Somente `p4d.24xlarge` e `p5.48xlarge`) Instale o Nvidia Fabric Manager.

   a. É necessário instalar a versão do Nvidia Fabric Manager que corresponde à versão do módulo do kernel Nvidia que você instalou na etapa anterior.

      Execute o seguinte comando para determinar a versão do módulo do kernel Nvidia.

      ```
      $ cat /proc/driver/nvidia/version | grep "Kernel Module"
      ```

      A seguir está um exemplo de saída.

      ```
      NVRM version: NVIDIA UNIX x86_64 Kernel Module  450.42.01  Tue Jun 15
       21:26:37 UTC 2021
      ```

      No exemplo acima, a versão principal `450` do módulo do kernel foi instalado. Isso significa que você precisa instalar a versão do Nvidia Fabric Manager `450`.

   b. Instale o Nvidia Fabric Manager. Execute o seguinte comando e especifique a versão principal identificada na etapa anterior.

      ```
      $ sudo apt install -o Dpkg::Options::='--force-overwrite' nvidia-
      fabricmanager-major_version_number
      ```

      Por exemplo, se a versão principal `450` do módulo do kernel foi instalado, use o seguinte comando para instalar a versão correspondente do Nvidia Fabric Manager.

```
$ sudo apt install -o Dpkg::Options::='--force-overwrite' nvidia-
fabricmanager-450
```

c. Inicie o serviço e certifique-se de que ele seja iniciado automaticamente quando a instância for executada. O Nvidia Fabric Manager é necessário para o gerenciamento do NV Switch.

```
$ sudo systemctl start nvidia-fabricmanager && sudo systemctl enable nvidia-
fabricmanager
```

8. Certifique-se de que os caminhos do CUDA sejam definidos cada vez que a instância for executada.

   - Em shells bash, adicione as seguintes instruções a /home/*username*/.bashrc e /home/*username*/.bash_profile.

   ```
   export PATH=/usr/local/cuda/bin:$PATH
   export LD_LIBRARY_PATH=/usr/local/cuda/lib64:/usr/local/cuda/extras/CUPTI/
   lib64:$LD_LIBRARY_PATH
   ```

   - Em shells tcsh, adicione as seguintes instruções a /home/*username*/.cshrc.

   ```
   setenv PATH=/usr/local/cuda/bin:$PATH
   setenv LD_LIBRARY_PATH=/usr/local/cuda/lib64:/usr/local/cuda/extras/CUPTI/
   lib64:$LD_LIBRARY_PATH
   ```

9. Para verificar se os drivers de GPU Nvidia estão funcionando, execute o comando a seguir.

   ```
   $ nvidia-smi -q | head
   ```

   O comando deve retornar informações sobre os as GPUs Nvidia, sobre os drivers de GPU Nvidia e sobre o toolkit Nvidia CUDA.

Etapa 4: instalar o GDRCopy

Instale o GDRCopy para melhorar a performance do Libfabric. Para obter mais informações sobre a GDRCopy, consulte o repositório do GDRCopy.

Amazon Linux 2023 and Amazon Linux 2

Para instalar o GDRCopy

1. Instale as dependências necessárias.

```
$ sudo yum -y install dkms rpm-build make check check-devel subunit subunit-
devel
```

2. Baixe e extraia o pacote do GDRCopy.

```
$ wget https://github.com/NVIDIA/gdrcopy/archive/refs/tags/v2.4.tar.gz \
&& tar xf v2.4.tar.gz ; cd gdrcopy-2.4/packages
```

3. Crie o pacote RPM do GDRCopy.

```
$ CUDA=/usr/local/cuda ./build-rpm-packages.sh
```

4. Instale o pacote RPM do GDRCopy.

```
$ sudo rpm -Uvh gdrcopy-kmod-2.4-1dkms.noarch*.rpm \
&& sudo rpm -Uvh gdrcopy-2.4-1.x86_64*.rpm \
&& sudo rpm -Uvh gdrcopy-devel-2.4-1.noarch*.rpm
```

Ubuntu 24.04 and Ubuntu 22.04

Para instalar o GDRCopy

1. Instale as dependências necessárias.

```
$ sudo apt -y install build-essential devscripts debhelper check libsubunit-dev
 fakeroot pkg-config dkms
```

2. Baixe e extraia o pacote do GDRCopy.

```
$ wget https://github.com/NVIDIA/gdrcopy/archive/refs/tags/v2.4.tar.gz \
&& tar xf v2.4.tar.gz \
&& cd gdrcopy-2.4/packages
```

3. Crie o pacote RPM do GDRCopy.

```
$ CUDA=/usr/local/cuda ./build-deb-packages.sh
```

4. Instale o pacote RPM do GDRCopy.

```
$ sudo dpkg -i gdrdrv-dkms_2.4-1_amd64.*.deb \
&& sudo dpkg -i libgdrapi_2.4-1_amd64.*.deb \
&& sudo dpkg -i gdrcopy-tests_2.4-1_amd64.*.deb \
&& sudo dpkg -i gdrcopy_2.4-1_amd64.*.deb
```

Etapa 5: instalar o software EFA

Instale o kernel habilitado para EFA, drivers EFA, Libfabric, plugin aws-ofi-nccl e pilha Open MPI, que são necessários para oferecer compatibilidade com EFA em sua instância.

Como instalar o software EFA

1. Conecte à instância que você iniciou. Para obter mais informações, consulte Conectar-se à instância do Linux usando SSH.
2. Faça download dos arquivos de instalação do software do EFA. Os arquivos de instalação do software são empacotados em um arquivo compactado tarball (`.tar.gz`). Para fazer download da última versão estável, use o seguinte comando:

   Também é possível obter a versão mais recente substituindo o número da versão por `latest` no comando acima.

   ```
   $ curl -O https://efa-installer.amazonaws.com/aws-efa-installer-1.47.0.tar.gz
   ```

3. (Opcional) Verifique a autenticidade e a integridade do arquivo do EFA tarball (`.tar.gz`).

   Recomendamos que você faça isso para verificar a identidade do fornecedor do software e para verificar se a aplicação não foi alterada ou corrompida desde que foi publicada. Se você não deseja verificar o arquivo tarball, ignore esta etapa.

> **Note**
>
> Como alternativa, se você preferir verificar o arquivo tarball usando uma soma de verificação MD5 ou SHA256, consulte Verificar o instalador EFA usando uma soma de verificação.

a. Faça download da chave GPG pública e importe-a para seu pen-drive.

```
$ wget https://efa-installer.amazonaws.com/aws-efa-installer.key && gpg --
import aws-efa-installer.key
```

O comando deve retornar um valor de chave. Anote o valor da chave, pois ele será necessário na próxima etapa.

b. Verifique a impressão digital da chave GPG. Execute o seguinte comando e especifique o valor de chave da etapa anterior.

```
$ gpg --fingerprint key_value
```

O comando deve retornar uma impressão digital idêntica a `4E90 91BC BB97 A96B 26B1 5E59 A054 80B1 DD2D 3CCC`. Se a impressão digital não corresponder, não execute o script de instalação do EFA e entre em contato com o Suporte.

c. Faça download do arquivo de assinatura e verifique a assinatura do arquivo tarball EFA.

```
$ wget https://efa-installer.amazonaws.com/aws-efa-installer-1.47.0.tar.gz.sig
 && gpg --verify ./aws-efa-installer-1.47.0.tar.gz.sig
```

Veja a seguir um exemplo de saída.

```
gpg: Signature made Wed 29 Jul 2020 12:50:13 AM UTC using RSA key ID DD2D3CCC
gpg: Good signature from "Amazon EC2 EFA <ec2-efa-maintainers@amazon.com>"
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the owner.
Primary key fingerprint: 4E90 91BC BB97 A96B 26B1  5E59 A054 80B1 DD2D 3CCC
```

Se o resultado incluir `Good signature` e a impressão digital corresponder à impressão digital retornada na etapa anterior, passe para a próxima etapa. Caso contrário, não execute o script de instalação do EFA e entre em contato com o Suporte.

4. Extraia os arquivos do arquivo compactado `.tar.gz` e navegue para o diretório extraído.

```
$ tar -xf aws-efa-installer-1.47.0.tar.gz && cd aws-efa-installer
```

5. Execute o script de instalação do software EFA.

> **Note**
>
> A partir do EFA 1.30.0, tanto a Open MPI 4.1 quanto a Open MPI 5 são instaladas por padrão. A menos que você precise da Open MPI 5, recomendamos que instale apenas a Open MPI 4.1. O comando a seguir instala apenas a Open MPI 4.1. Se quiser instalar a Open MPI 4.1 e a Open MPI 5, remova `--mpi=openmpi4`.

```
$ sudo ./efa_installer.sh -y --mpi=openmpi4
```

O Libfabric está instalado no diretório `/opt/amazon/efa`. O plugin aws-ofi-nccl está instalado no diretório `/opt/amazon/ofi-nccl`. O Open MPI está instalado no diretório `/opt/amazon/openmpi`.

6. Se o instalador do EFA solicitar que você reinicialize a instância, faça-o e, em seguida, reconecte-se à instância. Caso contrário, faça logout da instância e faça login novamente para concluir a instalação.
7. Confirme se os componentes do software EFA foram instalados com sucesso.

```
$ fi_info -p efa -t FI_EP_RDM
```

O comando deve retornar informações sobre as interfaces EFA Libfabric. O exemplo a seguir mostra a saída do comando.

- `p3dn.24xlarge` com interface de rede única

```
provider: efa
fabric: EFA-fe80::94:3dff:fe89:1b70
```

```
domain: efa_0-rdm
version: 2.0
type: FI_EP_RDM
protocol: FI_PROTO_EFA
```

- `p4d.24xlarge` e `p5.48xlarge` com várias interfaces de rede

```
provider: efa
fabric: EFA-fe80::c6e:8fff:fef6:e7ff
domain: efa_0-rdm
version: 111.0
type: FI_EP_RDM
protocol: FI_PROTO_EFA
provider: efa
fabric: EFA-fe80::c34:3eff:feb2:3c35
domain: efa_1-rdm
version: 111.0
type: FI_EP_RDM
protocol: FI_PROTO_EFA
provider: efa
fabric: EFA-fe80::c0f:7bff:fe68:a775
domain: efa_2-rdm
version: 111.0
type: FI_EP_RDM
protocol: FI_PROTO_EFA
provider: efa
fabric: EFA-fe80::ca7:b0ff:fea6:5e99
domain: efa_3-rdm
version: 111.0
type: FI_EP_RDM
protocol: FI_PROTO_EFA
```

Etapa 6: instalar NCCL

Instale a NCCL. Para obter mais informações sobre a NCCL, consulte o Repositório da NCCL.

Como instalar a NCCL

1. Navegue até o diretório `/opt`.

```
$ cd /opt
```

2. Clone o repositório oficial da NCCL para a instância e navegue até o repositório local clonado.

```
$ sudo git clone https://github.com/NVIDIA/nccl.git -b v2.23.4-1 && cd nccl
```

3. Compile e instale a NCCL e especifique o diretório de instalação do CUDA.

```
$ sudo make -j src.build CUDA_HOME=/usr/local/cuda
```

Etapa 7: Instalar os testes da NCCL

Instale os testes da NCCL. Os testes da NCCL permitem confirmar se a NCCL está instalada adequadamente se ela está funcionando conforme esperado. Para obter mais informações sobre os testes da NCCL, consulte o Repositório nccl-tests.

Como instalar os testes da NCCL

1. Navegue até o diretório inicial.

```
$ cd $HOME
```

2. Clone o repositório oficial de nccl-tests para a instância e navegue até o repositório local clonado.

```
$ git clone https://github.com/NVIDIA/nccl-tests.git && cd nccl-tests
```

3. Adicione o diretório do Libfabric à variável `LD_LIBRARY_PATH`.

   - Amazon Linux 2023 e Amazon Linux 2

```
$ export LD_LIBRARY_PATH=/opt/amazon/efa/lib64:$LD_LIBRARY_PATH
```

   - Ubuntu 24.04 e Ubuntu 22.04

```
$ export LD_LIBRARY_PATH=/opt/amazon/efa/lib:$LD_LIBRARY_PATH
```

4. Instale os testes da NCCL e especifique os diretórios de instalação da MPI da NCCL e do CUDA.

```
$ make MPI=1 MPI_HOME=/opt/amazon/openmpi NCCL_HOME=/opt/nccl/build CUDA_HOME=/usr/
local/cuda
```

Etapa 8: Testar a configuração do EFA e da NCCL

Execute um teste para verificar se a instância temporária está configurada adequadamente para o EFA e para a NCCL.

Como testar a configuração do EFA e da NCCL

1. Crie um arquivo de host que especifique os hosts nos quais executar os testes. O comando a seguir cria um arquivo de host chamado `my-hosts` que inclui uma referência à própria instância.

   IMDSv2

   ```
   [ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H
    "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
   && curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/
   meta-data/local-ipv4 >> my-hosts
   ```

   IMDSv1

   ```
   [ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/local-ipv4 >> my-
   hosts
   ```

2. Execute o teste e especifique o arquivo de host (`--hostfile`) e o número de GPUs a serem usadas (`-n`). O comando a seguir executa o teste `all_reduce_perf` em 8 GPUs na própria instância e especifica as variáveis de ambiente a seguir.

   - `FI_EFA_USE_DEVICE_RDMA=1`: (somente `p4d.24xlarge`) usa a funcionalidade RDMA do dispositivo para transferência unilateral e bilateral.
   - `NCCL_DEBUG=INFO` habilita a saída de depuração detalhada. Também é possível especificar `VERSION` para imprimir somente a versão da NCCL no início do teste ou `WARN` para receber somente mensagens de erro.

Para obter mais informações sobre os argumentos de teste da NCCL, consulte o README NCCL Tests no repositório oficial de nccl-tests.

- `p3dn.24xlarge`

```
$ /opt/amazon/openmpi/bin/mpirun \
-x LD_LIBRARY_PATH=/opt/nccl/build/lib:/usr/local/cuda/lib64:/opt/amazon/efa/
lib:/opt/amazon/openmpi/lib:/opt/amazon/ofi-nccl/lib:$LD_LIBRARY_PATH \
-x NCCL_DEBUG=INFO \
--hostfile my-hosts -n 8 -N 8 \
--mca pml ^cm --mca btl tcp,self --mca btl_tcp_if_exclude lo,docker0 --bind-to
 none \
$HOME/nccl-tests/build/all_reduce_perf -b 8 -e 1G -f 2 -g 1 -c 1 -n 100
```

- `p4d.24xlarge` e da `p5.48xlarge`

```
$ /opt/amazon/openmpi/bin/mpirun \
-x FI_EFA_USE_DEVICE_RDMA=1 \
-x LD_LIBRARY_PATH=/opt/nccl/build/lib:/usr/local/cuda/lib64:/opt/amazon/efa/
lib:/opt/amazon/openmpi/lib:/opt/amazon/ofi-nccl/lib:$LD_LIBRARY_PATH \
-x NCCL_DEBUG=INFO \
--hostfile my-hosts -n 8 -N 8 \
--mca pml ^cm --mca btl tcp,self --mca btl_tcp_if_exclude lo,docker0 --bind-to
 none \
$HOME/nccl-tests/build/all_reduce_perf -b 8 -e 1G -f 2 -g 1 -c 1 -n 100
```

3. É possível confirmar se EFA está ativo como o provedor subjacente para NCCL quando o log `NCCL_DEBUG` é impresso.

```
ip-192-168-2-54:14:14 [0] NCCL INFO NET/OFI Selected Provider is efa*
```

As seguintes informações adicionais são exibidas ao usar uma instância `p4d.24xlarge`.

```
ip-192-168-2-54:14:14 [0] NCCL INFO NET/OFI Running on P4d platform, Setting
 NCCL_TOPO_FILE environment variable to /home/ec2-user/install/plugin/share/aws-
ofi-nccl/xml/p4d-24xl-topo.xml
```

Etapa 9: Instalar as aplicações de machine learning

Instale as aplicações de machine learning na instância temporária. O procedimento de instalação varia dependendo da aplicação de machine learning específica. Para obter mais informações sobre instalação de software em sua instância do Linux, consulte Manage software on your Amazon Linux 2 instance.

> **Note**
>
> Pode ser necessário consultar a documentação da aplicação de machine learning para obter instruções de instalação.

Etapa 10: Criar um EFA e uma AMI habilitada para NCCL

Depois de instalar os componentes de software necessários, crie uma AMI que possa ser reutilizada para executar suas instâncias habilitadas para o EFA.

Para criar uma AMI a partir de sua instância temporária

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância, escolha Actions (Ações), Image (Imagem), Create image (Criar imagem).
4. Em Create image (Criar imagem), faça o seguinte:
   a. Em Image name (Nome da imagem), insira um nome descritivo para a AMI.
   b. (Opcional) Em Image description (Descrição da imagem), informe a descrição do propósito da AMI.
   c. Escolha Create Image (Criar imagem).
5. No painel de navegação, selecione AMIs.
6. Encontre a AMI que você criou na lista. Aguarde até que o status mude de `pending` para `available` antes de continuar para a próxima etapa.

Etapa 11: Encerrar a instância temporária

Neste ponto, você não precisa mais da instância temporária que você executou. É possível encerrar a instância para não incorrer mais em cobranças desnecessárias.

Para encerrar a instância temporária

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância temporária, escolha Actions (Ações), selecione Instance state (Estado da instância), Terminate instance (Encerrar instance).
4. Quando a confirmação for solicitada, escolha Terminate (Encerrar).

Etapa 12: Iniciar instâncias habilitadas para EFA e para NCCL em um grupo de posicionamento de cluster

Execute as instâncias habilitadas para EFA em um grupo de posicionamento de cluster usando a AMI habilitada para EFA criada e o grupo de segurança habilitado para EFA criado anteriormente.

> **Note**
>
> - Não é um requisito absoluto executar suas instâncias habilitadas para EFA em um placement group de cluster. No entanto, recomendamos a execução de suas instâncias habilitadas para EFA em um grupo de posicionamento de cluster ao executar as instâncias em um grupo de baixa latência em uma única zona de disponibilidade.
> - Para garantir que a capacidade esteja disponível à medida que escala as instâncias do cluster, é possível criar uma reserva de capacidade para o grupo de posicionamento de cluster. Para obter mais informações, consulte Usar reservas de capacidade em grupos de posicionamento de cluster.

New console

Para executar uma instância temporária

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Instances (Instâncias) e, depois, escolha Launch Instances (Iniciar instâncias) para abrir o novo assistente de inicialização de instância.
3. (Opcional) Na seção Name and tags (Nome e etiquetas), forneça um nome para a instância, como `EFA-instance`. O nome é atribuído à instância como uma etiqueta de recurso (`Name=`*`EFA-instance`*).

4. Na seção Application and OS Images (Imagens de aplicações e SO), selecione My AMIs (Minhas AMIs) e, em seguida, selecione a AMI que você criou na etapa anterior.
5. Na seção Instance type (Tipo de instância), selecione `p3dn.24xlarge` ou `p4d.24xlarge`.
6. Na seção Key pair (Par de chaves), selecione o par de chaves a ser usado na instância.
7. Na seção Network settings (Configurações da rede), escolha Edit (Editar) e faça o seguinte:

   a. Em Subnet (Sub-rede), escolha a sub-rede na qual deseja iniciar a instância. Se você não selecionar uma sub-rede, não será possível habilitar a instância para o EFA.

   b. Para Firewall (security groups) (Firewall/grupos de segurança), escolha Select existing security group (Selecione grupo de segurança existente) e, em seguida, selecione o grupo de segurança que você criou na etapa anterior.

   c. Expanda a seção Configuração de rede avançada.

      Para Interface de rede 1, selecione Índice da placa de rede = 0, Índice do dispositivo = 0 e Tipo de interface = EFA com ENA.

      (Opcional) Caso esteja usando um tipo de instância com várias placas, como `p4d.24xlarge` oup`5.48xlarge`, para cada interface de rede adicional necessária, selecione Adicionar interface de rede, em Índice da placa de rede, selecione o próximo índice não utilizado e, em seguida, selecione Índice do dispositivo = 1 e Tipo de interface = EFA com ENA ou exclusivamente EFA.
8. (Opcional) Na seção Storage (Armazenamento), configure os volumes conforme necessário.
9. Na seção Advanced details (Detalhes avançados), para Placement group name (Nome do grupo de posicionamento), selecione o grupo de posicionamento de cluster no qual iniciar a instância. Caso precise criar um novo grupo de posicionamento de cluster, escolha Create new placement group (Criar novo grupo de posicionamento).
10. No painel Summary (Resumo) à direita, em Number of instances (Número de instâncias), insira o número de instâncias habilitadas para EFA que você deseja iniciar e escolha Launch instance (Iniciar instância).

Old console

Para executar as instâncias habilitadas para EFA e NCCL em um grupo de posicionamento de cluster.

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

2. Escolha Launch Instance (Executar instância).
3. Na página Choose an AMI (Escolher uma AMI), selecione My AMIs (Minhas AMIs), localize a AMI criada anteriormente e escolha Select (Selecionar).
4. Na página Choose an Instance Type (Escolher um tipo de instância), escolha p3dn.24xlarge e selecione Next: Configure Instance Details (Próximo: configurar detalhes da instância).
5. Na página Configure Instance Details (Configurar detalhes da instância), faça o seguinte:
   a. Em Number of instances (Número de instâncias), insira o número de instâncias habilitadas para EFA e NCCL que você deseja executar.
   b. Em Network (Rede) e Subnet (Sub-rede), selecione a VPC e a sub-rede na qual executar as instâncias.
   c. Em Placement group, selecione Add instance to placement group (Adicionar instância ao placement group).
   d. Em Placement group name (Nome do grupo de posicionamento), selecione Add to a new placement group (Adicionar a um novo grupo de posicionamento) e, em seguida, insira um nome descritivo para o grupo de posicionamento. Em seguida, em Placement group strategy (Estratégia do grupo de posicionamento), selecione cluster.
   e. Para EFA, escolha Enable (Habilitar).
   f. Na seção Network Interfaces (Interfaces de rede), para dispositivo eth0, escolha New network interface (Nova interface de rede). Como opção, é possível especificar um endereço IPv4 principal e um ou mais endereços IPv4 secundários. Se estiver executando a instância em uma sub-rede que tenha um bloco CIDR IPv6 associado, será possível especificar opcionalmente um endereço IPv6 principal e um ou mais endereços IPv6 secundários.
   g. Escolha Next: Add Storage.
6. Na página Add Storage (Adicionar armazenamento), especifique os volumes para anexar às instâncias, além dos volumes especificados pela AMI (como o volume raiz). Depois, selecione Next: Add Tags (Próximo: adicionar tags).
7. Na página Add Tags (Adicionar tags), especifique tags para as instâncias, como nome amigável, e selecione Next: Configure Security Group (Próximo: Configurar grupo de segurança).
8. Na página Configure Security Group (Configurar grupo de segurança), para Assign a security group (Atribuir um grupo de segurança), selecione Select an existing security group

(Selecionar um grupo de segurança existente) e selecione o grupo de segurança que você criou anteriormente.

9. Escolha Review and Launch.
10. Na página Review Instance Launch (Revisar execução da instância), reveja as configurações, e escolha Launch (Executar) para escolher um par de chaves e executar a instâncias.

Etapa 13: Habilitar SSH sem senha

Para permitir que suas aplicações sejam executadas em todas as instâncias do cluster, é necessário habilitar o acesso SSH sem senha do nó líder para os nós membros. O nó líder é a instância a partir da qual você executa suas aplicações. As instâncias restantes no cluster são os nós membros.

Para habilitar SSH sem senha entre as instâncias no cluster

1. Selecione uma instância no cluster como o nó líder e conecte-se a ela.
2. Desabilite `strictHostKeyChecking` e habilite `ForwardAgent` no nó líder. Abra o `~/.ssh/config` usando o editor de texto de sua preferência e adicione o seguinte.

```
Host *
    ForwardAgent yes
Host *
    StrictHostKeyChecking no
```

3. Gere um par de chaves RSA.

```
$ ssh-keygen -t rsa -N "" -f ~/.ssh/id_rsa
```

   O par de chaves é criado no diretório do `$HOME/.ssh/`.

4. Altere as permissões da chave privada no nó líder.

```
$ chmod 600 ~/.ssh/id_rsa
chmod 600 ~/.ssh/config
```

5. Abra `~/.ssh/id_rsa.pub` usando seu editor de texto preferido e copie a chave.
6. Para cada nó de membro no cluster, faça o seguinte:

   a. Conecte-se à instância.

b. Abra `~/.ssh/authorized_keys` usando o editor de texto de sua preferência e adicione a chave pública que você copiou anteriormente.

7. Para testar se o SSH sem senha está funcionando como esperado, conecte-se ao seu nó líder e execute o comando a seguir.

```
$ ssh member_node_private_ip
```

É necessário se conectar ao nó membro sem receber uma solicitação para inserir uma chave ou senha.

Maximize a largura de banda da rede em instâncias do Amazon EC2 com várias placas de rede

Muitos tipos de instâncias que oferecem suporte ao EFA também têm várias placas de rede. Para obter mais informações, consulte Placas de rede. Se você planeja usar o EFA com um desses tipos de instâncias, recomendamos a seguinte configuração básica:

- Para a interface de rede primária (índice da placa de rede `0`, índice do dispositivo `0`), crie uma interface EFA (EFA com ENA). Você não pode usar uma interface de rede exclusiva do EFA como interface de rede primária.
- Para cada interface de rede adicional, use o próximo índice de placa da rede não utilizado, o índice do dispositivo 1 e uma interface de rede EFA (EFA com ENA) ou somente EFA, dependendo do seu caso de uso, como requisitos de largura de banda do ENA ou espaço de endereço IP. Para obter casos de uso de exemplo, consulte Configuração de EFA para instâncias P5 e P5e.

> **Note**
>
> As instâncias P5 exigem que as interfaces de rede sejam configuradas de uma maneira específica para permitir a máxima largura de banda da rede. Para obter mais informações, consulte Configuração de EFA para instâncias P5 e P5e.

Os exemplos a seguir mostram como iniciar uma instância com base nessas recomendações.

Instance launch

Para especificar EFAs durante a inicialização da instância usando o assistente de inicialização de instâncias

1. Na seção Configurações de rede, escolha Editar.
2. Expanda Configuração de rede avançada.
3. Para a interface de rede primária (Interface de rede 1), selecione Índice da placa de rede = 0, Índice do dispositivo = 0 e Tipo de interface = EFA com ENA.
4. Para cada interface de rede adicional necessária, selecione Adicionar interface de rede. Para Índice da placa de rede, selecione o próximo índice não utilizado e, em seguida, selecione Índice do dispositivo = 1 e Tipo de interface = EFA com ENA ou somente EFA.

Para especificar EFAs durante a execução da instância usando o comando run-instances

Para `--network-interfaces`, especifique o número necessário de interfaces de rede. Para a interface de rede primária, especifique `NetworkCardIndex=0`, `DeviceIndex=0`, e `InterfaceType=efa`. Para qualquer interface de rede adicional, para `NetworkCardIndex` especificar o próximo índice não utilizado,`DeviceIndex=1`, e `InterfaceType=efa` ou`efa-only`.

O exemplo de snippet de comando a seguir mostra uma solicitação com 32 dispositivos EFA e um dispositivo ENA.

```
$ aws ec2 run-instances \
 --instance-type p5.48xlarge \
 --count 1 \
 --key-name key_pair_name \
 --image-id ami-0abcdef1234567890 \
 --network-interfaces
 "NetworkCardIndex=0,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType
 \
"NetworkCardIndex=1,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=
 or efa-only" \
"NetworkCardIndex=2,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=
 or efa-only" \
"NetworkCardIndex=3,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=
 or efa-only" \
"NetworkCardIndex=4,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=
 or efa-only" \
```

```
"NetworkCardIndex=5,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=
 or efa-only" \
"NetworkCardIndex=6,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=
 or efa-only" \
"NetworkCardIndex=7,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=
 or efa-only" \
"NetworkCardIndex=8,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=
 or efa-only" \
"NetworkCardIndex=9,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=
 or efa-only" \
"NetworkCardIndex=10,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType
 or efa-only" \
"NetworkCardIndex=11,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType
 or efa-only" \
"NetworkCardIndex=12,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType
 or efa-only" \
"NetworkCardIndex=13,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType
 or efa-only" \
"NetworkCardIndex=14,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType
 or efa-only" \
"NetworkCardIndex=15,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType
 or efa-only" \
"NetworkCardIndex=16,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType
 or efa-only" \
"NetworkCardIndex=17,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType
 or efa-only" \
"NetworkCardIndex=18,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType
 or efa-only" \
"NetworkCardIndex=19,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType
 or efa-only" \
"NetworkCardIndex=20,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType
 or efa-only" \
"NetworkCardIndex=21,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType
 or efa-only" \
"NetworkCardIndex=22,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType
 or efa-only" \
"NetworkCardIndex=23,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType
 or efa-only" \
"NetworkCardIndex=24,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType
 or efa-only" \
"NetworkCardIndex=25,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType
 or efa-only" \
"NetworkCardIndex=26,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType
 or efa-only" \
```

```
"NetworkCardIndex=27,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType
 or efa-only" \
"NetworkCardIndex=28,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType
 or efa-only" \
"NetworkCardIndex=29,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType
 or efa-only" \
"NetworkCardIndex=30,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType
 or efa-only" \
"NetworkCardIndex=31,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType
 or efa-only"
...
```

Launch templates

Para adicionar EFAs a um modelo de execução usando o console do Amazon EC2

1. Na seção Configurações de rede, expanda Configuração de rede avançada.
2. Para adicionar a interface de rede primária (Interface de rede 1), selecione Adicionar interface de rede e selecione Índice da placa de rede = 0, Índice do dispositivo = 0 e Tipo de interface = EFA com ENA.
3. Para adicionar outras interfaces de rede, selecione Adicionar interface de rede. Para Índice da placa de rede, selecione o próximo índice não utilizado e, em seguida, selecione Índice do dispositivo = 1 e Tipo de interface = EFA com ENA ou somente EFA.

Para adicionar EFAs a um modelo de execução usando o comando create-launch-template

Para`NetworkInterfaces`, especifique o número necessário de interfaces de rede. Para a interface de rede primária, especifique `NetworkCardIndex=0`, `DeviceIndex=0`, e `InterfaceType=efa`. Para qualquer interface de rede adicional, para `NetworkCardIndex` especificar o próximo índice não utilizado,`DeviceIndex=1`, e `InterfaceType=efa` ou`efa-only`.

O trecho a seguir mostra um exemplo com 3 interfaces de rede das 32 interfaces de rede possíveis.

```
"NetworkInterfaces":[
{
  "NetworkCardIndex":0,
  "DeviceIndex":0,
  "InterfaceType": "efa",
```

```
  "AssociatePublicIpAddress":false,
  "Groups":[
    "security_group_id"
  ],
  "DeleteOnTermination":true
},
{
  "NetworkCardIndex": 1,
  "DeviceIndex": 1,
  "InterfaceType": "efa or efa-only",
  "AssociatePublicIpAddress":false,
  "Groups":[
    "security_group_id"
  ],
  "DeleteOnTermination":true
},
{
  "NetworkCardIndex": 2,
  "DeviceIndex": 1,
  "InterfaceType": "efa or efa-only",
  "AssociatePublicIpAddress":false,
  "Groups":[
    "security_group_id"
  ],
  "DeleteOnTermination":true
},
{
  "NetworkCardIndex": 3,
  "DeviceIndex": 1,
  "InterfaceType": "efa or efa-only",
  "AssociatePublicIpAddress":false,
  "Groups":[
    "security_group_id"
  ],
  "DeleteOnTermination":true
}
...
```

Configuração de EFA para instâncias P5 e P5e

As instâncias `p5.48xlarge` e `p5e.48xlarge` oferecem suporte a 32 placas de rede e têm uma capacidade total de largura de banda da rede de 3.200 Gbps, dos quais até 800 Gbps podem

ser utilizados para tráfego de rede IP. Como o tráfego de rede EFA e IP compartilha os mesmos recursos subjacentes, a largura de banda usada por um reduzirá a largura de banda disponível para o outro. Isso significa que você pode distribuir a largura de banda da rede entre o tráfego EFA e o tráfego IP em qualquer combinação, desde que a largura de banda total não exceda 3.200 Gbps e a largura de banda IP não exceda 800 Gbps. Por exemplo, se você usar 400 Gbps para a largura de banda IP, poderá atingir até 2.800 Gbps de largura de banda EFA ao mesmo tempo.

Caso de uso 1: salve endereços IP e evite possíveis problemas de IP do Linux

Essa configuração fornece até 3200 Gbps de largura de banda de rede EFA e até 100 Gbps de largura de banda de rede IP com um endereço IP privado. Essa configuração também ajuda a evitar possíveis problemas de IP do Linux, como atribuição automática não permitida de endereços IP públicos e desafios de roteamento IP (problemas de mapeamento de nome de host para endereço IP e incompatibilidade de endereço IP de origem), que podem surgir se uma instância tiver várias interfaces de rede.

- Para a interface de rede primária (índice da placa de rede 0, índice do dispositivo 0), use uma interface de rede EFA (EFA com ENA).
- Para as demais interfaces de rede (índices da placa de rede de 1 a 31, índice do dispositivo 1), use interfaces de rede somente EFA.

Caso de uso 2: largura de banda máxima de rede EFA e IP

Essa configuração fornece até 3200 Gbps de largura de banda de rede EFA e até 800 Gbps de largura de banda de rede IP com 8 endereços IP privados. Você não pode atribuir automaticamente endereços IP públicos com essa configuração. No entanto, você pode anexar um endereço IP elástico à interface de rede primária (índice da placa de rede 0, índice do dispositivo 0) após a execução para ter conectividade com a Internet.

- Para a interface de rede primária (índice da placa de rede 0, índice do dispositivo 0), use uma interface de rede EFA (EFA com ENA).
- Para as interfaces restantes, faça o seguinte:
  - Especifique interfaces de rede somente EFA nos índices 1, 2 e 3 da placa de rede e use o índice do dispositivo 1.
  - Especifique uma interface de rede EFA (EFA com ENA) e três interfaces de rede somente EFA em cada um dos seguintes subconjuntos de índice de placa de rede, e use o índice do dispositivo 1 em todas elas:

- [4,5,6,7]
- [8,9,10,11]
- [12,13,14,15]
- [16,17,18,19]
- [20,21,22,23]
- [24,25,26,27]
- [28,29,30,31]

O exemplo a seguir ilustra essa configuração:

```
$ aws --region $REGION ec2 run-instances \
 --instance-type p5.48xlarge \
 --count 1 \
 --key-name key_pair_name \
 --image-id ami_id \
 --network-interfaces
 "NetworkCardIndex=0,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
 \
"NetworkCardIndex=1,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=2,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=3,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=4,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
 \
"NetworkCardIndex=5,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=6,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=7,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=8,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
 \
"NetworkCardIndex=9,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=10,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=11,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
```

```
"NetworkCardIndex=12,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
 \
"NetworkCardIndex=13,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=14,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=15,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=16,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
 \
"NetworkCardIndex=17,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=18,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=19,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=20,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
 \
"NetworkCardIndex=21,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=22,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=23,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=24,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
 \
"NetworkCardIndex=25,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=26,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=27,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=28,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
 \
"NetworkCardIndex=29,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=30,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=31,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only"
...
```

Configuração da EFA para instâncias P6-B200

As instâncias P6-B200 têm uma capacidade total de largura de banda da rede de 3.200 Gbps, dos quais até 1600 Gbps podem ser utilizados para ENA. Elas têm 8 GPUs e 8 placas de rede, e cada placa de rede tem capacidade para até 400 Gbps de largura de banda EFA e 200 Gbps de largura de banda ENA. Como tráfego de rede EFA e ENA compartilha os mesmos recursos subjacentes, a largura de banda usada por um reduzirá a largura de banda disponível para o outro.

Caso de uso 1: salvar endereços IP

Essa configuração consome pelo menos um endereço IP privado por instância e tem capacidade para até 3200 Gbps de largura de banda EFA e 200 Gbps de largura de banda ENA.

- Para a interface de rede primária (índice da placa de rede 0, índice do dispositivo 0), use uma interface de rede EFA (EFA com ENA).
- Para as outras 7 placas de rede (índices da placa de rede de 1 a 7, índice do dispositivo 1), use interfaces de rede somente EFA.

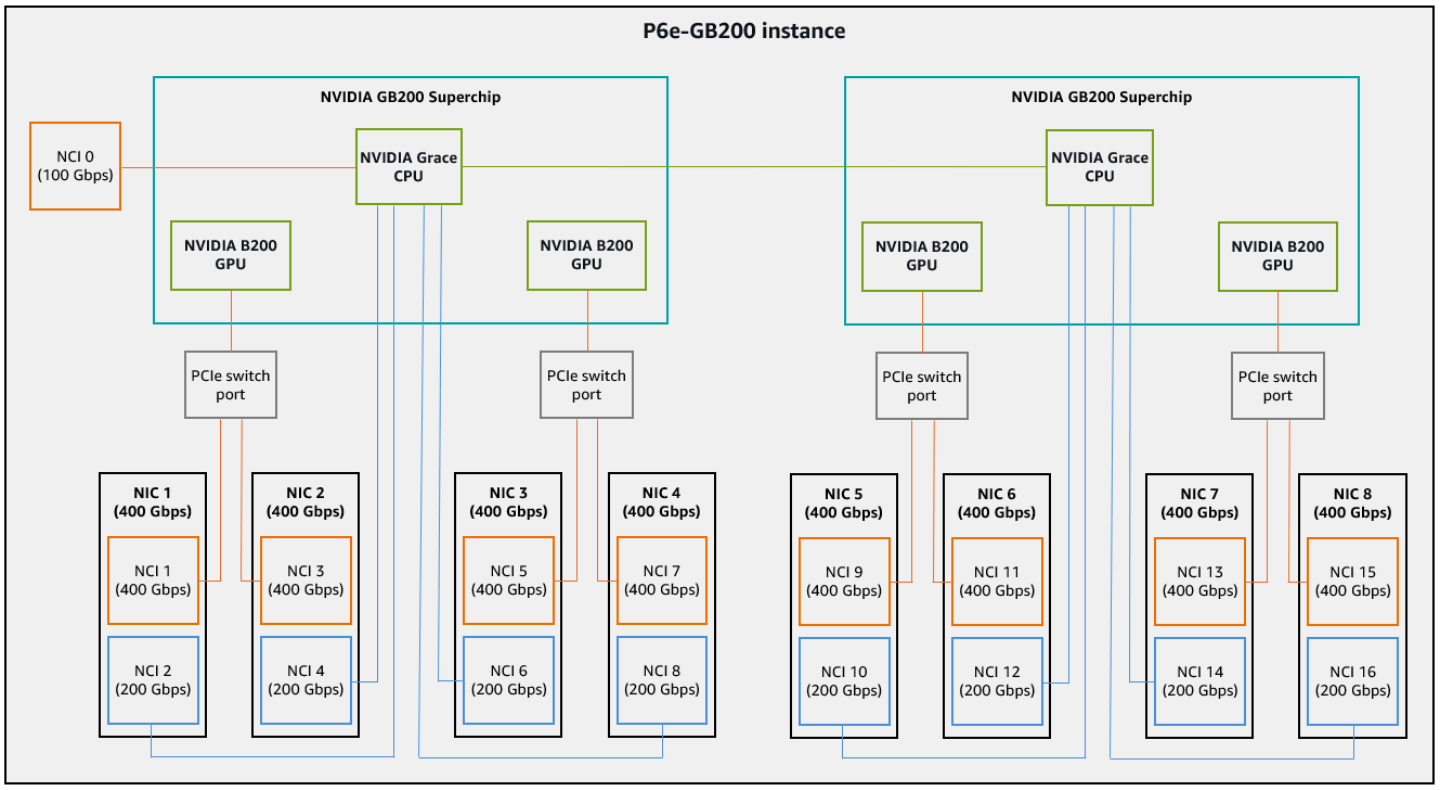
Caso de uso 2: largura de banda máxima para EFA e ENA

Essa configuração consome pelo menos oito endereços IP privados por instância e tem capacidade para até 3200 Gbps de largura de banda EFA e 1600 Gbps de largura de banda ENA.

- Para a interface de rede primária (índice da placa de rede 0, índice do dispositivo 0) e as demais 7 placas de rede (índices da placa de rede 1 a 7, índice do dispositivo 1), use interfaces de rede EFA (EFA com ENA).

Configuração do EFA para instâncias P6e-GB200

As instâncias P6e-GB200 podem ser configuradas com até 17 placas de rede. A imagem a seguir mostra o layout da placa de interface de rede (NIC) física para instâncias P6e-GB200, com o mapeamento dos índices de placa de rede (NCIs).



O NCI primário (índice 0) suporta até 100 Gbps de largura de banda ENA. Os NCIs com os seguintes índices suportam apenas interfaces de rede EFA e largura de banda EFA de 400 Gbps: [1, 3, 5, 7, 9, 11, 13, 15]. Os NCIs com os seguintes índices suportam largura de banda ENA ou EFA de até 200 Gbps: [2, 4, 6, 8, 10, 12, 14, 16].

Os NCIs nos seguintes grupos compartilham um NIC físico subjacente no host:

- [1 e 2]
- [3 e 4]
- [5 e 6]
- [7 e 8]
- [9 e 10]
- [11 e 12]
- [13 e 14]
- [15 e 16]

Cada NIC física suporta até 400 Gbps de largura de banda. Como os NCIs desses grupos compartilham a mesma NIC física subjacente, a largura de banda usada por um reduzirá a largura de

banda disponível para o outro. Por exemplo, se o NCI 2 usar 200 Gbps de largura de banda ENA, o NCI 1 poderá usar até 200 Gbps de largura de banda EFA ao mesmo tempo.

Cada GPU subjacente no host pode enviar tráfego diretamente pelos seguintes pares de NCIs:

- [1 e 3]
- [5 e 7]
- [9 e 11]
- [13 e 15]

Cada GPU suporta até 400 Gbps de largura de banda EFA. Como as placas de rede desses grupos compartilham a mesma GPU, a largura de banda usada por uma reduzirá a largura de banda disponível para a outra. Por exemplo, se o NCI 1 usar 200 Gbps de largura de banda EFA, o NCI 3 poderá usar até 200 Gbps de largura de banda EFA ao mesmo tempo. Portanto, para obter a máxima performance do EFA, recomendamos executar uma das seguintes ações para alcançar um total de 1.600 Gbps de largura de banda EFA:

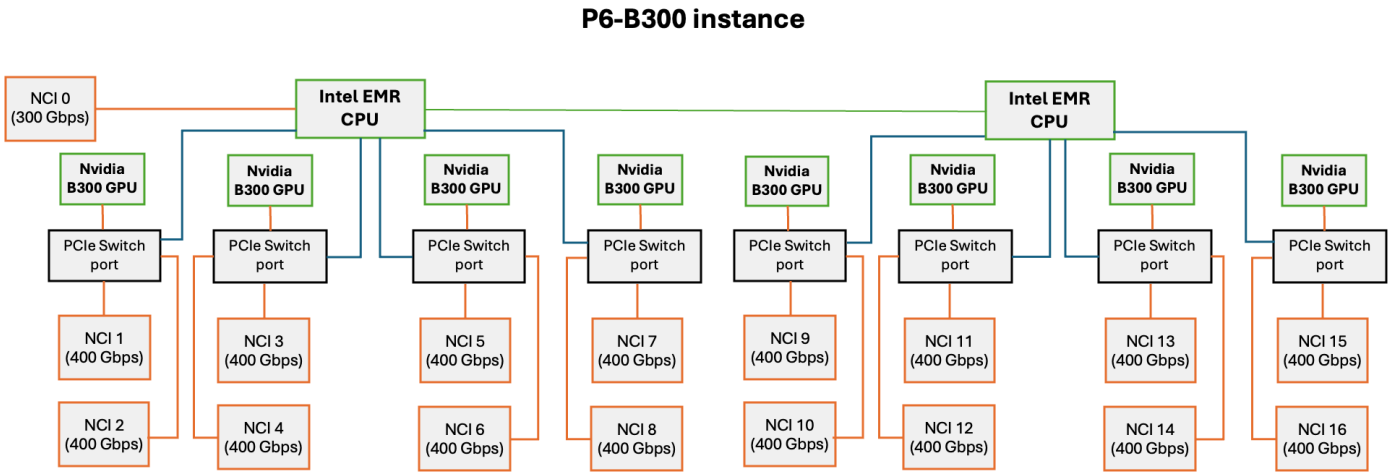
- Adicione uma interface de rede somente EFA a apenas um NCI em cada grupo para obter 400 Gbps por interface de rede (4 interfaces de rede EFA x 400 Gbps).
- Adicione uma interface de rede somente EFA a cada NCI em cada grupo para obter 200 Gbps por interface de rede (8 interfaces de rede EFA x 200 Gbps).

Por exemplo, a configuração a seguir fornece até 1.600 Gbps de largura de banda EFA usando uma única interface de rede somente EFA em cada grupo de NCI, e até 100 Gbps de largura de banda da rede ENA usando somente o NCI primário (índice 0).

- No NCI primário (índice de placa de rede 0, índice de dispositivo 0), use uma interface de rede ENA.
- Adicione interfaces de rede somente EFA aos seguintes índices:
  - NCI 1, índice de dispositivo 0
  - NCI 5, índice de dispositivo 0
  - NCI 9, índice de dispositivo 0
  - NCI 13, índice de dispositivo 0

Configuração da EFA para instâncias P6-B300

As instâncias P6-B300 têm uma capacidade total de largura de banda da rede de até 6400 Gbps para tráfego EFA e até 3870 Gbps para ENA. Elas têm 8 GPUs e 17 placas de rede, em que a placa de rede primária suporta apenas uma interface de rede ENA com até 350 Gbps de largura de banda. As placas de rede secundárias suportam até 400 Gbps EFA e até 220 Gbps de largura de banda ENA. Como tráfego de rede EFA e ENA compartilha os mesmos recursos subjacentes, a largura de banda usada por um reduzirá a largura de banda disponível para o outro.



Caso de uso 1: salvar endereços IP

Essa configuração consome pelo menos um endereço IP privado por instância e tem capacidade para até 6400 Gbps de largura de banda EFA e 350 Gbps de largura de banda ENA.

- Para a interface de rede primária (índice da placa de rede 0, índice do dispositivo 0), use uma interface de rede EFA.
- Para as outras placas de rede (índices da placa de rede de 1 a 16, índice do dispositivo 1), use interfaces de rede somente EFA.

```
--network-interfaces \
"NetworkCardIndex=0,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=int
 \
"NetworkCardIndex=1,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=2,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
```

```
"NetworkCardIndex=3,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=4,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=5,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=6,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=7,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=8,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=9,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=10,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=11,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=12,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=13,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=14,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=15,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=16,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only
```

Caso de uso 2: largura de banda máxima para EFA e ENA

Essa configuração consome pelo menos 17 endereços IP privados por instância e tem capacidade para até 6400 Gbps de largura de banda EFA e até 3870 Gbps de largura de banda ENA.

- Para a interface de rede primária (índice da placa de rede 0, índice do dispositivo 0), use uma interface de rede EFA.
- Para as placas de rede restantes, crie uma interface somente EFA (a placa de rede indexa de 1 a 16 índices de dispositivos (índice 1) e uma interface ENA (a placa de rede indexa de 1 a 16 índices de dispositivos (índice 2).

```
--network-interfaces \
```

```
"NetworkCardIndex=0,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=int
 \
"NetworkCardIndex=1,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=2,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=3,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=4,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=5,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=6,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=7,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=8,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=9,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=10,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=11,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=12,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=13,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=14,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=15,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=16,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=1,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ena
 \
"NetworkCardIndex=2,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ena
 \
"NetworkCardIndex=3,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ena
 \
"NetworkCardIndex=4,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ena
 \
"NetworkCardIndex=5,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ena
 \
```

```
"NetworkCardIndex=6,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ena
 \
"NetworkCardIndex=7,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ena
 \
"NetworkCardIndex=8,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ena
 \
"NetworkCardIndex=9,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ena
 \
"NetworkCardIndex=10,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=en
 \
"NetworkCardIndex=11,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=en
 \
"NetworkCardIndex=12,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=en
 \
"NetworkCardIndex=13,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=en
 \
"NetworkCardIndex=14,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=en
 \
"NetworkCardIndex=15,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=en
 \
"NetworkCardIndex=16,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=en
```

Criar e anexar um Elastic Fabric Adapter a uma instância do Amazon EC2

É possível criar um EFA e anexá-lo a uma instância do Amazon EC2 como qualquer outra interface de rede elástica no Amazon EC2. No entanto, ao contrário das interfaces de rede elástica, os EFAs não podem ser anexados ou desanexados de uma instância em um estado `running`.

Considerações

- É possível alterar o grupo de segurança associado a um EFA. Para habilitar a funcionalidade de desvio do sistema operacional, o EFA deve ser um membro de um grupo de segurança que permita todo o tráfego de entrada e saída de e para o próprio grupo de segurança. Para obter mais informações, consulte Etapa 1: Preparar um grupo de segurança habilitado para EFA.

  É possível alterar o grupo de segurança associado a um EFA da mesma forma como altera o grupo de segurança associado a uma interface de rede elástica. Para obter mais informações, consulte the section called “Modificar atributos da interface de rede”.
- Um endereço Elastic IP (IPv4) e IPv6 foi atribuído a uma interface de rede EFA (EFA com ENA) da mesma forma que um endereço IP foi atribuído a uma interface de rede elástica. Para obter mais informações, consulte Gerenciar endereços IP.

Não é possível atribuir um endereço IP a uma interface de rede exclusivamente EFA.

Tarefas

- Criar um EFA.
- Associar um EFA a uma instância interrompida
- Associar um EFA ao executar uma instância
- Adicionar um EFA a um modelo de execução

Criar um EFA.

É possível criar um EFA em uma sub-rede de uma VPC. Você não pode mover o EFA para outra sub-rede depois que ela é criada e só pode anexá-la a instâncias interrompidas na mesma zona de disponibilidade.

Console

Para criar uma interface de rede EFA (EFA com ENA ou somente ENA)

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Interfaces de rede e, em seguida, selecione Criar interface de rede.
3. Em Description (Descrição), insira um nome descritivo para o EFA.
4. Para Subnet (Sub-rede), selecione a sub-rede na qual criar o EFA.
5. Em Tipo de interface, escolha uma das seguintes opções:
   - EFA com ENA: para criar uma interface de rede que ofereça suporte a dispositivos ENA e EFA.
   - Somente EFA: para criar uma interface de rede somente com um dispositivo EFA.
6. (Somente para EFA com ENA) Configure o endereço IP e a atribuição de prefixo para a interface de rede. Os tipos de endereços IP e prefixos que você pode atribuir dependem da sub-rede selecionada. Para sub-redes somente IPv4, é possível atribuir somente endereços IP e prefixos IPv4. Para sub-redes somente IPv6, é possível atribuir somente endereços IP e prefixos IPv6. Para sub-redes de pilha dupla, é possível atribuir somente endereços IP e prefixos IPv4 e IPv6.

> **Note**
>
> Não é possível atribuir endereços IP a uma interface de rede somente EFA.

a. Em Endereço IPv4 privado e/ou Endereço IPv6, escolha Atribuição automática para que o Amazon EC2 atribua automaticamente um endereço IP da sub-rede selecionada ou escolha Personalizado para especificar manualmente o endereço IP a ser atribuído.

b. Se você atribuir um endereço IPv6, opcionalmente poderá habilitar Atribuir IP IPv6 primário. Fazer isso atribui um endereço unicast global (GUA) IPv6 primário à interface de rede. A atribuição de um endereço IPv6 primário permite evitar a interrupção do tráfego para instâncias ou ENIs. Para obter mais informações, consulte Endereços IPv6.

c. Em Delegação de prefixo IPv4 e/ou Delegação de prefixo IPv6, escolha Atribuição automática para que o Amazon EC2 atribua automaticamente um prefixo de bloco CIDR da sub-rede ou escolha Personalizado para especificar manualmente um prefixo de bloco CIDR da sub-rede. Se você especificar um prefixo, a AWS verificará se ele ainda não está atribuído a outro recurso. Para obter mais informações, consulte . Delegação de prefixo para interfaces de rede do Amazon EC2

d. (Opcional) Configure as opções de Tempo limite de rastreamento de conexão ociosa. Para obter mais informações, consulte . Tempo limite de rastreamento de conexão ociosa

   - Tempo limite para TCP estabelecido: o tempo limite, em segundos, para conexões TCP ociosas em um estado estabelecido. Mín: 60 segundos. Máx: 432.000 segundos (5 dias) Padrão: 432.000 segundos. Recomendado: menos de 432.000 segundos.
   - Tempo limite de UDP: o tempo limite, em segundos, para fluxos UDP ociosos que só observaram tráfego em uma única direção ou uma única transação de solicitação-resposta. Mín: 30 segundos. Máx: 60 segundos. Padrão: 30 segundos.
   - Tempo limite de fluxo UDP: o tempo limite, em segundos, para fluxos UDP ociosos classificados como fluxos que tiveram mais de uma transação de solicitação-resposta. Mín: 60 segundos. Máx: 180 segundos (3 minutos). Padrão: 180 segundos.

7. Para Security groups, selecione um ou mais security groups.
8. Clique em Criar interface de rede.

AWS CLI

Para criar uma EFA

Use o comando create-global-interface. Para `--interface-type`, especifique `efa` para uma interface de rede EFA ou `efa-only` para uma interface de rede somente EFA.

```
aws ec2 create-network-interface \
    --subnet-id subnet-0abcdef1234567890 \
    --interface-type efa \
    --description "my efa"
```

PowerShell

Para criar uma EFA

Use o cmdlet New-EC2NetworkInterface. Para `-InterfaceType`, especifique `efa` para uma interface de rede EFA ou `efa-only` para uma interface de rede somente EFA

```
New-EC2NetworkInterface `
    -SubnetId subnet-0abcdef1234567890 `
    -InterfaceType efa `
    -Description "my efa"
```

Associar um EFA a uma instância interrompida

É possível anexar um EFA a qualquer instância compatível que esteja no estado `stopped`.
É possível anexar um EFA a uma instância que esteja no estado `running`. Para obter mais informações sobre os tipos de instâncias compatíveis, consulte Tipos de instâncias compatíveis.

Anexe um EFA a uma instância da mesma forma como você anexa uma interface de rede a uma instância. Para obter mais informações, consulte Anexar interface de rede.

Associar um EFA ao executar uma instância

AWS CLI

Para anexar um EFA existente ao iniciar uma instância

Use o comando run-instances com a opção `--network-interfaces`. Para a interface de rede primária, especifique uma interface de rede EFA e `NetworkCardIndex=0`, `DeviceIndex=0`. Para conectar diversas interfaces de rede EFA, consulte Maximize a largura de banda da rede.

```
--network-interfaces "NetworkCardIndex=0, \
    DeviceIndex=0, \
    NetworkInterfaceId=eni-1234567890abcdef0, \
    Groups=sg-1234567890abcdef0, \
    SubnetId=subnet-0abcdef1234567890"
```

Para anexar um novo EFA ao iniciar uma instância

Use o comando run-instances com a opção `--network-interfaces`. Para a interface de rede primária, use `NetworkCardIndex=0`, `DeviceIndex=0`, e `InterfaceType=efa`. Caso esteja conectando diversas interfaces de rede EFA, consulte. Maximize a largura de banda da rede.

```
--network-interfaces "NetworkCardIndex=0, \
    DeviceIndex=0, \
    InterfaceType=efa, \
    Groups=sg-1234567890abcdef0, \
    SubnetId=subnet-0abcdef1234567890"
```

PowerShell

Para anexar um EFA existente ao iniciar uma instância

Use o cmdlet New-EC2Instance com o parâmetro `-NetworkInterfaces`.

```
-NetworkInterface $networkInterface
```

Defina a interface de rede conforme mostrado a seguir.

```
$networkInterface = New-Object
 Amazon.EC2.Model.InstanceNetworkInterfaceSpecification
$networkInterface.DeviceIndex = 0
$networkInterface.NetworkInterfaceId = "eni-1234567890abcdef0"
$networkInterface.Groups = @("sg-1234567890abcdef0")
$networkInterface.SubnetId = "subnet-0abcdef1234567890"
```

Para anexar um novo EFA ao iniciar uma instância

Use o cmdlet New-EC2Instance com o parâmetro `-NetworkInterfaces`.

```
-NetworkInterface $networkInterface
```

Defina a interface de rede conforme mostrado a seguir.

```
$networkInterface = New-Object
 Amazon.EC2.Model.InstanceNetworkInterfaceSpecification
$networkInterface.DeviceIndex = 0
$networkInterface.InterfaceType = "efa"
$networkInterface.Groups = @("sg-1234567890abcdef0")
$networkInterface.SubnetId = "subnet-0abcdef1234567890"
```

Adicionar um EFA a um modelo de execução

É possível criar um modelo de execução que contenha informações de configuração necessárias para executar instâncias habilitadas para EFA. É possível especificar interfaces de rede EFA e exclusivamente EFA no modelo de execução. Para criar um modelo de execução habilitado para EFA, crie um novo modelo de execução e especifique um tipo de instância compatível, sua AMI habilitada para EFA e um grupo de segurança habilitado para EFA. Para`NetworkInterfaces`, especifique as interfaces de rede EFA a serem conectadas. Para a interface de rede primária, use `NetworkCardIndex=0`, `DeviceIndex=0`, e `InterfaceType=efa`. Caso esteja conectando diversas interfaces de rede EFA, consulte. Maximize a largura de banda da rede em instâncias do Amazon EC2 com várias placas de rede

É possível aproveitar modelos de inicialização para executar instâncias habilitadas para EFA com outros produtos da AWS, como AWS Batch ou AWS ParallelCluster.

Para obter mais informações sobre como criar modelos do execução, consulte Criar um modelo de execução do Amazon EC2.

Desanexar e excluir um EFA de uma instância do Amazon EC2

É possível desanexar um EFA de uma instância do Amazon EC2 e excluí-lo da mesma forma como qualquer outra interface de rede elástica no Amazon EC2.

Desanexar um EFA

Para desanexar um EFA de uma instância, primeiro é necessário parar a instância. Você não pode desanexar um EFA de uma instância que está em estado de execução.

Você desanexa um EFA de uma instância da mesma maneira como desanexa uma interface de rede elástica de uma instância. Para obter mais informações, consulte Desanexar uma interface de rede.

Excluir um EFA

Para excluir um EFA, é necessário primeiro separá-lo da instância. Você não pode excluir um EFA enquanto está anexado a uma instância.

Você exclui EFAs da mesma maneira como visualiza interfaces de rede elástica. Para obter mais informações, consulte Excluir uma interface de rede.

Monitorar um Elastic Fabric Adapter no Amazon EC2

É possível usar os seguintes recursos para monitorar a performance dos seus Elastic Fabric Adapters.

Tópicos

- Métricas do driver do EFA para uma instância do Amazon EC2
- Logs de fluxo do Amazon VPC
- Amazon CloudWatch

Métricas do driver do EFA para uma instância do Amazon EC2

O driver Elastic Fabric Adapter (EFA) publica, em tempo real, várias métricas das instâncias que têm interfaces EFA anexadas. É possível usar essas métricas para solucionar problemas de performance da aplicação e da rede, escolher o tamanho de cluster ideal para uma workload, planejar proativamente as atividades de escalação e comparar aplicações para determinar se elas maximizam a performance da EFA disponível em uma instância.

Tópicos

- Métricas de driver do EFA disponíveis
- Recupere as métricas do driver EFA para sua instância

Métricas de driver do EFA disponíveis

O driver EFA publica as seguintes métricas para a instância em tempo real. Elas fornecem o número cumulativo de erros, eventos de conexão e pacotes ou bytes enviados, recebidos, retransmitidos

ou descartados pelos dispositivos EFA anexados desde a inicialização da instância ou da última redefinição do driver.

Métrica	Descrição	Tipos de instâncias compatíveis
`tx_bytes`	O número de bytes transmitidos. Unidade: bytes	Todos os tipos de instâncias compatíveis com EFA
`rx_bytes`	O número de bytes recebidos. Unidade: bytes	Todos os tipos de instâncias compatíveis com EFA
`tx_pkts`	O número de pacotes transmitidos. Unidade: contagem	Todos os tipos de instâncias compatíveis com EFA
`rx_pkts`	O número de pacotes recebidos. Unidade: contagem	Todos os tipos de instâncias compatíveis com EFA
`rx_drops`	O número total de pacotes recebidos e depois descartados. Unidade: contagem	Todos os tipos de instâncias compatíveis com EFA
`send_bytes`	O número de bytes enviados usando operações de envio. Unidade: bytes	Todos os tipos de instâncias compatíveis com EFA
`recv_bytes`	O número de bytes recebidos pelas operações de envio. Unidade: bytes	Todos os tipos de instâncias compatíveis com EFA

Métrica	Descrição	Tipos de instâncias compatíveis
`send_wrs`	O número de pacotes enviados usando operações de envio. Unidade: contagem	Todos os tipos de instâncias compatíveis com EFA
`recv_wrs`	O número de pacotes recebidos pelas operações de envio. Unidade: contagem	Todos os tipos de instâncias compatíveis com EFA
`rdma_write_wrs`	O número de operações de gravação de rdma concluídas. Unidade: contagem	Todos os tipos de instâncias compatíveis com EFA
`rdma_read_wrs`	O número de operações de leitura de rdma concluídas. Unidade: contagem	Todos os tipos de instâncias compatíveis com EFA
`rdma_write_bytes`	O número de bytes gravados nele por outras instâncias usando operações de gravação de rdma. Unidade: bytes	Todos os tipos de instâncias compatíveis com EFA
`rdma_read_bytes`	O número de bytes recebidos usando operações de leitura de rdma. Unidade: bytes	Todos os tipos de instâncias compatíveis com EFA

Métrica	Descrição	Tipos de instâncias compatíveis
`rdma_write_wr_err`	O número de operações de gravação de rdma que tiveram erros locais ou remotos. Unidade: contagem	Todos os tipos de instâncias compatíveis com EFA
`rdma_read_wr_err`	O número de operações de leitura de rdma que tiveram erros locais ou remotos. Unidade: contagem	Todos os tipos de instâncias compatíveis com EFA
`rdma_read_resp_bytes`	O número de bytes enviados em resposta às operações de leitura de rdma. Unidade: bytes	Todos os tipos de instâncias compatíveis com EFA
`rdma_write_recv_bytes`	O número de bytes recebidos pelas operações de gravação de rdma. Unidade: bytes	Todos os tipos de instâncias compatíveis com EFA
`retrans_bytes`	O número de bytes EFA SRD retransmitidos. Unidade: contagem	Tipos de instância do Nitro v4 e posteriores que são compatíveis com EFA
`retrans_pkts`	O número de pacotes EFA SRD retransmitidos. Unidade: bytes	Tipos de instância do Nitro v4 e posteriores que são compatíveis com EFA

Métrica	Descrição	Tipos de instâncias compatíveis
`retrans_timeout_events`	O número de vezes que o tráfego de EFA SRD atingiu o tempo limite e resultou em uma alteração no caminho de rede. Unidade: contagem	Tipos de instância do Nitro v4 e posteriores que são compatíveis com EFA
`impaired_remote_conn_events`	O número de vezes que as conexões EFA SRD entraram em um estado comprometido, resultando em um limite de taxa de throughput reduzido. Unidade: contagem	Tipos de instância do Nitro v4 e posteriores que são compatíveis com EFA
`unresponsive_remote_events`	O número de vezes que uma conexão remota EFA SRD deixou de responder. Unidade: contagem	Tipos de instância do Nitro v4 e posteriores que são compatíveis com EFA

Para obter mais informações sobre os tipos de instâncias que são compatíveis com EFA, consulte Tipos de instâncias compatíveis.

Recupere as métricas do driver EFA para sua instância

É possível usar a ferramenta de linha de comando rdma-tool para recuperar as métricas de todas as interfaces do EFA anexadas a uma instância da seguinte forma:

```
$ rdma -p statistic show
link rdmap0s31/1
    tx_bytes 0
    tx_pkts 0
    rx_bytes 0
    rx_pkts 0
    rx_drops 0
    send_bytes 0
    send_wrs 0
```

```
    recv_bytes 0
    recv_wrs 0
    rdma_read_wrs 0
    rdma_read_bytes 0
    rdma_read_wr_err 0
    rdma_read_resp_bytes 0
    rdma_write_wrs 0
    rdma_write_bytes 0
    rdma_write_wr_err 0
    retrans_bytes 0
    retrans_pkts 0
    retrans_timeout_events 0
    unresponsive_remote_events 0
    impaired_remote_conn_events 0
```

Você também pode recuperar as métricas de cada interface do EFA anexada a uma instância dos arquivos sys usando o comando a seguir.

```
$ more /sys/class/infiniband/device_number/ports/port_number/hw_counters/* | cat
```

Por exemplo

```
$ more /sys/class/infiniband/rdmap0s31/ports/1/hw_counters/* | cat
::::::::::::::
/sys/class/infiniband/rdmap0s31/ports/1/hw_counters/lifespan
::::::::::::::
12
::::::::::::::
/sys/class/infiniband/rdmap0s31/ports/1/hw_counters/rdma_read_bytes
::::::::::::::
0
::::::::::::::
/sys/class/infiniband/rdmap0s31/ports/1/hw_counters/rdma_read_resp_bytes
::::::::::::::
0
::::::::::::::
/sys/class/infiniband/rdmap0s31/ports/1/hw_counters/rdma_read_wr_err
::::::::::::::
0
::::::::::::::
/sys/class/infiniband/rdmap0s31/ports/1/hw_counters/rdma_read_wrs
::::::::::::::
0
```

```
::::::::::::::
/sys/class/infiniband/rdmap0s31/ports/1/hw_counters/rdma_write_bytes
::::::::::::::
0
::::::::::::::
/sys/class/infiniband/rdmap0s31/ports/1/hw_counters/rdma_write_recv_bytes
::::::::::::::
0
::::::::::::::
/sys/class/infiniband/rdmap0s31/ports/1/hw_counters/rdma_write_wr_err
::::::::::::::
0
::::::::::::::
/sys/class/infiniband/rdmap0s31/ports/1/hw_counters/rdma_write_wrs
::::::::::::::
0
::::::::::::::
/sys/class/infiniband/rdmap0s31/ports/1/hw_counters/recv_bytes
::::::::::::::
0
::::::::::::::
/sys/class/infiniband/rdmap0s31/ports/1/hw_counters/recv_wrs
::::::::::::::
0
::::::::::::::
/sys/class/infiniband/rdmap0s31/ports/1/hw_counters/rx_bytes
::::::::::::::
0
::::::::::::::
/sys/class/infiniband/rdmap0s31/ports/1/hw_counters/rx_drops
::::::::::::::
0
::::::::::::::
/sys/class/infiniband/rdmap0s31/ports/1/hw_counters/rx_pkts
::::::::::::::
0
::::::::::::::
/sys/class/infiniband/rdmap0s31/ports/1/hw_counters/send_bytes
::::::::::::::
0
::::::::::::::
/sys/class/infiniband/rdmap0s31/ports/1/hw_counters/send_wrs
::::::::::::::
0
```

```
::::::::::::::
/sys/class/infiniband/rdmap0s31/ports/1/hw_counters/tx_bytes
::::::::::::::
0
::::::::::::::
/sys/class/infiniband/rdmap0s31/ports/1/hw_counters/tx_pkts
::::::::::::::
0
::::::::::::::
/sys/class/infiniband/rdmap0s31/ports/1/hw_counters/retrans_bytes
::::::::::::::
0
/sys/class/infiniband/rdmap0s31/ports/1/hw_counters/retrans_pkts
::::::::::::::
0
/sys/class/infiniband/rdmap0s31/ports/1/hw_counters/retrans_timeout_events
::::::::::::::
0
/sys/class/infiniband/rdmap0s31/ports/1/hw_counters/unresponsive_remote_events
::::::::::::::
0
/sys/class/infiniband/rdmap0s31/ports/1/hw_counters/impaired_remote_conn_events
::::::::::::::
0
```

Logs de fluxo do Amazon VPC

É possível criar um log de fluxo da Amazon VPC para capturar informações sobre o tráfego de entrada e saída de um EFA. Os dados de log de fluxo podem ser publicados no Amazon CloudWatch Logs e no Amazon S3. Após criar um log de fluxo, será possível recuperar e visualizar seus dados no destino selecionado. Para obter mais informações, consulte Logs de fluxo da VPC no Guia do usuário da Amazon VPC.

Você cria um log de fluxo para um EFA da mesma forma como cria um log de fluxo para uma interface de rede elástica. Para mais informações, consulte Criar um log de fluxo no Guia do usuário da Amazon VPC.

Nas entradas do log de fluxo, o tráfego do EFA é identificado por `srcAddress` e `destAddress`, ambos formatados como endereços MAC, conforme mostrado no exemplo a seguir.

```
version accountId  eniId        srcAddress        destAddress       sourcePort destPort
 protocol packets bytes start      end        action log-status
```

```
2       3794735123 eni-10000001 01:23:45:67:89:ab 05:23:45:67:89:ab -          -
 -        9       5689  1521232534 1524512343 ACCEPT OK
```

Amazon CloudWatch

Se você estiver usando o EFA em um cluster do Amazon EKS, poderá monitorar seus EFAs usando o CloudWatch Container Insights. O Amazon CloudWatch Container Insights é compatível com todas as métricas de driver EFA, exceto: `retrans_bytes`, `retrans_pkts`, `retrans_timeout_events`, `unresponsive_remote_events` e `impaired_remote_conn_events`.

Para obter mais informações, consulte Métricas do Amazon EKS e Kubernetes Container Insights no Guia do usuário do Amazon CloudWatch.

Verificar o instalador EFA usando uma soma de verificação

Como opção, é possível verificar o tarball EFA (arquivo `.tar.gz`) usando uma soma de verificação MD5 ou SHA256. Recomendamos que você faça isso para verificar a identidade do fornecedor do software e para verificar se a aplicação não foi alterada ou corrompida desde que foi publicada.

Como verificar o tarball

Use o utilitário md5sum para a soma de verificação MD5 ou o utilitário sha256sum para a soma de verificação SHA256 e especifique o nome do arquivo tarball. Execute o comando a partir do diretório no qual salvou o arquivo tarball.

- MD5

```
$  md5sum tarball_filename.tar.gz
```

- SHA256

```
$  sha256sum tarball_filename.tar.gz
```

Os comandos devem retornar um valor de soma de verificação no formato a seguir.

```
checksum_value tarball_filename.tar.gz
```

Compare o valor de soma de verificação retornado pelo comando com o valor de soma de verificação fornecido na tabela abaixo. Se as somas de verificação corresponderem, então é seguro

executar o script de instalação. Se as somas de verificação não corresponderem, não execute o script de instalação e entre em contato com o Suporte.

Por exemplo, o comando a seguir verifica o tarball EFA 1.9.4 usando a soma de verificação SHA256.

```
$  sha256sum aws-efa-installer-1.9.4.tar.gz
```

Resultado do exemplo:

```
1009b5182693490d908ef0ed2c1dd4f813cc310a5d2062ce9619c4c12b5a7f14 aws-efa-
installer-1.9.4.tar.gz
```

A tabela a seguir lista as somas de verificação para versões recentes do EFA.

Versão	Somas de verificação
EFA 1.47.0	MD5: c81d4caf24dabc04a6e4818590620f5f SHA256: 2df4201e046833c7dc8160907bee7f52b76ff80ed147376a2d0ed8a0dd66b2db
EFA 1.46.0	MD5:a88bbd9b71624d7ca401b54bc2fc0c19 SHA256: 8302bd7849afb95c903a875d7dcb6f85b3d7629e9a8b67d020031cfc6f4d0ee1
EFA 1.45.1	MD5: 91c3c87e16bbcaca1513252c38b771bb SHA256: 9aeb20c645135b6039cc08986d8f14e63280f7839e882a74df5e83627ffeaa17
EFA 1.45.0	MD5:800aeddfa9d9c5f139a7b8f7c4fec627 SHA256: 25ba26a0877fe3317390dc126aad2f23e27fc461cf0b940004f032cb342fa539

Versão	Somas de verificação
EFA 1.44.0	MD5:d024f6bebe080db42745103b84ca7c43 SHA256: f129a5b44a49d593d2 47e55a59eb9bcb57121566e1c2e 42b832a4e794fa83d8a
EFA 1.43.3	MD5: 4dbc6eeecc516760253c10cbedb 6319d SHA256: 6c470ebce254c71653 47b5048895ac2996c8856727164 2297f4c597738300652
EFA 1.43.2	MD5: 7287b25a07c9747c0d4001e8fc5 f59b2 SHA256: de15c5bdbc83b952af bde876110830c604ad0796680e5 157c05f7c1979a41069
EFA 1.43.1	MD5: 7cfafc8debaea51dd4966fa0b2b ba673 SHA256:54211eda0c193138ee8ed09b5fb 41c41fc76fe0a77935fa4ec8d989466342740
EFA 1.43.0	MD5: f2b3dd7dc8670b541f7c23fd58e 5e503 SHA256: 786df3458c499237be 33bb8e50ffd4da7c18c20e25438 0ffc80fb90833d8cc73

Versão	Somas de verificação
EFA 1.42.0	MD5: 94b2b1db09da1dde08ec049db1f24370 SHA256: 4114fe612905ee05083ae5cb391a00a012510f3abfecc642d86c9a5ae4be9008
EFA 1.41.0	MD5: 086181c3ee3f8da512fc6e1c795e8936 SHA256: 3506354cdfbe31ff552fe75f5d0d9bb7efd29cf79bd99457347d29c751c38f9f
EFA 1.40.0	MD5: f3ec6f73fbeaccba082327507581157c SHA256: 30491b0fe7c3470d4439594538855c981b05fa69862d74f8c05eb9b97912368a
EFA 1.39.0	MD5: c223d5954a85a7fbcd248c942b866e43 SHA256: 2cbc028c03064633bb990782b47c36156637769e2f48704417a9c700a7a32101
EFA 1.38.1	MD5: f112569e828ab65187777f794bab542c SHA256: 83923374afd388b1cfcf4b3a21a2b1ba7cf46a01a587f7b519b8386cb95e4f81

Versão	Somas de verificação
EFA 1.38.0	MD5: 43a2a446b33a2506f40853d55059f1ea SHA256: 4f436954f35ad53754b4d005fd8d0be63de3b4184de41a695b504bdce0fecb22
EFA 1.37.0	MD5: 6328070192bae920eca45797ad4c1db1 SHA256: 2584fc3c8bb99f29b3285e275747ff09d67c18e162c2a652e36c976b72154bfb
EFA 1.36.0	MD5: 1bec83180fbffb23452ab6469ca21dfa SHA256: de183f333cfb58aeb7908a67bf9106985ba3ccb7f8638b851d2a0d8dbfacaec4
EFA 1.35.0	MD5: 252f03c978dca5f8e8d9f34e488b256e SHA256: 432b6ad4368ba0cd8b902729d14a908a97be7a3dcc5239422ea994a47f35a5e1
EFA 1.34.0	MD5: 5cd4b28d27a31677c16139b54c9acb45 SHA256: bd68839e741b0afd3ec2e37d50603803cfa7a279c120f0a736cc57c2ff2d7fdc

Versão	Somas de verificação
EFA 1.33.0	MD5: e2f61fccbcaa11e2ccfddd3660522276 SHA256: 0372877b87c6a7337bb7791d255e1053b907d030489fb2c3732ba70069185fce
EFA 1.32.0	MD5: db8d65cc028d8d08b5a9f2d88881c1b1 SHA256: 5f7233760be57f6fee6de8c09acbfbf59238de848e06048dc54d156ef578fc66
EFA 1.31.0	MD5: 856352f12bef2ccbadcd75e35aa52aaf SHA256: 943325bd37902a4300ac9e5715163537d56ecb4e7b87b37827c3e547aa1897bf
EFA 1.30.0	MD5: 31f48e1a47fe93ede8ebd273fb747358 SHA256: 876ab9403e07a0c3c91a1a34685a52eced890ae052df94857f6081c5f6c78a0a
EFA 1.29.1	MD5: e1872ca815d752c1d7c2b5c175e52a16 SHA256: 178b263b8c25845b63dc93b25bcdff5870df5204ec509af26f43e8d283488744

Versão	Somas de verificação
EFA 1.29.0	MD5: 39d06a002154d94cd982ed348133f385 SHA256: 836655f87015547e733e7d9f7c760e4e24697f8bbc261bb5f3560abd4206bc36
EFA 1.28.0	MD5: 9dc13b7446665822605e66febe074035 SHA256: 2e625d2d6d3e073b5178e8e861891273d896b66d03cb1a32244fd56789f1c435
EFA 1.27.0	MD5: 98bfb515ea3e8d93f554020f3837fa15 SHA256: 1d49a97b0bf8d964d91652a79ac851f2550e33a5bf9d0cf86ec9357ff6579aa3
EFA 1.26.1	MD5: 884e74671fdef4725501f7cd2d451d0c SHA256: c616994c924f54ebfabfab32b7fe8ac56947fae00a0ff453d975e298d174fc96
EFA 1.26.0	MD5: f8839f12ff2e3b9ba09ae8a82b30e663 SHA256: bc1abc1f76e97d204d3755d2a9ca307fc423e51c63141f798c2f15be3715aa11

Versão	Somas de verificação
EFA 1.25.1	MD5: 6d876b894547847a45bb8854d4431f18 SHA256: d2abc553d22b89a4ce92882052c1fa6de450d3a801fe005da718b7d4b9602b06
EFA 1.25.0	MD5: 1993836ca749596051da04694ea0d00c SHA256: 98b7b26ce031a2d6a93de2297cc71b03af647194866369ca53b60d82d45ad342
EFA 1.24.1	MD5: 211b249f39d53086f3cb0c07665f4e6f SHA256: 120cfeec233af0955623ac7133b674143329f9561a9a8193e473060f596aec62
EFA 1.24.0	MD5: 7afe0187951e2dd2c9cc4b572e62f924 SHA256: 878623f819a0d9099d76ecd41cf4f569d4c3aac0c9bb7ba9536347c50b6bf88e
EFA 1.23.1	MD5: 22491e114b6ee7160a8290145dca0c28 SHA256: 5ca848d8e0ff4d1571cd443c36f8d27c8cdf2a0c97e9068ebf000c303fc40797

Versão	Somas de verificação
EFA 1.23.0	MD5: `38a6d7c1861f5038dba4e441ca7683ca` SHA256: `555d497a60f22e3857fdeb3dfc53aa86d05926023c68c916d15d2dc3df6525bd`
EFA 1.22.1	MD5: `600c0ad7cdbc06e8e846cb763f92901b` SHA256: `f90f3d5f59c031b9a964466b5401e86fd0429272408f6c207c3f9048254e9665`
EFA 1.22.0	MD5: `8f100c93dc8ab519c2aeb5dab89e98f8` SHA256: `f329e7d54a86a03ea51da6ea9a5b68fb354fbae4a57a02f9592e21fce431dc3a`
EFA 1.21.0	MD5: `959ccc3a4347461909ec02ed3ba7c372` SHA256: `c64e6ca34ccfc3ebe8e82d08899ae8442b3ef552541cf5429c43d11a04333050`
EFA 1.20.0	MD5: `7ebfbb8e85f1b94709df4ab3db47913b` SHA256: `aeefd2681ffd5c4c631d1502867db5b831621d6eb85b61fe3ec80df983d1dcf0`

Versão	Somas de verificação
EFA 1.19.0	MD5: 2fd45324953347ec5518da7e3fefa0ec SHA256: 99b77821b9e72c8dea015cc92c96193e8db307deee05b91a58094cc331f16709
EFA 1.18.0	MD5: fc2571a72f5d3c7b7b576ce2de38d91e SHA256: acb18a0808aedb9a5e485f1469225b9ac97f21db9af78e4cd6939700debe1cb6
EFA 1.17.3	MD5: 0517df4a190356ab559235147174cafd SHA256: 5130998b0d2883bbae189b21ab215ecbc1b01ae0231659a9b4a17b0a33ebc6ca
EFA 1.17.2	MD5: a329dedab53c4832df218a24449f4c9a SHA256: bca1fdde8b32b00346e175e597ffab32a09a08ee9ab136875fb38283cc4cd099
EFA 1.17.1	MD5: 733ae2cfc9d14b52017eaf0a2ab6b0ff SHA256: f29322640a88ae9279805993cb836276ea240623820848463ca686c8ce02136f

Versão	Somas de verificação
EFA 1.17.0	MD5: d430fc841563c11c3805c5f82a4746b1 SHA256: 75ab0cee4fb6bd38889dce313183f5d3a83bd233e0a6ef6205d8352821ea901d
EFA 1.16.0	MD5: 399548d3b0d2e812d74dd67937b696b4 SHA256: cecec36495a1bc6fdc82f97761a541e4fb6c9a3cbf3cfcb145acf25ea5dbd45b
EFA 1.15.2	MD5: 955fea580d5170b05823d51acde7ca21 SHA256: 84df4fbc1b3741b6c073176287789a601a589313accc8e6653434e8d4c20bd49
EFA 1.15.1	MD5: c4610267039f72bbe4e35d7bf53519bc SHA256: be871781a1b9a15fca342a9d169219260069942a8bda7a8ad06d4baeb5e2efd7
EFA 1.15.0	MD5: 9861694e1cc00d884fadac07d22898be SHA256: b329862dd5729d2d098d0507fb486bf859d7c70ce18b61c302982234a3a5c88f

Versão	Somas de verificação
EFA 1.14.1	MD5: `50ba56397d359e57872fde1f74d4168a` SHA256: `c7b1b48e86fe4b3eaa4299d3600930919c4fe6d88cc6e2c7e4a408a3f16452c7`
EFA 1.14.0	MD5: `40805e7fd842c36ececb9fd7f921b1ae` SHA256: `662d62c12de85116df33780d40e0533ef7dad92709f4f613907475a7a1b60a97`
EFA 1.13.0	MD5: `c91d16556f4fd53becadbb345828221e` SHA256: `ad6705eb23a3fce44af3afc0f7643091595653a723ad0374084f4f2b715192e1`
EFA 1.12.3	MD5: `818aee81f097918cfaebd724eddea678` SHA256: `2c225321824788b8ca3fbc118207b944cdb096b847e1e0d1d853ef2f0d727172`
EFA 1.12.2	MD5: `956bb1fc5ae0d6f0f87d2e481d49fccf` SHA256: `083a868a2c212a5a4fcf3e4d732b685ce39cceb3ca7e5d50d0b74e7788d06259`

Versão	Somas de verificação
EFA 1.12.1	MD5: `f5bfe52779df435188b0a2874d0633ea` SHA256: `5665795c2b4f09d5f3f767506d4d4c429695b36d4a17e5758b27f033aee58900`
EFA 1.12.0	MD5: `d6c6b49fafb39b770297e1cc44fe68a6` SHA256: `28256c57e9ecc0b0778b41c1f777a9982b4e8eae782343dfe1246079933dca59`
EFA 1.11.2	MD5: `2376cf18d1353a4551e35c33d269c404` SHA256: `a25786f98a3628f7f54f7f74ee2b39bc6734ea9374720507d37d3e8bf8ee1371`
EFA 1.11.1	MD5: `026b0d9a0a48780cc7406bd51997b1c0` SHA256: `6cb04baf5ffc58ddf319e956b5461289199c8dd805fe216f8f9ab8d102f6d02a`
EFA 1.11.0	MD5: `7d9058e010ad65bf2e14259214a36949` SHA256: `7891f6d45ae33e822189511c4ea1d14c9d54d000f6696f97be54e915ce2c9dfa`

Versão	Somas de verificação
EFA 1.10.1	MD5: 78521d3d668be22976f46c6fecc7b730 SHA256: 61564582de7320b21de319f532c3a677d26cc46785378eb3b95c636506b9bcb4
EFA 1.10.0	MD5: 46f73f5a7afe41b4bb918c81888fefa9 SHA256: 136612f96f2a085a7d98296da0afb6fa807b38142e2fc0c548fa986c41186282
EFA 1.9.5	MD5: 95edb8a209c18ba8d250409846eb6ef4 SHA256: a4343308d7ea4dc943ccc21bcebed913e8868e59bfb2ac93599c61a7c87d7d25
EFA 1.9.4	MD5: f26dd5c350422c1a985e35947fa5aa28 SHA256: 1009b5182693490d908ef0ed2c1dd4f813cc310a5d2062ce9619c4c12b5a7f14
EFA 1.9.3	MD5: 95755765a097802d3e6d5018d1a5d3d6 SHA256: 46ce732d6f3fcc9edf6a6e9f9df0ad136054328e24675567f7029edab90c68f1

Versão	Somas de verificação
EFA 1.8.4	MD5: `85d594c41e831afc6c9305263140457e` SHA256: `0d974655a09b213d7859e658965e56dc4f23a0eee2dc44bb41b6d039cc5bab45`

Observações sobre o Elastic Fabric Adapter

A tabela a seguir descreve o histórico de versões e o registro de alterações do software Elastic Fabric Adapter.

Versão	Alterações	Data de lançamento

1.47.0	• Atualização para libfabric 2.4.0amzn1.0
	  • Refatorar o gerenciamento de pares: mova o endpoint→ hashmap do peer para o nível AV
	  • Adicionar um contador de geração de entrada de pacotes para evitar problemas de ABA
	  • Implementar o suporte de bloqueio de leitura de CQ (fi_cq_sread) com objetos de espera
	  • Corrigir o livre dobrado no processamento de pacotes RTM eager/mulreq/longread
	  • Corrigir sinalizadores de acesso IBV de registro de RM com base nos recursos RDMA do dispositivo
	  • Desativar FI_OPT_EFA_SENDRECV_IN_ORDER_ALIGNED_128_BYTES (retorna -FI_EOPNOTSUPP)
		29 de janeiro de 2026

Versão	Alterações	Data de lançamento
	• Otimizar a entrada de pacotes para caber em duas linhas de cache x86 (128 bytes) • Janela efa_rdm_srx_start e slide recv sempre bem-sucedida em erros de RTM/RTA • Desvincular as entradas do pacote RX antes de liberá-las durante a limpeza do endpoint • Atualização para libnccl-ofi 1.18.0 • Suporte ao P6-B300: decisões de sintonizador personali zadas adicionadas para o P6-B300 • Desempenho aprimorado do PAT no P6-B200, reduzindo o número de canais para tamanhos menores de mensagens • Padrões de protocolo alterados, padrão para o protocolo RDMA em Trn1 e padrão para o protocolo SENDRECV em g7e.8xlarge • Seleção dinâmica de plataforma: atributo adicionado para permitir otimizações da AWS em runtime com base na presença de NICs da AWS. Isso permite que um único binário de plug-in seja usado tanto para plataformas da AWS quanto para outras plataformas que não são da AWS. As otimizações da AWS ainda podem ser desativadas em tempo de compilação. • Suporte corrigido para provedores diferentes de FI_MR_Vir t_Addr no protocolo RDMA • Relatórios aprimorados de velocidade e largura do link NIC PCIe para NCCL •	

Versão	Alterações	Data de lançamento
	Modelo de encadeamento redesenhado para oferecer suporte a aplicações com vários encadeamentos sem exigir um domínio Libfabric diferente para cada encadeamento. • Suporte corrigido para provedores FI_MR_ENDPOINT (suporte somente para protocolo SENDRECV) limpando os recursos na ordem correta • Atualização para rdma-core 61.0 • Usar CQ de thread único se o domínio de thread tiver sido fornecido • Verificar o número QP nos processos CQE • Atualização para driver do efa 3.0.0 • Melhorar o tratamento de erros do administrador • Verificar a exatidão do número QP ao concluir a pesquisa • Remover o backport incondicional de descoberta do melhor tamanho de página • Imprimir strings errno para ponteiros de erro • Simplificar o código nos fluxos de criação de CQ • Alterações de backport upstream no CQ com fluxo de criação umem • Ajustar a configuração do DKMS para novas versões do DKMS • Atualização para Open MPI 5.0.9amzn1 •	

Versão	Alterações	Data de lançamento
	Correção de erro: defina o nível de segmentação do domínio com base no suporte de encadeamento MPI • Correção de erro: solicite o sinalizador FI_COMPLETION para garantir que as conclusões sejam geradas para todos os eventos de transferência de dados • Compartilhe domínios entre BTL e MTL para reduzir o número total de domínios criados para corrigir o esgotamento de recursos em sistemas com alto número de núcleos	
1.46.0	• Adição de compatibilidade com o Debian 13 • Atualização para efa-nv-peermem 1.2.3 • Correção de erros e avisos de compilação com novos kernels e DKMS • Atualização para libfabric 2.3.1amzn4.0 • Habilita o caminho de dados direto para o caminho do protocolo efa-rdm • Habilita a compatibilidade com ROCr HMEM • Nova opção FI_OPT_EFA_USE_UNSOLICITED_WRITE_RECV para desativar o recebimento de gravações não solicitadas • Otimização do tempo de estabelecimento da conexão • Adição de libnccl-ofi no RHEL 9, Rocky Linux 9 e Debian 13	12 de dezembro de 2025

Versão	Alterações	Data de lançamento
1.45.1	• Atualização para libfabric 2.3.1amzn3.0 • Corrija o bug que truncava cq_data para 2 bytes enquanto o provedor anunciava suporte para 4 bytes	26 de novembro de 2025

Versão	Alterações	Data de lançamento

1.45.0	• Atualização para rdma-core 60.amzn0
	  • Estenda a consulta DV CQ para retornar a campainha
	• Atualização para libfabric 2.3.1amzn2.0
	  • Ofereça suporte ao modo FI_RX_CQ_DATA para efa-direct
	  • Otimize a postagem do WQE no caminho direto do caminho de dados
	  • Corrija a condição de corrida no progresso do cntr
	  • Melhore o registro de mensagens de aviso
	  • Lida corretamente com o preenchimento de RMA para pares removidos
	  • Expulse as entradas AH do AV implícito quando o limite de AH for atingido
	• Atualização para libnccl-ofi 1.17.2
	  • Correção de uma falha com o NCCL v2.28.x quando a inicialização do Libfabric falhou
	  • Adição de suporte à família de instâncias g7e
	  • Correção de um problema em que a NCCL poderia tentar erroneamente usar um caminho RDMA GPUDirect em plataformas que suportam DMA-BUF
	  •
		17 de novembro de 2025

Versão	Alterações	Data de lançamento
	Correção de um problema de pedido de desligamento em NICs que exigem registro de memória por endpoint (Cray Slingshot)	

Versão	Alterações	Data de lançamento

1.44.0	• Atualização para rdma-core 59.amzn0
	  • Adição de suporte à vinculação de QPs e CQs a domínios de threads
	  • Adição de suporte à alocação de um domínio principal
	  • Adição de suporte à alocação de domínios de threads
	  • Adição de suporte às consultas de verbos diretos de QP e CQ
	  • Adição da opção para criar CQ com memória externa
	  • Correção da sondagem de CQ após destruição de QP
	• Atualização para libfabric 2.3.1amzn1.0
	• Atualização para Open MPI 5.0.8amzn1
	  • Melhorias de funcionalidade
	  • Correções de erros
	• Atualização para libnccl-ofi 1.17.1
	  • Compatível com a NCCL v2.28.3-1, mantendo compatibilidade reversa com a NCCL v2.17.1 e posteriores.
	  • A compilação com platform-aws requer a Libfabric v1.22.0amzn4.0 ou superior. Testes realizados com versões até Libfabric v2.3.1amzn1.0.
	  •
		29 de outubro de 2025

Versão	Alterações	Data de lançamento
	Correções para garantir compatibilidade entre as versões CUDA 12 e CUDA 13.	

1.43.3	• Atualização para efa driver 2.17.3
	  • Suporte P2P com drivers NVIDIA 580
	  • Ajuste do registro de MR para kernels 6.17 e posteriores
		1.º de outubro de 2025

1.43.2	• Atualização para libnccl-ofi 1.16.3
	  • Compatível com a NCCL v2.27.7-1, mantendo compatibilidade reversa com a NCCL v2.17.1 e posteriores.
	  • A compilação com platform-aws requer a Libfabric v1.22.0amzn4.0 ou superior. Testado com versões até a Libfabric 2.1.0amzn5.0.
	  • Habilite domain-per-thread por padrão em todos os tipos de instância do Amazon EC2 para melhorar a performance de algumas aplicações em que a NCCL cria vários threads de proxy
		15 de agosto de 2025

Versão	Alterações	Data de lançamento

1.43.1	• Atualização para libnccl-ofi 1.16.2
	  • Compatível com a NCCL v2.27.6-1, mantendo a compatibilidade reversa com a NCCL v2.17.1 e posteriores.
	  • A compilação com platform-aws requer a Libfabric v1.22.0amzn4.0 ou superior. Testado com versões até a Libfabric 2.1.0amzn4.0.
	  • Adicionada uma nova configuração de plataforma para permitir o uso do plug-in OFI NCCL no tipo de instância p5.4xlarge do Amazon EC2.
	• Atualização para libfabric 2.1.0amzn5.0
		31 de julho de 2025

Versão	Alterações	Data de lançamento

1.43.0	• Atualização para libnccl-ofi 1.16.1
	  • Compatível com a NCCL v2.27.6-1, mantendo a compatibilidade reversa com a NCCL v2.17.1 e posteriores.
	  • A compilação com platform-aws requer a Libfabric v1.22.0amzn4.0 ou superior. Testado com as versões até a Libfabric 2.1.0amzn3.
	  • Atualização para o formato de velocidade de link PCI informado no arquivo de topologia para corresponder ao kernel 5.7+.
	  • Adicionado SKIP_NICS_WITHOUT_ACCEL_AT_SAME_PCI_LEVEL para ignorar as nics libfabric que não tenham um acelerador no mesmo nível de pci.
	• Atualização para efa driver 2.17.2
	• Atualização para efa-nv-peermem 1.2.2
	• Atualização para libfabric 2.1.0amzn4.0
	• Atualização para rdma-core 58.amzn0
	  • Correção de uso duplo do índice de solicitações de trabalho
	  • Adição de comprimento de WQE ao tracepoint post_send
	• Habilitar otimizações para plataformas Graviton
	• Descontinuar o suporte para o Ubuntu 20.04
		25 de julho de 2025

Versão	Alterações	Data de lançamento

1.42.0	• Atualização para efa driver 2.15.3
	• Atualização para efa-nv-peermem 1.2.1
	• Atualização para rdma-core 57.amzn1
	  • Correção de uso duplo do índice de solicitações de trabalho
	• Atualização para libfabric 2.1.0amzn3.0
	• Atualização para libnccl-ofi 1.15.0
	  • Compatível com a NCCL 2.26.6-1, mantendo a compatibilidade reversa com a NCCL v2.17.1 e posteriores.
	  • A compilação com platform-aws requer a Libfabric v1.22.0amzn4.0 ou superior. Testado com as versões até a Libfabric 2.1.0amzn3.
	  • Compatibilidade com sistema e plataforma de compilação
	  • Adicionada compatibilidade com a plataforma Amazon EC2 P6-B200
	  • Alterado o nome da biblioteca de plugins padrão para libnccl-net-ofi.so e, por padrão, criação de um link simbólico de libnccl-net-ofi.so para libnccl-net.so para manter a compatibilidade reversa. Isso permite que os usuários definam NCCL_NET_PLUGIN=OFI para forçar a NCCL a usar o plug-in OFI para comunicação. Especificação de --disable-nccl-net-symlink para configurar ignorará o link simbólico, permitindo que vários plug-ins sejam instalados no mesmo contêiner.
	  • Sintonização e melhorias de performance
	  • Adicionada compatibilidade com sintonizador na plataforma P6-B200 para as regiões AllReduce, AllGather e ReduceScatter para máscaras de bits 0x0 e 0x7
		6 de junho de 2025

Versão	Alterações	Data de lançamento
	• Atualizada a latência padrão para as plataformas P5en e P6-B200 com base em resultados e análises empíricos • Atualização para usar a NCCL v10 API com compatibilidade com o parâmetro trafficClass para futura priorização de tráfego • Migrada a base de código de plugin de C para C++ • Adicionada compatibilidade com trabalhos em que o número de NICs por GPU é diferente entre os sistemas. Consulte a documentação da variável de ambiente de runtime OFI_NCCL_FORCE_NUM_RAILS para obter mais informações.	
1.41.0	• Atualização para o rdma-core 57.amzn0	16 de maio de 2025
1.40.0	• Atualização para o libfabric 2.1.0amzn2.0 • Atualização para o rdma-core 56.0 • Atualização para o efa-config 1.18. • Descontinuação da compatibilidade com o Debian 10 • Atualização para o libnccl-ofi 1.14.2 • Habilitação de compatibilidade com o Libfabric no ARM para Ubuntu e no Amazon Linux 2023 • Adição do libnccl-ofi no ARM para o Ubuntu e o Amazon Linux 2023	2 de maio de 2025
1.39.0	• Atualização para o libfabric 2.1.0 • Atualização para a Open MPI para a versão 5.0.6 • Atualização para o libnccl-ofi 1.14.1 • Atualização para o driver de efa 2.15.0	16 de abril de 2025
1.38.1	• Atualização para o `Libfabric 1.22.0amzn5.0`	3 de março de 2025

Versão	Alterações	Data de lançamento
1.38.0	• Adicionar `libnccl-ofi 1.13.2-1`	8 de janeiro de 2025
1.37.0	• Atualização para o `libfabric 1.22.0amzn4.0` • Atualização para o `rdma-core 54.amzn0`	18 de novembro de 2024
1.36.0	• Adição de compatibilidade com o Debian 12 • Distribuição do `efa_test.sh` como um script utilitário em `/opt/amazon/efa/bin` • Atualização para o driver de efa 2.13.0 • Atualização para o `libfabric 1.22.0amzn3.0` • Atualização para o `rdma-core 54.0` • Atualização para a open mpi 4.1.7	7 de novembro de 2024
1.35.0	• Atualização para a Open MPI 5.0.5 • Atualização para o PRRTE 3.0.6 e renomeação do pacote do RPM para prrte-aws • Renomeação do pacote do RPM da OpenPMIx para pmix-aws • Configuração das opções de compilação para as compilações de dpkg e RPM • Atualização para o `Libfabric 1.22.0amzn2.0` • Atualização para o driver do efa 2.12.1	14 de outubro de 2024
1.34.0	• Eliminação da compatibilidade com o CentOS 7 e o RHEL 7 • Ingestão do `Libfabric 1.22.0amzn1.0` • Atualização do pacote de efa-config para a versão 1.17	6 de agosto de 2024

Versão	Alterações	Data de lançamento
1.33.0	• Atualização para o driver do efa 2.10.0 • Atualização para o `rdma-core 52.0` • Atualização para o PRRTE 3.0.5 • Atualização para a Open MPI 5.0.3 • Adição de compatibilidade com o Ubuntu 24.04 LTS • Remoção da documentação do OpenPMIx, do PRRTE e da Open MPI. Os usuários devem consultar o site oficial. • Eliminação de compatibilidade com o openSUSE 15.4 ou anterior	20 de junho de 2024
1.32.0	• Atualização para o driver do efa 2.8.0 • Atualização para o driver do efa-nv-peermem 1.1.1 • Atualização do pacote de efa-config para a versão 1.16 • Atualização do pacote do efa-profile para a versão 1.7 • Atualização para o `rdma-core 50.0` • Atualização para o `libfabric 1.21.0amzn1.0` • Aprimoramento da `efa_test.sh` com a seleção da porta `fi_pingpong` • Instalação do mais novo rdma-core do sistema quando necessário	18 de abril de 2024
1.31.0	• Atualização para a OpenPMIx 4.2.8 • Atualização para o PRRTE 3.0.3 • Atualização para a Open MPI 5.0.2 e conversão de componentes do MCA para o DSO. • Atualização para o `Libfabric 1.20.1amzn1.0`	7 de março de 2024

Versão	Alterações	Data de lançamento
1.30.0	• Inclusão da OpenPMIx 4.2.7, instalado em `/opt/amazon/pmix` por padrão • Inclusão do PRRTE 3.0.2, instalado em `/opt/amazon/prrte` por padrão • Inclusão da Open MPI 5.0.0, instalado em `/opt/amazon/openmpi5` por padrão • Atualização do efa-profile para a versão 1.6	Dezembro de 2023
1.29.1	• Ingestão do `libfabric 1.19.0amzn4.0`	Dezembro de 2023
1.29.0	• Ingestão do driver de kernel do efa 2.6.0 • Ingestão do `libfabric 1.19.0amzn3.0`	Novembro de 2023
1.28.0	• Atualização da Open MPI para a versão 4.1.6 • Ingestão do `libfabric 1.19.0amzn2.0`	Outubro de 2023
1.27.0	• Adição do `Libfabric 1.19.0amzn1.0` ao programa de instalação • Habilitação dos atômicos integrados do GCC para a Open MPI 4	Setembro de 2023
1.26.1	• `efa_test.sh` : correção do bug de repetição infinita	Setembro de 2023
1.26.0	• Adição de compatibilidade com o RHEL9 • Correção da compilação de depuração em distribuições múltiplas • Ingestão do `libfabric 1.18.2amzn1.0` • `efa_test.sh` : adição de nova tentativa para `fi_pingpong`	Setembro de 2023

Versão	Alterações	Data de lançamento
1.25.1	• Ingestão do `libfabric 1.18.1amzn1.0` • Atualização dos tempos limite nos scripts de instalação de EFA	Setembro de 2023
1.25.0	• Adição de compatibilidade com o Amazon Linux 2023 • Correção de bug nos testes pós-instalação	Julho de 2023
1.24.1	• Atualização do libfabric para a versão 1.18.1 • Atualização do driver de efa para a versão 2.5.0	Julho de 2023
1.24.0	• Ingestão do `rdma-core 46.0` • Ingestão o driver de efa 2.4.1 • Compatibilidade com Debian 11	Junho de 2023
1.23.1	• Ingestão do `libfabric 1.18.0amzn2.0`	Junho de 2023
1.23.0	• Adição de compatibilidade com o Debian 10 • Eliminação de compatibilidade com o Ubuntu 18.04 LTS • Atualização do pacote de efa-config para a versão 1.14 • Ingestão do `libfabric 1.18.0amzn1.0`	Maio de 2023
1.22.1	• Atualização do libfabric para a versão 1.17.1	Março de 2023
1.22.0	• Atualização da Open MPI para a versão 4.1.5 • Atualização do libfabric para a versão 1.17.0 • Atualização do pacote de efa-config para a versão 1.13	Fevereiro de 2023

Versão	Alterações	Data de lançamento
1.21.0	• Adição de compatibilidade com o sistema operacional Rocky Linux 9 • Ingestão do driver de efa 2.1.1 • Ingestão do `libfabric 1.16.1amzn3.0` • Atualização do pacote de efa-config para a versão 1.12	Dezembro de 2022
1.20.0	• Adição de compatibilidade com o sistema operacional Rocky Linux 8. • Ingestão do driver de efa 2.1.0. • Ingestão do `rdma-core 43.0`. • Ingestão do `libfabric 1.16.1amzn1.0`	Novembro de 2022
1.19.0	• Ingestão do `libfabric 1.16.0` • Compilação da Open MPI com `--enable-orterun-prefix-by-default`	Outubro de 2022
1.18.0	• Adição de compatibilidade com o Ubuntu22.04	Agosto de 2022
1.17.3	• Atualização do libfabric para a versão `1.16.0~amzn4.0` . O ~ indica que essa é uma versão pré-lançamento do libfabric 1.16.0. • Extensão do tempo limite dos testes de pingue-pongue pós-instalação para 20 segundos	Agosto de 2022
1.17.2	• Atualização do libfabric para a versão `1.16.0~amzn3.0` . O ~ indica que essa é uma versão pré-lançamento do libfabric 1.16.0.	Julho de 2022

Versão	Alterações	Data de lançamento
1.17.1	• Atualização do libfabric para a versão `1.16.0~amzn2.0` . O ~ indica que essa é uma versão pré-lançamento do libfabric 1.16.0. • Desabilitação do provedor de rede experimental ao compilar o libfabric	Julho de 2022
1.17.0	• Atualização do `rdma-core` para a versão v41.0 • Atualização da Open MPI para a versão 4.1.4 • Atualização do libfabric para a versão `1.16.0~amzn1.0` . O ~ indica que essa é uma versão pré-lançamento do libfabric 1.16.0.	Julho de 2022
1.16.0	• Atualização do libfabric para a versão `1.15.1amzn1.0` , contém a alteração do nome da biblioteca neuron • Atualização para o efa-config 1.10 • Exclusão dos provedores opx e rxd na compilação do libfabric	Junho de 2022
1.15.2	• Atualização do libfabric para a versão 1.14.1	Maio de 2022
1.15.1	• Atualização do libfabric para a versão `1.14.0amzn1.0`	Março de 2022
1.15.0	• Correção de um bug que causa falha na instalação no openSUSE 15.3 • Eliminação de compatibilidade com o Open SuSE 15.2 (pois o Open SuSE 15.2 atingiu o fim da vida útil) • Eliminação de compatibilidade com o CentOS 8 (pois o CentOS 8 atingiu o fim da vida útil) • Atualização do libfabric para a versão 1.14.0 • Atualização do driver de kernel do efa para 1.16.0 • Atualização do `rdma-core` para a versão v39.0 • Atualização da Open MPI para a versão 4.1.2.	Fevereiro de 2022

Versão	Alterações	Data de lançamento
1.14.1	• Atualização do libfabric para a versão `1.13.2amzn1.0` .	Outubro de 2021
1.14.0	• Ingestão do driver de kernel do efa 1.14.2. • Transformação de `-g, --enable-gdr` no `efa_installer.sh` em opção não operacional, pois o driver de kernel do efa mais recente habilita a compatibilidade com GDR por padrão. • Ingestão do `rdma-core v37.0`. • Ingestão do `libfabric 1.13.2`. • Adição da lista de pacotes e comparação do RPM/DEB com a lista durante a instalação para evitar instalações de pacotes desconhecidos. • Adição de sleep no script de instalação para aguardar a aplicação da regra de udev após o driver de EFA ser recarregado.	Outubro de 2021
1.13.0	• Atualização do `rdma-core` para a versão v35.0. • Atualização do `libfabric` para a versão v1.13.0amzn1.0. • Adição de compatibilidade com o EFA para o CentOS/RHEL 8 na plataforma Graviton2. • Adição da lógica de comparação de versões no script de instalação para a instalação de pacote local ser pulada quando já houver um pacote de uma versão superior instalado.	Agosto de 2021
1.12.3	• Atualização do módulo de kernel do EFA para a versão 1.13.0. • Atualização do pacote de efa-config para a versão 1.9. Aprimoramento do cálculo da reserva de páginas muito grandes para lidar com tamanhos de páginas grandes usadas por padrão.	Julho de 2021

Versão	Alterações	Data de lançamento
1.12.2	• Atualização do módulo de kernel do EFA para 1.12.3. • Compilação de pacotes da Open MPI para debian com `--with-libevent=external` e `--with-hwloc=external` . • Aumento do ID de compilação do rpm do Open MPI rpm para 2 para corrigir o problema de compatibilidade retroativa do HWLOC no CentOS 8. • Remoção da instalação de pacotes do kernel-devel e kernel-source no SLES15SP2 e no openSUSE 15.2.	Junho de 2021
1.12.1	• Atualização do Libfabric para a versão 1.11.2amzon1.1. • Atualização do módulo de kernel do EFA para a versão 1.12.1.	Maio de 2021

Versão	Alterações	Data de lançamento
1.12.0	• Atualização da Open MPI para a versão 4.1.1. • Atualização do Libfabric para a versão 1.11.2amzn1.0. • Compilação do rdma-core para o Amazon Linux 2 usando a mesma configuração de empacotamento que o AL2 rdma-core. • Não forçar `-Wl,--enable-new-dtags` ao compilar RPMs da Open MPI. • Compilação da Open MPI com bibliotecas de sistema para o hwloc e o libevent. • Atualização do módulo de kernel do EFA para a versão 1.12.0 • Atualização do pacote de efa-config para a versão 1.8. Aprimoramento do cálculo de reserva de páginas muito grandes para instâncias de longa duração. • Atualização do pacote do efa-profile para a versão 1.5. Remoção do arquivo de ajuste de coletivos da Open MPI que funcionava como uma solução alternativa para corrigir o travamento da Open MPI 4.1.0 no P4d. • Atualização do `rdma-core` para a versão v32.1. • Eliminação da compatibilidade com o Amazon Linux 1 e o Ubuntu 16.04.	Maio de 2021
1.11.2	• Correção do travamento da Open MPI ao usar a Open MPI no P4d alterando o algoritmo padrão usado para implementar MPI_BARRIER por meio de um arquivo de configuração. • Desativação do uso de atomics integrados na Open MPI no ARM via `--disable-builtin-atomics` para contornar o problema do compilador.	Fevereiro de 2021

Versão	Alterações	Data de lançamento
1.11.1	• Atualização da Open MPI para a versão 4.1.0. • Atualização do pacote de efa-config para a versão 1.7. Aprimoramento do cálculo de número de reservas de páginas muito grandes. • Atualização do pacote do efa-profile para a versão 1.3. Remoção do arquivo de decisão de coletivos desnecessários agora que a Open MPI 4.1.0 é usada.	Dezembro de 2020
1.11.0	• Adição de compatibilidade com a plataforma Graviton2. • Atualização do `rdma-core` para a versão 31.2amzn. • Atualização do Libfabric para a versão 1.11.1amzn1.0. • Atualização do efa-config para a versão 1.6. • Atualização do efa-profile para a versão 1.2.	Dezembro de 2020
1.10.1	• Adição de compatibilidade com o CentOS/RHEL 8. • Adição de compatibilidade com o Ubuntu 20.04. • Adição de compatibilidade com o SUSE Linux Enterprise 15.	Novembro de 2020
1.10.0	• Adição de compatibilidade com o GPUDirect RDMA para a plataforma P4d. Uso da opção `--enable-gdr` do programa de instalação para instalar um módulo de kernel e um espaço de usuário que reconhecem GDR. • Atualização do módulo de kernel do EFA para a versão 1.10.2. • Atualização do `rdma-core` para a versão 31.amzn0. • Atualização do Libfabric para a versão 1.11.1. • Atualização da Open MPI para a versão 4.0.5. • Atualização do efa-config para a versão 1.5. • Atualização do efa-profile para a versão 1.1. Inclui o arquivo de decisão de coletivos da Open MPI aprimorado.	Outubro de 2020

Versão	Alterações	Data de lançamento
1.9.5	• Atualização do efa-config para a versão 1.4. Corrige o bug no arquivo de decisão coletiva da Open MPI.	Setembro de 2020
1.9.4	• Atualização da Open MPI para a versão 4.0.3. • Atualização do Libfabric para a versão 1.10.1amazon1.1. • Atualização do `rdma-core` para a versão 28.amzn0.	Julho de 2020
1.9.3	• Atualização do módulo de kernel do EFA para a versão 1.6.0. • Atualização do `rdma-core` para a versão 28.amzn0. • Atualização do Libfabric para a versão 1.10.1amzn1.1. • Atualização do efa-config para a versão 1.3. Adição do arquivo de ajuste de coletivos da Open MPI. • Não instalação do dkms se ele já estiver instalado. • Correção do modo de instalação do `--skip-kmod` para de fato funcionar.	Junho de 2020
1.8.4	• Mudança dos arquivos de configuração para os pacotes do efa-config e efa-profile para que sejam rastreados pelo gerenciador de pacotes do sistema operacional. • Atualização da Open MPI para a versão 4.0.3.	Abril de 2020
1.8.3	• Atualização do módulo de kernel do EFA para a versão 1.5.1. • DKMS distribuído em algumas plataformas em vez do uso de repositórios EPEL, para aumentar a confiabilidade da instalação. • No RHEL 7, instalação de RPMs compilados no CentOS 7 em vez de RPMs compilados no Amazon Linux 2.	Fevereiro de 2020
1.8.2	• Reversão do `rdma-core` para a versão 25 devido a uma incompatibilidade de nomenclatura de dispositivo entre o módulo de kernel e o `rdma-core` .	Janeiro de 2020

Versão	Alterações	Data de lançamento
1.8.1	• Atualização do Libfabric para a versão 1.9.0amzn1.1.	Janeiro de 2020
1.8.0	• Atualização do `rdma-core` para a versão 27.0. • Atualização do módulo de kernel do EFA para a versão 1.5.0. • Atualização do Libfabric para a versão 1.9.0amzn1.0. • Adição da opção `--minimal` para instalar apenas o módulo de kernel do EFA e o `rdma-core` .	Dezembro de 2019
1.7.1	• Atualização do Libfabric para a versão 1.8.1amzn1.3.	Dezembro de 2019
1.7.0	• Adição do arquivo do módulo Libfabric. • Atualização do Libfabric para a versão 1.8.1amzn1.1.	Novembro de 2019
1.6.2	• Atualização da Open MPI para a versão 1.6.2.	Outubro de 2019
1.6.1	• Atualização do Libfabric para a versão 1.8.1amzn1.0. • Atualização da Open MPI para a versão 4.0.1. • Atualização do `rdma-core` para a versão 26.0.	Outubro de 2019
1.5.4	• Atualização do módulo de kernel do EFA para a versão 1.4.1.	Setembro de 2019
1.5.3	• Atualização do módulo de kernel do EFA para a versão 1.3.1. • Não instalação dos pacotes de `kernel-devel` ou `linux-headers` , a menos que esteja instalando o driver de kernel.	Setembro de 2019
1.5.1	• Configuração de páginas muito grandes apenas quando o dispositivo EFA estiver presente.	Agosto de 2019
1.5.0	• Atualização do Libfabric para a versão 1.8.0amzn1.1. • Atualização do `rmda-core` para a versão 25.0.	Agosto de 2019

Versão	Alterações	Data de lançamento
1.4.1	• Adição dos caminhos das bibliotecas Libfabric e Open MPI (`/opt/amazon/efa/lib64` e `/opt/amazon/efa/openmpi/lib`) ao `/etc/ld.so.conf.d/efa.conf` para garantir que as bibliotecas compartilhadas Open MPI e Libfabric estejam localizadas corretamente.	Julho de 2019
1.4.0	• Atualização do módulo de kernel do EFA para a versão 1.3.0. • Atualização do Libfabric para a versão 1.8.0amzn1.0 • Primeira versão compatível com o Intel MPI 2019 Atualização 4.	Julho de 2019

Topologia do Amazon EC2

A topologia do Amazon EC2 fornece uma visão hierárquica da proximidade relativa da capacidade de computação. Essas informações podem ser usadas para gerenciar, de forma escalável, a infraestrutura de computação voltada para computação de alta performance (HPC), machine learning (ML) e IA generativa.

APIs disponíveis

O Amazon EC2 fornece duas APIs para auxiliar na compreensão da topologia do EC2:

- DescribeInstanceTopology
  - Mostra a localização das instâncias em execução na hierarquia da rede, apresentando como elas se relacionam entre si.
  - Auxilia na otimização da execução das workloads nas instâncias existentes.
- DescribeCapacityReservationTopology
  - Mostra a localização relativa da capacidade reservada em relação às demais capacidades na hierarquia da rede antes de iniciar novas instâncias.
  - Auxilia no planejamento da capacidade, permitindo que você saiba a localização da capacidade reservada antes de iniciar instâncias.

Benefícios principais

A topologia do EC2 fornece os seguintes benefícios principais:

- Gerenciamento de capacidade: otimize o uso de recursos.
- Agendamento de trabalhos: tome decisões informadas sobre a alocação de workloads.
- Classificação de nós: compreenda a proximidade relativa para garantir a otimização da performance em instâncias fortemente acopladas.

Considerações

- Os tipos de visualização de topologia estão disponíveis somente para:
  - Instâncias no estado `running`
  - Reservas de capacidade no estado `pending` ou `active`
- Cada visualização de topologia é exclusiva para cada conta da Conta da AWS.
- Não é possível visualizar a topologia com o Console de gerenciamento da AWS.
- Embora as informações de topologia ajudem na compreensão do posicionamento das instâncias, você não pode usá-las para iniciar uma nova instância fisicamente próxima a uma instância existente. Para influenciar o posicionamento da instância, você pode criar reservas de capacidade em grupos de posicionamento de cluster.

Preços

Você pode descrever a topologia do EC2 sem incorrer em custos adicionais.

Conteúdo

- Funcionamento da topologia do Amazon EC2
- Pré-requisitos para a topologia do Amazon EC2
- Exemplos de topologia de instância do Amazon EC2

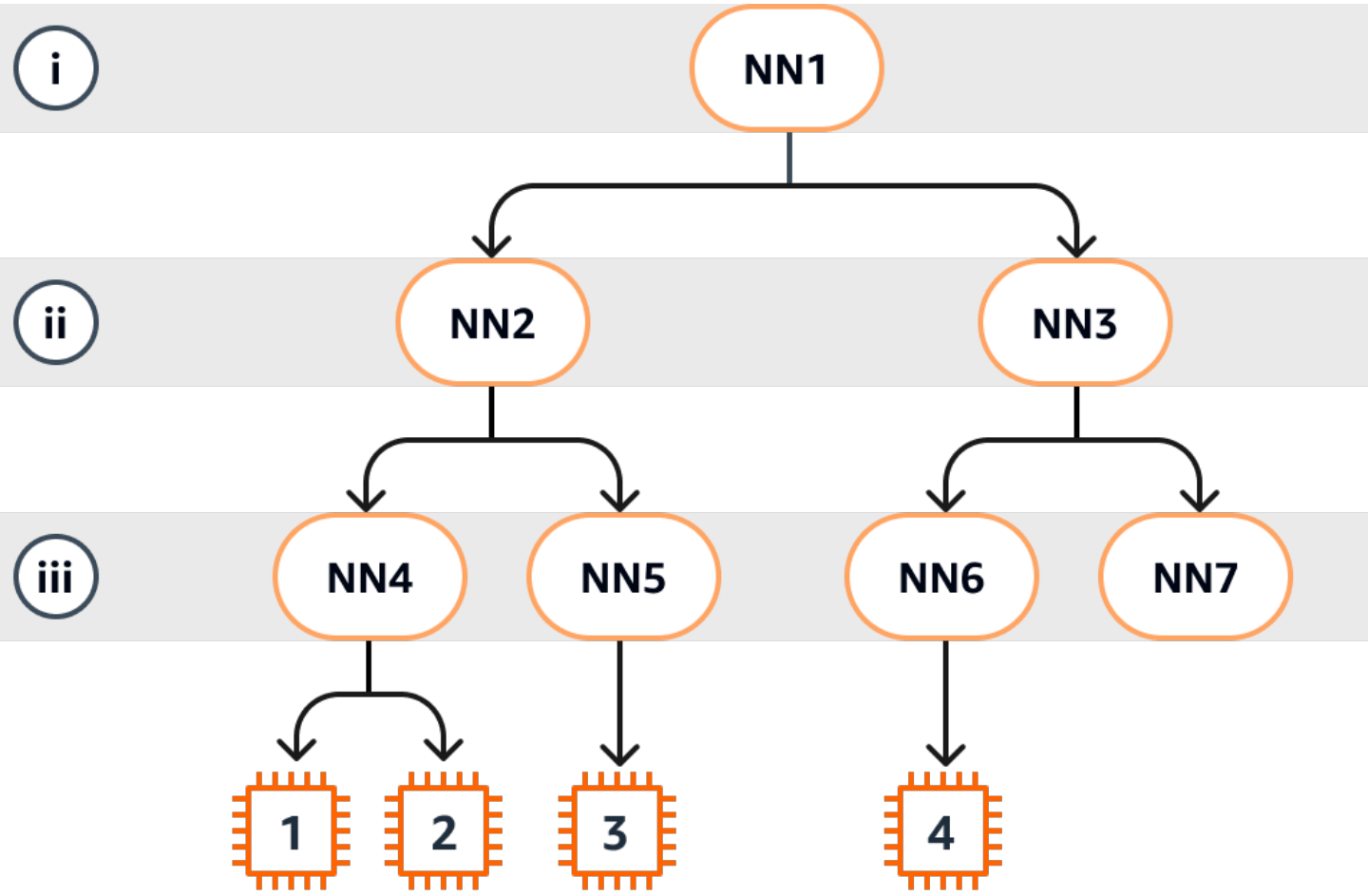
Funcionamento da topologia do Amazon EC2

A rede da AWS é organizada em uma hierarquia de camadas. As instâncias do EC2 se conectam à rede na terceira camada ou abaixo dela, dependendo do tipo de instância. A topologia de uma instância é descrita por um conjunto de nós, com um nó em cada camada da rede. O conjunto de

nós na resposta das APIs DescribeInstanceTopology ou DescribeCapacityReservationTopology fornece uma representação hierárquica da rede de cima para baixo, com o nó inferior conectado a uma instância.

> **Note**
>
> Alguns tipos de instâncias incluem quatro nós de rede em um conjunto de nós, representando quatro camadas na rede, enquanto outros compreendem três nós de rede, representando três camadas da rede. Para obter os tipos de instância compatíveis, consulte Tipos de instância.
> Conforme o tipo de reserva de capacidade, podem ser exibidos apenas um, dois ou três nós de rede.

O diagrama apresentado a seguir fornece uma representação visual que você pode usar para compreender a topologia do EC2. Os nós da rede são identificados como NN1 – NN7. Os números i, ii e iii identificam as camadas de rede. Os números 1, 2, 3 e 4 identificam as instâncias do EC2. As instâncias se conectam a um nó na camada inferior, identificado por iii no diagrama a seguir. Mais de uma instância podem se conectar ao mesmo nó.



Neste exemplo:

- A instância 1 se conecta ao nó de rede 4 (NN4) na camada iii. O NN4 se conecta ao nó de rede 2 (NN2) na camada ii e o NN2 se conecta ao nó de rede 1 (NN1) na camada i, que é o topo da hierarquia da rede neste exemplo. O conjunto de nós de rede compreende NN1, NN2 e NN4, expressos hierarquicamente das camadas superiores até a camada mais inferior.
- A instância 2 também se conecta ao nó de rede 4 (NN4). A instância 1 e a instância 2 compartilham o mesmo conjunto de nós de rede: NN1, NN2 e NN4.
- A instância 3 se conecta ao nó de rede 5 (NN5). O nó NN5 se conecta ao nó NN2, e o nó NN2 se conecta ao nó NN1. O conjunto de nós de rede para a instância 3 é NN1, NN2 e NN5.
- A instância 4 se conecta ao nó de rede 6 (NN6). Seu conjunto de nós de rede é NN1, NN3 e NN6.

Ao considerar a proximidade das instâncias 1, 2 e 3, as instâncias 1 e 2 estão mais próximas uma da outra porque se conectam ao mesmo nó de rede (NN4), enquanto a instância 3 está mais distante porque se conecta a um nó de rede diferente (NN5).

Ao considerar a proximidade de todas as instâncias neste diagrama, as instâncias 1, 2 e 3 estão mais próximas umas das outras do que da instância 4 porque compartilham NN2 em seu conjunto de nós de rede.

Como regra geral, se o nó de rede conectado a quaisquer duas instâncias for o mesmo, essas instâncias estarão fisicamente próximas uma da outra, como é o caso das instâncias 1 e 2. Além disso, quanto menor o número de saltos entre os nós de rede, mais próximas umas das outras as instâncias estão. Por exemplo, as instâncias 1 e 3 têm menos saltos para um nó de rede comum (NN2) do que para o nó de rede (NN1) que têm em comum com a instância 4 e, portanto, estão mais próximas umas das outras do que da instância 4.

Não há instâncias sendo executadas no nó de rede 7 (NN7) neste exemplo e, portanto, a saída da API não incluirá NN7.

Como interpretar a saída DescribeInstanceTopology

É possível descrever a topologia da instância usando a API DescribeInstanceTopology. A saída fornece uma visão hierárquica da topologia de rede subjacente de uma instância.

O exemplo de saída a seguir corresponde às informações de topologia de rede das quatro instâncias no diagrama anterior. Os comentários são incluídos na saída do exemplo para os propósitos deste exemplo.

É importante observar as seguintes informações na saída:

- `NetworkNodes` descreve o conjunto de nós de rede de uma única instância.
- Em cada conjunto de nós de rede, os nós de rede são listados em ordem hierárquica de cima para baixo.
- O nó de rede conectado à instância é o último nó de rede na lista (a camada inferior).
- Para descobrir quais instâncias estão próximas umas das outras, primeiro encontre os nós de rede comuns na camada inferior. Se não houver nós de rede comuns na camada inferior, encontre nós de rede comuns nas camadas superiores.

Na saída de exemplo a seguir, `i-1111111111example` e `i-2222222222example` estão localizadas mais próximas uma da outra em comparação com as outras instâncias neste exemplo porque elas têm o nó de rede `nn-4444444444example` em comum na camada inferior.

> **Note**
>
> A resposta contém três nós de rede ou mais. Para obter informações sobre o número de nós de rede na resposta para cada tipo de instância compatível, consulte Tipos de instância.

```
{
    "Instances": [
        {
            "InstanceId": "i-1111111111example",  //Corresponds to instance 1
            "InstanceType": "p4d.24xlarge",
            "GroupName": "ML-group",
            "NetworkNodes": [
                "nn-1111111111example",           //Corresponds to NN1 in layer i
                "nn-2222222222example",           //Corresponds to NN2 in layer ii
                "nn-4444444444example"            //Corresponds to NN4 in layer iii -
 bottom layer, connected to the instance
            ],
            "CapacityBlockId": "null",
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        },
        {
            "InstanceId": "i-2222222222example",  //Corresponds to instance 2
            "InstanceType": "p4d.24xlarge",
            "NetworkNodes": [
                "nn-1111111111example",           //Corresponds to NN1 - layer i
                "nn-2222222222example",           //Corresponds to NN2 - layer ii
                "nn-4444444444example"            //Corresponds to NN4 - layer iii -
 connected to instance
            ],
            "CapacityBlockId": "null",
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        },
        {
            "InstanceId": "i-3333333333example",  //Corresponds to instance 3
            "InstanceType": "trn1.32xlarge",
            "NetworkNodes": [
                "nn-1111111111example",           //Corresponds to NN1 - layer i
                "nn-2222222222example",           //Corresponds to NN2 - layer ii
```

```
                "nn-5555555555example"           //Corresponds to NN5 - layer iii -
 connected to instance
            ],
            "CapacityBlockId": "null",
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        },
        {
            "InstanceId": "i-444444444example",  //Corresponds to instance 4
            "InstanceType": "trn1.2xlarge",
            "NetworkNodes": [
                "nn-1111111111example",          //Corresponds to NN1 - layer i
                "nn-3333333333example",          //Corresponds to NN3 - layer ii
                "nn-6666666666example"           //Corresponds to NN6 - layer iii -
 connected to instance
            ],
            "CapacityBlockId": "null",
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

Como interpretar a saída DescribeCapacityReservationTopology

É possível descrever a topologia da reserva de capacidade usando a API DescribeCapacityReservationTopology. A saída fornece uma visão hierárquica da topologia de rede subjacente para a capacidade reservada.

A saída do exemplo a seguir corresponde às informações da topologia de rede no diagrama anterior. Os comentários são incluídos na saída do exemplo para os propósitos deste exemplo.

É importante observar as seguintes informações na saída:

- `NetworkNodes` descreve o conjunto de nós de rede de uma única reserva de capacidade.
- Em cada conjunto de nós de rede, os nós de rede são listados em ordem hierárquica de cima para baixo.
- O nó de rede conectado à reserva de capacidade é o último nó apresentado na lista, representando a camada mais baixa da hierarquia.

- Para avaliar a proximidade entre as reservas de capacidade, identifique primeiro os nós de rede que aparecem em comum na camada mais baixa da saída. Se não houver nós de rede comuns na camada inferior, encontre nós de rede comuns nas camadas superiores.

Na saída de exemplo a seguir, `cr-1111111111example` está localizado em `nn-2222222222example` e `cr-2222222222example` está localizado em `nn-3333333333example`. Como essas reservas de capacidade residem em diferentes nós de rede na camada `layer ii`, a comunicação entre suas instâncias será prejudicada em termos de eficiência.

> **Note**
>
> A resposta contém um, dois ou três nós de rede, dependendo do tipo de reserva de capacidade.

```
{
    "CapacityReservations": [
        {
            "CapacityReservationId": "cr-1111111111example",
            "CapacityBlockId": "null",
            "State": "active",
            "InstanceType": "p4d.24xlarge",
            "NetworkNodes": [
                "nn-1111111111example",      //Corresponds to NN1 - layer i
                "nn-2222222222example"       //Corresponds to NN2 - layer ii
                // Visibility of additional nodes requires an instance launch and
                // the DescribeInstanceTopology API
            ],
            "AvailabilityZone": "us-west-2a"
        },
        {
            "CapacityReservationId": "cr-2222222222example",
            "CapacityBlockId": "null",
            "State": "active",
            "InstanceType": "trn1.2xlarge",
            "NetworkNodes": [
                "nn-1111111111example",      //Corresponds to NN1 - layer i
                "nn-3333333333example"       //Corresponds to NN3 - layer ii
                // Visibility of additional nodes requires an instance launch and
```

```
                // the DescribeInstanceTopology API
            ],
            "AvailabilityZone": "us-west-2a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

Diferenças entre DescribeInstanceTopology e DescribeCapacityReservationTopology

A tabela abaixo apresenta uma comparação das principais diferenças entre as APIs DescribeInstanceTopology e DescribeCapacityReservationTopology:

Ponto de comparação	DescribeInstanceTopology	DescribeCapacityReservation Topology
Fase de uso	Após a inicialização (modo de execução)	Antes da inicialização (modo de planejamento e gerenciam ento)
Propósito principal	Otimizar workloads em instâncias em execução	Realizar o planejamento de capacidade e o gerenciam ento da reserva de capacidad e, incluindo mesclar, dividir, atribuir, antes da inicialização da instância
Número de nós de rede	Mostra todos os nós de uma instância em execução. Se a instância estiver em uma reserva de capacidade, os primeiros nós coincidem com a topologia da reserva de capacidade correspondente, seguidos pelos nós adicionais para estabelecer conexão com a instância.	Mostra um conjunto parcial de nós, que varia conforme o estado (`pending` ou `active`) e o tipo da reserva de capacidade.*

Ponto de comparação	DescribeInstanceTopology	DescribeCapacityReservationTopology
Estado	As instâncias devem estar no estado `running`	As reservas de capacidade devem estar no estado `pending` ou `active`
Casos de uso	• Otimização da workload • Ajuste de performance • Análise de topologia em runtime	• Planejamento de capacidade • Gerenciamento da reserva de capacidade (que inclui mesclar, dividir e atribuir) • Avaliação da topologia antes da inicialização

* Nos blocos de capacidade para UltraServers, o conjunto de nós de rede é idêntico ao descrever a topologia de uma reserva de capacidade `active` ou da instância correspondente em execução.

Pré-requisitos para a topologia do Amazon EC2

Antes de descrever a topologia do Amazon EC2, confirme que as instâncias e as reservas de capacidade satisfazem os pré-requisitos a seguir.

Pré-requisitos para:

- Regiões da AWS
- Tipos de instância
- Estado
- permissões do IAM

Regiões da AWS

Regiões da AWS compatíveis:

- Leste dos EUA (Norte da Virgínia), Leste dos EUA (Ohio), Oeste dos EUA (Norte da Califórnia), Oeste dos EUA (Oregon)
- África (Cidade do Cabo)

- Ásia-Pacífico (Jacarta), Ásia-Pacífico (Hong Kong), Ásia-Pacífico (Hyderabad), Ásia-Pacífico (Melbourne), Ásia-Pacífico (Mumbai), Ásia-Pacífico (Osaka), Ásia-Pacífico (Seul), Ásia-Pacífico (Singapura), Ásia-Pacífico (Sydney) e Ásia-Pacífico (Tóquio)
- Canadá (Central)
- Europa (Frankfurt), Europa (Irlanda), Europa (Londres), Europa (Paris), Europa (Espanha), Europa (Estocolmo) e Europa (Zurique)
- Israel (Tel Aviv)
- Oriente Médio (Bahrein) e Oriente Médio (Emirados Árabes Unidos)
- América do Sul (São Paulo)
- AWS GovCloud (Oeste dos EUA)

A API DescribeCapacityReservationTopology não está disponível para regiões Israel (Tel Aviv) e AWS GovCloud (Oeste dos EUA).

Tipos de instância

Tipos de instâncias compatíveis:

- Retorna três* nós de rede na resposta:
  - `g6e.xlarge` | `g6e.2xlarge` | `g6e.4xlarge` | `g6e.8xlarge` | `g6e.12xlarge` | `g6e.16xlarge` | `g6e.24xlarge` | `g6e.48xlarge` | `g7e.2xlarge` | `g7e.4xlarge` | `g7e.8xlarge` | `g7e.12xlarge` | `g7e.24xlarge` | `g7e.48xlarge`
  - `hpc6a.48xlarge` | `hpc6id.32xlarge` | `hpc7g.4xlarge` | `hpc7g.8xlarge` | `hpc7g.16xlarge` | `hpc7a.12xlarge` | `hpc7a.24xlarge` | `hpc7a.48xlarge` | `hpc7a.96xlarge` | `hpc8a.96xlarge`
  - `p3dn.24xlarge` | `p4d.24xlarge` | `p4de.24xlarge` | `p5.48xlarge` | `p5e.48xlarge` | `p5en.48xlarge` | `p6e-gb200.36xlarge`
  - `trn1.2xlarge` | `trn1.32xlarge` | `trn1n.32xlarge` | `trn2.48xlarge` | `trn2u.48xlarge`
- Retorna quatro* nós de rede na resposta:
  - `p6-b200.48xlarge` | `p6-b300.48xlarge`

* O número de nós de rede indicado na resposta é relevante apenas para chamadas da API DescribeInstanceTopology. Na API DescribeCapacityReservationTopology, o número de nós de rede retornados varia conforme o tipo e o estado da reserva de capacidade.

Os tipos de instância disponíveis variam de acordo com a região. Para obter mais informações, consulte Tipos de instância do Amazon EC2 por região.

Estado

- Para `DescribeInstanceTopology`, as instâncias devem estar no estado `running`.
- Para `DescribeCapacityReservationTopology`, as reservas de capacidade devem estar nos estados `pending` ou `active`.

As informações de topologia não estão disponíveis para instâncias ou reservas de capacidade que não estejam nos estados especificados.

permissões do IAM

Sua identidade do IAM (usuário, grupo de usuários ou perfil) exige as seguintes permissões:

- `ec2:DescribeInstanceTopology`
- `ec2:DescribeCapacityReservationTopology`

Exemplos de topologia de instância do Amazon EC2

É possível usar o comando describe-instance-topology para descrever a topologia das instâncias do EC2. Além disso, você pode usar o comando describe-capacity-reservation-topology para descrever a topologia das reservas de capacidade.

Se você usar os comandos `describe-instance-topology` ou `describe-capacity-reservation-topology` sem fornecer parâmetros ou filtros, a resposta retornará todas as instâncias ou reservas de capacidade que se encaixem nos tipos de instância compatíveis com esse comando na região especificada, de acordo com o comando escolhido. É possível especificar a região incluindo o parâmetro `--region` ou definindo uma região padrão. Para obter mais informações sobre a definição de uma região padrão, consulte Selecionar uma região para os recursos do Amazon EC2.

Você pode fornecer parâmetros para que a resposta inclua somente as instâncias ou as reservas de capacidade que correspondam a determinados IDs de instância, IDs de reserva de capacidade ou nomes de grupos de posicionamento. Você também pode incluir filtros para retornar instâncias ou reservas de capacidade que correspondam a um tipo ou a uma família de instâncias especificados,

ou instâncias ou reservas de capacidade em uma zona de disponibilidade ou zona local específica. É possível incluir um único parâmetro ou filtro, ou uma combinação de parâmetros e filtros.

Por padrão, as saídas são apresentadas em páginas, com um máximo de 20 instâncias ou reservas de capacidade por página. É possível especificar até 100 instâncias ou reservas de capacidade por página usando o parâmetro `--max-results`.

Para obter mais informações, consulte describe-instance-topology e describe-reservation-topology-topology.

Permissões obrigatórias

As seguintes permissões são necessárias:

- `ec2:DescribeInstanceTopology`: para descrever a topologia da instância
- `ec2:DescribeCapacityReservationTopology`: para descrever a topologia da reserva de capacidade

Exemplos

- Exemplo 1: DescribeInstanceTopology para IDs das instâncias
- Exemplo 2: DescribeInstanceTopology para o parâmetro do nome do grupo de posicionamento
- Exemplo 3: DescribeInstanceTopology para o filtro de tipo de instância
  - Exemplo 3a: filtro de correspondência exata para um tipo de instância especificado
  - Exemplo 3b: filtro com curinga para uma família de instâncias
  - Exemplo 3c: filtros combinados de família de instâncias e correspondência exata
- Exemplo 4: DescribeInstanceTopology para o filtro de ID da zona
  - Exemplo 4a: filtro de zona de disponibilidade
  - Exemplo 4b: filtro de zona local
  - Exemplo 4c: filtros combinados de zona de disponibilidade e zona local
- Exemplo 5: DescribeInstanceTopology para filtros de tipo de instância e de ID da zona
- Exemplo 6: DescribeCapacityReservationTopology para IDs das reservas de capacidade
- Exemplo 7: DescribeCapacityReservationTopology para o filtro de tipo de instância

Exemplo 1: DescribeInstanceTopology para IDs das instâncias

AWS CLI

Para descrever a topologia de instâncias específicas

Use o comando describe-instance-topology com o parâmetro `--instance-ids`. A saída inclui somente as instâncias que correspondem aos IDs de instância especificados.

```
aws ec2 describe-instance-topology \
    --region us-west-2 \
    --instance-ids i-1111111111example i-2222222222example
```

O seguinte é um exemplo de saída.

```
{
    "Instances": [
        {
            "InstanceId": "i-1111111111example",
            "InstanceType": "p4d.24xlarge",
            "GroupName": "ML-group",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3333333333example"
            ],
            "CapacityBlockId": "null",
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        },
        {
            "InstanceId": "i-2222222222example",
            "InstanceType": "trn1n.32xlarge",
            "GroupName": "HPC-group",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3214313214example"
            ],
            "CapacityBlockId": "null",
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        }
```

```
    ],
    "NextToken": "SomeEncryptedToken"
}
```

PowerShell

Para descrever a topologia de instâncias específicas

Use o cmdlet Get-EC2InstanceTopology.

```
Get-EC2InstanceTopology `
    -InstanceId i-1111111111example, i-2222222222example
```

Exemplo 2: DescribeInstanceTopology para o parâmetro do nome do grupo de posicionamento

AWS CLI

Para descrever a topologia das instâncias em um grupo de posicionamento específico

Use o comando describe-instance-topology com o parâmetro `group-names`. A saída inclui somente as instâncias que estão em qualquer um dos grupos de posicionamento especificados.

```
aws ec2 describe-instance-topology \
    --region us-west-2 \
    --group-names ML-group HPC-group
```

O seguinte é um exemplo de saída.

```
{
    "Instances": [
        {
            "InstanceId": "i-1111111111example",
            "InstanceType": "p4d.24xlarge",
            "GroupName": "ML-group",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3333333333example"
            ],
```

```
            "CapacityBlockId": "null",
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        },
        {
            "InstanceId": "i-2222222222example",
            "InstanceType": "trn1n.32xlarge",
            "GroupName": "HPC-group",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3214313214example"
            ],
            "CapacityBlockId": "null",
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

PowerShell

Para descrever a topologia das instâncias em um grupo de posicionamento específico

Use o cmdlet Get-EC2InstanceTopology.

```
Get-EC2InstanceTopology `
    -GroupName ML-group, HPC-group
```

Exemplo 3: DescribeInstanceTopology para o filtro de tipo de instância

É possível filtrar por um tipo de instância especificado (correspondência exata) ou filtrar por uma família de instâncias (usando um caractere curinga). Você também pode combinar um filtro um tipo de instância e um filtro de família de instâncias.

Exemplo 3a: filtro de correspondência exata para um tipo de instância especificado

AWS CLI

Para descrever a topologia de instâncias com um tipo de instância específico

Use o comando describe-instance-topology com o filtro de `instance-type`. A saída inclui somente as instâncias com o tipo de instância especificado.

```
aws ec2 describe-instance-topology \
    --region us-west-2 \
    --filters Name=instance-type,Values=trn1n.32xlarge
```

O seguinte é um exemplo de saída.

```
{
    "Instances": [
        {
            "InstanceId": "i-2222222222example",
            "InstanceType": "trn1n.32xlarge",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3333333333example"
            ],
            "CapacityBlockId": "null",
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

PowerShell

Para descrever a topologia de instâncias com um tipo de instância específico

Use o cmdlet Get-EC2InstanceTopology.

```
Get-EC2InstanceTopology `
    -Filter @{Name="instance-type"; Values="trn1n.32xlarge"}
```

Exemplo 3b: filtro com curinga para uma família de instâncias

AWS CLI

Para descrever a topologia de instâncias com uma família de instâncias específica

Use o comando describe-instance-topology com o filtro de `instance-type`. A saída inclui somente as instâncias com a família de instâncias especificada.

```
aws ec2 describe-instance-topology \
    --region us-west-2 \
    --filters Name=instance-type,Values=trn1*
```

O seguinte é um exemplo de saída.

```
{
    "Instances": [
        {
            "InstanceId": "i-2222222222example",
            "InstanceType": "trn1n.32xlarge",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3333333333example"
            ],
            "CapacityBlockId": "null",
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        },
        {
            "InstanceId": "i-3333333333example",
            "InstanceType": "trn1.32xlarge",
            "NetworkNodes": [
                "nn-1212121212example",
                "nn-1211122211example",
                "nn-1311133311example"
            ],
            "CapacityBlockId": "null",
            "ZoneId": "usw2-az4",
            "AvailabilityZone": "us-west-2d"
        },
        {
            "InstanceId": "i-444444444example",
            "InstanceType": "trn1.2xlarge",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-5434334334example",
                "nn-1235301234example"
            ],
```

```
            "CapacityBlockId": "null",
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

PowerShell

Para descrever a topologia de instâncias com uma família de instâncias específica

Use o cmdlet Get-EC2InstanceTopology.

```
Get-EC2InstanceTopology `
    -Filter @{Name="instance-type"; Values="trn1*"}
```

Exemplo 3c: filtros combinados de família de instâncias e correspondência exata

AWS CLI

Para descrever a topologia de instâncias com uma família de instâncias ou um tipo de instância

Use o comando describe-instance-topology com o filtro de `instance-type`. A saída inclui somente as instâncias que atendem aos critérios especificados.

```
aws ec2 describe-instance-topology \
    --region us-west-2 \
    --filters "Name=instance-type,Values=p4d*,trn1n.32xlarge"
```

O seguinte é um exemplo de saída.

```
{
    "Instances": [
        {
            "InstanceId": "i-1111111111example",
            "InstanceType": "p4d.24xlarge",
            "GroupName": "ML-group",
            "NetworkNodes": [
                "nn-1111111111example",
```

```
                "nn-2222222222example",
                "nn-3333333333example"
            ],
            "CapacityBlockId": "null",
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        },
        {
            "InstanceId": "i-2222222222example",
            "InstanceType": "trn1n.32xlarge",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-4343434343example"
            ],
            "CapacityBlockId": "null",
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

PowerShell

Para descrever a topologia de instâncias com uma família de instâncias ou um tipo de instância

Use o cmdlet Get-EC2InstanceTopology.

```
Get-EC2InstanceTopology `
    -Filter @{Name="instance-type"; Values="p4d*", "trn1n.32xlarge"}
```

Exemplo 4: DescribeInstanceTopology para o filtro de ID da zona

É possível usar o filtro `zone-id` para filtrar por uma zona de disponibilidade ou zona local. Você também pode combinar um filtro de zona de disponibilidade e um filtro de zona local.

Exemplo 4a: filtro de zona de disponibilidade

AWS CLI

Para descrever a topologia das instâncias em uma zona de disponibilidade específica

Use o comando describe-instance-topology com o filtro de `zone-id`. A saída inclui somente as instâncias na zona de disponibilidade especificada.

```
aws ec2 describe-instance-topology \
    --region us-east-1 \
    --filters Name=zone-id,Values=use1-az1
```

O seguinte é um exemplo de saída.

```
{
    "Instances": [
        {
            "InstanceId": "i-2222222222example",
            "InstanceType": "trn1n.32xlarge",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3214313214example"
            ],
            "CapacityBlockId": "null",
            "ZoneId": "use1-az1",
            "AvailabilityZone": "us-east-1a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

PowerShell

Para descrever a topologia das instâncias em uma zona de disponibilidade específica

Use o cmdlet Get-EC2InstanceTopology.

```
Get-EC2InstanceTopology `
    -Filter @{Name="zone-id"; Values="use1-az1"}
```

Exemplo 4b: filtro de zona local

AWS CLI

Para descrever a topologia das instâncias em uma zona local específica

Use o comando describe-instance-topology com o filtro de `zone-id`. A saída inclui somente as instâncias na zona local especificada.

```
aws ec2 describe-instance-topology \
    --region us-east-1 \
    --filters Name=zone-id,Values=use1-atl2-az1
```

O seguinte é um exemplo de saída.

```
{
    "Instances": [
        {
            "InstanceId": "i-1111111111example",
            "InstanceType": "p4d.24xlarge",
            "GroupName": "ML-group",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3333333333example"
            ],
            "CapacityBlockId": "null",
            "ZoneId": "use1-atl2-az1",
            "AvailabilityZone": "us-east-1-atl-2a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

PowerShell

Para descrever a topologia das instâncias em uma zona local específica

Use o cmdlet Get-EC2InstanceTopology.

```
Get-EC2InstanceTopology `
    -Filter @{Name="zone-id"; Values="use1-atl2-az1"}
```

Exemplo 4c: filtros combinados de zona de disponibilidade e zona local

AWS CLI

Para descrever a topologia das instâncias em uma zona específica

Use o comando describe-instance-topology com o filtro de `zone-id`. A saída inclui somente as instâncias que estão em qualquer uma das zonas especificadas.

```
aws ec2 describe-instance-topology \
    --region us-east-1 \
    --filters Name=zone-id,Values=use1-az1,use1-atl2-az1
```

O seguinte é um exemplo de saída.

```
{
    "Instances": [
        {
            "InstanceId": "i-1111111111example",
            "InstanceType": "p4d.24xlarge",
            "GroupName": "ML-group",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3333333333example"
            ],
            "CapacityBlockId": "null",
            "ZoneId": "use1-atl2-az1",
            "AvailabilityZone": "us-east-1-atl-2a"
        },
        {
            "InstanceId": "i-2222222222example",
            "InstanceType": "trn1n.32xlarge",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3214313214example"
            ],
            "CapacityBlockId": "null",
            "ZoneId": "use1-az1",
            "AvailabilityZone": "us-east-1a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

PowerShell

Para descrever a topologia das instâncias em uma zona específica

Use o cmdlet Get-EC2InstanceTopology.

```
Get-EC2InstanceTopology `
    -Filter @{Name="zone-id"; Values="use1-az1", "use1-atl2-az1"}
```

Exemplo 5: DescribeInstanceTopology para filtros de tipo de instância e de ID da zona

É possível combinar os filtros em um único comando.

AWS CLI

Para descrever a topologia de instâncias com tipos de instância, famílias de instâncias e zonas específicos

Use o comando describe-instance-topology com os filtros de `instance-type` e `zone-id`. A resposta contém quaisquer instâncias com qualquer um dos tipos de instância especificados e que estão em qualquer uma das zonas especificadas.

```
aws ec2 describe-instance-topology \
    --region us-east-1 \
    --filters "Name=instance-type,Values=p4d*,trn1n.32xlarge" \
              "Name=zone-id,Values=use1-az1,use1-atl2-az1"
```

O seguinte é um exemplo de saída.

```
{
    "Instances": [
        {
            "InstanceId": "i-1111111111example",
            "InstanceType": "p4d.24xlarge",
            "GroupName": "ML-group",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3333333333example"
            ],
            "CapacityBlockId": "null",
            "ZoneId": "use1-atl2-az1",
            "AvailabilityZone": "us-east-1-atl-2a"
        },
        {
```

```
            "InstanceId": "i-2222222222example",
            "InstanceType": "trn1n.32xlarge",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3214313214example"
            ],
            "CapacityBlockId": "null",
            "ZoneId": "use1-az1",
            "AvailabilityZone": "us-east-1a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

PowerShell

Para descrever a topologia de instâncias com tipos de instância, famílias de instâncias e zonas específicos

Use o cmdlet Get-EC2InstanceTopology.

```
Get-EC2InstanceTopology `
    -Filter @{Name="instance-type"; Values="p4d*", "trn1n.32xlarge"} `
            @{Name="zone-id"; Values="use1-az1", "use1-atl2-az1"}
```

Exemplo 6: DescribeCapacityReservationTopology para IDs das reservas de capacidade

AWS CLI

Para descrever a topologia de reservas de capacidade específicas

Use o comando describe-capacity-reservation-topology com o parâmetro `capacity-reservation-id`. A saída inclui apenas as reservas de capacidade que correspondem aos IDs de reservas de capacidade especificados.

```
aws ec2 describe-capacity-reservation-topology \
    --region us-east-1 \
    --capacity-reservation-id cr-1111111111example cr-2222222222example
```

O seguinte é um exemplo de saída.

```
{
    "CapacityReservations": [
        {
            "CapacityReservationId": "cr-1111111111example",
            "CapacityBlockId": "null",
            "State": "active",
            "InstanceType": "p5.48xlarge",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example"
            ],
            "AvailabilityZone": "us-east-1a"
        },
        {
            "CapacityReservationId": "cr-2222222222example",
            "CapacityBlockId": "null",
            "State": "active",
            "InstanceType": "p5en.48xlarge",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example"
            ],
            "AvailabilityZone": "us-east-1a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

PowerShell

Para descrever a topologia de reservas de capacidade específicas

Use o cmdlet Get-EC2CapacityReservationTopology.

```
Get-EC2CapacityReservationTopology `
    -CapacityReservationId cr-1111111111example cr-2222222222example
```

Exemplo 7: DescribeCapacityReservationTopology para o filtro de tipo de instância

É possível filtrar por um tipo de instância especificado (correspondência exata) ou filtrar por uma família de instâncias (usando um caractere curinga). Você também pode combinar um filtro um tipo de instância e um filtro de família de instâncias.

AWS CLI

Para descrever a topologia de reservas de capacidade que contam com um tipo de instância específico

Use o comando describe-capacity-reservation-topology com o filtro de `instance-type`. A resposta retorna todas as instâncias correspondentes ao tipo de instância especificado.

```
aws ec2 describe-capacity-reservation-topology \
    --region us-east-1 \
    --filters Name=instance-type,Values=p5en.48xlarge
```

O seguinte é um exemplo de saída.

```
{
    "CapacityReservations": [
        {
            "CapacityReservationId": "cr-2222222222example",
            "CapacityBlockId": "null",
            "State": "active",
            "InstanceType": "p5en.48xlarge",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example"
            ],
            "AvailabilityZone": "us-east-1a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

PowerShell

Para descrever a topologia de reservas de capacidade que contam com um tipo de instância específico

Use o cmdlet Get-EC2CapacityReservationTopology.

```
Get-EC2CapacityReservationTopology `
    -Filter @{Name="instance-type"; Values="p5en.48xlarge"}
```

Grupos de posicionamento para as instâncias do Amazon EC2

Para atender às necessidades de sua workload, você pode iniciar um grupo de instâncias do EC2 interdependentes em um grupo de posicionamento para influenciar seu posicionamento.

Dependendo do tipo de workload, é possível criar um grupo de posicionamento com uma das seguintes estratégias de posicionamento:

- Cluster: agrupa as instâncias em uma zona de disponibilidade. Essa estratégia permite que as workloads atinjam a performance de rede de baixa latência necessária para a comunicação de nó a nó totalmente acoplada que é típica das aplicações de computação de alta performance (HPC).
- Partição: distribui as instâncias entre partições lógicas, de tal modo que as instâncias em uma partição não compartilhem o hardware subjacente com os grupos de instâncias em outras partições. Essa estratégia é normalmente usada por grandes workloads distribuídas e replicadas, como Hadoop, Cassandra e Kafka.
- Distribuir: posiciona estritamente um pequeno grupo de instâncias no hardware subjacente distinto a fim de reduzir as falhas correlacionadas.

Os grupos de posicionamento são opcionais. Se você não iniciar suas instâncias em um grupo de posicionamento, o EC2 tentará posicionar as instâncias de tal forma que todas elas sejam distribuídas pelo hardware subjacente para minimizar as falhas correlacionadas.

Preços

Não há custo para a criação de um grupo de posicionamento.

Regras e limitações

Antes de usar os grupos de posicionamento, esteja ciente das seguintes regras:

- Uma instância pode ser colocada em um grupo de posicionamento por vez; você não pode colocar uma instância em vários grupos de posicionamento.
- Não é possível mesclar grupos de posicionamento.

- O recurso Reservas de capacidade sob demanda e as Instâncias reservadas de zona permitem que você reserve capacidade para instâncias do EC2 em zonas de disponibilidade. Quando você executa uma instância, se os atributos da instância corresponderem aos especificados por uma reserva de capacidade sob demanda ou por uma instância reservada por zona, a capacidade reservada será usada automaticamente pela instância. Isso também é verdade se você executar a instância em um grupo de posicionamento.
- Não é possível iniciar os hosts dedicados em grupos de posicionamento.
- Você não pode iniciar uma instância spot que esteja configurada para parar ou hibernar em caso de interrupção em um grupo de posicionamento.

Conteúdo

- Estratégias de posicionamento para os grupos de posicionamento
- Criar um grupo de posicionamento para instâncias do EC2
- Alterar o posicionamento para uma instância do EC2
- Excluir um grupo de posicionamento.
- Grupos de posicionamento compartilhados
- Grupos de posicionamento no AWS Outposts

Estratégias de posicionamento para os grupos de posicionamento

É possível criar um grupo de posicionamento para suas instâncias do EC2 usando uma das estratégias de posicionamento a seguir.

Estratégias de posicionamento

- Grupos de posicionamento de cluster
- Placement groups de partição
- Grupos com posicionamento distribuído

Grupos de posicionamento de cluster

Um grupo de posicionamento de cluster é um agrupamento lógico de instâncias dentro de uma única zona de disponibilidade. As instâncias não estão isoladas em um rack único. Um grupo de posicionamento de cluster pode abranger redes privadas virtuais (VPCs) emparelhadas na mesma região. As instâncias no mesmo grupo de posicionamento de cluster dispõem de um limite de

throughput por fluxo superior para tráfego TCP/IP e são colocadas no mesmo segmento de largura de banda de bisseção alta da rede.

A imagem a seguir mostra instâncias colocadas em um grupo de posicionamento de cluster.

Os grupos de posicionamento de cluster são recomendados para aplicações que se beneficiam de baixa latência de rede, alta throughput de rede ou ambos. Eles também são recomendados quando a maioria do tráfego de rede está entre as instâncias no grupo. Para fornecer a menor latência possível e a melhor performance de rede de pacote por segundo para seu grupo de posicionamento, escolha um tipo de instância que comporte rede avançada. Para obter mais informações, consulte Redes aprimoradas.

Recomendamos executar suas instâncias da seguinte maneira:

- Use uma única solicitação de execução para executar o número de instâncias necessárias no placement group.
- Use o mesmo tipo de instância para todas as instâncias no placement group.

Se você tentar adicionar mais instâncias ao grupo de posicionamento depois ou se tentar executar mais de um tipo de instância no grupo de posicionamento, 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 no início se não houver capacidade suficiente para a instância.

Se você receber um erro de capacidade ao executar uma instância em um placement group que já tenha instâncias em execução, interrompa e inicie todas as instâncias no placement group e tente

executá-lo novamente. Iniciar as instâncias pode migrá-las para o hardware com capacidade para todas as instâncias solicitadas.

Regras e limitações

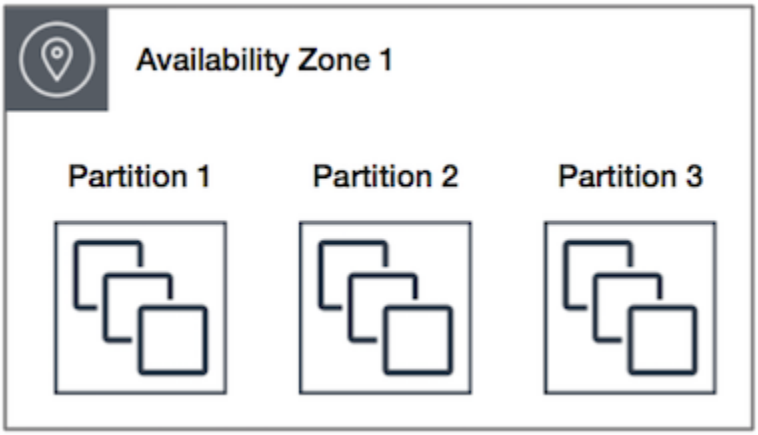
As seguintes regras se aplicam aos grupos de posicionamento de cluster:

- Somente os seguintes tipos de instância são compatíveis:
  - Instâncias da geração atual, exceto as instâncias de desempenho expansíveis (por exemplo, T2), as instâncias Mac1 e as instâncias M7i-flex.
  - As seguintes instâncias da geração anterior: A1, C3, C4, I2, M4, R3 e R4.
- Um grupo de posicionamento de cluster não pode abranger várias zonas de disponibilidade.
- A velocidade máxima de throughput de rede do tráfego entre duas instâncias em um grupo de posicionamento de cluster é limitada pela instância mais lenta. Para aplicações com requisitos de throughput 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 grupo de posicionamento de cluster podem usar até 10 Gbps para tráfego de fluxo único. As instâncias que não estiverem dentro de um grupo de posicionamento de cluster poderão usar até 5 Gbps para tráfego de fluxo único.
  - O tráfego para e de buckets do Amazon S3 na mesma região pelo espaço de endereço IP público ou por um VPC endpoint pode usar toda a largura de banda agregada da instância disponível.
- É possível executar vários tipos de instâncias em um grupo de posicionamento 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 grupo de posicionamento de cluster.
- Recomendamos que você reserve capacidade explicitamente em um grupo de posicionamento de cluster para criar uma reserva de capacidade sob demanda no grupo de posicionamento de cluster. Observe que você não pode reservar capacidade usando instâncias reservadas por zona, pois elas não podem reservar capacidade explicitamente em um grupo de posicionamento.
- O tráfego de rede para a Internet e por meio de uma conexão do Direct Connect com recursos on-premises é limitado a 5 Gbps para grupos com posicionamento em cluster.

Placement groups de partição

Os grupos de posicionamento de partição ajudam a reduzir a probabilidade de falhas de hardware correlacionadas da aplicação. Ao usar grupos de posicionamento de partição, o Amazon EC2 divide cada grupo em segmentos lógicos chamados de partições. O Amazon EC2 garante que cada partição em um grupo de posicionamento tenha seu próprio conjunto de racks. Cada rack tem sua própria rede e fonte de energia. Não há duas partições em um grupo de posicionamento que compartilhem os mesmos racks, permitindo que você isole o impacto da falha de hardware na aplicação.

A imagem a seguir é uma representação visual simples de um grupo de posicionamento de partição em uma única zona de disponibilidade. Ela mostra instâncias que são colocadas em um placement grupo de posicionamento de partição com três partições — Partition 1 (Partição 1), Partition 2 (Partição 2) e Partition 3 (Partição 3). Cada partição é composta por várias instâncias. As instâncias em cada partição não compartilham racks com as instâncias nas outras partições, contendo o impacto de uma única falha de hardware apenas na partição associada.



Grupos de posicionamento de partição podem ser usados para implantar grandes workloads distribuídas e replicadas, como HDFS, HBase e Cassandra, em racks distintos. Ao executar instâncias em um grupo de posicionamento de partição, o Amazon EC2 tenta distribuir as instâncias uniformemente pelo número de partições especificado por você. Também é possível executar instâncias em uma partição específica para ter mais controle sobre onde as instâncias são colocadas.

Um grupo de posicionamento de partição pode ter partições em várias zonas de disponibilidade na mesma região. Um grupo de posicionamento de partição pode ter, no máximo, sete partições por zona de disponibilidade. O número de instâncias que podem ser executadas em um grupo de posicionamento de partição é limitado somente pelos limites da sua conta.

Além disso, grupos de posicionamento de partição oferecem visibilidade nas partições — é possível ver quais instâncias estão em quais partições. É possível compartilhar essas informações com aplicações que reconhecem a topologia, como HDFS, HBase e Cassandra. Essas aplicações usam essas informações para tomar decisões inteligentes de replicação de dados para aumentar a disponibilidade e a durabilidade dos dados.

Se você iniciar ou executar uma instância em um grupo de posicionamento 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.

Regras e limitações

As seguintes regras se aplicam aos grupos de posicionamento de partição:

- Um grupo de posicionamento de partição oferece suporte a, no máximo, sete partições por zona de disponibilidade. O número de instâncias que podem ser executadas em um grupo de posicionamento de partição é limitado somente pelos limites da sua conta.
- Quando as instâncias são executadas em um grupo de posicionamento de partição, o Amazon EC2 tenta distribuir as instâncias uniformemente em todas as partições. O Amazon EC2 não garante uma distribuição uniforme de instâncias em todas as partições.
- Um grupo de posicionamento de partição com Instâncias dedicadas pode ter, no máximo, duas partições.
- Reservas de capacidade não reservam capacidade em um grupo de posicionamento de partição.

Grupos com posicionamento distribuído

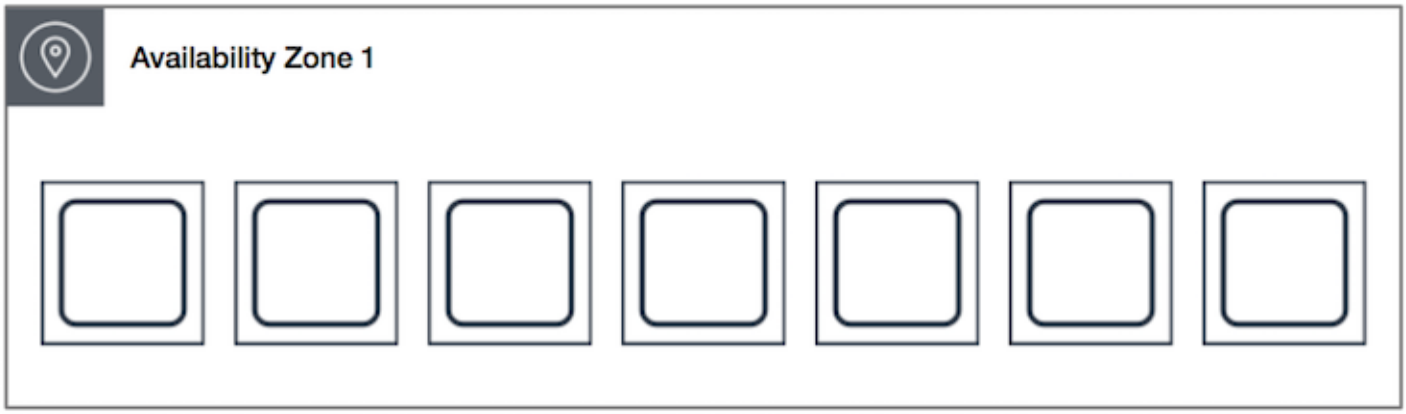
Um grupo de posicionamento de distribuição é um grupo de instâncias que são colocadas cada uma em hardware distinto.

Os grupos de posicionamento de distribuição são recomendados para aplicações com uma pequena quantidade de instâncias críticas que devem ser mantidas separadas umas das outras. Executar instâncias em um grupo de posicionamento de nível de distribuição reduz o risco de falhas simultâneas que podem ocorrer quando as instâncias compartilham os mesmos equipamentos. Os grupos de posicionamento em nível de distribuição concedem acesso a equipamentos distintos e, portanto, são adequados para combinar tipos de instâncias ou executar instâncias ao longo do tempo.

Se você iniciar ou executar uma instância em um grupo de posicionamento disseminado e não houver uma quantidade suficiente de hardware exclusivo para atender à solicitação, ocorrerá uma falha. O Amazon EC2 disponibiliza mais hardware distinto ao longo do tempo, portanto, tente reenviar sua solicitação mais tarde. Grupos de posicionamento podem distribuir instâncias em racks ou hosts. É possível usar grupos com posicionamento distribuído em nível de rack em regiões da AWS e AWS Outposts. Você pode usar grupos com posicionamento distribuído em nível de host somente com AWS Outposts.

Grupos com posicionamento distribuído em nível de rack

A imagem a seguir mostra sete instâncias em uma única zona de disponibilidade que são colocadas em um grupo de posicionamento de distribuição. As sete instâncias são colocadas em sete racks diferentes, cada um com sua própria rede e fonte de energia.



Um grupo com posicionamento distribuído em nível de rack pode abranger várias zonas de disponibilidade na mesma região. Em uma região, um grupo com posicionamento distribuído em nível de rack pode ter no máximo sete instâncias em execução por zona de disponibilidade por grupo. Com o Outposts, seu grupo com posicionamento distribuído em nível de rack pode armazenar o mesmo número de instâncias que o número de racks que você tiver em sua implantação do Outpost.

Grupos de posicionamento de distribuição em host

Os grupos com posicionamento distribuído em host estão disponíveis apenas com AWS Outposts. Um grupo com posicionamento distribuído em nível de host pode conter o mesmo número de instâncias que o número de hosts da sua implantação do Outpost. Para obter mais informações, consulte the section called “Grupos de posicionamento no AWS Outposts”.

Regras e limitações

As seguintes regras se aplicam aos grupos de posicionamento de distribuição:

- Um grupo de posicionamento de distribuição em rack suporta, no máximo, sete instâncias em execução por zona de disponibilidade. Por exemplo, em uma região com três zonas de disponibilidade, é possível executar um total de 21 instâncias no grupo, com sete instâncias em cada zona de disponibilidade. Se você tentar iniciar uma oitava instância na mesma zona de disponibilidade e no mesmo grupo de posicionamento de distribuição, ela não será executada. Se você precisar de mais de sete instâncias em uma zona de disponibilidade, recomendamos usar vários grupos de posicionamento de distribuição. O uso de vários grupos de posicionamento de dispersão não fornece garantias sobre a disseminação de instâncias entre grupos, mas ajuda a garantir a dispersão para cada grupo, limitando assim o impacto de certas classes de falhas.
- Os grupos de posicionamento de distribuição não são compatíveis com o Instâncias dedicadas.
- Grupos de posicionamento de distribuição em host apenas são compatíveis com grupos de posicionamento AWS Outposts. Um grupo com posicionamento distribuído em nível de host pode conter o mesmo número de instâncias que o número de hosts da sua implantação do Outpost.
- Em uma região, um grupo com posicionamento distribuído em nível de rack pode ter no máximo sete instâncias em execução por zona de disponibilidade por grupo. Com o AWS Outposts, seu grupo com posicionamento distribuído em nível de rack pode armazenar o mesmo número de instâncias que o número de racks que você tiver em sua implantação do Outpost.
- Reservas de capacidade não reservam capacidade em um grupo de posicionamento de espalhamento.

Criar um grupo de posicionamento para instâncias do EC2

Você pode usar um grupo de posicionamento para controlar o posicionamento das instâncias em relação umas às outras. Após criar um grupo de posicionamento, você pode executar instâncias nele.

Limitação

Você pode criar no máximo 500 grupos de posicionamento por região.

Console

Para criar um grupo de posicionamento

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Placement Groups.
3. Escolha Criar grupo de posicionamento.
4. Especifique um nome para o grupo.
5. Escolha a estratégia de posicionamento para o grupo: Cluster, Distribuído ou Partição.

   Se escolher Distribuído, você deverá escolher o nível de distribuição: Rack ou Host.

   Se escolher Partição, você deverá inserir o número de partições para o grupo.
6. (Opcional) Para adicionar uma tag, escolha Adicionar nova tag e insira a chave e o valor.
7. Escolha Criar grupo.

AWS CLI

Use o comando create-placement-group.

Para criar um grupo de posicionamento de cluster

O exemplo a seguir cria um grupo de posicionamento que usa a estratégia de posicionamento de `cluster` e a aplica uma tag com uma chave de `purpose` e um valor de `production`.

```
aws ec2 create-placement-group \
    --group-name my-cluster \
    --strategy cluster \
    --tag-specifications 'ResourceType=placement-
group,Tags={Key=purpose,Value=production}'
```

Para criar um grupo com posicionamento em partições

O exemplo a seguir cria um grupo de posicionamento que usa a estratégia de posicionamento de `partition` e especifica as cinco partições usando o parâmetro `--partition-count`.

```
aws ec2 create-placement-group \
    --group-name HDFS-Group-A \
    --strategy partition \
```

```
    --partition-count 5
```

PowerShell

Use o cmdlet New-EC2PlacementGroup.

Para criar um grupo de posicionamento de cluster

O exemplo a seguir cria um grupo de posicionamento de cluster.

```
New-EC2PlacementGroup `
    -GroupName my-placement-group `
    -Strategy cluster
```

Criar um grupo com posicionamento em partições

O exemplo a seguir cria um grupo com posicionamento em partições.

```
New-EC2PlacementGroup `
    -GroupName my-placement-group `
    -Strategy partition `
    -PartitionCount 5
```

Alterar o posicionamento para uma instância do EC2

É possível alterar o grupo de posicionamento de uma instância da seguinte maneira:

- Adicionar uma instância para um grupo de posicionamento
- Mova uma instância de um grupo de posicionamento para outro
- Remova uma instância de um grupo de posicionamento

Requisito

Antes de você poder alterar o grupo de posicionamento para uma instância, ela deve estar no estado `stopped`.

Console

Para alterar o posicionamento de 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 a instância.
4. Escolha Actions (Ações), Instance Settings (Configurações da instância) e Modify Instance Placement (Modificar posicionamento da instância).
5. Para Grupo de posicionamento, faça um dos seguintes:
   - Para adicionar a instância a um grupo de posicionamento, escolha o grupo de posicionamento.
   - Para mover a instância de um grupo de posicionamento para outro, escolha o grupo de posicionamento.
   - Para remover a instância do grupo de posicionamento, escolha Nenhum.
6. Escolha Salvar.

AWS CLI

Para mover uma instância para um grupo de posicionamento

Use o seguinte comando modify-instance-placement.

```
aws ec2 modify-instance-placement \
    --instance-id i-0123a456700123456 \
    --group-name MySpreadGroup
```

Para remover uma instância de um grupo de posicionamento

Use o seguinte comando modify-instance-placement. Quando você especifica uma string vazia para o nome do grupo de posicionamento, isso remove a instância do grupo de posicionamento atual.

```
aws ec2 modify-instance-placement \
    --instance-id i-0123a456700123456 \
    --group-name ""
```

PowerShell

Para mover uma instância para um grupo de posicionamento

Use o cmdlet Edit-EC2InstancePlacement com o nome do grupo de posicionamento.

```
Edit-EC2InstancePlacement `
    -InstanceId i-0123a456700123456 `
    -GroupName MySpreadGroup
```

Para remover uma instância de um grupo de posicionamento

Use o cmdlet Edit-EC2InstancePlacement com uma string vazia para o nome do grupo de posicionamento.

```
Edit-EC2InstancePlacement `
    -InstanceId i-0123a456700123456 `
    -GroupName ""
```

Excluir um grupo de posicionamento.

Se precisar substituir um grupo de posicionamento ou se não precisar mais dele, será possível excluí-lo. Para excluir um grupo de posicionamento, ele não deve conter instâncias. Você pode encerrar as instâncias, movê-las para outro grupo de posicionamento ou removê-las do grupo de posicionamento.

Console

Para excluir um grupo de posicionamento

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Placement Groups.
3. Selecione o grupo de posicionamento e escolha Actions (Ações), Delete (Excluir).
4. Quando a confirmação for solicitada, insira **`Delete`** e escolha Delete (Excluir).

AWS CLI

Excluir um grupo de posicionamento

Use o comando delete-placement-group.

```
aws ec2 delete-placement-group --group-name my-cluster
```

PowerShell

Excluir um grupo de posicionamento

Use o cmdlet Remove-EC2PlacementGroup.

```
Remove-EC2PlacementGroup -GroupName my-cluster
```

Grupos de posicionamento compartilhados

O compartilhamento de grupos de posicionamento permite que você influencie o posicionamento de instâncias interdependentes que pertencem a Contas da AWS distintas. Um proprietário compartilhar um grupo de posicionamento em várias Contas da AWS ou em sua organização. Um participante pode executar instâncias em um grupo de posicionamento que é compartilhado com sua conta.

O proprietário de um grupo de posicionamento pode compartilhar um grupo de posicionamento com:

- Contas específicas da AWS que são internas ou externas à organização
- Uma unidade organizacional dentro de sua organização da
- Toda a sua organização da

Você pode usar o emparelhamento de VPC para conectar instâncias pertencentes a contas distintas da AWS e obter todos os benefícios de latência oferecidos pelos grupo com posicionamento em cluster compartilhados.

Conteúdo

- Regras e limitações
- Permissões obrigatórias
- Compartilhamento entre zonas de disponibilidade
- Compartilhamento do grupo de posicionamento
- Desfazer o compartilhamento do grupo de posicionamento

Regras e limitações

As regras e limitações a seguir se aplicam quando você compartilha um grupo de posicionamento ou quando um grupo de posicionamento é compartilhado com você.

- Para compartilhar um grupo de posicionamento, é necessário que você seja o proprietário dele na sua conta da AWS. Não é possível compartilhar um grupo de posicionamento que tenha sido compartilhado com você.
- Quando você compartilha um grupo com posicionamento em partições ou um grupo com posicionamento distribuído, os limites do grupo de posicionamento não mudam. Um grupo com posicionamento em partições compartilhado é compatível com, no máximo, sete partições por zona de disponibilidade e um grupo com posicionamento distribuído compartilhado é compatível com, no máximo sete instâncias em execução por zona de disponibilidade.
- Para compartilhar um grupo com posicionamento com a organização ou com uma unidade organizacional em sua organização, você deve habilitar o compartilhamento com o AWS Organizations. Para mais informações, consulte Compartilhar seus recursos da AWS.
- Ao usar o Console de gerenciamento da AWS para executar uma instância, você pode selecionar qualquer grupo de posicionamento que foi compartilhado com você. Ao usar o AWS CLI para iniciar uma instância, você deve especificar um grupo de posicionamento compartilhado por ID, não por nome. Você poderá usar o nome do grupo com posicionamento somente se for o proprietário do grupo de posicionamento compartilhado.
- Você é responsável por gerenciar as instâncias de que é proprietário em um grupo de posicionamento compartilhado.
- Você não pode visualizar nem modificar instâncias e reservas de capacidade associadas a um grupo de posicionamento compartilhado do qual não é proprietário.
- O nome do recurso da Amazon (ARN) de um grupo com posicionamento contém o ID da conta proprietária do grupo com posicionamento. É possível usar uma parte do ID da conta de um ARN de grupo de posicionamento para identificar o proprietário de um grupo com posicionamento que é compartilhado com você.

Permissões obrigatórias

Para compartilhar um grupo de posicionamento, os usuários devem ter permissões para as seguintes ações:

- `ec2:PutResourcePolicy`

- `ec2:DeleteResourcePolicy`

Compartilhamento entre zonas de disponibilidade

Para garantir a distribuição de recursos entre as zonas de disponibilidade de uma região, mapeamos as zonas de disponibilidade de forma independente para os nomes de cada conta. Isso pode resultar em diferenças na nomenclatura de zonas de disponibilidade entre contas. Por exemplo, a zona de disponibilidade `us-east-1a` de sua conta da AWS pode não ter o mesmo local que a `us-east-1a` de outra conta da AWS.

Para especificar o local de seus Hosts dedicados relativo a suas contas, use o ID da zona de disponibilidade (ID da AZ). O AZ ID é um identificador exclusivo e consistente de uma zona de disponibilidade em todas as contas da AWS. Por exemplo, `use1-az1` é um ID de zona de disponibilidade da região `us-east-1` e é o mesmo local em cada conta da AWS. Para obter mais informações, consulte IDs de AZs.

Compartilhamento do grupo de posicionamento

Para compartilhar um grupo de posicionamento, é necessário adicioná-lo a um compartilhamento de recursos. Um compartilhamento de recursos é um recurso do AWS RAM que permite que você compartilhe seus recursos entre contas da AWS. Um compartilhamento de recursos especifica os recursos a serem compartilhados, e os clientes com os quais compartilhá-los.

Se você fizer parte de uma organização no AWS Organizations e o compartilhamento estiver habilitado na sua organização, os consumidores da organização terão acesso ao grupo de posicionamento compartilhado.

Se o grupo de posicionamento for compartilhado com uma conta da AWS fora da sua organização, o proprietário da conta da AWS receberá um convite para participar do compartilhamento de recursos. Ele poderá acessar o grupo de posicionamento compartilhado depois que aceitar o convite.

Você pode compartilhar um grupo de posicionamento entre AWS contas da usando AWS Resource Access Manager. Para obter mais informações, consulte Criar um compartilhamento de recurso no Guia do usuário do AWS RAM.

Desfazer o compartilhamento do grupo de posicionamento

O proprietário do grupo de posicionamento pode cancelar o compartilhamento de um grupo de posicionamento compartilhado a qualquer momento. Quando você cancela o compartilhamento de um grupo de posicionamento compartilhado, as seguintes alterações ocorrem:

- As contas da AWS com as quais um grupo de posicionamento foi compartilhado não podem mais iniciar instâncias nem reservar capacidade.
- Qualquer instância sendo executada em um grupo de posicionamento compartilhado será desassociada do grupo de posicionamento, mas continuará sendo executada normalmente em sua conta da AWS.
- Todas as reservas de capacidade em um grupo de posicionamento compartilhado são desassociadas do grupo de posicionamento, mas permanecem disponíveis para você em sua conta da AWS.

Para obter detalhes adicionais, consulte Excluir um compartilhamento de recursos no Guia do Usuário AWS RAM.

Grupos de posicionamento no AWS Outposts

O AWS Outposts é um serviço totalmente gerenciado que estende a infraestrutura, os serviços, as APIs e as ferramentas da AWS no local do cliente. Ao fornecer acesso local à infraestrutura gerenciada pela AWS, o AWS Outposts permite que os clientes criem e executem aplicações on-premises usando as mesmas interfaces de programação que nas regiões da AWS, ao mesmo tempo que usam recursos locais de computação e armazenamento para menor latência e necessidades de processamento de dados locais.

Um Outpost é um grupo de capacidade de computação e armazenamento da AWS implantado em um local do cliente. A AWS opera, monitora e gerencia essa capacidade como parte de uma região da AWS.

É possível criar grupos de posicionamento em Outposts que você criou na sua conta. Isso permite que você distribua instâncias no hardware de base em um Outpost no local. Você cria e utiliza grupos de posicionamento em Outposts da mesma forma que cria e utiliza grupos de posicionamento em zonas de disponibilidade regulares. Ao criar um grupo de posicionamento com uma estratégia de distribuição em um Outpost, você pode optar por fazer com que o grupo de posicionamento distribua instâncias entre hosts ou racks. A distribuição de instâncias entre hosts permite usar uma estratégia de distribuição com um único rack do Outpost.

Considerações

- Um grupo com posicionamento distribuído em nível de rack pode armazenar o mesmo número de instâncias que o número de racks que você tiver em sua implantação do Outpost.

- Um grupo com posicionamento distribuído em nível de host pode conter o mesmo número de instâncias que o número de hosts da sua implantação do Outpost.

Pré-requisito

É necessário ter um Outpost instalado em seu local. Para obter mais informações, consulte Criar um Outpost e solicitar capacidade do Outpost no Manual do usuário do AWS Outposts.

Para utilizar um grupo de posicionamento em um Outpost

1. Crie uma sub-rede no Outpost. Para obter mais informações, consulte Criar uma sub-rede no Manual do usuário do AWS Outposts.
2. Crie um grupo de posicionamento na região associada do Outpost. Se você criar um grupo de posicionamento com uma estratégia de distribuição, poderá escolher o nível de distribuição em nível host ou de rack para determinar como o grupo distribuirá instâncias pelo hardware de base no Outpost. Para obter mais informações, consulte the section called “Criar um grupo de posicionamento.”.
3. Inicie uma instância no grupo de posicionamento. Para Subnet (Sub-rede), escolha a sub-rede criada na Etapa 1 e para Placement group name (Nome do grupo de posicionamento), selecione o grupo de posicionamento criado na Etapa 2. Para obter mais informações, consulte Executar uma instância no Outpost no Manual do usuário do AWS Outposts.

Unidade de transmissão máxima (MTU) de rede para a instância do EC2

A unidade de transmissão máxima (MTU) de uma conexão de rede é o tamanho, em bytes, do maior pacote permissível que pode ser passado pela conexão. Quanto maior a MTU de uma conexão, mais dados podem ser passados em um único pacote. Os quadros de Ethernet consistem no pacote, ou nos dados em si que você envia, e nas informações de overhead de rede que o cercam.

Os quadros de ethernet podem vir em diferentes formatos, sendo o mais comum o Ethernet v2 padrão. Ele é compatível com 1.500 MTU, que é o maior tamanho de pacote de Ethernet compatível na maior parte da Internet. A MTU máxima compatível com uma instância depende do tipo de instância.

Todos os tipos de instância do EC2 são compatíveis com 1.500 MTU.

Conteúdo

- Frames jumbo (9001 MTU)
- Path MTU Discovery
- Definir a MTU para as instâncias do Amazon EC2
- Solução de problemas

Frames jumbo (9001 MTU)

Com os frames jumbo, você pode aumentar o tamanho da carga útil por pacote, aumentando assim a porcentagem do pacote que não é sobrecarga de pacotes. Com os frames jumbo, menos pacotes são necessários para enviar a mesma quantidade de dados utilizáveis. No entanto, certos tipos de tráfego estão sujeitos às seguintes cargas úteis máximas:

Limite de MTU de 1500 bytes

- Tráfego em um gateway de Internet
- Tráfego através de ligações VPN
- Tráfego entre regiões da AWS, a menos que um gateway de trânsito seja usado

Limite de MTU de 8500 bytes

- Tráfego em uma conexão de emparelhamento de VPC entre regiões

Se os pacotes estiverem acima do limite de MTU, eles serão fragmentados, ou descartados se o marcador `Don't Fragment` for definido no cabeçalho IP.

Os frames Jumbo devem ser usados com cuidado para o tráfego voltado para Internet ou qualquer tráfego que saia de uma VPC. Os pacotes são fragmentados por sistemas intermediários, que retarda o tráfego. Para usar frames jumbo dentro de uma VPC e não diminuir o tráfego vinculado para fora da VPC, é possível 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 grupo de posicionamento de cluster, os frames jumbo ajudam a alcançar a máxima throughput de rede possível e são recomendados neste caso. Para obter mais informações, consulte Grupos de posicionamento para as instâncias do Amazon EC2.

É possível usar quadros jumbo para tráfego entre suas VPCs e suas redes on-premises por meio do Direct Connect. Para obter mais informações e para saber como verificar se há capacidade de frames jumbo, consulte MTU para interfaces virtuais privadas ou interfaces virtuais de trânsito no Guia do usuário do Direct Connect.

Todas as instâncias da geração atual são compatíveis com frames jumbo. Os seguintes tipos de instância da geração anterior são compatíveis com frames jumbo: A1, C3, I2, M3 e R3.

Recursos relacionados

- Para gateways NAT, consulte NAT gateway basics no Manual do usuário da Amazon VPC.
- Para gateways de trânsito, consulte Maximum transmission unit no Guia do usuário do Transit Gateways da Amazon VPC.
- Para zonas locais, consulte Considerations no AWS Local Zones User Guide.
- Para AWS Wavelength, consulte Maximum transmission unit no Guia do usuário do AWS Wavelength.
- Para o Outposts, consulte Service link maximum transmission unit requirements no Guia do usuário do AWS Outposts.

Path MTU Discovery

A Path MTU Discovery (PMTUD) é usada para determinar a MTU do caminho entre dois dispositivos. A MTU do caminho é o tamanho de pacote máximo com suporte no caminho entre o host de origem e o host de recepção. Quando há alguma diferença no tamanho da MTU da rede entre dois hosts, a PMTUD permite que o host de recepção responda ao host de origem com uma mensagem de ICMP. Essa mensagem instrui o host de origem a usar o menor tamanho de MTU no caminho de rede para enviar novamente a solicitação. Sem essa negociação, a perda de pacotes pode ocorrer porque a solicitação é muito grande para o host aceitar.

Para o IPv4, quando um host enviar um pacote que for maior que a MTU do host de recebimento ou que a MTU de um dispositivo ao longo do caminho, o host ou o dispositivo de recebimento eliminará o pacote e retornará a seguinte mensagem ICMP: `Destination Unreachable: Fragmentation Needed and Don't Fragment was Set` (Tipo 3, Código 4). Isso instrui o host de transmissão a dividir a carga útil em vários pacotes menores e, em seguida, retransmiti-los.

O protocolo IPv6 não é compatível com a fragmentação na rede. Se um host enviar um pacote que for maior que a MTU do host de recebimento ou que a MTU de um dispositivo ao longo do caminho,

o host ou dispositivo de recebimento eliminará o pacote e retornará a seguinte mensagem ICMP: `ICMPv6 Packet Too Big (PTB)` (Tipo 2). Isso instrui o host de transmissão a dividir a carga útil em vários pacotes menores e, em seguida, retransmiti-los.

As conexões feitas por meio de alguns componentes, como gateways NAT e balanceadores de carga, são rastreadas automaticamente. Isso significa que o rastreamento de grupos de segurança é habilitado automaticamente para suas tentativas de conexão de saída. Se as conexões forem rastreadas automaticamente ou se as regras do seu grupo de segurança permitirem tráfego ICMP de entrada, será possível receber respostas do PMTUD.

Observe que o tráfego ICMP pode ser bloqueado mesmo se o tráfego for permitido no nível do grupo de segurança, como se você tiver uma entrada na lista de controle de acesso à rede que negue o tráfego ICMP para a sub-rede.

> **Important**
>
> O Path MTU Discovery não garante que os quadros Jumbo não sejam descartados por alguns roteadores. Um gateway da Internet na VPC encaminhará somente pacotes de até 1.500 bytes. São recomendados pacotes de 1.500 MTU para o tráfico de Internet.

Para regras de MTU sobre gateways NAT, consulte Unidade de transmissão máxima (MTU) no Guia do usuário do Amazon VPC. Para regras de MTU sobre gateways de trânsito, consulte Unidade de transmissão máxima (MTU) no Guia do usuário do AWS Transit Gateway.

Definir a MTU para as instâncias do Amazon EC2

A unidade de transmissão máxima (MTU) de uma conexão de rede é o tamanho, em bytes, do maior pacote permissível que pode ser passado pela conexão. Todas as instâncias do Amazon EC2 são compatíveis com quadros padrão (1.500 MTU), e todos os tipos de instância da geração atual são compatíveis com quadros jumbo (9.001 MTU).

É possível visualizar a MTU para as instâncias do Amazon EC2, visualizar a MTU do caminho entre a instância e outro host e configurar as instâncias para usar quadros padrão ou jumbo.

Tarefas

- Verificar o MTU do caminho entre dois hosts
- Verificação da MTU para a instância
- Definição da MTU para a instância

Verificar o MTU do caminho entre dois hosts

É possível verificar a MTU do caminho entre a instância EC2 e outro host. É possível especificar um nome DNS ou um endereço IP como o destino. Se o destino for outra instância do EC2, verifique se o grupo de segurança permite tráfego UDP de entrada.

O procedimento usado dependerá do sistema operacional da instância.

Instâncias do Linux

Execute o comando tracepath na instância para verificar a MTU do caminho entre a instância EC2 e o destino especificado. Esse comando faz parte do pacote `iputils`, que está disponível, por padrão, em muitas distribuições do Linux.

Este exemplo verifica a MTU do caminho entre a instância do EC2 e o arquivo `amazon.com`.

```
[ec2-user ~]$ tracepath amazon.com
```

Neste exemplo de saída, a MTU do caminho é 1500.

```
 1?: [LOCALHOST]     pmtu 9001
 1:  ip-172-31-16-1.us-west-1.compute.internal (172.31.16.1)   0.187ms pmtu 1500
 1:  no reply
 2:  no reply
 3:  no reply
 4:  100.64.16.241 (100.64.16.241)                              0.574ms
 5:  72.21.222.221 (72.21.222.221)                             84.447ms asymm 21
 6:  205.251.229.97 (205.251.229.97)                           79.970ms asymm 19
 7:  72.21.222.194 (72.21.222.194)                             96.546ms asymm 16
 8:  72.21.222.239 (72.21.222.239)                             79.244ms asymm 15
 9:  205.251.225.73 (205.251.225.73)                           91.867ms asymm 16
...
31:  no reply
     Too many hops: pmtu 1500
     Resume: pmtu 1500
```

Instâncias do Windows

Para verificar a MTU do caminho usando mturoute

1. Faça o download de mturoute.exe para a instância do EC2 em https://elifulkerson.com/projects/mturoute.php.

2. Abra uma janela do prompt de comando e altere para o diretório para onde você fez o download de mturoute.exe.
3. Use o comando apresentado a seguir para verificar a MTU do caminho entre a instância do EC2 e o destino especificado. Este exemplo verifica a MTU do caminho entre a instância do EC2 e o arquivo `www.elifulkerson.com`.

```
.\mturoute.exe www.elifulkerson.com
```

Neste exemplo de saída, a MTU do caminho é 1500.

```
* ICMP Fragmentation is not permitted. *
* Speed optimization is enabled. *
* Maximum payload is 10000 bytes. *
+ ICMP payload of 1472 bytes succeeded.
- ICMP payload of 1473 bytes is too big.
Path MTU: 1500 bytes.
```

Verificação da MTU para a instância

É possível verificar o valor da MTU para a instância. Algumas instâncias são configuradas para usar frames jumbo, e outras são configuradas para usar tamanhos de quadro padrão.

O procedimento usado dependerá do sistema operacional da instância.

Instâncias do Linux

Para verificar a configuração de MTU em uma instância do Linux

Execute o comando ip apresentado a seguir na instância do EC2. Se a interface de rede primária não for `eth0`, substitua `eth0` pela sua interface de rede.

```
[ec2-user ~]$ ip link show eth0
```

Neste exemplo de saída, *mtu 9001* indica que a instância usa frames jumbo.

```
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
```

Instâncias do Windows

O procedimento usado dependerá do driver da instância.

ENA driver

Versão 2.1.0 e versões posteriores

Para obter o valor da MTU, use o comando Get-NetAdapterAdvancedProperty apresentado a seguir na instância do EC2. Use o caractere curinga (asterisco) para obter todos os nomes Ethernet. Verifique a saída para o nome da interface `*JumboPacket`. Um valor de 9015 indica que os frames jumbo estão ativados. Os frames jumbo ficam desativados por padrão.

```
Get-NetAdapterAdvancedProperty -Name "Ethernet*"
```

Versão 1.5 e versões anteriores

Para obter o valor da MTU, use o comando Get-NetAdapterAdvancedProperty apresentado a seguir na instância do EC2. Verifique a saída para o nome da interface `MTU`. Um valor de 9001 indica que os frames jumbo estão ativados. Os frames jumbo ficam desativados por padrão.

```
Get-NetAdapterAdvancedProperty -Name "Ethernet"
```

Intel SRIOV 82599 driver

Para obter o valor da MTU, use o comando Get-NetAdapterAdvancedProperty apresentado a seguir na instância do EC2. Verifique entrada do nome da interface `*JumboPacket`. Um valor de 9014 indica que os frames jumbo estão ativados. (Observe que o tamanho do MTU inclui o cabeçalho e a carga.) Os frames jumbo ficam desativados por padrão.

```
Get-NetAdapterAdvancedProperty -Name "Ethernet"
```

AWS PV driver

Para obter o valor da MTU, use o comando apresentado a seguir na instância do EC2. O nome da interface pode variar. Na saída, procure uma entrada intitulada "Ethernet", "Ethernet 2" ou "Conexão Local". Você precisará do nome da interface para ativar ou desativar os frames jumbo. Um valor de 9001 indica que os frames jumbo estão ativados.

```
netsh interface ipv4 show subinterface
```

Definição da MTU para a instância

É possível querer usar frames jumbo para o tráfego de rede na VPC e frames padrão para o tráfego para a Internet. Seja qual for o seu caso de uso, recomendamos verificar se a instância se comporta conforme o esperado.

O procedimento usado dependerá do sistema operacional da instância.

Instâncias do Linux

Para definir o valor de MTU em uma instância do Linux

1. Execute o comando ip apresentado a seguir na instância. O comando define o valor da MTU desejado para 1500, mas é possível usar 9001. Se a interface de rede primária não for `eth0`, substitua `eth0` pela interface de rede real.

   ```
   [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.

   - Amazon Linux 2023: modifique a seção `[Link]` do arquivo de configuração. O arquivo de configuração padrão é `/usr/lib/systemd/network/80-ec2.network`, ou você pode atualizar qualquer arquivo de configuração personalizado criado em /run/systemd/network/, em que o nome do arquivo é *priority*-*interface*.network. Para obter mais informações, consulte Networking service na documentação do Amazon Linux.

     ```
     MTUBytes=1500
     ```

   - Amazon Linux 2: adicione a seguinte linha ao arquivo `/etc/sysconfig/network-scripts/ifcfg-eth0`:

     ```
     MTU=1500
     ```

     Adicione a linha a seguir ao arquivo `/etc/dhcp/dhclient.conf`:

     ```
     request subnet-mask, broadcast-address, time-offset, routers, domain-name,
      domain-search, domain-name-servers, host-name, nis-domain, nis-servers, ntp-
     servers;
     ```

- Outras distribuições do Linux: consulte a documentação específica.

3. (Opcional) Reinicialize sua instância e verifique se a configuração de MTU está correta.

Instâncias do Windows

O procedimento usado dependerá do driver da instância.

ENA driver

É possível alterar a MTU usando o Gerenciador de Dispositivos ou o comando Set-NetAdapterAdvancedProperty na instância.

Versão 2.1.0 e versões posteriores

Use o comando apresentado a seguir para habilitar frames jumbo.

```
Set-NetAdapterAdvancedProperty -Name "Ethernet" -RegistryKeyword "*JumboPacket" -
RegistryValue 9015
```

Use o comando apresentado a seguir para desabilitar frames jumbo.

```
Set-NetAdapterAdvancedProperty -Name "Ethernet" -RegistryKeyword "*JumboPacket" -
RegistryValue 1514
```

Versão 1.5 e versões anteriores

Use o comando apresentado a seguir para habilitar frames jumbo.

```
Set-NetAdapterAdvancedProperty -Name "Ethernet" -RegistryKeyword "MTU" -
RegistryValue 9001
```

Use o comando apresentado a seguir para desabilitar frames jumbo.

```
Set-NetAdapterAdvancedProperty -Name "Ethernet" -RegistryKeyword "MTU" -
RegistryValue 1500
```

Intel SRIOV 82599 driver

É possível alterar a MTU usando o Gerenciador de Dispositivos ou o comando Set-NetAdapterAdvancedProperty na instância.

Use o comando apresentado a seguir para habilitar frames jumbo.

```
Set-NetAdapterAdvancedProperty -Name "Ethernet" -RegistryKeyword "*JumboPacket" -
RegistryValue 9014
```

Use o comando apresentado a seguir para desabilitar frames jumbo.

```
Set-NetAdapterAdvancedProperty -Name "Ethernet" -RegistryKeyword "*JumboPacket" -
RegistryValue 1514
```

AWS PV driver

É possível alterar a MTU usando o comando netsh na instância. Não é possível alterar a MTU usando o Gerenciador de Dispositivos.

Use o comando apresentado a seguir para habilitar frames jumbo.

```
netsh interface ipv4 set subinterface "Ethernet" mtu=9001
```

Use o comando apresentado a seguir para desabilitar frames jumbo.

```
netsh interface ipv4 set subinterface "Ethernet" mtu=1500
```

Solução de problemas

Se você tiver problemas de conectividade entre a instância do EC2 e um cluster do Amazon Redshift ao usar jumbo frames, consulte As consultas parecem travar e às vezes não se comunicam com o cluster no Guia de gerenciamento do Amazon Redshift.

Nuvens privadas virtuais para as instâncias do EC2

O Amazon Virtual Private Cloud (Amazon VPC) permite que você defina uma rede virtual em sua própria área logicamente isolada na nuvem AWS, conhecida como uma nuvem privada virtual ou VPC. É possível criar recursos da AWS, como instâncias do Amazon EC2, nas sub-redes da sua VPC. Sua VPC assemelha-se a uma rede tradicional que é possívelria operar no seu próprio data center, com os benefícios de usar a infraestrutura escalável da AWS. É possível configurar seu VPC, selecionar o intervalo de endereços IP dele, criar sub-redes e definir tabelas de rotas, gateways de

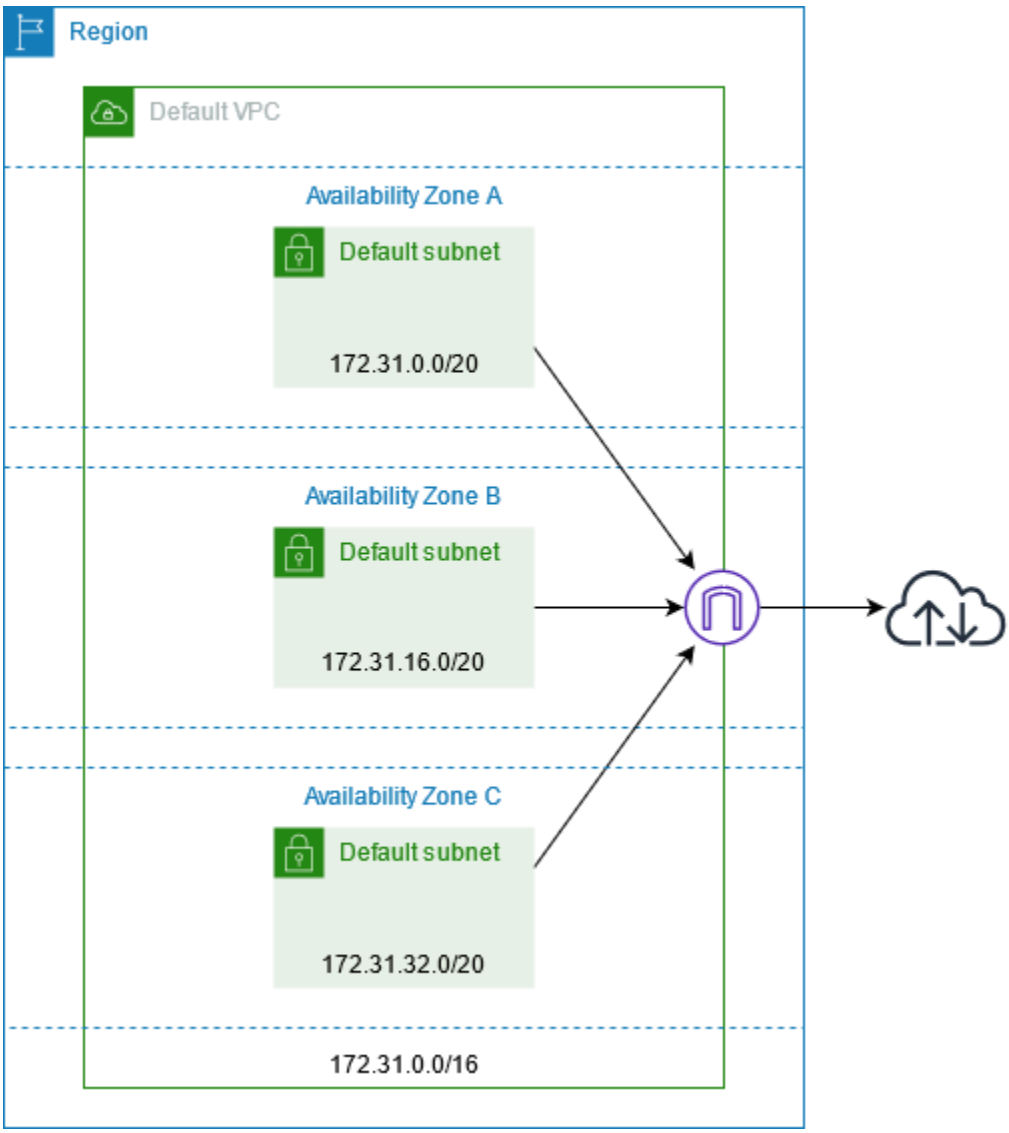
rede e configurações de segurança. É possível conectar instâncias na VPC à Internet ou ao seu próprio data center.

Conteúdo

- Suas VPCs padrão
- VPCs não padrão
- Acesso à Internet
- Sub-redes compartilhadas
- Sub-redes somente IPv6

Suas VPCs padrão

Quando você cria sua conta da AWS, nós criamos uma VPC padrão em cada região. Uma VPC padrão é uma VPC que já está configurada e pronta para uso. Por exemplo, há uma sub-rede padrão para cada zona de disponibilidade em cada VPC padrão, um gateway da Internet vinculado à VPC, e há uma rota na tabela de rotas principal que envia todo o tráfego (0.0.0.0/0) para o gateway da Internet. É possível modificar a configuração das suas VPCs padrão, conforme necessário. Por exemplo, você pode adicionar sub-redes e tabelas de rotas.



VPCs não padrão

Em vez de usar uma VPC padrão para seus recursos, você pode criar sua própria VPC, conforme descrito em Crie uma VPC no Guia do usuário da Amazon VPC.

Considere o seguinte ao criar uma VPC para suas instâncias do EC2.

- Você pode usar a sugestão padrão para o bloco CIDR IPv4 ou inserir o bloco CIDR exigido pela sua aplicação ou rede.
- Para garantir alta disponibilidade, crie sub-redes em várias zonas de disponibilidade.
- Se for necessário tornar suas instâncias acessíveis pela Internet, faça o seguinte:

- Se as instâncias puderem ficar em uma sub-rede pública, adicione sub-redes públicas. Mantenha as duas opções de DNS habilitadas. Opcionalmente, você pode adicionar sub-redes privadas agora ou mais tarde.
- Se as instâncias precisarem estar em uma sub-rede privada, adicione somente sub-redes privadas. Você pode adicionar um gateway NAT para fornecer acesso à internet às instâncias nas sub-redes privadas. Se suas instâncias enviarem ou receberem um volume significativo de tráfego nas zonas de disponibilidade, crie um gateway NAT em cada zona de disponibilidade. Caso contrário, você pode criar um gateway NAT em apenas uma das zonas de disponibilidade e executar instâncias que enviam ou recebem tráfego entre zonas na mesma zona de disponibilidade do gateway NAT.

Acesso à Internet

As instâncias iniciadas para uma sub-rede padrão em uma VPC padrão têm acesso à Internet, pois as VPCs padrão estão configuradas para atribuir endereços IP públicos e nomes de host do DNS, e a tabela de rotas principal está configurada com uma rota para um gateway da Internet conectado à VPC.

Para instâncias iniciadas em sub-redes e VPCs não padrão, você pode usar uma das seguintes opções para garantir que as instâncias iniciadas nessas sub-redes tenham acesso à Internet:

- Configurar um gateway da Internet. Para obter mais informações, consulte Estabelecer conexão com a Internet usando um gateway da Internet no Guia do usuário da Amazon VPC.
- Configure um gateway NAT público. Para mais informações, consulte Acessar a Internet de uma sub-rede privada no Guia do usuário da Amazon VPC.

Sub-redes compartilhadas

Ao iniciar instâncias do EC2 em sub-redes de VPC compartilhadas, observe o seguinte:

- Os participantes podem executar instâncias em uma sub-rede especificando o ID da sub-rede compartilhada. Os participantes devem ser os proprietários de qualquer interface de rede que especificarem.
- Os participantes podem iniciar, interromper, encerrar e descrever as instâncias que eles criaram em uma sub-rede compartilhada. Os participantes não podem iniciar, interromper, encerrar nem descrever as instâncias criadas pelo proprietário da VPC em uma sub-rede compartilhada.

- Os proprietários da VPC não podem iniciar, interromper, encerrar nem descrever as instâncias criadas pelos participantes em uma sub-rede compartilhada.
- Os participantes podem se conectar a uma instância em uma sub-rede compartilhada usando o endpoint de conexão de instância do EC2. O participante deve criar um endpoint de conexão de instância do EC2 na sub-rede compartilhada. Os participantes não podem usar o endpoint de conexão de instância do EC2 que o proprietário da VCP criou na sub-rede compartilhada.

Para obter informações sobre recursos compartilhados do Amazon EC2, consulte o seguinte:

- the section called “Gerenciar o compartilhamento de uma AMI com uma organização ou uma UO”
- the section called “Reservas de capacidade compartilhadas”
- the section called “Grupos de posicionamento compartilhados”
- Compartilhamento de host dedicado do Amazon EC2 entre contas

Para obter mais informações sobre o compartilhamento de sub-redes, consulte Compartilhar sua VPC com outras contas no Guia do usuário da Amazon VPC.

Sub-redes somente IPv6

Uma instância do EC2 iniciada em uma sub-rede exclusivamente IPv6 recebe um endereço IPv6, mas não um endereço IPv4. Qualquer instância que você execute em uma sub-rede somente IPv6 precisa ser uma instância baseada em Nitro.

Redes secundárias

Redes secundárias são redes virtuais criadas especificamente para casos de uso de redes especializadas. Essas redes são isoladas logicamente dentro das partições da Nuvem AWS. Você pode criar recursos como sub-redes secundárias em sua rede secundária. As redes secundárias são fortemente acopladas às Amazon VPCs, de forma que instâncias selecionadas são hospedadas em várias hospedagens e lançadas em uma VPC e em uma rede secundária.

Atualmente, as redes secundárias estão disponíveis para tipos de instância selecionados e por meio de reservas de capacidade com compromissos de longo prazo. Entre em contato com sua equipe de contas para obter mais informações se achar que redes secundárias podem ser benéficas para sua workload.

Conteúdo

- O que são redes secundárias?
- Principais conceitos
- Arquitetura
- Considerações adicionais
- Introdução
- Gerenciar recursos de rede secundária
- Práticas recomendadas de projeto de rede
- Solução de problemas
- Cotas e limites

O que são redes secundárias?

As redes secundárias fornecem uma rede lógica e isolada, usada em combinação com uma rede VPC, de forma que as instâncias sejam hospedadas em várias redes independentes. Os benefícios das redes secundárias incluem:

- Redes de alto desempenho para casos de uso e protocolos especializados, como conectividade leste-oeste para workloads de ML
- Suporte multilocatário com isolamento lógico
- As instâncias se integram perfeitamente a VPCs e serviços da AWS

Principais conceitos

Rede secundária

Um constructo de rede regional que fornece uma rede lógica de camada 3 com um bloco CIDR IPv4 (variando de /28 a /12). As redes secundárias operam independentemente das VPCs em uma infraestrutura de rede particionada fisicamente.

Sub-rede secundária

Um constructo específico da zona de disponibilidade em uma rede secundária, semelhante às sub-redes VPC. As sub-redes secundárias suportam blocos CIDR que variam de /28 a /12.

Interface secundária

Interfaces de rede conectadas a placas de rede secundárias, fornecendo conectividade leste-oeste em sub-redes secundárias. Essas interfaces são física e logicamente separadas das Interfaces de Rede Elástica (ENIs).

Arquitetura

As instâncias do EC2 que oferecem suporte a redes secundárias têm vários hospedeiros, o que significa que podem se comunicar simultaneamente em uma VPC e em uma rede secundária:

- VPC: fornece conectividade TCP/IP norte-sul a serviços da AWS, armazenamento, bancos de dados, serviços de rede e Internet
- Rede secundária: fornece conectividade leste-oeste entre instâncias especializadas compatíveis

Considerações adicionais

- As interfaces secundárias são gerenciadas por meio de RunInstances e não podem ser criadas ou excluídas de forma independente.
- As interfaces secundárias não podem ser anexadas/desanexadas depois que a instância é iniciada.
- Os endereços IP das interfaces secundárias não podem ser alterados depois de iniciados.
- Atributos da VPC, como grupos de segurança, NACLs e logs de fluxo, não são compatíveis com redes secundárias.

Introdução

Pré-requisitos

Antes de iniciar instâncias com redes secundárias, verifique se você também configurou sua VPC na região de destino e uma sub-rede na zona de disponibilidade desejada de sua capacidade do EC2.

Etapa 1: criar uma rede secundária

Crie uma rede secundária na mesma região da sua VPC. Esse é um recurso regional que fornece isolamento lógico para seu tráfego RDMA.

```
aws ec2 create-secondary-network \
  --type rdma \
  --ipv4-cidr-block 172.31.0.0/16 \
  --region us-east-2
```

Parâmetros:

- `--type`: tipo de rede (atualmente somente rdma é compatível)
- `--ipv4-cidr-block`: bloco CIDR IPv4 entre /28 e /12
- `--region`: região da AWS (US-East-2)

> **Note**
>
> Prática recomendada: escolha um bloco CIDR que não se sobreponha ao CIDR da VPC para simplificar o roteamento no nível da instância.

Etapa 2: criar uma sub-rede secundária

Crie uma sub-rede secundária na mesma zona de disponibilidade da sua sub-rede VPC. Esse é um recurso específico do AZ.

```
aws ec2 create-secondary-subnet \
  --secondary-network-id sn-1234567890abcdef0 \
  --ipv4-cidr-block 172.31.24.0/24 \
  --availability-zone us-east-2a
```

> **Note**
>
> Reserva de endereços IP: como sub-redes da VPC, a Amazon reserva os primeiros 4 endereços IP e o último endereço IP em cada sub-rede secundária para uso interno.

Etapa 3: iniciar uma instância

Inicie uma instância na sub-rede VPC e na sub-rede secundária. A instância terá vários hospedeiros com conectividade com as duas redes.

```
aws ec2 run-instances \
  --image-id ami-12345678 \
  --count 1 \
  --instance-type <instance> \
  --key-name MyKeyPair \
  --instance-market-options '{"MarketType": "capacity-block"}' \
  --capacity-reservation-specification '{"CapacityReservationTarget": \
  {"CapacityReservationId": "cr-1234567890abcdef0"}}' \
  --network-interfaces \
    "NetworkCardIndex=0,DeviceIndex=0,Groups=sg-12345678,\
    SubnetId=subnet-0987654321fedcba0,InterfaceType=interface" \
  --secondary-interfaces \
    "NetworkCardIndex=1,DeviceIndex=0,SecondarySubnetId=ss-98765421yxz,\
    InterfaceType=secondary,PrivateIpAddressCount=1,DeleteOnTermination=true", \
    "NetworkCardIndex=2,DeviceIndex=0,SecondarySubnetId=ss-98765421yxz,\
    InterfaceType=secondary,PrivateIpAddressCount=1,DeleteOnTermination=true", \
    "NetworkCardIndex=3,DeviceIndex=0,SecondarySubnetId=ss-98765421yxz,\
    InterfaceType=secondary,PrivateIpAddressCount=1,DeleteOnTermination=true", \
    "NetworkCardIndex=4,DeviceIndex=0,SecondarySubnetId=ss-98765421yxz,\
    InterfaceType=secondary,PrivateIpAddressCount=1,DeleteOnTermination=true", \
    "NetworkCardIndex=5,DeviceIndex=0,SecondarySubnetId=ss-98765421yxz,\
    InterfaceType=secondary,PrivateIpAddressCount=1,DeleteOnTermination=true", \
    "NetworkCardIndex=6,DeviceIndex=0,SecondarySubnetId=ss-98765421yxz,\
    InterfaceType=secondary,PrivateIpAddressCount=1,DeleteOnTermination=true", \
    "NetworkCardIndex=7,DeviceIndex=0,SecondarySubnetId=ss-98765421yxz,\
    InterfaceType=secondary,PrivateIpAddressCount=1,DeleteOnTermination=true", \
    "NetworkCardIndex=8,DeviceIndex=0,SecondarySubnetId=ss-98765421yxz,\
    InterfaceType=secondary,PrivateIpAddressCount=1,DeleteOnTermination=true"
```

Principais parâmetros:

- `--network-interfaces`: especifica o Nitro ENI primário para conectividade VPC (índice de placa de rede 0)
- `--secondary-interfaces`: especifica 8 interfaces secundárias para conectividade leste-oeste em sub-redes secundárias (índices de placa de rede de 1 a 8)
- `InterfaceType=secondary`: indica uma interface secundária

Gerenciar recursos de rede secundária

Noções básicas sobre redes secundárias

Visualizar detalhes sobre suas redes secundárias:

```
aws ec2 describe-secondary-networks \
  --secondary-network-id sn-1234567890abcdef0
```

Noções básicas sobre as sub-redes secundárias

Visualizar detalhes sobre suas sub-redes secundárias:

```
aws ec2 describe-secondary-subnets \
  --secondary-subnet-id ss-98765421yxz
```

Noções básicas sobre interfaces secundárias

Visualize os detalhes sobre as interfaces de rede secundárias conectadas às suas instâncias:

```
aws ec2 describe-secondary-interfaces \
  --filters "Name=attachment.instance-id,Values=i-1234567890abcdef0"
```

Excluir recursos

Excluir uma sub-rede secundária:

```
aws ec2 delete-secondary-subnet \
  --secondary-subnet-id ss-98765421yxz
```

Excluir uma rede secundária:

```
aws ec2 delete-secondary-network \
  --secondary-network-id sn-1234567890abcdef0
```

Important

Você deve encerrar todas as instâncias e excluir todas as sub-redes secundárias antes de excluir uma rede secundária.

Práticas recomendadas de projeto de rede

Planejamento CIDR

Evite a sobreposição de CIDRs: embora as redes secundárias estejam fisicamente isoladas das VPCs, o uso de blocos CIDR não sobrepostos simplifica a configuração de roteamento no nível do sistema operacional da instância.

> **Note**
>
> A Amazon reserva 5 endereços IP por sub-rede.

Segmentação de tráfego

Segregar por rede secundária: crie redes secundárias separadas para diferentes projetos, equipes ou limites de segurança. As redes secundárias fornecem isolamento lógico entre instâncias. As instâncias não podem se comunicar em diferentes redes secundárias.

Use várias sub-redes: em uma rede secundária, use várias sub-redes secundárias para segmentar o tráfego por índice de GPU, zona de disponibilidade ou tipo de workload. Como exemplo, um padrão de arquitetura comum é implantar uma única rede secundária com 4 ou 8 sub-redes secundárias, onde cada sub-rede secundária está alinhada a um grupo de GPUs de índices comuns.

Solução de problemas

Falhas ao iniciar a instância

Problema: falhas na inicialização da instância com interfaces de rede secundária.

Soluções:

- Verifique se sua AMI inclui suporte adequado ao driver
- Verifique se sua sub-rede secundária tem endereços IP disponíveis suficientes
- Confirme se sua reserva de capacidade está no estado “ativo”
- Verifique se sua sub-rede secundária está na mesma zona de disponibilidade que sua sub-rede VPC

Problemas de conectividade

Problema: não foi possível estabelecer conectividade RDMA entre instâncias.

Soluções:

- Verifique se todas as instâncias estão na mesma rede secundária e sub-rede secundária
- Verifique se os drivers da interface secundária estão carregados corretamente na instância
- Verifique se sua aplicação está vinculada às interfaces de rede corretas
- As instâncias dentro da mesma sub-rede secundária podem ser acessadas por meio de rotas diretas. A comunicação entre sub-redes está disponível por meio de uma rota estática fornecida via DHCP.

Erros de API

Problema: as chamadas de API para operações de rede secundária e sub-rede secundária falham.

Soluções:

- Verifique as permissões do IAM para ec2:CreateSecondaryNetwork, ec2:CreateSecondarySubnet etc.
- Verifique se os blocos CIDR estão dentro do intervalo suportado (/28 a /12)
- Verifique se você está usando a região e zona de disponibilidade corretas

Cotas e limites

Para solicitar um aumento de cota, use o AWSService Quotas ou entre em contato com o AWS Support.

Cotas e limites de redes secundárias

Recurso	Limite	Ajustável
Redes secundárias por região	5	Sim
Sub-redes secundárias por rede secundária	200	Sim

Recurso	Limite	Ajustável
Tamanho do bloco CIDR	/28 a /12	Não

Segurança no Amazon EC2

A segurança na nuvem na AWS é a nossa maior prioridade. Como cliente da AWS, você se beneficiará de um data center e de uma arquitetura de rede criados para atender aos requisitos das empresas com as maiores exigências de segurança.

A segurança é uma responsabilidade compartilhada entre a AWS e você. O modelo de responsabilidade compartilhada descreve isso como a segurança da nuvem e a segurança na nuvem:

- Segurança da nuvem: a AWS é responsável pela proteção da infraestrutura que executa serviços AWS na Nuvem AWS. A AWS também fornece serviços que podem ser usados com segurança. Auditores de terceiros testam e verificam regularmente a eficácia da nossa segurança como parte dos Programas de conformidade da AWS. Para saber mais sobre os programas de compatibilidade que se aplicam ao Amazon EC2, consulte Serviços da AWS em escopo por programa de compatibilidade.
- Segurança na nuvem: sua responsabilidade inclui as seguintes áreas:
  - Controlar o acesso à rede para as instâncias, por exemplo, por meio da configuração da VPC e dos grupos de segurança. Para obter mais informações, consulte Controlar o tráfego de rede.
  - Gerenciar as credenciais usadas para a conexão às instâncias.
  - Gerenciar o sistema operacional convidado e o software implantado no sistema operacional convidado, incluindo atualizações e patches de segurança. Para obter mais informações, consulte Gerenciamento de atualizações para instâncias do Amazon EC2.
  - Configurar as funções do IAM anexadas à instância e as permissões associadas a estas funções. Para obter mais informações, consulte Funções do IAM para Amazon EC2.

Esta documentação ajuda a entender como aplicar o modelo de responsabilidade compartilhada ao usar o Amazon EC2. Ela mostra como configurar o Amazon EC2 para atender aos objetivos de segurança e conformidade. Saiba também como usar outros serviços da AWS que ajudam você a monitorar e proteger os recursos do Amazon EC2.

Conteúdo

- Proteção de dados no Amazon EC2
- Segurança da infraestrutura no Amazon EC2
- Resiliência no Amazon EC2

- Validação de conformidade do Amazon EC2
- Identity and Access Management para o Amazon EC2
- Gerenciamento de atualizações para instâncias do Amazon EC2
- Práticas recomendadas de segurança para instâncias do Windows
- Pares de chaves do Amazon EC2 e instâncias do Amazon EC2
- Grupos de segurança do Amazon EC2 para as instâncias do EC2
- NitroTPM para instâncias do Amazon EC2
- Atestação de instância do Amazon EC2
- Credential Guard para instâncias do Windows
- Acessar o Amazon EC2 usando um endpoint da VPC de interface

Proteção de dados no Amazon EC2

O modelo de responsabilidade compartilhada da AWS se aplica à proteção de dados no Amazon Elastic Compute Cloud. Conforme descrito nesse modelo, a AWS é responsável por proteger a infraestrutura global que executa toda a Nuvem AWS. Você é responsável por manter o controle sobre o conteúdo hospedado nessa infraestrutura. Você também é responsável pelas tarefas de configuração e gerenciamento de segurança dos Serviços da AWS que usa. Para saber mais sobre a privacidade de dados, consulte as Data Privacy FAQ. Para saber mais sobre a proteção de dados na Europa, consulte a postagem do blog AWS Shared Responsibility Model and RGPD no Blog de segurança da AWS.

Para fins de proteção de dados, recomendamos que você proteja as credenciais da Conta da AWS e configure as contas de usuário individuais com Centro de Identidade do AWS IAM ou AWS Identity and Access Management (IAM). Dessa maneira, cada usuário receberá apenas as permissões necessárias para cumprir suas obrigações de trabalho. Recomendamos também que você proteja seus dados das seguintes formas:

- Use uma autenticação multifator (MFA) com cada conta.
- Use SSL/TLS para se comunicar com os recursos da AWS. Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Configure os logs de API e atividade do usuário com AWS CloudTrail. Para saber mais sobre como usar as trilhas do CloudTrail para capturar atividades da AWS, consulte Working with CloudTrail trails no Guia do usuário do AWS CloudTrail.

- Use as soluções de criptografia AWS, juntamente com todos os controles de segurança padrão em Serviços da AWS.
- Use serviços gerenciados de segurança avançada, como o Amazon Macie, que ajuda a localizar e proteger dados sensíveis armazenados no Amazon S3.
- Se você precisar de módulos criptográficos validados pelo FIPS 140-3 ao acessar a AWS por meio de uma interface de linha de comandos ou de uma API, use um endpoint do FIPS. Para saber mais sobre os endpoints FIPS disponíveis, consulte Federal Information Processing Standard (FIPS) 140-3.

É altamente recomendável que nunca sejam colocadas informações confidenciais ou sensíveis, como endereços de e-mail de clientes, em tags ou campos de formato livre, como um campo Nome. Isso também vale para o uso do Amazon EC2 ou de outros Serviços da AWS com o console, a API, a AWS CLI ou os AWS SDKs. Quaisquer dados inseridos em tags ou em campos de texto de formato livre usados para nomes podem ser usados para logs de faturamento ou de diagnóstico. Se você fornecer um URL para um servidor externo, é fortemente recomendável que não sejam incluídas informações de credenciais no URL para validar a solicitação nesse servidor.

Conteúdo

- Segurança de dados do Amazon EBS
- Criptografia em repouso
- Criptografia em trânsito

Segurança de dados do Amazon EBS

Os volumes do Amazon EBS são apresentados a você como dispositivos de bloco brutos e não formatados. Eles são dispositivos lógicos criados na infraestrutura do EBS, e o serviço Amazon EBS garante que os dispositivos estejam logicamente vazios (ou seja, os blocos brutos são zerados ou contêm dados pseudorrandomizados criptograficamente) antes de qualquer uso ou reutilização por um cliente.

Se você tiver procedimentos que exigem que todos os dados sejam apagados usando um método específico, após ou antes do uso (ou ambos), como aqueles detalhados em DoD 5220,22-M (Manual Operacional do Programa Nacional de Segurança Industrial) ou em NIST 800-88 (Diretrizes para higienização de mídia), será possível fazer isso no Amazon EBS. Essa atividade em nível de bloco será refletida na mídia de armazenamento subjacente dentro do serviço do Amazon EBS.

Criptografia em repouso

Volumes do EBS

A criptografia do Amazon EBS é uma solução de criptografia para snapshots e volumes do EBS. Ele usa a AWS KMS keys. Para obter mais informações, consulte Criptografia do Amazon EBS no Guia do usuário do Amazon EBS.

[Instâncias do Windows] Você também pode usar permissões do Microsoft EFS e do NTFS para criptografia em nível de pastas e de arquivos.

Volumes de armazenamento de instâncias

Os dados nos volumes de armazenamento de instâncias de NVMe são criptografados usando uma criptografia XTS-AES-256 implementada em um módulo de hardware na instância. As chaves usadas para criptografar dados gravados em dispositivos de armazenamento NVMe conectados localmente são por cliente e por volume. As chaves são geradas e residem apenas dentro do módulo de hardware, que é inacessível para o pessoal da AWS. As chaves de criptografia são destruídas quando a instância é interrompida ou encerrada e não podem ser recuperadas. Você não pode desativar essa criptografia e não pode fornecer sua própria chave de criptografia.

Os dados em volumes de armazenamento de instância HDD em instâncias H1, D3 e D3en são criptografados usando XTS-AES-256 e chaves de uso único.

Quando você interrompe, hiberna ou termina uma instância, cada bloco de armazenamento no volume do armazenamento de instância é redefinido. Portanto, seus dados não podem ser acessados por meio do armazenamento de instâncias de outra instância.

Memória

A criptografia de memória está habilitada nas seguintes instâncias:

- Instâncias com processadores AWS Graviton2 ou AWS Graviton posteriores são compatíveis com criptografia de memória sempre ativa. As chaves de criptografia são geradas com segurança dentro do sistema host, não saem do sistema host e são destruídas quando o host é reinicializado ou desligado. Para obter mais informações, consulte Processadores AWS Graviton.
- Instâncias com processadores Intel Xeon Scalable de 3ª geração (Ice Lake), como instâncias M6i, e processadores Intel Xeon Scalable de 4ª geração (Sapphire Rapids), como instâncias M7i. Esses processadores são compatíveis com criptografia de memória sempre ativa usando a Intel Total Memory Encryption (TME).

- Instâncias com processadores AMD EPYC de 3ª geração (Milan), como instâncias M6a, e processadores AMD EPYC de 4ª geração (Genoa), como instâncias M7a. Esses processadores são compatíveis com criptografia de memória always-on usando Secure Memory Encryption (SME) da AMD.
- O Secure Encrypted Virtualization-Secure Nested Paging (SEV-SNP) do AMD é compatível com alguns tipos de instâncias baseadas em AMD. Para obter mais informações, consulte Encontrar tipos de instância do EC2 que são compatíveis com o AMD SEV-SNP.

Criptografia em trânsito

Criptografia na camada física

Todos os dados fluindo pelas regiões da AWS por meio da rede global da AWS é automaticamente criptografada na camada física antes de sair das instalações seguras da AWS. Todo o tráfego entre AZs é criptografado. Camadas adicionais de criptografia, inclusive as listadas nesta seção, podem fornecer mais proteções.

Criptografia fornecida pelo emparelhamento da Amazon VPC e do Transit Gateway entre regiões

Todo o tráfego entre regiões que usa o emparelhamento da Amazon VPC e do Transit Gateway é automaticamente criptografado em massa ao sair de uma região. Uma camada adicional de criptografia é fornecida automaticamente à camada física para todo o tráfego antes que ele saia das instalações seguras da AWS, conforme observado anteriormente nesta seção.

Criptografia entre instâncias

A AWS fornece conectividade privada e segura entre instâncias do EC2 de todos os tipos. Além disso, alguns tipos de instância usam os recursos de descarregamento do hardware subjacente Nitro System para criptografar automaticamente o tráfego em trânsito entre instâncias. Essa criptografia usa algoritmos de criptografia autenticada com dados associados (AEAD) com criptografia de 256 bits. Não há impacto na performance da rede. Para oferecer suporte a essa criptografia adicional de tráfego em trânsito entre instâncias, os seguintes requisitos devem ser atendidos:

- As instâncias usam os seguintes tipos de instância:
  - Uso geral: M5dn, M5n, M5zn, M6a, M6i, M6id, M6idn, M6in, M7a, M7g, M7gd, M7i, M7i-flex, M8a, M8azn, M8g, M8gb, M8gd, M8gn, M8i, M8id, M8i-flex, Mac-m4, Mac-m4pro
  - Otimizadas para computação: C5n, C6a, C6gn, C6i, C6id, C6in, C7a, C7g, C7gd, C7gn, C7i, C7i-flex, C8a, C8g, C8gb, C8gd, C8gn, C8i, C8id, C8i-flex

  - Otimizadas para memória: R5dn, R5n, R6a, R6i, R6id, R6idn, R6in, R7a, R7g, R7gd, R7i, R7iz, R8a, R8g, R8gb, R8gd, R8gn, R8i, R8id, R8i-flex, U-3tb1, U-6tb1, U-9tb1, U-12tb1, U-18tb1, U-24tb1, U7i-6tb, U7i-8tb, U7i-12tb, U7in-16tb, U7in-24tb, U7in-32tb, U7inh-32tb, X2idn, X2iedn, X2iezn, X8g, X8aedz, X8i
  - Otimizadas para armazenamento: D3, D3en, I3en, I4g, I4i, I7i, I7ie, I8g, I8ge, Im4gn, Is4gen
  - Computação acelerada: DL1, DL2q, F2, G4ad, G4dn, G5, G6, G6e, G6f, Gr6, Gr6f, G7e, Inf1, Inf2, P3dn, P4d, P4de, P5, P5e, P5en, P6-B200, P6-B300, P6e-GB200, Trn1, Trn1n, Trn2, Trn2u, VT1
  - Computação de alta performance: Hpc6a, Hpc6id, Hpc7a, Hpc7g, Hpc8a
- As instâncias estão na mesma região.
- As instâncias estão na mesma VPC ou VPCs emparelhadas, e o tráfego não passa por um dispositivo ou serviço de rede virtual, como um balanceador de carga ou um gateway de trânsito.

Uma camada adicional de criptografia é fornecida automaticamente à camada física para todo o tráfego antes que ele saia das instalações seguras da AWS, conforme observado anteriormente nesta seção.

Para visualizar os tipos de instância que criptografam o tráfego em trânsito entre instâncias usando o AWS CLI

Use o comando describe-instance-types a seguir.

```
aws ec2 describe-instance-types \
    --filters Name=network-info.encryption-in-transit-supported,Values=true \
    --query "InstanceTypes[*].[InstanceType]" \
    --output text | sort
```

Criptografia de e para o AWS Outposts

Um Outpost cria conexões de rede especiais chamadas links de serviço à região da AWS inicial e, opcionalmente, conectividade privada com uma sub-rede da VPC especificada. Todo o tráfego que passa por essas conexões é totalmente criptografado. Para obter mais informações, consulte Conectividade por meio de links de serviço e Criptografia em trânsito no Manual do usuário do AWS Outposts.

Criptografia de acesso remoto

Os protocolos SSH e RDP fornecem canais de comunicação seguros para acesso remoto às instâncias, seja diretamente, seja por meio do EC2 Instance Connect. O acesso remoto às instâncias usando o Gerenciador de Sessões ou o Run Command do AWS Systems Manager é criptografado usando TLS 1.2, e as solicitações para criar uma conexão são assinadas usando SigV4 e autenticadas e autorizadas pelo AWS Identity and Access Management.

É de sua responsabilidade usar um protocolo de criptografia, como o Transport Layer Security (TLS), para criptografar dados sigilosos em trânsito entre clientes e suas instâncias do Amazon EC2.

(Instâncias do Windows) Certifique-se de permitir somente conexões criptografadas entre as instâncias do EC2 e os endpoints da API da AWS ou outros serviços de rede remota confidenciais. Isso pode ser imposto por meio do uso de grupo de segurança de saída ou regras de Firewall do Windows.

Segurança da infraestrutura no Amazon EC2

Como um serviço gerenciado, o Amazon Elastic Compute Cloud é protegido pela segurança da rede global da AWS. Para obter informações sobre serviços de segurança da AWS e como a AWS protege a infraestrutura, consulte Segurança na Nuvem AWS. Para projetar seu ambiente da AWS usando as práticas recomendadas de segurança da infraestrutura, consulte Proteção de Infraestrutura em Pilar de Segurança: AWS Estrutura bem arquitetada.

Você usa chamadas à API publicadas pela AWS para acessar o Amazon EC2 por meio da rede. Os clientes devem oferecer compatibilidade com:

- Transport Layer Security (TLS). Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Conjuntos de criptografia com perfect forward secrecy (PFS) como DHE (Ephemeral Diffie-Hellman) ou ECDHE (Ephemeral Elliptic Curve Diffie-Hellman). A maioria dos sistemas modernos, como Java 7 e versões posteriores, comporta esses modos.

Para obter mais informações, consulte Proteção de infraestrutura no Pilar de Segurança: AWS Well-Architected Framework.

Isolamento de rede

Uma nuvem virtual privada (VPC) é uma rede virtual na área isolada logicamente na Nuvem AWS. Use VPCs separadas para isolar a infraestrutura por workload ou entidade organizacional.

Uma sub-rede é um intervalo de endereços IP em uma VPC. Quando executa uma instância, você a executa em uma sub-rede em sua VPC. Use sub-redes para isolar as camadas de sua aplicação (por exemplo, Web, aplicação e banco de dados) em uma única VPC. Use sub-redes privadas para as instâncias que não devem ser acessadas diretamente pela Internet.

Para chamar a API do Amazon EC2 da sua VPC usando endereços IP privados, use o AWS PrivateLink. Para obter mais informações, consulte Acessar o Amazon EC2 usando um endpoint da VPC de interface.

Isolamento em hosts físicos

Diferentes instâncias do EC2 no mesmo host físico são isoladas umas das outras como se estivessem em hosts físicos separados. O hipervisor isola a CPU e a memória, e as instâncias recebem discos virtualizados em vez de acesso aos dispositivos de disco bruto.

Quando você interrompe ou encerra uma instância, a memória alocada para ela é apagada (definida como zero) pelo hipervisor antes que ela seja alocada para uma nova instância, e cada bloco de armazenamento é redefinido. Isso garante que seus dados não sejam expostos acidentalmente para outra instância.

Os endereços MAC de rede são atribuídos dinamicamente às instâncias pela infraestrutura da rede da AWS. Os endereços IP são atribuídos dinamicamente a instâncias pela infraestrutura de rede da AWS ou atribuídos por um administrador do EC2 por meio de solicitações autenticadas da API. A rede da AWS permite que as instâncias enviem tráfego somente de endereços MAC e IP atribuídos a elas. Caso contrário, o tráfego será descartado.

Por padrão, uma instância não pode receber tráfego que não seja endereçado especificamente a ela. Se for necessário executar a conversão de endereço de rede (NAT), o roteamento ou os serviços de firewall em sua instância, será possível desabilitar a verificação de origem/destino da interface de rede.

Controlar o tráfego de rede

Considere as seguintes opções de controle de tráfego de rede para suas instâncias do EC2:

- Restrinja o acesso a suas instâncias usando grupos de segurança. Configure regras que permitam o tráfego de rede mínimo necessário. Por exemplo, é possível permitir o tráfego somente dos intervalos de endereços da rede corporativa ou apenas para protocolos específicos, como HTTPS. Para instâncias do Windows, permita o tráfego de gerenciamento do Windows e as conexões de saída mínimas.

- Use os grupos de segurança como o mecanismo primário a fim de controlar o acesso à rede para instâncias do Amazon EC2. Quando necessário, use as ACLs de rede para fornecer controle de rede sem estado e de alta granularidade. Os grupos de segurança são mais versáteis que as ACLs de rede devido à capacidade de realizar a filtragem de pacotes com estado e criar regras que fazem referência a outros grupos de segurança. No entanto, as ACLs de rede podem ser eficientes como um controle secundário para negar um subconjunto ou tráfego específico ou fornecer grades de proteção de sub-rede de alto nível. Além disso, como as ACLs de rede se aplicam a toda uma sub-rede, elas podem ser usadas como defesa em profundidade caso uma instância seja iniciada de forma não intencional sem um grupo de segurança correto.
- [Instâncias do Windows] Gerencie as configurações do Firewall do Windows, de maneira centralizada, com os Objetos de Política de Grupo (GPO) para aprimorar ainda mais os controles de rede. Os clientes costumam usar o Firewall do Windows para obter maior visibilidade do tráfego de rede e para complementar os filtros de grupo de segurança, criando regras avançadas para impedir que aplicações específicas acessem a rede ou filtrem o tráfego de endereços IP de um subconjunto. Por exemplo, o Firewall do Windows pode limitar o acesso ao endereço IP do serviço de metadados do EC2 para usuários ou aplicações específicas. Como alternativa, um serviço voltado para o público pode usar grupos de segurança para restringir o tráfego a portas específicas e o Firewall do Windows a manter uma lista negra de endereços IP explicitamente bloqueados.
- Use sub-redes privadas para as instâncias que não devem ser acessadas diretamente pela Internet. Use um bastion host ou gateway NAT para acesso à Internet em uma instância em uma sub-rede privada.
- [Instâncias do Windows] Use protocolos de administração seguros, como o encapsulamento de RDP sobre SSL e TLS. O Quick Start para Gateway de Desktop Remoto fornece as melhores práticas para implantar um gateway de desktop remoto remota, incluindo a configuração de RDP para usar SSL/TLS.
- [Instâncias do Windows] Use o Active Directory ou o Directory Service para controlar e monitorar, de forma rígida e centralizada, o acesso interativo de usuários e de grupos às instâncias do Windows e evitar permissões de usuários locais. Evite também usar Administradores de domínio e, em vez disso, crie contas baseadas em função mais granulares e específicas para a aplicação. A Administração Suficiente (JEA) permite que as alterações nas instâncias do Windows sejam gerenciadas sem acesso interativo ou de administrador. Além disso, a JEA permite que as organizações bloqueiem o acesso administrativo ao subconjunto dos comandos do Windows PowerShell necessários para a administração da instância. Para obter informações adicionais, consulte a seção "Gerenciamento de acesso a nível de SO para o Amazon EC2" no whitepaper Práticas recomendadas de segurança da AWS.

- [Instâncias do Windows] Os administradores de sistema devem usar contas do Windows com acesso limitado para realizar atividades diárias e elevar o acesso somente quando necessário para realizar alterações específicas na configuração. Além disso, somente acesse as instâncias do Windows diretamente quando absolutamente necessário. Em vez disso, use os sistemas de gerenciamento de configuração central, como o Run Command do EC2, o Systems Center Configuration Manager (SCCM), o Windows PowerShell DSC ou o Amazon EC2 Systems Manager (SSM), para enviar as alterações aos servidores Windows.
- Configure as tabelas de rotas de sub-rede da Amazon VPC com as rotas de rede mínimas necessárias. Por exemplo, insira somente as instâncias do Amazon EC2 que exijam acesso direto à Internet nas sub-redes com rotas para um gateway da Internet e insira somente instâncias do Amazon EC2 que precisem de acesso direto a redes internas nas sub-redes com rotas para um gateway privado virtual.
- Considere usar grupos de segurança adicionais ou interfaces de rede para controlar e auditar o tráfego de gerenciamento de instâncias do Amazon EC2 separadamente do tráfego de aplicação regular. Esta abordagem permite que os clientes implementem políticas do IAM especiais para o controle de alterações, facilitando a auditoria de alterações às regras de grupo de segurança ou scripts automáticos de verificação de regras. O uso de diversas interfaces de rede também oferece opções adicionais para controlar o tráfego de rede, incluindo a capacidade de criar políticas de roteamento baseadas em host ou aproveitar diferentes regras de roteamento de sub-rede da VPC com base na sub-rede atribuída da interface de rede.
- Use o AWS Virtual Private Network ou o Direct Connect para estabelecer conexões privadas de suas redes remotas com suas VPCs. Para obter mais informações, consulte Opções de conectividade entre a rede e a Amazon VPC.
- Use Logs de fluxo da VPC para monitorar o tráfego recebido nas instâncias.
- Use a proteção contra malware do GuardDuty para identificar comportamentos suspeitos indicativos de softwares mal-intencionados em suas instâncias que podem comprometer a workload, redirecionar recursos para o uso mal-intencionado e obter acesso não autorizado aos dados.
- Use o monitoramento do runtime do GuardDuty para identificar e responder a possíveis ameaças às instâncias. Para obter mais informações, consulte How Runtime Monitoring works with Amazon EC2 instances.
- Use o AWS Security Hub CSPM, o Reachability Analyzer ou o Analisador de Acesso à Rede para verificar a existência de acessibilidade à rede não intencional proveniente das suas instâncias.
- Use o EC2 Instance Connect para se conectar a suas instâncias usando Secure Shell (SSH) sem a necessidade de compartilhar e gerenciar chaves SSH.

- Use o Gerenciador de Sessões do AWS Systems Manager para acessar as instâncias remotamente em vez de abrir portas SSH ou RDP de entrada e gerenciar pares de chaves.
- Use o Run Command do AWS Systems Manager para automatizar as tarefas administrativas comuns em vez de realizar conexão com as instâncias.
- [Instâncias do Windows] Muitos dos perfis do sistema operacional do Windows e das aplicações de negócios da Microsoft também fornecem funcionalidades aprimoradas, como restrições de intervalo de endereços IP no IIS, políticas de filtragem de TCP/IP no Microsoft SQL Server e políticas de filtragem de conexão no Microsoft Exchange. A funcionalidade de restrição de rede na camada de aplicação pode fornecer camadas adicionais de defesa para servidores de aplicação de negócios críticos.

A Amazon VPC oferece suporte a controles adicionais de segurança de rede, como gateways, servidores proxy e opções de monitoramento de rede. Para obter mais informações, consulte Control network traffic no Guia do usuário da Amazon VPC.

Resiliência no Amazon EC2

A infraestrutura global da AWS é criada com base em regiões e zonas de disponibilidade da AWS. As regiões fornecem várias zonas de disponibilidade separadas e isoladas fisicamente, que são conectadas com baixa latência, alta throughput e redes altamente redundantes. Com as zonas de disponibilidade, é possível projetar e operar aplicações e bancos de dados que automaticamente executam o failover entre as zonas sem interrupção. As zonas de disponibilidade são mais altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de data center tradicionais.

Se você precisar replicar seus dados ou aplicações para distâncias geográficas maiores, use as zonas locais da AWS. Uma zona local da AWS é uma extensão de uma região da AWS na proximidade geográfica de seus usuários. As zonas locais têm suas próprias conexões com a Internet e suporte no Direct Connect. Como todas as regiões da AWS, as zonas locais da AWS são completamente isoladas de outras zonas da AWS.

Se você precisar replicar seus dados ou aplicações em uma zona local da AWS, a AWS recomenda que você use uma das seguintes zonas como zona de failover:

- Outra zona local
- Uma zona de disponibilidade na região que não é a zona principal. É possível usar o comando describe-availability-zones para visualizar a zona principal.

Para obter mais informações sobre regiões e zonas de disponibilidade da AWS, consulte Infraestrutura global da AWS.

Além da infraestrutura global da AWS, o Amazon EC2 oferece os seguintes recursos para oferecer suporte à resiliência de seus dados:

- Copiar AMIs entre regiões
- Copiar snapshots do EBS entre regiões
- Automatizando AMIs compatíveis com EBS usando o Amazon Data Lifecycle Manager
- Automatizar snapshots do EBS usando o Amazon Data Lifecycle Manager
- Manter a integridade e a disponibilidade da frota usando o Amazon EC2 Auto Scaling
- Distribuir o tráfego de entrada entre instâncias em uma única zona de disponibilidade ou em várias zonas de disponibilidade usando o Elastic Load Balancing.

Validação de conformidade do Amazon EC2

Para saber se um AWS service (Serviço da AWS) está no escopo de programas específicos de conformidade, consulte Serviços da AWS in Scope by Compliance Program e escolha o programa de conformidade em que tem interesse. Para obter informações gerais, consulte Programas de Conformidade da AWS.

É possível baixar relatórios de auditoria de terceiros usando o AWS Artifact. Para saber mais, consulte Baixar relatórios no AWS Artifact.

Sua responsabilidade de conformidade ao usar o Serviços da AWS é determinada pela confidencialidade dos seus dados, pelos objetivos de conformidade da sua empresa e pelos regulamentos e leis aplicáveis. Para ter mais informações sobre sua responsabilidade pela conformidade ao usar Serviços da AWS, consulte a Documentação de segurança da AWS.

Identity and Access Management para o Amazon EC2

O AWS Identity and Access Management (IAM) é um serviço da AWS service (Serviço da AWS) que ajuda um administrador a controlar com segurança o acesso aos recursos da AWS. Os administradores do IAM controlam quem pode ser autenticado (conectado) e autorizado (tem permissões) a usar os recursos do Amazon EC2. O IAM é um AWS service (Serviço da AWS) que pode ser usado sem custo adicional.

As credenciais de segurança identificam você para os serviços na AWS e concedem acesso aos recursos da AWS, como os recursos do Amazon EC2. É possível usar os recursos do Amazon EC2 e do IAM para permitir que outros usuários, serviços e aplicações usem seus recursos do Amazon EC2 sem compartilhar suas credenciais de segurança. É possível usar o IAM para controlar como outros usuários usam recursos na Conta da AWS, e pode usar grupos de segurança para controlar o acesso às instâncias do Amazon EC2. É possível optar por permitir uso completo ou limitado dos recursos do Amazon EC2.

Caso seja um desenvolvedor, será possível usar os perfis do IAM para gerenciar as credenciais de segurança necessárias para as aplicações que você executa nas instâncias do EC2. Depois de anexar um perfil do IAM à sua instância, as aplicações em execução na instância podem recuperar as credenciais do serviço de metadados de instância (IMDS).

Para conhecer as práticas recomendadas de proteção dos recursos da AWS usando o IAM, consulte Práticas recomendadas de segurança no IAM no Guia do usuário do IAM.

Conteúdo

- Políticas baseadas em identidade do Amazon EC2
- Exemplo de políticas para controlar o acesso à API do Amazon EC2
- Exemplo de políticas para controlar o acesso ao console do Amazon EC2
- Políticas gerenciadas pela AWS para o Amazon EC2
- Funções do IAM para Amazon EC2

Políticas baseadas em identidade do Amazon EC2

Por padrão, os usuários não têm permissão para criar ou modificar recursos do Amazon EC2 ou para executar tarefas usando a API do Amazon EC2, o colsole do Amazon EC2 ou a CLI. Para permitir que os usuários criem ou modifiquem recursos e realizem tarefas, você precisa criar políticas do IAM 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, ou perfis do IAM que exijam essas permissões.

Quando você anexa uma política a um usuário, um grupo de usuários ou um perfil, 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 IAM no Guia do usuário do IAM. Para obter mais informações sobre o gerenciamento e a criação de políticas do IAM;, consulte Gerenciamento de políticas do IAM.

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.

Para começar a usar, você pode verificar se as políticas gerenciadas pela AWS para o Amazon EC2 atendem às suas necessidades. Caso contrário, você pode criar suas próprias políticas personalizadas. Para obter mais informações, consulte the section called “AWSPolíticas gerenciadas pela ”.

Conteúdo

- Sintaxe da política
- Ações do Amazon EC2
- Permissões no nível do recurso com suporte para ações de API do Amazon EC2
- Nomes de recurso da Amazon (ARNs) para o Amazon EC2
- Chaves de condição do Amazon EC2
- Controlar o acesso usando acesso baseado em atributos
- Conceder permissões a usuários, grupos e perfis
- Verificar se os usuários têm as permissões necessárias

Sintaxe da política

A política do IAM é um documento JSON que consiste em uma ou mais declarações. Cada instrução é estruturada da maneira a seguir.

```
{
  "Statement":[{
    "Effect":"effect",
    "Action":"action",
    "Resource":"arn",
    "Condition":{
      "condition":{
        "key":"value"
        }
      }
    }
  ]
```

```
}
```

Existem vários elementos que compõem uma instrução:

- Efeito: o efeito pode ser `Allow` ou `Deny`. Por padrão, os usuários 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.
- Resource: o recurso afetado pela ação. Algumas ações de API do Amazon EC2 permitem incluir recursos específicos na política que podem ser criados ou modificados pela ação. Você especifica um recurso usando um nome de recurso da Amazon (ARN) ou usando o caractere curinga (*) para indicar que a instrução se aplica a todos os recursos. Para obter mais informações, consulte Permissões no nível do recurso com suporte para ações de API do Amazon EC2.
- 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.

Para obter mais informações sobre requisitos de políticas, consulte a Referência de política JSON do IAM no Guia do usuário do IAM. Para obter um exemplo de declarações de políticas do IAM para o Amazon EC2, consulte Exemplo de políticas para controlar o acesso à API do Amazon EC2.

Ações do Amazon EC2

Em uma declaração de política do IAM, é possível 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"]
```

Também é possível especificar várias ações usando caracteres curinga. Por exemplo, é possível especificar todas as ações cujo nome começa com a palavra "Describe" da seguinte forma:

```
"Action": "ec2:Describe*"
```

> **Note**
>
> No momento, as ações de API do Amazon EC2 não são compatíveis com permissões em nível de recurso. Para obter mais informações sobre permissões no nível do recurso para o Amazon EC2, consulte Políticas baseadas em identidade do Amazon EC2.

Para especificar todas as ações de API do Amazon EC2, use o curinga "*" da seguinte maneira:

```
"Action": "ec2:*"
```

Para obter uma lista de ações de Amazon EC2, consulte Ações definidas pelo Amazon EC2 na Referência de autorização do serviço.

Permissões no nível do recurso com suporte para ações de API do Amazon EC2

Permissões no nível do recurso se referem à capacidade de especificar em quais recursos os usuários têm permissão para realizar ações. O Amazon EC2 tem suporte parcial para permissões no nível do recurso. Isso significa que, para determinadas ações do Amazon EC2, é possível 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, é possível conceder aos usuários permissões para ativar instâncias, mas apenas de um tipo específico, e usando uma AMI específica.

Para especificar um recurso em uma declaração de política do IAM, use o respectivo nome de recurso da Amazon (ARN). Para obter mais informações sobre como especificar o valor do ARN, consulte Nomes de recurso da Amazon (ARNs) para o Amazon EC2. Se uma ação de API não oferecer suporte a ARNs individuais, você deverá usar um curinga (*) para especificar que todos os recursos podem ser afetados pela ação.

Para visualizar tabelas que identificam quais ações de API do Amazon EC2 oferecem suporte a permissões no nível do recurso e os ARNs e chaves de condição que é possível usar em uma política, consulte Ações, recursos e chaves de condição do Amazon EC2 .

Lembre-se de que é possível aplicar permissões em nível de recurso baseadas em tags às políticas do IAM que você usa para a maioria das ações da API do Amazon EC2. Isso oferece a você mais controle sobre quais recursos o usuário pode criar, modificar ou usar. Para obter mais informações, consulte Conceder permissão para marcar recursos do Amazon EC2 durante a criação.

Nomes de recurso da Amazon (ARNs) para o Amazon EC2

Cada declaração de política do IAM se aplica aos recursos que você especifica usando os ARNs.

Um ARN tem a seguinte sintaxe geral:

```
arn:aws:[service]:[region]:[account-id]:resourceType/resourcePath
```

service

O serviço (por exemplo, `ec2`).

region

A região do recurso (por exemplo, `us-east-1`).

account-id

O ID da conta da AWS, sem hifens (por exemplo, `123456789012`).

resourceType

O tipo de recurso (por exemplo, `instance`).

resourcePath

Um caminho que identifica o recurso. É possível usar o curinga * nos caminhos.

Por exemplo, é possível indicar uma instância específica (`i-1234567890abcdef0`) na declaração usando o ARN da maneira a seguir.

```
"Resource": "arn:aws:ec2:us-east-1:123456789012:instance/i-1234567890abcdef0"
```

É possível especificar todas as instâncias pertencentes a uma conta específica usando o caractere curinga * da maneira a seguir.

```
"Resource": "arn:aws:ec2:us-east-1:123456789012:instance/*"
```

Também é possível especificar todos os recursos do Amazon EC2 pertencentes a uma conta específica usando o caractere curinga * da maneira a seguir.

```
"Resource": "arn:aws:ec2:us-east-1:123456789012:*"
```

Para especificar todos os recursos ou caso uma ação de API específica não dê suporte a ARNs, use o curinga * no elemento `Resource` da maneira a seguir.

```
"Resource": "*"
```

Muitas ações da API do Amazon EC2 envolvem vários recursos. Por exemplo, `AttachVolume` anexa um volume do Amazon EBS a uma instância, portanto, um usuário precisa ter permissões para usar o volume e a instância. Para especificar vários recursos em uma única instrução, separe seus ARNs com vírgulas, como se segue.

```
"Resource": ["arn1", "arn2"]
```

Para obter uma lista de ARNs para recursos do Amazon EC2, consulte Tipos de recursos definidos pelo Amazon EC2.

Chaves de condição do Amazon EC2

Ema uma instrução de política, também é possível 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 global da AWS, além de chaves de condição específicas do serviço adicionais.

Para obter uma lista de chaves de condição específicas do serviço para o Amazon EC2, consulte Condition keys for Amazon EC2 (Chaves de condição para o Amazon EC2). O Amazon EC2 também implementa as chaves de condição globais da 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: restringir acesso a uma região específica.

Para usar uma chave de condição em sua política do IAM, use a instrução `Condition`. Por exemplo, a política a seguir concede aos usuários permissão para adicionar e remover regras de entrada e saída para qualquer grupo de segurança. Ela usa a chave de condição `ec2:Vpc` para especificar que essas ações só podem ser executadas em grupos de segurança em uma VPC específica.

JSON

```
{
"Version":"2012-10-17",
  "Statement":[{
    "Effect":"Allow",
    "Action": [
       "ec2:AuthorizeSecurityGroupIngress",
       "ec2:AuthorizeSecurityGroupEgress",
       "ec2:RevokeSecurityGroupIngress",
       "ec2:RevokeSecurityGroupEgress"],
     "Resource": "arn:aws:ec2:us-east-1:111122223333:security-group/*",
      "Condition": {
        "StringEquals": {
          "ec2:Vpc": "arn:aws:ec2:us-east-1:111122223333:vpc/
vpc-11223344556677889"
        }
      }
    }
  ]
}
```

Caso você especifique várias condições ou várias chaves em uma única condição, avaliamos essas condições usando uma operação AND lógica. Caso você especifique uma única condição com vários valores para uma chave, avaliamos a condição usando uma operação OR lógica. Para que as permissões sejam concedidas, todas as condições devem ser atendidas.

Também é possível usar espaços reservados quando especifica as condições. Para obter mais informações, consulte Elementos de política do IAM: variáveis e tags no Guia do usuário do IAM.

Important

Muitas chaves de condição são específicas a um recurso, e algumas ações da API usam vários recursos. Se você gravar uma política com uma chave de condição, use o elemento `Resource` da declaração para especificar o recurso ao qual a chave de condição se aplica. Caso contrário, as políticas podem impedir que os usuários executem a ação, porque a verificação da condição falha para os recursos aos quais a chave de condição não se aplica. Se você não quiser especificar um recurso, ou se escreveu o elemento `Action` da política para incluir várias ações da API, será necessário 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.

Chaves de condição

- ec2:AttributeChave da condição
- ec2:ResourceIDChaves de condição do
- ec2:SourceInstanceARNChave da condição

ec2:AttributeChave da condição

A chave de condição `ec2:Attribute` pode ser usada para condições que filtram o acesso por um atributo de um recurso.

A chave de condição é compatível somente com propriedades de um tipo de dados primitivos (como strings ou inteiros) ou objetos AttributeValue complexos que contêm apenas uma propriedade Value (como os objetos Description ou ImdsSupport da ação ModifyImageAttribute da API). A chave de condição não pode ser usada com objetos complexos que contêm várias propriedades, como o objeto LaunchPermission da açãoModifyImageAttribute da API.

Por exemplo, a política a seguir usa a chave de condição `ec2:Attribute/Description` para filtrar o acesso pelo objeto complexo Descrição da ação da API ModifyImageAttribute. A chave de condição permite somente solicitações que modifiquem a descrição de uma imagem para `Production` ou `Development`.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:ModifyImageAttribute",
      "Resource": "arn:aws:ec2:us-east-1::image/ami-*",
      "Condition": {
        "StringEquals": {
          "ec2:Attribute/Description": [
            "Production",
            "Development"
```

```
          ]
        }
      }
    }
  ]
}
```

A política a seguir usa a chave de condição `ec2:Attribute` para filtrar o acesso pela propriedade primitiva Atributo da ação da API ModifyImageAttribute. A chave de condição recusa todas as solicitações que tentam modificar a descrição de uma imagem.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": "ec2:ModifyImageAttribute",
      "Resource": "arn:aws:ec2:us-east-1::image/ami-*",
      "Condition": {
        "StringEquals": {
          "ec2:Attribute": "Description"
        }
      }
    }
  ]
}
```

ec2:ResourceIDChaves de condição do

Quando as chaves de condição `ec2:ResourceID` a seguir forem usadas com as ações de API especificadas, o valor da chave de condição será usado para especificar o recurso resultante criado pela ação da API. As chaves de condição `ec2:ResourceID` não podem ser usadas para especificar um recurso de origem especificado na solicitação da API. Se você usar uma das chaves de condição `ec2:ResourceID` a seguir com uma API especificada, será necessário especificar sempre o curinga (*). Se você especificar um valor diferente, a condição sempre será resolvida para * em runtime. Por exemplo, para usar a chave de condição `ec2:ImageId` com a API CopyImage, será necessário especificar a chave de condição da seguinte forma:

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:CopyImage",
      "Resource": "arn:aws:ec2:us-east-1::image/ami-*",
      "Condition": {
        "StringEquals": {
          "ec2:ImageID": "*"
        }
      }
    }
  ]
}
```

Recomendamos evitar usar estas chaves de condição com estas ações de API:

- `ec2:DhcpOptionsID` – `CreateDhcpOptions`
- `ec2:ImageID` – `CopyImage`, `CreateImage`, `ImportImage` e `RegisterImage`
- `ec2:InstanceID` – `RunInstances` e `ImportInstance`
- `ec2:InternetGatewayID` – `CreateInternetGateway`
- `ec2:NetworkAclID` – `CreateNetworkAcl`
- `ec2:NetworkInterfaceID` – `CreateNetworkInterface`
- `ec2:PlacementGroupName` – `CreatePlacementGroup`
- `ec2:RouteTableID` – `CreateRouteTable`
- `ec2:SecurityGroupID` – `CreateSecurityGroup`
- `ec2:SnapshotID` – `CopySnapshot`, `CreateSnapshot`, `CreateSnapshots` e `ImportSnapshots`
- `ec2:SubnetID` – `CreateSubnet`
- `ec2:VolumeID` – `CreateVolume` e `ImportVolume`
- `ec2:VpcID` – `CreateVpc`
- `ec2:VpcPeeringConnectionID` – `CreateVpcPeeringConnection`

Para filtrar o acesso com base em IDs de recursos específicos, recomendamos usar o elemento de política `Resource` conforme descrito a seguir.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:CopyImage",
      "Resource": "arn:aws:ec2:us-east-1::image/ami-01234567890abcdef"
    }
  ]
}
```

ec2:SourceInstanceARNChave da condição

Use `ec2:SourceInstanceARN` para especificar o ARN da instância a partir da qual uma solicitação é feita. Essa é uma chave de condição global da AWS, o que significa que é possíve usá-la com outros serviços além do Amazon EC2. Para ver um exemplo de política, consulte Exemplo: permitir que uma instância específica visualize recursos em outros serviços da AWS.

Controlar o acesso usando acesso baseado em atributos

Ao criar uma política do IAM que conceda permissão aos usuários para usar recursos do EC2, é possível incluir informações de tag no elemento `Condition` da política para controlar o acesso com base em tags. Isso é conhecido como controle de acesso baseado em atributo (ABAC). O ABAC oferece um controle melhor sobre quais recursos um usuário pode modificar, usar ou excluir. Para obter mais informações, consulte O que é ABAC para a AWS?

Por exemplo, é possível criar uma política que permite que os usuários encerrem uma instância, mas nega a ação se a instância tiver a tag `environment=production`. Para fazer isso, use a chave de condição `aws:ResourceTag` para permitir ou negar acesso ao recurso com base nas tags anexadas ao recurso.

```
"StringEquals": { "aws:ResourceTag/environment": "production" }
```

Para saber se uma ação de API do Amazon EC2 oferece suporte ao controle de acesso usando a chave de condição `aws:ResourceTag`, consulte Ações, recursos e chaves de condição para Amazon EC2 . Como as ações de `Describe` não oferecem suporte a permissões em nível de recurso, especifique-as em uma declaração separada sem condições.

Para obter exemplos de políticas do IAM, consulte Exemplo de políticas para controlar o acesso à API do Amazon EC2.

Se você permitir ou negar aos usuários o acesso a recursos com base em tags, considere negar explicitamente aos usuários a capacidade de adicionar essas tags ou removê-las dos mesmos recursos. Caso contrário, é possível que um usuário contorne suas restrições e obtenha acesso a um recurso modificando as tags.

Conceder permissões a usuários, grupos e perfis

Para conceder acesso, adicione as permissões aos seus usuários, grupos ou perfis:

- Usuários e grupos no Centro de Identidade do AWS IAM:

  Crie um conjunto de permissões. Siga as instruções em Criação de um conjunto de permissões no Guia do usuário do Centro de Identidade do AWS IAM.
- Usuários gerenciados no IAM com provedor de identidades:

  Crie um perfil para a federação de identidades. Siga as instruções em Criando um perfil para um provedor de identidades de terceiros (federação) no Guia do Usuário do IAM.
- Usuários do IAM:
  - Crie um perfil que seu usuário possa assumir. Siga as instruções em Criação de um perfil para um usuário do IAM no Guia do usuário do IAM.
  - (Não recomendado) Vincule uma política diretamente a um usuário ou adicione um usuário a um grupo de usuários. Siga as instruções em Adição de permissões a um usuário (console) no Guia do usuário do IAM.

Verificar se os usuários têm as permissões necessárias

Depois que você tiver criado uma política do IAM, recomendaremos verificar se ela concede aos usuários as permissões para usar as ações de API e os recursos específicos de que eles precisam antes de colocar a política em produção.

Primeiro, crie um usuário para fins de teste e anexe a política do IAM que você criou ao usuário de teste. Em seguia, faça uma solicitação como o usuário de teste.

Se a ação do Amazon EC2 que você estiver testando criar ou modificar um recurso, será necessário fazer a solicitação usando o parâmetro `DryRun` (ou executar o comando da AWS CLI com a opção `--dry-run`). Nesse caso, a chamada conclui a verificação da autorização, mas não conclui a operação. Por exemplo, é possível 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, é possível 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. É possível decodificar a mensagem usando a ação `DecodeAuthorizationMessage`. Para obter mais informações, consulte DecodeAuthorizationMessage na Referência de API do AWS Security Token Service e decode-authorization-message.

Exemplo de políticas para controlar o acesso à API do Amazon EC2

É possível usar as políticas do IAM para conceder aos usuários as permissões necessárias para que eles trabalhem com o Amazon EC2. Para obter instruções detalhadas, consulte Criação de políticas do IAM no Guia do usuário do IAM.

Os exemplos a seguir mostram declarações de políticas que você pode usar para conceder aos usuários as permissões para o uso do Amazon EC2. Essas políticas são criadas para solicitações feitas com a AWS CLI ou com o AWS SDK. Nos exemplos a seguir, substitua cada *espaço reservado* por suas próprias informações.

Exemplos

- Exemplo: acesso somente leitura
- Exemplo: restringir acesso a uma região específica
- Trabalhar com instâncias
- Executar instâncias (RunInstances)
- Trabalhar com Instâncias spot
- Exemplo: trabalhar com Instâncias reservadas
- Exemplo: marcar recursos
- Exemplo: trabalhar com funções do IAM
- Exemplo: trabalhar com tabelas de rotas
- Exemplo: permitir que uma instância específica visualize recursos em outros serviços da AWS
- Exemplo: trabalhar com modelos de execução
- Trabalhar com metadados de instância
- Trabalhar com volumes e snapshots do Amazon EBS

Para obter exemplos de políticas para trabalhar no console do Amazon EC2, consulte Exemplo de políticas para controlar o acesso ao console do Amazon EC2.

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 é possível usar com quais ações de API do Amazon EC2, consulte Ações, recursos e chaves de condição do Amazon EC2 no .

Os usuários não têm permissão para executar nenhuma ação nos recursos (a menos que outra declaração conceda a eles permissão para fazer isso) porque, por padrão, a permissão para usar ações da API é negada para os usuários.

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [
```

```
    {
      "Effect": "Allow",
      "Action": "ec2:Describe*",
      "Resource": "*"
    }
   ]
}
```

Exemplo: restringir acesso a uma região específica

A política a seguir nega permissão aos usuários para uso de todas as ações da API do Amazon EC2 a menos que a região seja a Europa (Frankfurt). Ela usa a chave de condição global `aws:RequestedRegion`, que é compatível com todas as ações da API do Amazon EC2.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
       {
      "Effect": "Deny",
      "Action": "ec2:*",
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "aws:RequestedRegion": "eu-central-1"
        }
      }
    }
  ]
}
```

Como alternativa, é possível 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.

JSON

```
{
  "Version":"2012-10-17",
```

```
  "Statement": [
       {
      "Effect": "Deny",
      "Action": "ec2:*",
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "ec2:Region": "eu-central-1"
        }
      }
    }
  ]
}
```

Trabalhar com instâncias

Exemplos

- Exemplo: descrever, executar, interromper, iniciar e encerrar todas as instâncias
- Exemplo: descrever todas as instâncias e interromper, iniciar e encerrar somente instâncias específicas

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 é possível usar com quais ações de API do Amazon EC2, consulte Ações, recursos e chaves de condição do Amazon EC2 no .

Os usuários não têm permissão para usar qualquer outra ação da API (a menos que outra declaração conceda a eles permissão para fazer isso) porque, por padrão, a permissão para usar ações da API são negadas para os usuários.

JSON

```
{
   "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 na 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 é possível usar com quais ações de API do Amazon EC2, consulte Ações, recursos e chaves de condição do Amazon EC2 no .

A segunda declaração usa permissões em nível de recurso para as ações `StopInstances` e `StartInstances`. As instâncias específicas são indicadas por seus ARNs no elemento `Resource`.

A terceira declaração permite que os usuários encerrem todas as instâncias em na região `us-east-1` que pertencem à conta da AWS especificada, mas somente quando a instância tiver a tag "`purpose=test`". O elemento `Condition` qualifica quando a declaração de política está em vigor.

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [
   {
   "Effect": "Allow",
      "Action": "ec2:DescribeInstances",
      "Resource": "*"
   },
   {
      "Effect": "Allow",
      "Action": [
        "ec2:StopInstances",
        "ec2:StartInstances"
      ],
      "Resource": [
        "arn:aws:ec2:us-east-1:111122223333:instance/i-1234567890abcdef0",
        "arn:aws:ec2:us-east-1:111122223333:instance/i-0598c7d356eba48d7"
      ]
    },
    {
      "Effect": "Allow",
      "Action": "ec2:TerminateInstances",
      "Resource": "arn:aws:ec2:us-east-1:111122223333:instance/*",
      "Condition": {
         "StringEquals": {
            "aws:ResourceTag/purpose": "test"
         }
      }
   }

   ]
}
```

Executar instâncias (RunInstances)

A ação da API RunInstances inicia uma ou mais Instâncias on-demand ou uma ou mais Instâncias spot. `RunInstances` requer uma AMI e cria uma instância. Os usuários podem especificar um par de chaves e um grupo de segurança na solicitação. A inicialização em uma VPC requer uma sub-rede, e cria uma interface de rede. A inicialização de uma AMI baseada no Amazon EBS cria

um volume. Portanto, o usuário deve ter permissões para usar esses recursos do Amazon EC2. É possível criar um declaração de política que exija que os usuários especifiquem um parâmetro opcional em `RunInstances` ou restringir os usuários a valores específicos para um parâmetro.

Para obter mais informações sobre as permissões em nível de recurso que são necessárias para executar uma instância, consulte Ações, recursos e chaves de condição do Amazon EC2 no .

Observe que, por padrão, os usuários não têm permissões para descrever, iniciar, interromper ou encerrar as instâncias resultantes. Uma maneira de conceder aos usuários permissão para gerenciar as instâncias resultantes é criar uma tag específica para cada instância e criar uma declaração que permita que eles gerenciem instâncias com aquela tag. Para obter mais informações, consulte Trabalhar com instâncias.

Recursos

- AMIs
- Tipos de instância
- Sub-redes
- Volumes do EBS
- Tags
- Tags em um modelo de execução
- GPUs elásticas
- Modelos de execução

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).

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [
   {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
```

```
      "Resource": [
        "arn:aws:ec2:us-east-1::image/ami-9e1670f7",
        "arn:aws:ec2:us-east-1::image/ami-45cf5c3c",
        "arn:aws:ec2:us-east-1:111122223333:instance/*",
        "arn:aws:ec2:us-east-1:111122223333:volume/*",
        "arn:aws:ec2:us-east-1:111122223333:key-pair/*",
        "arn:aws:ec2:us-east-1:111122223333:security-group/*",
        "arn:aws:ec2:us-east-1:111122223333:subnet/*",
        "arn:aws:ec2:us-east-1:111122223333:network-interface/*"
      ]
    }
   ]
}
```

Como alternativa, a política a seguir permite que os usuários executem instâncias em todas as AMIs pertencentes à Amazon ou a determinados parceiros confiáveis e verificados. 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).

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [
         {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
         "arn:aws:ec2:us-east-1::image/ami-*"
      ],
      "Condition": {
         "StringEquals": {
            "ec2:Owner": "amazon"
         }
      }
   },
   {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
```

```
            "arn:aws:ec2:us-east-1:111122223333:instance/*",
            "arn:aws:ec2:us-east-1:111122223333:subnet/*",
            "arn:aws:ec2:us-east-1:111122223333:volume/*",
            "arn:aws:ec2:us-east-1:111122223333:network-interface/*",
            "arn:aws:ec2:us-east-1:111122223333:key-pair/*",
            "arn:aws:ec2:us-east-1:111122223333: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 é possível 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`.

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [
        {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
         "arn:aws:ec2:us-east-1:111122223333:instance/*"
      ],
      "Condition": {
         "StringEquals": {
            "ec2:InstanceType": ["t2.micro", "t2.small"]
         }
      }
   },
   {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
         "arn:aws:ec2:us-east-1::image/ami-*",
         "arn:aws:ec2:us-east-1:111122223333:subnet/*",
```

```
            "arn:aws:ec2:us-east-1:111122223333:network-interface/*",
            "arn:aws:ec2:us-east-1:111122223333:volume/*",
            "arn:aws:ec2:us-east-1:111122223333:key-pair/*",
            "arn:aws:ec2:us-east-1:111122223333:security-group/*"
            ]
        }
    ]
}
```

Se desejar, é possível criar uma política que negue aos usuários permissões para executar qualquer instância, com exceção dos tipos de instância `t2.micro` e `t2.small`.

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [
        {
      "Effect": "Deny",
      "Action": "ec2:RunInstances",
      "Resource": [
         "arn:aws:ec2:us-east-1:111122223333:instance/*"
      ],
      "Condition": {
         "StringNotEquals": {
            "ec2:InstanceType": ["t2.micro", "t2.small"]
         }
      }
   },
   {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
         "arn:aws:ec2:us-east-1::image/ami-*",
         "arn:aws:ec2:us-east-1:111122223333:network-interface/*",
         "arn:aws:ec2:us-east-1:111122223333:instance/*",
         "arn:aws:ec2:us-east-1:111122223333:subnet/*",
         "arn:aws:ec2:us-east-1:111122223333:volume/*",
         "arn:aws:ec2:us-east-1:111122223333:key-pair/*",
         "arn:aws:ec2:us-east-1:111122223333: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).

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
        "arn:aws:ec2:us-east-1:111122223333:subnet/subnet-12345678",
        "arn:aws:ec2:us-east-1:111122223333:network-interface/*",
        "arn:aws:ec2:us-east-1:111122223333:instance/*",
        "arn:aws:ec2:us-east-1:111122223333:volume/*",
        "arn:aws:ec2:us-east-1::image/ami-*",
        "arn:aws:ec2:us-east-1:111122223333:key-pair/*",
        "arn:aws:ec2:us-east-1:111122223333:security-group/*"
      ]
    }
   ]
}
```

Se desejar, é possível 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.

JSON

```
{
```

```
   "Version":"2012-10-17",
   "Statement": [
         {
      "Effect": "Deny",
      "Action": "ec2:RunInstances",
      "Resource": [
         "arn:aws:ec2:us-east-1:111122223333:network-interface/*"
      ],
      "Condition": {
         "ArnNotEquals": {
            "ec2:Subnet": "arn:aws:ec2:us-east-1:111122223333:subnet/
subnet-12345678"
         }
      }
   },
   {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
         "arn:aws:ec2:us-east-1::image/ami-*",
         "arn:aws:ec2:us-east-1:111122223333:network-interface/*",
         "arn:aws:ec2:us-east-1:111122223333:instance/*",
         "arn:aws:ec2:us-east-1:111122223333:subnet/*",
         "arn:aws:ec2:us-east-1:111122223333:volume/*",
         "arn:aws:ec2:us-east-1:111122223333:key-pair/*",
         "arn:aws:ec2:us-east-1:111122223333:security-group/*"
         ]
      }
   ]
}
```

Volumes do EBS

A política a seguir permite que os usuários executem instâncias somente se os volumes do EBS para a instância estiverem criptografados. O usuário deve executar uma instância em uma AMI criada com snapshots criptografados, para garantir que o volume raiz esteja criptografado. Qualquer volume adicional que o usuário anexe à instância durante a execução também deve estar criptografado.

JSON

```
{
```

```
    "Version":"2012-10-17",
    "Statement": [
                {
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": [
                "arn:aws:ec2:*:*:volume/*"
            ],
            "Condition": {
                "Bool": {
                    "ec2:Encrypted": "true"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": [
                "arn:aws:ec2:*::image/ami-*",
                "arn:aws:ec2:*:*:network-interface/*",
                "arn:aws:ec2:*:*:instance/*",
                "arn:aws:ec2:*:*:subnet/*",
                "arn:aws:ec2:*:*:key-pair/*",
                "arn:aws:ec2:*:*:security-group/*"
            ]
        }
    ]
}
```

Tags

Marque instâncias na criação

A política a seguir permite que os usuários executem instâncias e as marquem durante a criação. Para ações de criação de recursos que aplicam tags, os usuários devem ter permissões para usar a ação `CreateTags`. A segunda declaração usa a chave de condição `ec2:CreateAction` para permitir que os usuários criem tags somente no contexto de `RunInstances` e somente para instâncias. Os usuários não podem marcar recursos existentes e não podem marcar volumes usando a solicitação `RunInstances`.

Para obter mais informações, consulte Conceder permissão para marcar recursos do Amazon EC2 durante a criação.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
         "ec2:RunInstances"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
         "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:us-east-1:111122223333:instance/*",
      "Condition": {
         "StringEquals": {
             "ec2:CreateAction" : "RunInstances"
          }
       }
    }
  ]
}
```

Marque instâncias e volumes na criação com tags específicas

As política a seguir inclui a chave de condição `aws:RequestTag` que requer que os usuários marquem todas as instâncias e os volumes criados por `RunInstances` com as tags `environment=production` e `purpose=webserver`. Se os usuários não passarem essas tags específicas ou não especificarem nenhuma tag, haverá talha na solicitação.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
   {
```

```
      "Effect": "Allow",
      "Action": [
         "ec2:RunInstances"
      ],
      "Resource": [
         "arn:aws:ec2:us-east-1::image/*",
         "arn:aws:ec2:us-east-1:111122223333:subnet/*",
         "arn:aws:ec2:us-east-1:111122223333:network-interface/*",
         "arn:aws:ec2:us-east-1:111122223333:security-group/*",
         "arn:aws:ec2:us-east-1:111122223333:key-pair/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
         "ec2:RunInstances"
      ],
      "Resource": [
          "arn:aws:ec2:us-east-1:111122223333:volume/*",
          "arn:aws:ec2:us-east-1:111122223333:instance/*"
      ],
      "Condition": {
         "StringEquals": {
            "aws:RequestTag/environment": "production" ,
            "aws:RequestTag/purpose": "webserver"
          }
       }
    },
    {
      "Effect": "Allow",
      "Action": [
         "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:us-east-1:111122223333:*/*",
      "Condition": {
         "StringEquals": {
            "ec2:CreateAction" : "RunInstances"
          }
       }
    }
  ]
}
```

Marque instâncias e volumes na criação com pelo menos uma tag específica

A política a seguir usa o modificador `ForAnyValue` na condição `aws:TagKeys` para indicar que pelo menos uma tag deve ser especificada na solicitação e deve conter a chave `environment` ou `webserver`. A tag deve ser aplicada a instâncias e a volumes. Qualquer valor de tag pode ser especificado na solicitação.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
   {
      "Effect": "Allow",
      "Action": [
         "ec2:RunInstances"
      ],
      "Resource": [
         "arn:aws:ec2:us-east-1::image/*",
         "arn:aws:ec2:us-east-1:111122223333:subnet/*",
         "arn:aws:ec2:us-east-1:111122223333:network-interface/*",
         "arn:aws:ec2:us-east-1:111122223333:security-group/*",
         "arn:aws:ec2:us-east-1:111122223333:key-pair/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
          "ec2:RunInstances"
      ],
      "Resource": [
          "arn:aws:ec2:us-east-1:111122223333:volume/*",
          "arn:aws:ec2:us-east-1:111122223333:instance/*"
      ],
      "Condition": {
          "ForAnyValue:StringEquals": {
              "aws:TagKeys": ["environment","webserver"]
          }
       }
    },
    {
      "Effect": "Allow",
```

```
      "Action": [
          "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:us-east-1:111122223333:*/*",
      "Condition": {
          "StringEquals": {
              "ec2:CreateAction" : "RunInstances"
          }
       }
    }
  ]
}
```

Se forem marcadas na criação, as instâncias deverão ser marcadas com uma tag específica

Na política a seguir, os usuários não precisam especificar tags na solicitação, mas se o fizerem, a tag deverá ser `purpose=test`. Nenhuma outra tag é permitida. Os usuários podem aplicar as tags a qualquer recurso marcável na solicitação `RunInstances`.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
         "ec2:RunInstances"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
         "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:us-east-1:111122223333:*/*",
      "Condition": {
         "StringEquals": {
             "aws:RequestTag/purpose": "test",
             "ec2:CreateAction" : "RunInstances"
```

```
          },
          "ForAllValues:StringEquals": {
              "aws:TagKeys": "purpose"
          }
       }
    }
  ]
}
```

Para não permitir que ninguém adicione tags na criação para RunInstances

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowRun",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1::image/*",
                "arn:aws:ec2:us-east-1:*:subnet/*",
                "arn:aws:ec2:us-east-1:*:network-interface/*",
                "arn:aws:ec2:us-east-1:*:security-group/*",
                "arn:aws:ec2:us-east-1:*:key-pair/*",
                "arn:aws:ec2:us-east-1:*:volume/*",
                "arn:aws:ec2:us-east-1:*:instance/*",
                "arn:aws:ec2:us-east-1:*:spot-instances-request/*"
            ]
        },
        {
            "Effect": "Deny",
            "Action": "ec2:CreateTags",
            "Resource": "*"
        }
    ]
}
```

Permitir apenas tags específicas para spot-instances-request. A inconsistência surpresa número 2 entra em jogo aqui. Em circunstâncias normais, não especificar tag alguma resultará em Não autenticado. No caso de spot-instances-request, esta política não será avaliada se não houver tags spot-instances-request, portanto, uma solicitação Spot on Run sem tag será bem-sucedida.

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.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
   {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": "*",
      "Condition": {
         "ArnLike": {
             "ec2:LaunchTemplate": "arn:aws:ec2:us-east-1:111122223333:launch-
template/lt-09477bcd97b0d310e"
          },
          "Bool": {
             "ec2:IsLaunchTemplateResource": "true"
          }
       }
    },
    {
      "Effect": "Allow",
      "Action": [
         "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:us-east-1:111122223333: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` garante que as instâncias usem o tipo de GPU elástico `eg1.medium` ou `eg1.large`.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
             {
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:*:111122223333:elastic-gpu/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:Region": "us-east-2",
                    "ec2:ElasticGpuType": [
                        "eg1.medium",
                        "eg1.large"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
```

```
            "Action": "ec2:RunInstances",
            "Resource": [
                "arn:aws:ec2:*::image/ami-*",
                "arn:aws:ec2:*:111122223333:network-interface/*",
                "arn:aws:ec2:*:111122223333:instance/*",
                "arn:aws:ec2:*:111122223333:subnet/*",
                "arn:aws:ec2:*:111122223333:volume/*",
                "arn:aws:ec2:*:111122223333:key-pair/*",
                "arn:aws:ec2:*:111122223333: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`.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
        {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": "*",
      "Condition": {
         "ArnLike": {
             "ec2:LaunchTemplate": "arn:aws:ec2:us-east-1:111122223333:launch-
template/lt-09477bcd97b0d310e"
          }
       }
    }
  ]
}
```

Neste exemplo, os usuários poderão executar instâncias apenas se usarem um modelo de execução. A política usa a chave de condição `ec2:IsLaunchTemplateResource` para impedir que os usuários substituam os ARNs pré-existentes no modelo de execução.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
        {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": "*",
      "Condition": {
         "ArnLike": {
             "ec2:LaunchTemplate": "arn:aws:ec2:us-east-1:111122223333: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.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
        {
```

```
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "NotResource": ["arn:aws:ec2:us-east-1:111122223333:subnet/*",
                      "arn:aws:ec2:us-east-1:111122223333:network-interface/*" ],
      "Condition": {
         "ArnLike": {
             "ec2:LaunchTemplate": "arn:aws:ec2:us-east-1:111122223333:launch-
template/*"
          }
       }
    },
   {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": ["arn:aws:ec2:us-east-1:111122223333:subnet/*",
                   "arn:aws:ec2:us-east-1:111122223333:network-interface/*" ],
      "Condition": {
         "ArnLike": {
             "ec2:LaunchTemplate": "arn:aws:ec2:us-east-1:111122223333:launch-
template/*"
          },
          "Bool": {
             "ec2:IsLaunchTemplateResource": "true"
          }
       }
    }
  ]
}
```

O exemplo a seguir permitirá que os usuários executem instâncias somente se usarem um modelo de execução, e somente se o modelo de execução tiver a tag `Purpose=Webservers`. Os usuários não podem substituir nenhum dos parâmetros do modelo de execução na ação `RunInstances`.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
        {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
```

```
      "NotResource": "arn:aws:ec2:us-east-1:111122223333:launch-template/*",
      "Condition": {
         "ArnLike": {
             "ec2:LaunchTemplate": "arn:aws:ec2:us-east-1:111122223333:launch-
template/*"
          },
         "Bool": {
             "ec2:IsLaunchTemplateResource": "true"
          }
       }
    },
    {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": "arn:aws:ec2:us-east-1:111122223333:launch-template/*",
      "Condition": {
       "StringEquals": {
           "aws:ResourceTag/Purpose": "Webservers"
        }
       }
     }
  ]
}
```

Trabalhar com Instâncias spot

É possível usar a ação RunInstances para criar solicitações de instância spot e marcar solicitações de instância spot na criação. O recurso a ser especificado para RunInstances é `spot-instances-request`.

O recurso `spot-instances-request` é avaliado na política do IAM da seguinte forma:

- Se você não marcar uma solicitação de instância spot na criação, o Amazon EC2 não avaliará o recurso `spot-instances-request` na instrução RunInstances.
- Se você marcar uma solicitação de instância spot na criação, o Amazon EC2 avaliará o recurso `spot-instances-request` na instrução RunInstances.

Portanto, para o recurso `spot-instances-request`, as seguintes regras se aplicam à diretiva do IAM:

- Caso você use RunInstances para criar uma solicitação de instância spot e não pretenda marcar a solicitação de instância spot na criação, não será necessário permitir explicitamente o recurso `spot-instances-request`. A chamada terá êxito.
- Caso use RunInstances para criar uma solicitação de instância spot e pretenda marcar a solicitação de instância spot na criação, será necessário incluir o recurso `spot-instances-request` na instrução de permissão RunInstances, caso contrário, a chamada falhará.
- Caso você use RunInstances para criar uma solicitação de instância spot e pretenda marcar a solicitação de instância spot na criação, especifique o recurso `spot-instances-request` ou um curinga `*` na instrução de permissão CreateTags, caso contrário, a chamada falhará.

É possível solicitar Instâncias spot usando RunInstances ou RequestSpotInstances. Os exemplos de políticas do IAM a seguir se aplicam somente ao solicitar Instâncias spot usando RunInstances.

Exemplo: solicitar Instâncias spot usando RunInstances

A política a seguir permite que os usuários solicitem Instâncias spot usando a ação RunInstances. O recurso `spot-instances-request`, que é criado por RunInstances, solicita Instâncias spot.

> **Note**
>
> Para usar RunInstances a fim de criar solicitações de instância spot, é possível omitir `spot-instances-request` da lista `Resource` caso pretenda marcar as solicitações de instância spot na criação. Isso ocorre porque o Amazon EC2 não avalia o recurso `spot-instances-request` na instrução RunInstances se a solicitação de instância spot não estiver marcada na criação.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowRun",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
```

```
            "Resource": [
                "arn:aws:ec2:us-east-1::image/*",
                "arn:aws:ec2:us-east-1:*:subnet/*",
                "arn:aws:ec2:us-east-1:*:network-interface/*",
                "arn:aws:ec2:us-east-1:*:security-group/*",
                "arn:aws:ec2:us-east-1:*:key-pair/*",
                "arn:aws:ec2:us-east-1:*:volume/*",
                "arn:aws:ec2:us-east-1:*:instance/*",
                "arn:aws:ec2:us-east-1:*:spot-instances-request/*"
            ]
        }
    ]
}
```

Warning

NÃO COMPATÍVEL – Exemplo: negar permissão aos usuários para solicitar Instâncias spot usando RunInstances

A política a seguir não é compatível com o recurso `spot-instances-request`.

A política a seguir destina-se a conceder permissão aos usuários para iniciar Instâncias on-demand, mas negar a permissão de solicitação Instâncias spot. O recurso `spot-instances-request`, criado por RunInstances, é o recurso que solicita Instâncias spot. A segunda instrução destina-se a negar a ação RunInstances para o recurso `spot-instances-request`. No entanto, esta condição não é compatível porque o Amazon EC2 não avalia o recurso `spot-instances-request` na instrução RunInstances se a solicitação de instância spot não estiver marcada na criação.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowRun",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
```

```
                "arn:aws:ec2:us-east-1::image/*",
                "arn:aws:ec2:us-east-1:*:subnet/*",
                "arn:aws:ec2:us-east-1:*:network-interface/*",
                "arn:aws:ec2:us-east-1:*:security-group/*",
                "arn:aws:ec2:us-east-1:*:key-pair/*",
                "arn:aws:ec2:us-east-1:*:volume/*",
                "arn:aws:ec2:us-east-1:*:instance/*"
            ]
        },
        {
            "Sid": "DenySpotInstancesRequestsNOTSUPPORTEDDONOTUSE",
            "Effect": "Deny",
            "Action": "ec2:RunInstances",
            "Resource": "arn:aws:ec2:us-east-1:*:spot-instances-request/*"
        }
    ]
}
```

Exemplo: marcar solicitações de instância spot na criação

A política a seguir permite que os usuários marquem todos os recursos criados durante o lançamento da instância. A primeira instrução permite que RunInstances crie os recursos listados. O recurso `spot-instances-request`, criado por RunInstances, é o recurso que solicita Instâncias spot. A segunda instrução fornece um curinga * para permitir que todos os recursos sejam marcados quando criados no momento da execução da instância.

> **Note**
>
> Se você marcar uma solicitação de instância spot na criação, o Amazon EC2 avaliará o recurso `spot-instances-request` na instrução RunInstances. Portanto, permita explicitamente o recurso `spot-instances-request` para a ação RunInstances, caso contrário, a chamada falhará.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
```

```
        {
            "Sid": "AllowRun",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1::image/*",
                "arn:aws:ec2:us-east-1:*:subnet/*",
                "arn:aws:ec2:us-east-1:*:network-interface/*",
                "arn:aws:ec2:us-east-1:*:security-group/*",
                "arn:aws:ec2:us-east-1:*:key-pair/*",
                "arn:aws:ec2:us-east-1:*:volume/*",
                "arn:aws:ec2:us-east-1:*:instance/*",
                "arn:aws:ec2:us-east-1:*:spot-instances-request/*"
            ]
        },
        {
            "Sid": "TagResources",
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "*"
        }
    ]
}
```

Exemplo: negar marcações na criação para solicitações de instância spot

A política a seguir nega aos usuários a permissão para marcar os recursos criados durante a execução da instância.

A primeira instrução permite que RunInstances crie os recursos listados. O recurso `spot-instances-request`, criado por RunInstances, é o recurso que solicita Instâncias spot. A segunda instrução fornece um curinga `*` para evitar que todos os recursos sejam marcados, quando criados, no momento da execução da instância. Se `spot-instances-request` ou qualquer outro recurso estiver marcado na criação, a chamada RunInstances falhará.

JSON

```
{
    "Version":"2012-10-17",
```

```
    "Statement": [
        {
            "Sid": "AllowRun",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1::image/*",
                "arn:aws:ec2:us-east-1:*:subnet/*",
                "arn:aws:ec2:us-east-1:*:network-interface/*",
                "arn:aws:ec2:us-east-1:*:security-group/*",
                "arn:aws:ec2:us-east-1:*:key-pair/*",
                "arn:aws:ec2:us-east-1:*:volume/*",
                "arn:aws:ec2:us-east-1:*:instance/*",
                "arn:aws:ec2:us-east-1:*:spot-instances-request/*"
            ]
        },
        {
            "Sid": "DenyTagResources",
            "Effect": "Deny",
            "Action": "ec2:CreateTags",
            "Resource": "*"
        }
    ]
}
```

Warning

NÃO COMPATÍVEL – Exemplo: permitir a criação de uma solicitação de instância spot apenas se lhe for atribuída uma etiqueta específica

A política a seguir não é compatível com o recurso `spot-instances-request`.

A política a seguir destina-se a conceder permissão à RunInstances para criar uma solicitação de instância spot somente se a solicitação for marcada com uma tag específica.

A primeira instrução permite que RunInstances crie os recursos listados.

A segunda instrução destina-se a conceder permissão aos usuários para criar uma solicitação de instância spot somente se a solicitação tiver a etiqueta `environment=production`. Se essa condição for aplicada a outros recursos criados por RunInstances, não especificar nenhuma tag gerará um erro `Unauthenticated`. No entanto, se nenhuma etiqueta for especificada para a solicitação de instância spot, o Amazon EC2

não avaliará o recurso `spot-instances-request` na instrução RunInstances, o que resultará em solicitações de instância spot não marcadas sendo criadas pela RunInstances. Observe que especificar outra etiqueta, além de `environment=production` gera um erro `Unauthenticated`, pois se um usuário marca uma solicitação de instância spot, o Amazon EC2 avalia o recurso `spot-instances-request` na instrução RunInstances.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowRun",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1::image/*",
                "arn:aws:ec2:us-east-1:*:subnet/*",
                "arn:aws:ec2:us-east-1:*:network-interface/*",
                "arn:aws:ec2:us-east-1:*:security-group/*",
                "arn:aws:ec2:us-east-1:*:key-pair/*",
                "arn:aws:ec2:us-east-1:*:volume/*",
                "arn:aws:ec2:us-east-1:*:instance/*"
            ]
        },
        {
            "Sid":
 "RequestSpotInstancesOnlyIfTagIsEnvironmentProductionNOTSUPPORTEDDONOTUSE",
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": "arn:aws:ec2:us-east-1:*:spot-instances-request/
*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/environment": "production"
                }
            }
        },
        {
            "Sid": "TagResources",
```

```
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "*"
        }

    ]
}
```

Exemplo: negar a criação de uma solicitação de instância spot se lhe for atribuída uma etiqueta específica

A política a seguir nega à RunInstances a permissão para criar uma solicitação de instância spot se a solicitação estiver marcada com `environment=production`.

A primeira instrução permite que RunInstances crie os recursos listados.

A segunda instrução nega permissão aos usuários para criar uma solicitação de instância spot se a solicitação tiver a etiqueta `environment=production`. Especificar `environment=production` como tag gerará um erro `Unauthenticated`. Especificar outras tags ou não especificar tags resultará na criação de uma solicitação de instância spot.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowRun",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1::image/*",
                "arn:aws:ec2:us-east-1:*:subnet/*",
                "arn:aws:ec2:us-east-1:*:network-interface/*",
                "arn:aws:ec2:us-east-1:*:security-group/*",
                "arn:aws:ec2:us-east-1:*:key-pair/*",
                "arn:aws:ec2:us-east-1:*:volume/*",
                "arn:aws:ec2:us-east-1:*:instance/*",
```

```
                "arn:aws:ec2:us-east-1:*:spot-instances-request/*"
            ]
        },
        {
            "Sid": "DenySpotInstancesRequests",
            "Effect": "Deny",
            "Action": "ec2:RunInstances",
            "Resource": "arn:aws:ec2:us-east-1:*:spot-instances-request/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/environment": "production"
                }
            }
        },
        {
            "Sid": "TagResources",
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "*"
        }
    ]
}
```

Exemplo: trabalhar com Instâncias reservadas

A política a seguir concede aos usuários permissão para visualizar, modificar e comprar Instâncias reservadas na sua conta.

Não é possível definir permissões em nível de recurso para instâncias reservadas. Essa política significa que os usuários têm acesso a todas as Instâncias reservadas na conta.

O elemento `Resource` usa um caractere curinga * para indicar que os usuários podem especificar todos os recursos com a ação. Nesse caso, os usuários podem listar e modificar todas as Instâncias reservadas na conta. Eles também podem comprar Instâncias reservadas usando as credenciais da conta. O caractere curinga * também é necessário em casos onde a ação da API não é compatível com as permissões em nível de recurso.

JSON

```
{
   "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.

JSON

```
{
  "Version":"2012-10-17",
   "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeReservedInstances",
        "ec2:ModifyReservedInstances",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource": "*"
    }
  ]
}
```

Exemplo: marcar recursos

A política a seguir permite que os usuários usem a ação `CreateTags` para aplicar tags a uma instância somente se a tag contiver a chave `environment` e o valor `production`. Nenhuma outra tag é permitida, e o usuário não pode aplicar tags em nenhum outro tipo de recurso.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
              {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:us-east-1:111122223333:instance/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/environment": "production"
                }
            }
        }
    ]
}
```

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. Além disso, os usuários devem especificar uma tag com uma chave de `anycompany:environment-type` e um valor de `test` ou de `prod` na solicitação. Os usuários podem especificar tags adicionais na solicitação.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
              {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:us-east-1:111122223333:*/*",
            "Condition": {
                "StringEquals": {
```

```
                    "aws:RequestTag/anycompany:environment-type":
 ["test","prod"],
                    "aws:ResourceTag/owner": "${aws:username}"
                }
            }
        }
    ]
}
```

É possível 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.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
       {
      "Effect": "Allow",
      "Action": "ec2:DeleteTags",
      "Resource": "arn:aws:ec2:us-east-1:111122223333: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 do `owner` e com um valor do nome de usuário. Os usuários não podem excluir nenhuma outra tag de um recurso.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
      {
      "Effect": "Allow",
      "Action": [
        "ec2:DeleteTags"
      ],
      "Resource": "arn:aws:ec2:us-east-1:111122223333:*/*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/environment": "prod",
          "aws: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 devem ter permissão para usar a ação `iam:PassRole` para passar o perfil para a instância.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:AssociateIamInstanceProfile",
        "ec2:ReplaceIamInstanceProfileAssociation",
        "ec2:DisassociateIamInstanceProfile"
      ],
      "Resource": "arn:aws:ec2:us-east-1:111122223333:instance/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/department":"test"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": "ec2:DescribeIamInstanceProfileAssociations",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "arn:aws:iam::111122223333:role/DevTeam*"
    }
  ]
}
```

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.

JSON

```
{
    "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::111122223333: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.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
              {
            "Effect": "Allow",
            "Action": [
```

```
                "ec2:DeleteRoute",
                "ec2:CreateRoute",
                "ec2:ReplaceRoute"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1:111122223333:route-table/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:Vpc": "arn:aws:ec2:us-east-1:111122223333: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 é possível anexar a uma função do IAM. A política permite que uma instância exiba recursos em vários serviços da AWS. Ela usa a chave de condição global `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.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
              {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeVolumes",
                "s3:ListAllMyBuckets",
                "dynamodb:ListTables",
                "rds:DescribeDBInstances"
            ],
            "Resource": [
```

```
                "*"
            ],
            "Condition": {
                "ArnEquals": {
                    "ec2:SourceInstanceARN": "arn:aws:ec2:us-
east-1:111122223333: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.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
   {
      "Action": [
        "ec2:CreateLaunchTemplateVersion",
        "ec2:ModifyLaunchTemplate"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:ec2:us-east-1:111122223333: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`.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
       {
      "Action": [
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:ec2:us-east-1:111122223333:launch-template/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/Purpose": "Testing"
        }
      }
    }
  ]
}
```

Trabalhar com metadados de instância

As políticas a seguir garantem que os usuários possam recuperar somente metadados de instância usando o Serviço de metadados da instância versão 2 (IMDSv2). É possível combinar as quatro políticas a seguir em uma única política com quatro instruções. Quando combinadas como uma única política, é possível usar a política como uma política de controle de serviços (SCP). Ela pode funcionar tão bem como uma política de negação aplicada a uma política existente do IAM (retirando e limitando a permissão existente) ou como uma SCP aplicada globalmente em uma conta, uma unidade organizacional (UO) ou uma organização inteira.

> **Note**
>
> As seguintes políticas de opções de metadados de RunInstances devem ser usadas em conjunto com uma política que concede ao principal permissões para executar uma instância com RunInstances. Se o principal também não tiver permissões para RunInstances, não poderá executar uma instância. Para obter mais informações, consulte as políticas em Trabalhar com instâncias e Executar instâncias (RunInstances).

Important

Se você usar grupos do Auto Scaling e precisar exigir o uso do IMDSv2 em todas as novas instâncias, seus grupos do Auto Scaling deverão usar modelos de execução.
Quando um grupo do Auto Scaling usa um modelo de execução, as permissões de `ec2:RunInstances` do principal do IAM são verificadas quando um novo grupo do Auto Scaling é criado. Elas também são verificadas quando um grupo existente do Auto Scaling é atualizado para usar um novo modelo de execução ou uma nova versão de um modelo de execução.
As restrições sobre o uso do IMDSv1 em principais do IAM para `RunInstances` são verificadas somente quando um grupo do Auto Scaling que está usando um modelo de inicialização é criado ou atualizado. Para um grupo do Auto Scaling configurado para usar o modelo de execução `Latest` ou `Default`, as permissões não são verificadas quando uma nova versão do modelo de execução é criada. Para que as permissões sejam verificadas, configure o grupo do Auto Scaling para usar uma versão específica do modelo de execução.

Para impor o uso do IMDSv2 em instâncias executadas por grupos do Auto Scaling, as seguintes etapas adicionais são necessárias:

1. Desabilite o uso de configurações de execução para todas as contas em sua organização usando SCPs (service control policies - políticas de controle de serviço) ou limites de permissões do IAM para novos principais criados. Para principais existentes do IAM com permissões de grupo do Auto Scaling, atualize suas políticas associadas com essa chave de condição. Para desabilitar o uso de configurações de execução, crie ou modifique a SCP relevante, o limite de permissões ou a política do IAM com a `"autoscaling:LaunchConfigurationName"` chave de condição com o valor especificado como `null`.
2. Para novos modelos de execução, configure as opções de metadados da instância no modelo de execução. Para modelos de execução existentes, crie uma versão do modelo de execução e configure as opções de metadados da instância na nova versão.
3. Na política que concede a qualquer principal permissão para usar um modelo de execução, restrinja a associação de `$latest` e `$default` especificando `"autoscaling:LaunchTemplateVersionSpecified": "true"`. Ao restringir o uso a uma versão específica de um modelo de execução, é possível garantir que novas instâncias serão executadas usando a versão na qual as opções de metadados da instância estão configuradas. Para obter mais informações, consulte

LaunchTemplateSpecification no Referência da API do Amazon EC2 Auto Scaling, especificamente o parâmetro `Version`.

4. Para um grupo do Auto Scaling que usa uma configuração de execução, substitua a configuração de execução por um modelo de execução. Para obter mais informações, consulte Migração de seus grupos do Auto Scaling para a execução de modelos no Guia do usuário do Amazon EC2 Auto Scaling.
5. Para um grupo do Auto Scaling que usa um modelo de execução, certifique-se de que ele usa um novo modelo de execução com as opções de metadados da instância configuradas ou usa uma nova versão do modelo de execução atual com as opções de metadados da instância configuradas. Para obter mais informações, consulte update-auto-scaling-group.

Exemplos

- Exigir o uso de IMDSv2
- Negar a rejeição do IMDSv2
- Especificar o limite máximo de saltos
- Limitar quem pode modificar as opções de metadados da instância
- Exigir que as credenciais de função sejam recuperadas de IMDSv2

Exigir o uso de IMDSv2

A política a seguir especifica que não é possível chamar a API RunInstances a menos que a instância também esteja optada para exigir o uso de IMDSv2 (indicado por `"ec2:MetadataHttpTokens": "required"`). Se você não especificar que a instância requer IMDSv2, receberá um erro `UnauthorizedOperation` ao chamar a API RunInstances.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
                {
            "Sid": "RequireImdsV2",
            "Effect": "Deny",
            "Action": "ec2:RunInstances",
```

```
            "Resource": "arn:aws:ec2:*:*:instance/*",
            "Condition": {
                "StringNotEquals": {
                    "ec2:MetadataHttpTokens": "required"
                }
            }
        }
    ]
}
```

Negar a rejeição do IMDSv2

A política a seguir especifica que não é possível chamar a API `ModifyInstanceMetadataOptions` e permitir a opção de IMDSv1 ou IMDSv2. Se você chamar a API `ModifyInstanceMetadataOptions`, o atributo `HttpTokens` deverá ser definido como `required`.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [{
        "Sid": "DenyIMDSv1HttpTokensModification",
        "Effect": "Deny",
        "Action": "ec2:ModifyInstanceMetadataOptions",
        "Resource": "arn:aws:ec2:*:*:instance/*",
        "Condition": {
            "StringNotEquals": {
                "ec2:Attribute/HttpTokens": "required"
            },
            "Null": {
                "ec2:Attribute/HttpTokens": false
            }
        }
    }]
}
```

Especificar o limite máximo de saltos

A política a seguir especifica que não é possível chamar a API RunInstances a menos que também especifique um limite de saltos, que não pode ser superior a 3. Se isso não for feito, você receberá um erro `Unauthorized0peration` ao chamar a API RunInstances.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
                {
            "Sid": "MaxImdsHopLimit",
            "Effect": "Deny",
            "Action": "ec2:RunInstances",
            "Resource": "arn:aws:ec2:*:*:instance/*",
            "Condition": {
                "NumericGreaterThan": {
                    "ec2:MetadataHttpPutResponseHopLimit": "3"
                }
            }
        }
    ]
}
```

Limitar quem pode modificar as opções de metadados da instância

A política a seguir permite que apenas usuários com o perfil `ec2-imds-admins` façam alterações. nas opções de metadados da instância. Se qualquer principal diferente da função `ec2-imds-admins` tentar chamar a API ModifyInstanceMetadataOptions, receberá um erro `Unauthorized0peration`. Essa instrução pode ser usada para controlar o uso da API ModifyInstanceMetadataOptions. No momento, não há controles de acesso refinados (condições) para a API ModifyInstanceMetadataOptions.

Exigir que as credenciais de função sejam recuperadas de IMDSv2

A política a seguir especifica que, se essa política for aplicada a uma função e a função for assumida pelo serviço do EC2 e as credenciais resultantes forem usadas para assinar uma solicitação, a solicitação deverá ser assinada pelas credenciais de função do EC2 recuperadas do IMDSv2. Caso contrário, todas as suas chamadas de API receberão um erro `Unauthorized0peration`. Essa

instrução/política pode ser aplicada de modo geral porque, se a solicitação não for assinada por credenciais de função do EC2, ela não terá efeito.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
                {
            "Sid": "RequireAllEc2RolesToUseV2",
            "Effect": "Deny",
            "Action": "*",
            "Resource": "*",
            "Condition": {
                "NumericLessThan": {
                    "ec2:RoleDelivery": "2.0"
                }
            }
        }
    ]
}
```

Trabalhar com volumes e snapshots do Amazon EBS

Para obter exemplos de políticas para trabalhar com volumes e snapshots do Amazon EBS, consulte Exemplos de políticas baseadas em identidade para o Amazon EBS.

Exemplo de políticas para controlar o acesso ao console do Amazon EC2

É possível usar as políticas do IAM para conceder aos usuários as permissões necessárias para que eles trabalhem com o Amazon EC2. Para obter instruções detalhadas, consulte Criação de políticas do IAM no Guia do usuário do IAM.

O console usa ações de API adicionais para seus recursos, portanto, essas políticas talvez não funcionem como esperado. Por exemplo, um usuário que tem permissão para usar somente a ação da API `DescribeVolumes` encontrará erros ao tentar visualizar volumes no console. Esta seção demonstra políticas que permitem que os usuários trabalhem com partes específicas do console. Para obter informações adicionais sobre como criar políticas para o console do Amazon EC2, consulte a seguinte postagem do Blog de segurança da AWS: Granting Users Permission to Work in

the Amazon EC2 Console (Conceder permissão aos usuários para trabalhar no console do Amazon EC2).

Os exemplos a seguir mostram declarações de políticas que você pode usar para conceder aos usuários as permissões para o uso do Amazon EC2. Substitua cada *espaço reservado para entrada do usuário* por suas próprias informações. Essas políticas são criadas para solicitações feitas com o Console de gerenciamento da AWS. O console do Amazon EC2 pode chamar várias ações de API para exibir um único recurso, e isso talvez não seja óbvio até que o usuário tente uma tarefa e o console exiba um erro. Para obter mais informações adicionais, consulte a seguinte postagem do Blog de segurança da AWS: Granting Users Permission to Work in the Amazon EC2 Console.

Exemplos

- Exemplo: acesso somente leitura
- Exemplo: uso do assistente de início de instância do EC2
- Exemplo: trabalhar com grupos de segurança
- Exemplo: trabalhar com endereços IP elásticos
- Exemplo: trabalhar com Instâncias reservadas

Para obter ajuda para descobrir quais ações de API são necessárias para a execução de tarefas no console, você pode usar um serviço para registrar chamadas, como o AWS CloudTrail. Se sua política não conceder permissão para criar ou modificar um recurso específico, o console exibirá uma mensagem codificada com informações de diagnóstico. É possível decodificar a mensagem usando a ação de API DecodeAuthorizationMessage para AWS STS, ou o comando decode-authorization-message na AWS CLI.

Exemplo: acesso somente leitura

Para permitir que os usuários visualizem todos os recursos no console do Amazon EC2, é possível usar a mesma política como no exemplo a seguir: Exemplo: acesso somente leitura. 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, é possível 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, é possível remover essa ação para permitir que os usuários visualizem somente AMIs privadas.

JSON

```
{
   "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 é possível usar com quais ações de API do Amazon EC2, consulte Ações, recursos e chaves de condição do Amazon EC2 no .

Visualizar instâncias e métricas do CloudWatch

A política a seguir permite que os usuários visualizem instâncias no console do Amazon EC2, bem como alarmes e métricas do CloudWatch na guia Monitoring (Monitoramento) da página Instances (Instâncias). O console do Amazon EC2 usa a API do CloudWatch para exibir os

alarmes e as métricas, portanto, você deve conceder aos usuários permissão para usar as ações `cloudwatch:DescribeAlarms`, `cloudwatch:DescribeAlarmsForMetric`, `cloudwatch:ListMetrics`, `cloudwatch:GetMetricStatistics` e `cloudwatch:GetMetricData`.

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": [
         "ec2:DescribeInstances",
         "ec2:DescribeInstanceTypes",
         "cloudwatch:DescribeAlarms",
         "cloudwatch:DescribeAlarmsForMetric",
         "cloudwatch:ListMetrics",
         "cloudwatch:GetMetricStatistics",
         "cloudwatch:GetMetricData"
      ],
      "Resource": "*"
   }
   ]
}
```

Exemplo: uso do assistente de início de instância do EC2

O assistente de início de instância do Amazon EC2 é uma tela com opções para configurar e iniciar 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 início de instância

Para concluir uma execução com êxito, os usuários devem receber permissão para usar a ação de API `ec2:RunInstances` e, pelo menos, as seguintes ações de API:

- `ec2:DescribeImages`: para visualizar e selecionar uma AMI.
- `ec2:DescribeInstanceTypes`: para visualizar e selecionar um tipo de instância.

- `ec2:DescribeVpcs`: para ver as opções de rede disponíveis.
- `ec2:DescribeSubnets`: para visualizar todas as sub-redes disponíveis da VPC escolhida.
- `ec2:DescribeSecurityGroups` ou `ec2:CreateSecurityGroup`: para visualizar e selecionar um grupo de segurança existente ou criar um.
- `ec2:DescribeKeyPairs` ou `ec2:CreateKeyPair`: para selecionar um par de chaves ou criar um par.
- `ec2:AuthorizeSecurityGroupIngress`: para adicionar regras de entrada.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeImages",
                "ec2:DescribeInstanceTypes",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeVpcs",
                "ec2:DescribeSubnets",
                "ec2:DescribeSecurityGroups",
                "ec2:CreateSecurityGroup",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateKeyPair"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": "*"
        }
    ]
}
```

É possível adicionar ações de API à sua política para fornecer mais opções aos usuários, por exemplo:

- `ec2:DescribeAvailabilityZones`: para ver e selecionar uma zona de disponibilidade específica.
- `ec2:DescribeNetworkInterfaces`: para visualizar e selecionar interfaces de rede existentes para a sub-rede selecionada.
- Para adicionar regras de saída para grupos de segurança da VPC, os usuários devem receber a permissão para usar a ação de API `ec2:AuthorizeSecurityGroupEgress`. Para modificar ou excluir regras existentes, os usuários devem receber permissão para usar a ação de API relevante `ec2:RevokeSecurityGroup*`.
- `ec2:CreateTags`: para marcar os recursos criados por `RunInstances`. Para obter mais informações, consulte Conceder permissão para marcar recursos do Amazon EC2 durante a criação. Se os usuários não tiverem permissão para usar essa ação e tentarem aplicar tags na página de marcação do assistente de início de instância, haverá falha na execução.

  > **Important**
  >
  > Especifique um Name (Nome) ao iniciar uma instância cria uma etiqueta e exige a ação `ec2:CreateTags`. Tenha cuidado ao conceder aos usuários permissão para usar a ação `ec2:CreateTags`, pois isso limita sua capacidade de usar a chave de condição `aws:ResourceTag` para restringir o uso de outros recursos. Se você conceder aos usuários permissão para usar a ação `ec2:CreateTags`, eles poderão alterar a tag de um recurso para contornar essas restrições. Para obter mais informações, consulte Controlar o acesso usando acesso baseado em atributos.

- Para usar parâmetros do Systems Manager ao selecionar uma AMI, você deve adicionar `ssm:DescribeParameters` e `ssm:GetParameters` à sua política. O `ssm:DescribeParameters` concede aos usuários a permissão para visualizar e selecionar parâmetros do Systems Manager. O `ssm:GetParameters` concede aos usuários a permissão para obter os valores dos parâmetros do Systems Manager. Também é possível restringir o acesso a parâmetros específicos do Systems Manager. Para obter mais informações, consulte Restringir acesso a parâmetros específicos do Systems Manager posteriormente nesta seção.

Atualmente, as ações da API `Describe*` do Amazon EC2 não oferecem suporte a permissões em nível de recurso, portanto, não é possível restringir quais recursos individuais os usuários podem

visualizar no assistente de início de instância. Contudo, é possível aplicar permissões em nível de recurso na ação de API `ec2:RunInstances` para restringir os recursos que os usuários podem usar para executar uma instância. Haverá falha na execução se os usuários selecionarem opções que não estão autorizados a usar.

Restringir o acesso a um tipo de instância, uma sub-rede e uma região específicos

A política a seguir permite que os usuários executem instâncias `t2.micro` usando AMIs de propriedade da Amazon e apenas em uma sub-rede específica (`subnet-1a2b3c4d`). Os usuários só podem iniciar na região especificada. Se os usuários selecionarem uma região diferente ou se selecionarem outro tipo de instância, outra AMI ou outra sub-rede no assistente de início de instância, a execução falhará.

A primeira declaração concede aos usuários permissão para visualizar as opções no assistente de início de instância ou criar novas, conforme explicado no exemplo acima. A segunda declaração concede aos usuários permissão para usarem a interface de rede, o volume, o par de chaves, o grupo de segurança 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). A terceira e a quarta declaração concedem aos usuários permissão para usarem a instância e os recursos das AMIs respectivamente, mas somente se a instância for uma instância `t2.micro` e somente se a AMI pertencer à Amazon ou a determinados parceiros confiáveis e verificados.

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": [
         "ec2:DescribeInstances",
         "ec2:DescribeImages",
         "ec2:DescribeInstanceTypes",
         "ec2:DescribeKeyPairs",
         "ec2:CreateKeyPair",
         "ec2:DescribeVpcs",
         "ec2:DescribeSubnets", "ec2:DescribeSecurityGroups",
         "ec2:CreateSecurityGroup",
         "ec2:AuthorizeSecurityGroupIngress"
   ],
```

```
    "Resource": "*"
    },
    {
       "Effect": "Allow",
       "Action":"ec2:RunInstances",
       "Resource": [
          "arn:aws:ec2:us-east-2:111122223333:network-interface/*",
          "arn:aws:ec2:us-east-2:111122223333:volume/*",
          "arn:aws:ec2:us-east-2:111122223333:key-pair/*",
          "arn:aws:ec2:us-east-2:111122223333:security-group/*",
          "arn:aws:ec2:us-east-2:111122223333:subnet/subnet-1a2b3c4d"
       ]
    },
    {
       "Effect": "Allow",
       "Action": "ec2:RunInstances",
       "Resource": [
          "arn:aws:ec2:us-east-2:111122223333:instance/*"
       ],
       "Condition": {
          "StringEquals": {
             "ec2:InstanceType": "t2.micro"
          }
       }
    },
    {
       "Effect": "Allow",
       "Action": "ec2:RunInstances",
       "Resource": [
             "arn:aws:ec2:us-east-2::image/ami-*"
       ],
       "Condition": {
          "StringEquals": {
             "ec2:Owner": "amazon"
          }
       }
    }
    ]
}
```

Restringir o acesso a parâmetros específicos do Systems Manager

A política a seguir concede acesso para usar parâmetros do Systems Manager com um nome específico.

A primeira instrução concede aos usuários permissão para visualizar parâmetros do Systems Manager ao selecionar uma AMI no assistente de início de instância. A segunda instrução concede aos usuários a permissão para usar somente parâmetros denominados `prod-*`.

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": [
         "ssm:DescribeParameters"
      ],
      "Resource": "*"
   },
   {
      "Effect": "Allow",
      "Action": [
         "ssm:GetParameters"
      ],
     "Resource": "arn:aws:ssm:us-east-2:123456123456:parameter/prod-*"
   }
   ]
}
```

Exemplo: trabalhar com grupos de segurança

Visualizar grupos de segurança e adicionar e remover regras

A política a seguir concede aos usuários permissão para visualizar grupos de segurança no console do Amazon EC2, adicionar e remover regras de entrada e de saída, bem como listar e modificar descrições de regras de grupo de segurança existentes que têm a etiqueta `Department=Test`.

Na primeira declaração, a ação `ec2:DescribeTags` permite que os usuários visualizem tags no console, o que facilita a identificação dos grupos de segurança que eles têm permissão para modificar.

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": [
         "ec2:DescribeSecurityGroups",
         "ec2:DescribeSecurityGroupRules",
         "ec2:DescribeTags"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
         "ec2:AuthorizeSecurityGroupIngress",
         "ec2:RevokeSecurityGroupIngress",
         "ec2:AuthorizeSecurityGroupEgress",
         "ec2:RevokeSecurityGroupEgress",
         "ec2:ModifySecurityGroupRules",
         "ec2:UpdateSecurityGroupRuleDescriptionsIngress",
         "ec2:UpdateSecurityGroupRuleDescriptionsEgress"
      ],
      "Resource": [
         "arn:aws:ec2:us-east-2:111122223333:security-group/*"
      ],
      "Condition": {
         "StringEquals": {
            "aws:ResourceTag/Department": "Test"
         }
      }
   },
   {
      "Effect": "Allow",
      "Action": [
         "ec2:ModifySecurityGroupRules"
      ],
      "Resource": [
         "arn:aws:ec2:us-east-2:111122223333:security-group-rule/*"
      ]
   }
```

```
]}
```

Trabalhar com a caixa de diálogo Create Security Group (Criar grupo de segurança

É possível 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 grupo de segurança.
- `ec2:DescribeVpcs`: para visualizar uma lista de VPCs existentes na lista VPC.

Com essas permissões, os usuários podem criar um novo grupo de segurança com êxito, mas não podem adicionar nenhuma regra a ele. Para trabalhar com regras na caixa de diálogo Create Security Group (Criar grupo de segurança), é possível adicionar as seguintes ações de API à sua política:

- `ec2:AuthorizeSecurityGroupIngress`: para adicionar regras de entrada.
- `ec2:AuthorizeSecurityGroupEgress`: para adicionar regras de saída aos grupos de segurança 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 (Criar grupo de segurança) e preenche-a com as mesmas regras do security group que foi selecionado.
- `ec2:RevokeSecurityGroupEgress`: para modificar ou excluir regras de saída de grupos de segurança 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 grupo de segurança e, em seguida, adiciona as regras especificadas. Se as regras forem inválidas, a ação falhará, e o console tentará excluir o grupo de segurança. O usuário permanece na caixa de diálogo Create Security Group (Criar grupo de segurança) 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 grupo de segurança com regras inválidas, o grupo de segurança será criado sem nenhuma regra, e o usuário deverá adicioná-las posteriormente.

- `ec2:UpdateSecurityGroupRuleDescriptionsIngress`: para adicionar ou atualizar descrições de regras de grupo de segurança de entrada (inbound).
- `ec2:UpdateSecurityGroupRuleDescriptionsEgress`: para adicionar ou atualizar descrições de regras de grupo de segurança de saída (outbound).
- `ec2:ModifySecurityGroupRules`: para modificar as regras do grupo de segurança.
- `ec2:DescribeSecurityGroupRules`: para listar as regras do grupo de segurança.

A política a seguir concede aos usuários permissão para usar a caixa de diálogo Create Security Group (Criar grupo de segurança) e criar regras de entrada e de saída para grupos de segurança associados a uma VPC específica (`vpc-1a2b3c4d`). Os usuários podem criar grupos de segurança para uma VPC, mas não podem adicionar nenhuma regra a eles. Da mesma forma, os usuários não podem adicionar nenhuma regra aos grupos de segurança existentes não associados à VPC `vpc-1a2b3c4d`. Os usuários também recebem permissão para visualizar todos os grupos de segurança no console. Isso facilita aos usuários identificar os grupos de segurança aos quais podem adicionar regras de entrada. Essa política também concede permissão aos usuários para excluir grupos de segurança associados à VPC `vpc-1a2b3c4d`.

JSON

```
{
   "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:us-east-2:111122223333:security-group/*",
      "Condition":{
```

```
          "ArnEquals": {
             "ec2:Vpc": "arn:aws:ec2:us-east-2:111122223333:vpc/vpc-1a2b3c4d"
          }
       }
     }
    ]
}
```

Exemplo: trabalhar com endereços IP elásticos

Para permitir que os usuários visualizem endereços IP elásticos no console do Amazon EC2, conceda aos usuários permissão para usar a ação `ec2:DescribeAddresses`.

Para permitir que os usuários trabalhem com endereços IP elásticos, é possível 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.

JSON

```
{
    "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 permite que os usuários visualizem e modifiquem instâncias reservadas em sua conta e que adquiram novas instâncias reservadas no Console de gerenciamento da AWS.

Esta política permite que os usuários visualizem todas as Instâncias reservadas, bem como Instâncias on-demand, na conta. Não é possível definir permissões em nível de recurso para Instâncias reservadas individuais.

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": [
         "ec2:DescribeReservedInstances",
         "ec2:ModifyReservedInstances",
         "ec2:PurchaseReservedInstancesOffering",
         "ec2:DescribeInstances",
         "ec2:DescribeInstanceTypes",
         "ec2:DescribeAvailabilityZones",
         "ec2:DescribeReservedInstancesOfferings"
      ],
      "Resource": "*"
   }
   ]
}
```

A ação `ec2:DescribeAvailabilityZones` é necessária para garantir que o console do Amazon EC2 possa exibir informações sobre as zonas de disponibilidade nas quais é possível 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.

É possível ajustar as ações de API para limitar o acesso do usuário, por exemplo, a remoção de `ec2:DescribeInstances` e de `ec2:DescribeAvailabilityZones` significa que o usuário tem acesso somente leitura.

Políticas gerenciadas pela AWS para o Amazon EC2

Para adicionar permissões a usuários, grupos e perfis, é mais fácil usar políticas gerenciadas pela AWS do que gravar políticas por conta própria. É necessário tempo e experiência para criar políticas gerenciadas pelo cliente do IAM que fornecem à sua equipe apenas as permissões de que precisam. Para começar rapidamente, é possível usar nossas políticas gerenciadas pela AWS. Essas políticas abrangem casos de uso comuns e estão disponíveis na sua conta da AWS. Para obter mais informações sobre políticas gerenciadas pela AWS, consulte Políticas gerenciadas pela AWS no Guia do usuário do IAM.

Os serviços da AWS mantêm e atualizam políticas gerenciadas pela AWS. Não é possível alterar as permissões em políticas gerenciadas pela AWS. Os serviços ocasionalmente acrescentam permissões adicionais a uma política gerenciada pela AWS para oferecer suporte a novos recursos. Esse tipo de atualização afeta todas as identidades (usuários, grupos e funções) em que a política está anexada. É mais provável que os serviços atualizem uma política gerenciada pela AWS quando um novo recurso for iniciado ou novas operações se tornarem disponíveis. Os serviços não removem permissões de uma política gerenciada pela AWS, portanto, as atualizações de políticas não suspendem suas permissões existentes.

Além disso, a AWS é compatível com políticas gerenciadas por perfis de trabalho que abrangem vários serviços. Por exemplo, a política ReadOnlyAccess política gerenciada pela AWS fornece acesso somente leitura a todos os serviços e recursos da AWS. Quando um serviço executa um novo atributo, a AWS adiciona permissões somente leitura para novas operações e recursos. Para obter uma lista e descrições das políticas de funções de trabalho, consulte Políticas gerenciadas pela AWS para funções de trabalho no Guia do usuário do IAM.

AWS Política gerenciada da: AmazonEC2FullAccess

É possível anexar a política `AmazonEC2FullAccess` a suas identidades do IAM. Essa política concede permissões que possibilitam acesso total ao Amazon EC2.

Para visualizar as permissões para esta política, consulte AmazonEC2FullAccess na Referência de políticas gerenciadas pela AWS.

Política gerenciada da AWS: AmazonEC2ReadOnlyAccess

É possível anexar a política `AmazonEC2ReadOnlyAccess` às identidades do IAM. Esta política concede permissões que oferecem acesso somente leitura ao Amazon EC2.

Para visualizar as permissões para esta política, consulte AmazonEC2ReadOnlyAccess na Referência de políticas gerenciadas pela AWS.

AWS Política gerenciada da: AmazonEC2ImageReferencesAccessPolicy

É possível anexar a política `AmazonEC2ImageReferencesAccessPolicy` às identidades do IAM. Esta política concede as permissões necessárias para usar a API DescribeImageReferences do EC2, incluindo permissão para visualizar instâncias do EC2, modelos de inicialização, parâmetros do Systems Manager e fórmulas do Image Builder. A política é compatível com o sinalizador `IncludeAllResourceTypes` e continuará funcionando quando a AWS adicionar suporte para novos tipos de recursos, eliminando a necessidade de futuras atualizações de políticas.

Para visualizar as permissões para esta política, consulte AmazonEC2ImageReferencesAccessPolicy na Referência de políticas gerenciadas pela AWS.

AWS Política gerenciada da: AWSEC2CapacityReservationFleetRolePolicy

Essa política é anexada ao perfil vinculado a serviço denominado AWSServiceRoleForEC2CapacityReservationFleet para permitir que o serviço crie, modifique e cancele reservas de capacidade em uma Frota de reservas de capacidade em seu nome. Para obter mais informações, consulte Uso de funções vinculadas aos serviços para a frota de reserva de capacidade.

Para visualizar as permissões para esta política, consulte AWSEC2CapacityReservationFleetRolePolicy na Referência de políticas gerenciadas pela AWS.

AWS Política gerenciada da: AWSEC2FleetServiceRolePolicy

Esta política é anexada à função vinculada ao serviço de nome AWSServiceRoleForEC2Fleet para permitir que o EC2 Fleet solicite, inicie, encerre e aplique tags nas instâncias para você. Para obter mais informações, consulte Função vinculada ao serviço para Frota do EC2.

Para visualizar as permissões para esta política, consulte AWSEC2FleetServiceRolePolicy na Referência de políticas gerenciadas pela AWS.

AWS Política gerenciada da: AWSEC2SpotFleetServiceRolePolicy

Esta política é anexada à função vinculada ao serviço de nome AWSServiceRoleForEC2SpotFleet para permitir que a frota spot inicie e gerencie instâncias para você. Para obter mais informações, consulte Função vinculada ao serviço para frota spot.

Para visualizar as permissões para esta política, consulte AWSEC2SpotFleetServiceRolePolicy na Referência de políticas gerenciadas pela AWS.

AWS Política gerenciada da: AWSEC2SpotServiceRolePolicy

Esta política é anexada à função vinculada ao serviço de nome AWSServiceRoleForEC2Spot para permitir que o Amazon EC2 inicie e gerencie instâncias spot para você. Para obter mais informações, consulte Função vinculada ao serviço para solicitações de instâncias spot.

Para visualizar as permissões para esta política, consulte AWSEC2SpotServiceRolePolicy na Referência de políticas gerenciadas pela AWS.

AWS Política gerenciada da: AWSEC2VssSnapshotPolicy

É possível anexar essa política gerenciada à função do perfil de instância do IAM usada para as instâncias do Windows do Amazon EC2. A política concede permissões que possibilitam que o Amazon EC2 crie e gerencie snapshots do VSS em seu nome.

Para visualizar as permissões para esta política, consulte AWSEC2VssSnapshotPolicy na Referência de políticas gerenciadas pela AWS.

AWS Política gerenciada da: DeclarativePoliciesEC2Report

Essa política é anexada ao perfil vinculado a serviço denominado `AWSServiceRoleForDeclarativePoliciesEC2Report` para fornecer acesso a APIs somente leitura necessárias para gerar o relatório de status da conta para políticas declarativas.

Para visualizar as permissões para esta política, consulte DeclarativePoliciesEC2Report na Referência de políticas gerenciadas pela AWS.

AWS Política gerenciada da: EC2FastLaunchFullAccess

É possível anexar a política de `EC2FastLaunchFullAccess` ao perfil de instância ou a outro perfil do IAM. Essa política concede total acesso às ações e às permissões direcionadas do EC2 Fast Launch como se segue.

Detalhes da permissão

- EC2 Fast Launch: acesso administrativo é concedido para que o perfil possa habilitar ou desabilitar o EC2 Fast Launch e descrever as imagens do EC2 Fast Launch.
- Amazon EC2: é concedido acesso para as operações RunInstances, CreateTags, Describe e Create and Modify Launch Template do Amazon EC2. Também é concedido acesso para criar recursos de rede e grupos de segurança, autorizar regras de entrada e excluir recursos criados pelo EC2 Fast Launch.
- IAM: acesso é concedido para obter e usar perfis de instância cujo nome contenha `ec2fastlaunch` para criar o perfil vinculada ao serviço EC2FastLaunchServiceRolePolicy.
- CloudFormation – é concedido acesso ao EC2 Fast Launch para descrever e criar pilhas do CloudFormation, e para excluir as pilhas que ele criou.

Para visualizar as permissões para esta política, consulte EC2FastLaunchFullAccess na Referência de políticas gerenciadas pela AWS.

AWS Política gerenciada da: AWSEC2CapacityManagerServiceRolePolicy

Esta política é anexada ao perfil vinculado ao serviço AWSServiceRoleForEC2CapacityManager para permitir que o EC2 Capacity Manager gerencie recursos de capacidade e se integre ao AWS Organizations para você. Para obter mais informações, consulte Perfis vinculados ao serviço para o EC2 Capacity Manager.

Para visualizar as permissões para esta política, consulte AWSEC2CapacityManagerServiceRolePolicy na Referência de políticas gerenciadas pela AWS.

AWS Política gerenciada da: EC2FastLaunchServiceRolePolicy

Esta política é anexada ao perfil vinculado ao serviço denominado AWSServiceRoleForEC2FastLaunch para permitir que o Amazon EC2 crie e gerencie um conjunto

de snapshots pré-provisionados que reduzem o tempo necessário para iniciar instâncias usando a AMI habilitada para EC2 Fast Launch. Para obter mais informações, consulte the section called "Perfil vinculado a serviço".

Para visualizar as permissões para esta política, consulte EC2FastLaunchServiceRolePolicy na Referência de políticas gerenciadas pela AWS.

AWS Política gerenciada da: Ec2InstanceConnect

É possível anexar a política `Ec2InstanceConnect` às suas identidades do IAM. Esta política concede permissões para que os clientes chamem o EC2 Instance Connect para publicar chaves efêmeras em suas instâncias do EC2 e se conectem via ssh ou pela CLI do EC2 Instance Connect.

Para visualizar as permissões para esta política, consulte Ec2InstanceConnect na Referência de políticas gerenciadas pela AWS.

AWS Política gerenciada da: Ec2InstanceConnectEndpoint

Essa política é anexada a um perfil vinculado a serviço chamado AWSServiceRoleForEC2InstanceConnect para permitir que o EC2 Instance Connect Endpoint execute ações em seu nome. Para obter mais informações, consulte Perfil vinculado ao serviço para o EC2 Instance Connect Endpoint.

Para visualizar as permissões para esta política, consulte Ec2InstanceConnectEndpoint na Referência de políticas gerenciadas pela AWS. Para obter uma descrição das atualizações desta política, consulte Atualizações do Amazon EC2 para políticas gerenciadas pela AWS.

Atualizações do Amazon EC2 para políticas gerenciadas pela AWS

Visualize detalhes sobre atualizações em políticas gerenciadas pela AWS para o Amazon EC2 desde que esse serviço começou a rastrear essas alterações.

Alteração	Descrição	Data
AWSEC2CapacityManagerServiceRolePolicy – Nova política	O Amazon EC2 adicionou essa política para permitir que você gerencie recursos de capacidade e se integre ao AWS Organizations para você.	15 de outubro de 2025

Alteração	Descrição	Data
AmazonEC2ImageReferencesAccessPolicy – nova política	O Amazon EC2 adicionou essa política para fornecer permissão para verificar todos os tipos de recursos compatíveis com a API DescribeImageReferences do EC2.	26 de agosto de 2025
Ec2InstanceConnectEndpoint – Atualizar política	Para oferecer suporte à modificação dos endpoints de conexão de instâncias existentes, o Amazon EC2 atualizou essa política para adicionar permissões para atribuir e cancelar a atribuição de endereços IPv6 e modificar grupos de segurança em interfaces de rede criadas pelo endpoint de conexão de instância do EC2. O Amazon EC2 também atualizou essa política para substituir o operador de condição `Null` pelo operador de condição `StringLike` .	31 de julho de 2025
EC2FastLaunchServiceRolePolicy – Atualizar política	Para ajudar a evitar recursos órfãos, o Amazon EC2 atualizou essa política para adicionar permissão para descrever volumes, atributos de volume e interfaces de rede, e para excluir volumes e interfaces de rede criados pelo EC2 Fast Launch.	17 de julho de 2025

Alteração	Descrição	Data
EC2FastLaunchFullAccess – Atualizar política	O Amazon EC2 atualizou essa política para incluir as operações Create and Modify Launch Template, para criar recursos de rede e grupos de segurança, autorizar regras de entrada e excluir recursos criados pelo EC2 Fast Launch. Ela também pode descrever e criar pilhas do CloudFormation, e excluir pilhas criadas pelo EC2 Fast Launch.	14 de maio de 2025
EC2FastLaunchServiceRolePolicy – Atualizar política	O Amazon EC2 atualizou essa política para adicionar acesso ao Amazon EventBridge para criar e gerenciar regras de eventos para o EC2 Fast Launch. Além disso, o EC2 Fast Launch agora pode descrever pilhas do CloudFormation, iniciar uma instância a partir de uma AMI associada ao AWS License Manager, obter uma lista das concessões do AWS KMS que ele criou e que podem ser retiradas, e excluir os modelos de inicialização que ele criou.	14 de maio de 2025

Alteração	Descrição	Data
AWSEC2CapacityReservationFleetRolePolicy: Permissões atualizadas	O Amazon EC2 atualizou a política gerenciada `AWSEC2CapacityReservationFleetRolePolicy` para utilizar o operador de condição `ArnLike` em vez do operador de condição `StringLike` .	03 de março de 2025
AmazonEC2ReadOnlyAccess – adicionou permissões	O Amazon EC2 adicionou uma permissão que permite recuperar grupos de segurança usando a operação `GetSecurityGroupsForVpc` .	27 de dezembro de 2024
EC2FastLaunchFullAccess – nova política	O Amazon EC2 adicionou essa política para realizar ações de API relacionadas ao atributo EC2 Fast Launch em uma instância. A política pode ser anexada ao perfil de instância para uma instância que é iniciada usando uma AMI habilitada para o EC2 Fast Launch.	14 de maio de 2024
AWSEC2VssSnapshotPolicy – nova política	O Amazon EC2 adicionou a política `AWSEC2VssSnapshotPolicy` que contém permissões para criar e adicionar tags a images de máquina da Amazon (AMIs) e a snapshots do EBS.	28 de março de 2024

Alteração	Descrição	Data
Ec2InstanceConnectEndpoint – nova política	A Amazon EC2 adicionou a política `Ec2InstanceConnectEndpoint` . Essa política está anexada ao perfil vinculado ao serviço AWSServiceRoleForEC2InstanceConnect, para permitir que o Amazon EC2 execute ações em seu nome quando você criar um endpoint de conexão de instância do EC2.	24 de janeiro de 2023
EC2FastLaunchServiceRolePolicy – nova política	O Amazon EC2 adicionou o atributo EC2 Fast Launch para habilitar as AMIs do Windows a executar instâncias mais rapidamente criando um conjunto de snapshots pré-provisionados.	26 de novembro de 2021
O Amazon EC2 passou a monitorar as alterações	O Amazon EC2 passou a controlar as alterações nas políticas gerenciadas pela AWS.	1.º de março de 2021

Funções do IAM para Amazon EC2

As aplicações devem assinar suas solicitações de API com as credenciais da AWS. Portanto, se você for um desenvolvedor de aplicações, precisará de uma estratégia para gerenciar credenciais para suas aplicações que executam em instâncias do EC2. Por exemplo, é possível distribuir de maneira segura suas credenciais da AWS para as instâncias, permitindo que as aplicações nessas instâncias usem suas credenciais para assinar solicitações, enquanto protege suas credenciais de outros usuários. Contudo, é um desafio distribuir credenciais para cada instância de maneira segura,

especialmente aquelas que a AWS cria em seu nome, como instâncias spot ou instâncias em grupos do Auto Scaling. Você também deve poder atualizar as credenciais em cada instância quando alterna suas credenciais da AWS.

Projetamos funções do IAM para que suas aplicações possam fazer solicitações de API de suas instâncias de maneira segura, sem exigir que você gerencie as credenciais de segurança que as aplicações usam. Em vez de criar e distribuir suas credenciais da AWS, é possível delegar permissão para fazer solicitações de API usando funções do IAM da seguinte forma:

1. Crie uma função do IAM.
2. Defina quais contas ou serviços da AWS podem assumir a função.
3. Defina quais ações e recursos de API a aplicação pode usar depois de assumir a função.
4. Especifique a função quando você executar a instância ou anexe a função a uma instância existente.
5. Faça com que a aplicação recupere um conjunto de credenciais temporárias e use-as.

Por exemplo, é possível usar funções do IAM para conceder permissões a aplicações em execução em suas instâncias que precisam usar um bucket no Amazon S3. É possível especificar permissões para funções do IAM criando uma política em formato JSON. Essas são semelhantes às políticas que você cria para os usuários do . Se você alterar uma função, a alteração será propagada para todas as instâncias.

> **Note**
>
> As credenciais do perfil do IAM do Amazon EC2 não estão sujeitas às durações máximas de sessão configuradas no perfil. Para obter mais informações, consulte Métodos para assumir um perfil no Manual do usuário do IAM.

Ao criar funções do IAM, associe políticas do IAM de privilégio mínimo que restringem o acesso às chamadas de API específicas exigidas pela aplicação. Para comunicação Windows para Windows, use grupos e funções bem definidos e bem documentados do Windows para conceder acesso no nível de aplicação entre instâncias do Windows. Grupos e funções permitem que os clientes definam permissões de aplicação de privilégio mínimo e no nível de pasta do NTFS para limitar o acesso a requisitos específicos da aplicação.

Você só pode anexar uma função do IAM a uma instância, mas pode anexar a mesma função a muitas instâncias. Para obter mais informações sobre como criar e usar funções do IAM, consulte Funções no Guia do usuário do IAM.

É possível aplicar permissões em nível de recurso às políticas do IAM para controlar a capacidade de anexar, substituir ou desanexar funções do IAM de uma instância. Para obter mais informações, consulte Permissões no nível do recurso com suporte para ações de API do Amazon EC2 e o seguinte exemplo: Exemplo: trabalhar com funções do IAM.

Tópicos

- Perfis de instância
- Permissões para seu caso de uso
- Recuperar credenciais de segurança dos metadados da instância
- Conceder permissões para anexar um perfil do IAM a uma instância
- Anexar uma função do IAM a uma instância
- Perfis de identidade da instância para instâncias do Amazon EC2

Perfis de instância

O Amazon EC2 usa um perfil de instância como um contêiner para uma função do IAM. Se você criar uma função do IAM usando o console do IAM 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 iniciar 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. É possível incluir um perfil do IAM em vários perfis de instâncias.

Para atualizar as permissões de uma instância, substitua o perfil da instância. Não é recomendável remover um perfil de um perfil de instância, pois existe um atraso de até uma hora antes que essa alteração entre em vigor.

Para obter mais informações, consulte Usar perfis de instâncias no Guia do usuário do IAM.

Permissões para seu caso de uso

Quando você cria uma função do IAM pela primeira vez para suas aplicações, às vezes é possível conceder permissões além do que é necessário. Antes de iniciar sua aplicação em seu ambiente de produção, é possível gerar uma política do IAM baseada na atividade de acesso para uma função do IAM. O IAM Access Analyzer revisa seus logs do AWS CloudTrail e gera um modelo de política que contém as permissões que foram usadas pela função no intervalo de datas especificado. É possível usar o modelo para criar uma política gerenciada com permissões refinadas e anexá-la à função do IAM. Dessa forma, você concede apenas as permissões necessárias à interação com os recursos da AWS, de acordo com a especificidade do caso de uso. Isso ajuda você a aderir às melhores práticas de conceder privilégio mínimo. Para obter mais informações, consulte Geração de política do IAM Access Analyzer no Guia do usuário do IAM.

Recuperar credenciais de segurança dos metadados da instância

Uma aplicação na instância recupera as credenciais de segurança fornecidas pela função no item `iam/security-credentials/`role-name dos metadados da instância. A aplicação recebe as permissões para as ações e recursos que você definiu para a função por meio das credenciais de segurança associadas à função. Essas credenciais de segurança são temporárias e são alternadas automaticamente. Tornamos novas credenciais disponíveis pelo menos cinco minutos antes da expiração das credenciais antigas.

Para obter mais informações sobre os metadados da instância, consulte Usar metadados da instância para gerenciar a instância do EC2.

> **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.

Para suas workloads do Amazon EC2, recomendamos recuperar as credenciais da sessão usando o método descrito abaixo. Essas credenciais devem permitir que sua workload faça solicitações da API da AWS sem precisar usar `sts:AssumeRole` para assumir a mesma função que já está associada à instância. A menos que seja necessário passar etiquetas de sessão para controle de acesso por atributo (ABAC) ou passar uma política de sessão para restringir ainda mais as permissões da

função, essas chamadas de suposição de função são desnecessárias, pois criam um novo conjunto das mesmas credenciais de sessão de função temporária.

Se sua workload usa uma função para assumir a si mesma, é necessário criar uma política de confiança que permita explicitamente que essa função se assuma sozinha. Se a política de confiança não for criada, o erro `AccessDenied` ocorrerá. Para obter mais informações, consulte Atualização de uma política de confiança de perfil no Guia do usuário do IAM.

IMDSv2

Linux

Execute o seguinte comando em sua instância Linux para recuperar as credenciais de segurança de um perfil do IAM.

```
TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
    && curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/iam/security-credentials/role-name
```

Windows

Execute o seguinte cmdlet em sua instância Windows para recuperar as credenciais de segurança de um perfil do IAM.

```
[string]$token = Invoke-RestMethod `
    -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} `
    -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
Invoke-RestMethod `
    -Headers @{"X-aws-ec2-metadata-token" = $token} `
    -Method GET -Uri http://169.254.169.254/latest/meta-data/iam/security-credentials/role-name
```

IMDSv1

Linux

Execute o seguinte comando em sua instância Linux para recuperar as credenciais de segurança de um perfil do IAM.

```
curl http://169.254.169.254/latest/meta-data/iam/security-credentials/role-name
```

Windows

Execute o seguinte cmdlet em sua instância Windows para recuperar as credenciais de segurança de um perfil do IAM.

```
Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/iam/security-
credentials/role-name
```

O seguinte é um exemplo de saída. Se você não conseguir recuperar as credenciais de segurança, consulte Não é possível acessar as credenciais de segurança temporárias em minha instância do EC2 no Guia do usuário do IAM.

```
{
  "Code" : "Success",
  "LastUpdated" : "2012-04-26T16:39:16Z",
  "Type" : "AWS-HMAC",
  "AccessKeyId" : "ASIAIOSFODNN7EXAMPLE",
  "SecretAccessKey" : "wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY",
  "Token" : "token",
  "Expiration" : "2017-05-17T15:09:54Z"
}
```

Para comandos de aplicações, AWS CLI e Tools for Windows PowerShell que são executados na instância, não é necessário obter as credenciais de segurança temporárias explicitamente – os AWS SDKs, a AWS CLI e o Tools for Windows PowerShell obtêm automaticamente as credenciais do serviço de metadados da instância do EC2 e as usam. Para fazer uma chamada fora da instância usando credenciais de segurança temporárias (por exemplo, para testar as políticas do IAM), forneça a chave de acesso, a chave secreta e o token da sessão. Para obter mais informações, consulte Usar credenciais de segurança temporárias para solicitar acesso aos recursos da AWS no Manual do usuário do IAM.

Conceder permissões para anexar um perfil do IAM a uma instância

As identidades em sua Conta da AWS, como usuários do IAM, devem ter permissões específicas para executar uma instância do Amazon EC2 com um perfil do IAM, anexar um perfil do IAM a uma instância, substituir o perfil do IAM por uma instância ou desanexar um perfil do IAM de

uma instância. Você deve conceder permissão para usar as seguintes ações de API, conforme necessário:

- `iam:PassRole`
- `ec2:AssociateIamInstanceProfile`
- `ec2:DisassociateIamInstanceProfile`
- `ec2:ReplaceIamInstanceProfileAssociation`

> **Note**
>
> Se você especificar o recurso para `iam:PassRole` como `*`, isso concederá acesso para passar qualquer um dos perfis do IAM para uma instância. Para seguir a prática recomendada de privilégio mínimo, especifique os ARNs de perfis específicos do IAM com `iam:PassRole`, conforme mostrado no exemplo de política abaixo.

Exemplo de política para acesso programático

A política do IAM a seguir concede permissões para executar instâncias com um perfil do IAM, anexar um perfil do IAM a uma instância ou substituir um perfil do IAM por uma instância usando a AWS CLI ou a API do Amazon EC2.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
         "ec2:RunInstances",
         "ec2:AssociateIamInstanceProfile",
         "ec2:DisassociateIamInstanceProfile",
         "ec2:ReplaceIamInstanceProfileAssociation"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
```

```
      "Action": "iam:PassRole",
      "Resource": "arn:aws:iam::123456789012:role/DevTeam*"
    }
  ]
}
```

Requisito adicional para acesso ao console

Para conceder permissões para concluir as mesmas tarefas usando o console do Amazon EC2, você também deve incluir a ação da API `iam:ListInstanceProfiles`.

Anexar uma função do IAM a uma instância

É possível criar uma função do IAM e anexá-la a uma instância durante ou depois da execução. Você também pode substituir ou desanexar perfis do IAM.

Para anexar um perfil do IAM a uma instância na execução usando o console do Amazon EC2, expanda Detalhes avançados. Para Perfil de instância do IAM, selecione o perfil do IAM.

> **Note**
>
> Caso tenha criado o perfil do IAM usando o console do IAM, o perfil da instância terá sido criado para você e terá o mesmo nome do perfil. Caso tenha criado o perfil do IAM usando a AWS CLI, a API ou um SDK da AWS, é possível que você tenha dado um nome diferente do perfil para o perfil da instância.

É possível anexar um perfil do IAM a uma instância que está em execução ou interrompida. Se a instância já tiver um perfil do IAM anexado, você deverá substituí-lo pelo novo perfil do IAM.

Console

Como anexar uma função do IAM a uma instância

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância.
4. Selecione Actions (Ações), Security (Segurança), Modify IAM role (Modificar perfil do IAM).

5. Para Perfil do IAM, selecione o perfil de instância do IAM.
6. Escolha Atualizar perfil do IAM.

AWS CLI

Como anexar uma função do IAM a uma instância

Use o comando associate-iam-instance-profile para anexar o perfil do IAM à instância. Ao especificar o perfil de instância, você pode usar o nome do recurso da Amazon (ARN) do perfil de instância ou o seu nome.

```
aws ec2 associate-iam-instance-profile \
    --instance-id i-1234567890abcdef0 \
    --iam-instance-profile Name="TestRole-1"
```

PowerShell

Como anexar uma função do IAM a uma instância

Use o cmdlet Register-EC2IamInstanceProfile.

```
Register-EC2IamInstanceProfile `
    -InstanceId i-1234567890abcdef0 `
    -IamInstanceProfile_Name TestRole-1
```

Para substituir o perfil do IAM em uma instância que já tenha um perfil do IAM anexado, essa instância deve estar em execução. Será possível fazer isso se você quiser alterar a função do IAM de uma instância sem desanexar a existente primeiro. Por exemplo, é possível fazer isso para garantir que as ações de API desempenhadas por aplicações executadas na instância não sejam interrompidas.

Console

Como substituir uma função do IAM para uma instância

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância.

4. Selecione Actions (Ações), Security (Segurança), Modify IAM role (Modificar perfil do IAM).
5. Para Perfil do IAM, selecione o perfil de instância do IAM.
6. Escolha Atualizar perfil do IAM.

AWS CLI

Como substituir uma função do IAM para uma instância

1. Se necessário, use o comando describe-iam-instance-profile-associations para obter o ID da associação.

```
aws ec2 describe-iam-instance-profile-associations \
    --filters Name=instance-id,Values=i-1234567890abcdef0 \
    --query IamInstanceProfileAssociations.AssociationId
```

2. Use o comando replace-iam-instance-profile-association. Especifique o ID de associação do perfil de instância existente e o ARN ou o nome do novo perfil de instância.

```
aws ec2 replace-iam-instance-profile-association \
    --association-id iip-assoc-0044d817db6c0a4ba \
    --iam-instance-profile Name="TestRole-2"
```

PowerShell

Como substituir uma função do IAM para uma instância

1. Se necessário, use o cmdlet Get-EC2IamInstanceProfileAssociation para obter o ID da associação.

```
(Get-EC2IamInstanceProfileAssociation -Filter @{Name="instance-id";
 Values="i-0636508011d8e966a"}).AssociationId
```

2. Use o cmdlet Set-EC2IamInstanceProfileAssociation. Especifique o ID de associação do perfil de instância existente e o ARN ou o nome do novo perfil de instância.

```
Set-EC2IamInstanceProfileAssociation `
    -AssociationId iip-assoc-0044d817db6c0a4ba `
    -IamInstanceProfile_Name TestRole-2
```

É possível desvincular um perfil do IAM de uma instância que esteja em execução ou interrupção.

Console

Como desanexar uma função do IAM de uma instância

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância.
4. Selecione Actions (Ações), Security (Segurança), Modify IAM role (Modificar perfil do IAM).
5. Em IAM role (Função do IAM), selecione No IAM Role (Nenhuma função do IAM).
6. Escolha Atualizar perfil do IAM.
7. Quando a confirmação for solicitada, insira Desanexar e depois escolha Desanexar.

AWS CLI

Como desanexar uma função do IAM de uma instância

1. Se necessário, use describe-iam-instance-profile-associations para obter o ID de associação do perfil de instância do IAM a ser desanexado.

```
aws ec2 describe-iam-instance-profile-associations \
    --filters Name=instance-id,Values=i-1234567890abcdef0 \
    --query IamInstanceProfileAssociations.AssociationId
```

2. Use o comando disassociate-iam-instance-profile.

```
aws ec2 disassociate-iam-instance-profile --association-id iip-
assoc-0044d817db6c0a4ba
```

PowerShell

Como desanexar uma função do IAM de uma instância

1. Se necessário, use Get-EC2IamInstanceProfileAssociation para obter o ID de associação do perfil de instância do IAM a ser desanexado.

```
(Get-EC2IamInstanceProfileAssociation -Filter @{Name="instance-id";
 Values="i-0636508011d8e966a"}).AssociationId
```

2. Use o cmdlet Unregister-EC2IamInstanceProfile.

```
Unregister-EC2IamInstanceProfile -AssociationId iip-assoc-0044d817db6c0a4ba
```

Perfis de identidade da instância para instâncias do Amazon EC2

Cada instância do Amazon EC2 inicializada tem um perfil de identidade da instância que representa sua identidade. Um perfil de identidade de instância é um tipo de perfil do IAM. Serviços da AWS e recursos integrados para usar o perfil de identidade da instância podem usá-lo para identificar a instância com o serviço.

As credenciais do perfil de identidade da instância podem ser acessadas no Serviço de metadados da instância (IMDS) em `/identity-credentials/ec2/security-credentials/ec2-instance`. As credenciais consistem em um par temporário de chave de acesso da AWS e um token de sessão. Eles são usados para assinar solicitações AWS Sigv4 para os serviços da AWS que usam o perfil de identidade da instância. As credenciais estão presentes nos metadados da instância, independentemente de um serviço ou recurso que faça uso dos perfils de identidade da instância estar habilitado na instância.

Os perfis de identidade da instância são criados automaticamente quando uma instância é iniciada, não possuem nenhum documento de política de confiança de perfil e não estão sujeitos a nenhuma política de identidade ou de recursos.

Serviços com suporte

Os serviços da AWS a seguir usam o perfil de identidade da instância:

- Amazon EC2: o EC2 Instance Connect usa o perfil de identidade da instância para atualizar as chaves de host de uma instância do Linux.
- Amazon GuardDuty: o monitoramento de runtime do GuardDuty usa o perfil de identidade da instância para permitir que o agente de runtime envie telemetria de segurança para o endpoint da VPC do GuardDuty.
- AWS Security Token Service (AWS STS): as credenciais do perfil de identidade da instância podem ser usadas com a ação AWS STS `GetCallerIdentity`.

- AWS Systems Manager: ao usar a Configuração padrão de gerenciamento de host, o AWS Systems Manager usa a identidade fornecida pelo perfil de identidade da instância para registrar instâncias do EC2. Depois de identificar sua instância, o Systems Manager pode passar seu perfil do IAM `AWSSystemsManagerDefaultEC2InstanceManagementRole` para sua instância.

Os perfis de identidade da instância não podem ser usados com outros serviços ou recursos da AWS, pois eles não têm uma integração com os perfis de identidade da instância.

ARN de perfil de identidade da instância

O ARN de perfil de identidade da instância assume o seguinte formato:

```
arn:aws-partition:iam::account-number:assumed-role/aws:ec2-instance/instance-id
```

Por exemplo:

```
arn:aws:iam::0123456789012:assumed-role/aws:ec2-instance/i-1234567890abcdef0
```

Para obter mais informações sobre ARNs, consulte Nome do recurso da Amazon (ARN) no Guia do usuário do IAM.

Gerenciamento de atualizações para instâncias do Amazon EC2

Recomendamos que você aplique patches, atualize e proteja regularmente o sistema operacional e as aplicações em suas instâncias do EC2. É possível usar o Gerenciador de patches do AWS Systems Manager para automatizar o processo de instalação de atualizações relacionadas à segurança para o sistema operacional e para a aplicação.

Para instâncias do EC2 em um grupo de Auto Scaling, você pode usar o AWS-PatchAsgInstance runbook para ajudar a evitar que instâncias que estão passando por patches sejam substituídas Como alternativa, é possível usar qualquer serviço de atualização automática ou processos recomendados para instalar atualizações fornecidas pelo fornecedor da aplicação.

Recursos

- AL2023: Atualização do AL2023 no Guia do usuário do Amazon Linux 2023
- AL2: Gerenciamento de software na sua instância do Amazon Linux 2 no Guia do usuário do Amazon Linux 2
- Instâncias do Windows – the section called “Gerenciamento de atualizações”

Práticas recomendadas de segurança para instâncias do Windows

Recomendamos seguir estas práticas recomendadas de segurança para as instâncias do Windows.

Conteúdo

- Práticas recomendadas de segurança de alto nível
- Gerenciamento de atualizações
- Gerenciamento de configuração
- Gerenciamento de alterações
- Auditoria e responsabilidade para instâncias do Windows do Amazon EC2

Práticas recomendadas de segurança de alto nível

Você deve seguir as seguintes práticas recomendadas de segurança de alto nível para as instâncias do Windows:

- Menos acesso: conceda acesso somente a sistemas e locais confiáveis e esperados. Isso se aplica a todos os produtos da Microsoft, como o Active Directory, servidores de produtividade empresarial da Microsoft e serviços de infraestrutura, como Serviços de área de trabalho remota, servidores de proxy reverso, servidores Web IIS e outros. Use os recursos da AWS, como os grupos de segurança da instância do Amazon EC2, listas de controle de acesso (ACLs) à rede e sub-redes públicas/privadas da Amazon VPC, para colocar a segurança em camadas em vários locais em uma arquitetura. Em uma instância do Windows, os clientes podem usar o Firewall do Windows para colocar mais uma camada na estratégia de defesa completa em sua implantação. Instale apenas os componentes e as aplicações do sistema operacional necessários para que o sistema funcione conforme projetado. Configure serviços de infraestrutura, como o IIS, para serem executados em contas de serviço ou para usar recursos como identidades de grupo de aplicações para acessar recursos local e remotamente na infraestrutura.
- Privilégio mínimo: determine o conjunto mínimo de privilégios de que as instâncias e contas precisam para executar as funções. Restringir esses servidores e usuários para permitir apenas essas permissões definidas. Use técnicas, como controles de acesso baseados em função, para reduzir a área de superfície das contas administrativas e criar as funções mais limitadas para realizar uma tarefa. Use recursos do sistema operacional, como o Encrypting File System (EFS – Criptografia do sistema de arquivos) dentro do NTFS, para criptografar dados confidenciais em repouso e controlar o acesso de aplicações e de usuários a ele.

- Gerenciamento de configuração: crie uma configuração de linha de base do servidor que incorpore a aplicação de patches de segurança atualizados e pacotes de proteção baseados em host que incluem antivírus, antimalware, detecção e prevenção de invasões, e monitoramento da integridade dos arquivos. Avalie cada servidor em relação à linha de base registrada atual para identificar e sinalizar quaisquer desvios. Verifique se cada servidor está configurado para gerar e armazenar com segurança os dados adequados de log e auditoria.
- Gerenciamento de alterações: crie processos para controlar as alterações nas linhas de base da configuração do servidor e trabalhe em processos de alterações totalmente automatizados. Além disso, aproveite Just Enough Administration (JEA) com o Windows PowerShell DSC para limitar o acesso administrativo às funções mínimas necessárias.
- Gerenciamento de patches: implemente processos que corrijam, atualizem e protejam o sistema operacional e as aplicações, regularmente, nas instâncias do EC2.
- Logs de auditoria: audite o acesso e todas as alterações nas instâncias do Amazon EC2 para verificar a integridade do servidor e garantir que somente alterações autorizadas sejam feitas. Utilize funcionalidades como Enhanced Log for IIS (Log aprimorado para IIS) para melhorar os recursos de registo de log padrão. Os recursos da AWS como Logs de fluxo da VPC e AWS CloudTrail também estão disponíveis para auditar o acesso à rede, incluindo solicitações permitidas/negadas e chamadas de API, respectivamente.

Gerenciamento de atualizações

Para garantir os melhores resultados ao executar o Windows Server no Amazon EC2, recomendamos implantar as seguintes práticas recomendadas:

- Configure Windows Update
- Update drivers
- Use the latest Windows AMIs
- Test performance before migration
- Update launch agents
- Reiniciar a instância do Windows após instalar as atualizações. Para obter mais informações, consulte Reinicializar uma instância do Amazon EC2.

Para obter informações sobre como atualizar ou migrar uma instância do Windows para uma versão mais recente do Windows Server, consulte Atualizar uma instância do Windows do EC2 para uma versão mais recente do Windows Server.

Configurar o Windows Update

Por padrão, as instâncias iniciadas usando AMIs do AWS Windows Server não recebem atualizações por meio do Windows Update.

Atualizar drivers do Windows

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

- Use tópicos do SNS para receber atualizações de novos lançamentos de driver.
- Use o runbook do AWS Systems Manager Automation AWSSupport-UpgradeWindowsAWSDrivers para aplicar facilmente as atualizações em todas as instâncias.

Executar instâncias usando as AMIs mais recentes do Windows

A AWS realiza o lançamento de AMIs do Windows todos os meses. Essas AMIs contêm os patches, os drivers e os agentes de inicialização mais recentes para o sistema operacional. É necessário utilizar a AMI mais recente ao executar novas instâncias ou ao criar suas próprias imagens personalizadas.

- Para visualizar atualizações para cada versão das AMIs do Windows na AWS, consulte Histórico de versões da AMI do Windows na AWS.
- Para criar com as AMIs mais recentes disponíveis, consulte Consulta para a AMI mais recente do Windows usando o Systems Manager Parameter Store.
- Para obter mais informações sobre as AMIs do Windows especializadas que você pode usar para executar instâncias para o seu banco de dados e casos de uso de hardening de conformidade, consulte Specialized Windows AMIs na Referência de AMI do Windows da AWS.

Testar a performance do sistema/aplicação antes da migração

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

- Os tipos de instância estão configurados corretamente, incluindo o tamanho da instância, as redes avançadas e a locação (compartilhada ou dedicada).

- A topologia da instância é apropriada para a workload e utiliza recursos de alta performance quando necessário, com locação dedicada, grupos de alocação, volumes de armazenamento de instâncias e bare metal.

Instalar a versão mais recente do EC2Launch v2

Instale o agente EC2Launch v2 mais recente para garantir que os aprimoramentos mais recentes sejam aplicados em toda a sua frota. Para obter mais informações, consulte Instalar o EC2Launch v2.

Se você tiver uma frota mista ou quiser continuar usando os agentes EC2Launch (Windows Server 2016 e 2019) ou EC2 Config (somente SO herdado), atualize para as versões mais recentes dos respectivos agentes.

Há suporte para as atualizações automáticas nas seguintes combinações de agentes de execução e versão do Windows Server. É possível optar por receber atualizações automáticas no console SSM Quick Setup Host Management em Amazon EC2 Launch Agents.

Versão do Windows	EC2Launch v1	EC2Launch v2
2016	✓	✓
2019	✓	✓
2022		✓

- Para obter mais informações sobre a atualização para o EC2Launch v2, consulte the section called “Instalar o EC2Launch v2”.
- Para obter informações sobre como atualizar manualmente o EC2Config, consulte the section called “Instalar o EC2Config”.
- Para obter informações sobre como atualizar manualmente o EC2Launch, consulte the section called “Instalar o EC2Launch”.

Gerenciamento de configuração

As imagens de máquina da Amazon (AMIs) fornecem uma configuração inicial para uma instância do Amazon EC2, que inclui o sistema operacional Windows e personalizações opcionais específicas

do cliente, como aplicações e controles de segurança. Crie um catálogo de AMI que contém linhas de base de configuração de segurança personalizadas para garantir que todas as instâncias do Windows sejam iniciadas com controles de segurança padrão. As linhas de base de segurança podem ser incorporadas em uma AMI, inicializadas dinamicamente quando uma instância do EC2 é executada ou empacotadas como um produto para distribuição uniforme por meio de portfólios do AWS Service Catalog. Para obter mais informações sobre como proteger uma AMI, consulte Práticas recomendadas para criar uma AMI.

Cada instância do Amazon EC2 deve aderir aos padrões de segurança organizacional. Não instale nenhuma função e recurso do Windows que não seja necessário e instale software (antivírus, antimalware, mitigação de vulnerabilidades) para proteger contra códigos mal-intencionados, monitore a integridade do host e execute a detecção de intrusões. Configure o software de segurança para monitorar e manter as configurações de segurança do SO, proteger a integridade de arquivos críticos do SO e alertar sobre desvios da linha de base de segurança. Considere implementar benchmarks recomendados de configuração de segurança publicados pela Microsoft, pelo Centro de Segurança da Internet (CIS) ou pelo National Institute of Standards and Technology (NIST). Considere usar outras ferramentas da Microsoft para servidores de aplicações específicos, como o Analisador de melhores práticas para SQL Server.

AWSOs clientes da também podem executar avaliações do Amazon Inspector para aprimorar a segurança e a conformidade das aplicações implantadas nas instâncias do Amazon EC2. O Amazon Inspector avalia automaticamente as aplicações quanto a vulnerabilidades ou desvios das práticas recomendadas e inclui uma base de conhecimento de centenas de regras mapeadas para padrões comuns de conformidade de segurança (por exemplo, PCI DSS) e definições de vulnerabilidade. Exemplos de regras incorporadas incluem verificar se o início remoto de sessão raiz está habilitado ou se versões de software vulneráveis estão instaladas. Essas regras são atualizadas regularmente pelos pesquisadores de segurança da AWS.

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

Gerenciamento de alterações

Depois que as linhas de base de segurança iniciais forem aplicadas às instâncias do Amazon EC2 durante a execução, controle as alterações contínuas do Amazon EC2 para manter a segurança das máquinas virtuais. Estabeleça um processo de gerenciamento de alterações para autorizar e incorporar alterações aos recursos da AWS (como grupos de segurança, tabelas de rotas e ACLs de rede), bem como a configurações do SO e de aplicações (como aplicação de patches do Windows ou da aplicação, atualizações de software ou atualizações de arquivos de configuração).

A AWS fornece várias ferramentas para ajudar a gerenciar alterações nos recursos da AWS, incluindo o AWS CloudTrail, o AWS Config, o CloudFormation e o AWS Elastic Beanstalk, além de pacotes de gerenciamento para o Systems Center Operations Manager e o System Center Virtual Machine Manager. Observe que a Microsoft lança patches do Windows na segunda terça-feira de cada mês (ou conforme necessário), e a AWS atualiza todas as AMIs do Windows gerenciadas pela AWS em até cinco dias após a Microsoft lançar um patch. Portanto, é importante corrigir continuamente todas as AMIs de linha de base, atualizar modelos do CloudFormation e configurações de grupo de Auto Scaling com os IDs de AMI mais recentes e implementar ferramentas para automatizar o gerenciamento de patches de instâncias em execução.

A Microsoft fornece várias opções para gerenciar o sistema operacional Windows e as alterações de aplicações. O SCCM, por exemplo, fornece cobertura completa do ciclo de vida das modificações do ambiente. Selecione ferramentas que atendam aos requisitos comerciais e controlem como as alterações afetarão os SLAs de aplicações, a capacidade, a segurança e os procedimentos de recuperação de desastres. Evite alterações manuais e, em vez disso, utilize o software de gerenciamento de configuração automatizado ou ferramentas da linha de comando, como o Run Command do EC2 ou o Windows PowerShell, para implementar processos de alteração com script e repetíveis. Para ajudar com esse requisito, use bastion hosts com registro em log aprimorado para todas as interações com suas instâncias do Windows para garantir que todos os eventos e tarefas sejam gravados automaticamente.

Auditoria e responsabilidade para instâncias do Windows do Amazon EC2

O AWS CloudTrail, o AWS Config e o Regras do AWS Config fornecem recursos de auditoria e controle de alterações para a auditoria de alterações de recursos da AWS. Configure os logs de eventos do Windows para enviar arquivos de log locais a um sistema centralizado de gerenciamento de logs a fim de preservar os dados de log para a análise de comportamento operacional e de segurança. O Microsoft System Center Operations Manager (SCOM) agrega informações sobre aplicações da Microsoft implantadas em instâncias do Windows e aplica conjuntos de regras

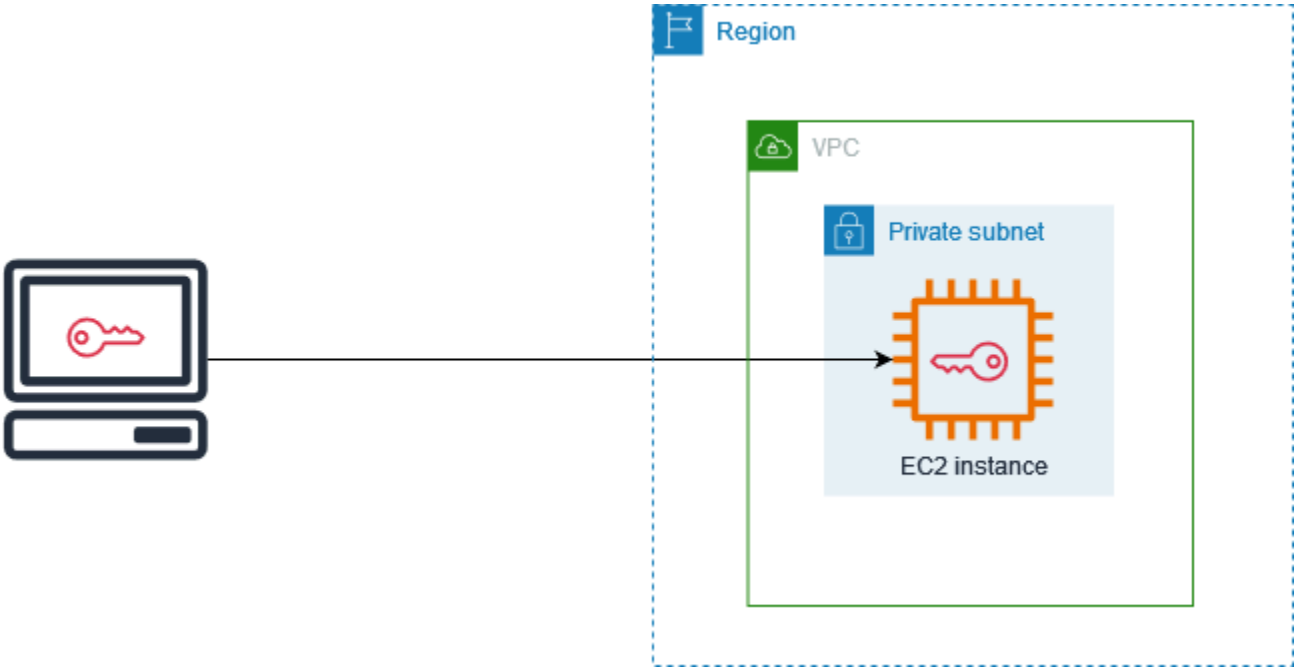
pré-configurados e personalizados com base em funções e serviços de aplicações. Os Pacotes de Gerenciamento do System Center são baseados no SCOM para fornecer monitoramento e orientações de configuração específicos da aplicação. Esses Pacotes de Gerenciamento oferecem suporte ao Windows Server Active Directory, SharePoint Server 2013, Exchange Server 2013, Lync Server 2013, SQL Server 2014 e muitos mais servidores e tecnologias.

Além das ferramentas de gerenciamento de sistemas da Microsoft, os clientes podem usar o Amazon CloudWatch para monitorar a utilização da CPU da instância, a performance do disco, a E/S da rede e realizar verificações de status do host e da instância. Os agentes de inicialização EC2Config, EC2Launch e EC2Launch v2 fornecem acesso a recursos avançados adicionais para instâncias do Windows. Por exemplo, eles podem exportar logs do sistema, de segurança, de aplicações e de Serviços de Informações da Internet (IIS) do Windows para o CloudWatch Logs, os quais poderão ser integrados a métricas e alarmes do Amazon CloudWatch. Os clientes também podem criar scripts que exportam contadores de performance do Windows para métricas personalizadas do Amazon CloudWatch.

Pares de chaves do Amazon EC2 e instâncias do Amazon EC2

Um par de chaves, que consiste em uma chave pública e uma chave privada, trata-se de um conjunto de credenciais de segurança usadas para provar sua identidade ao se conectar a uma instância do Amazon EC2. Para instâncias do Linux, a chave privada permite usar o SSH com segurança en sua instância. Para instâncias do Windows, a chave privada é necessária para descriptografar a senha de administrador, que poderá então ser usada para se conectar à instância.

O Amazon EC2 armazena a chave pública na instância, e você armazena a chave privada, conforme mostrado no diagrama a seguir. É importante armazenar sua chave privada em um local seguro, pois qualquer pessoa que tiver acesso a ela poderá se conectar a suas instâncias que usam o par de chaves.



Ao iniciar uma instância, é possível especificar um par de chaves para poder se conectar à instância usando um método que requer um par de chaves. Dependendo de como você gerencia sua segurança, é possível especificar o mesmo par de chaves para todas as suas instâncias ou especificar pares de chaves diferentes.

Para instâncias do Linux, quando a instância é inicializada pela primeira vez, a chave pública que você especificou na inicialização é colocada na instância do Linux em uma entrada dentro de `~/.ssh/authorized_keys`. Ao conectar-se à instância do Linux usando SSH, especifique a chave privada que corresponde à chave pública para fazer login.

Para obter mais informações sobre como se conectar à instância do EC2, consulte Conexão com a instância do EC2.

> **Important**
>
> Como o Amazon EC2 não mantém uma cópia da sua chave privada, não há como recuperar a chave privada caso você a perca. No entanto, ainda pode haver uma maneira de se conectar a instâncias para as quais você perdeu a chave privada. Para obter mais informações, consulte . Perdi minha chave privada. Como posso me conectar à instância?

Como alternativa aos pares de chaves, é possível usar AWS Systems Manager Session Manager para se conectar à instância como um shell interativo de um clique baseado no navegador ou a AWS Command Line Interface (AWS CLI).

Conteúdo

- Criar um par de chaves para sua instância do Amazon EC2
- Descrever seus pares de chaves
- Excluir o par de chaves
- Adicionar ou substituir uma chave pública na instância do Linux
- Verificar a impressão digital do par de chaves

Criar um par de chaves para sua instância do Amazon EC2

É possível usar o Amazon EC2 para criar seus pares de chaves ou usar uma ferramenta de terceiros para criar seus pares de chaves e depois importá-los para o Amazon EC2.

O Amazon EC2 é compatível com as chaves SSH-2 RSA de 2.048 bits para instâncias do Linux e do Windows. Além disso, o Amazon EC2 é compatível com chaves ED25519 para instâncias do Linux.

Para obter as instruções sobre como se conectar à instância depois de criar um par de chaves, consulte the section called “Conectar-se à instância do Linux usando SSH” e the section called “Conectar-se à instância do Windows no usando RDP”.

Conteúdo

- Criar um par de chaves usando o Amazon EC2
- Criar um par de chaves usando o AWS CloudFormation
- Criar um par de chaves usando uma ferramenta de terceiros e importe a chave pública para o Amazon EC2

Criar um par de chaves usando o Amazon EC2

Quando você criar um par de chaves usando o Amazon EC2, a chave pública será armazenada no Amazon EC2 e você armazenará a chave privada.

É possível criar até 5.000 pares de chaves por região. Para solicitar um aumento de cota, crie um caso de suporte. Para obter mais informações, consulte Criação de um caso de suporte no Guia do usuário do Suporte.

Console

Para criar um par de chaves usando o 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, selecione Pares de chaves.
3. Escolha Create key pair (Criar par de chaves).
4. Em Name (Nome), insira um nome descritivo para o par de chaves. O Amazon EC2 associa a chave pública ao nome especificado como o nome da chave. Um nome de chave pode incluir até 255 caracteres ASCII. Não pode incluir espaços no início nem no final.
5. Selecione um tipo de par de chaves apropriado para seu sistema operacional:

   (Instâncias do Linux) Em Tipo de par de chaves, escolha RSA ou ED25519.

   (Instâncias do Windows) Em Tipo de par de chaves, escolha RSA. As chaves ED25519 não são compatíveis com as instâncias do Windows.
6. Para Formato de arquivo de chave privada, escolha o formato no qual salvar a chave privada. Para salvar a chave privada em um formato que possa ser usado com o OpenSSH, escolha pem. Para salvar a chave privada em um formato que possa ser usado com o PuTTY, escolha ppk.
7. Para adicionar uma etiqueta à chave pública, escolha Adicionar etiqueta, e insira a chave e o valor da etiqueta. Repita esse procedimento para cada tag.
8. Escolha Create key pair (Criar par de chaves).
9. O arquivo de chave privada é baixado automaticamente pelo navegador. O nome do arquivo base é o nome especificado como o nome do par de chaves, e a extensão do nome do arquivo é determinada pelo formato do arquivo escolhido. Salve o arquivo de chave privada em um lugar seguro.

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

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

```
chmod 400 key-pair-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.

AWS CLI

Para criar um par de chaves usando o Amazon EC2

1. Use o comando create-key-pair da seguinte forma para gerar um par de chaves e salvar a chave privada em um arquivo `.pem`. A opção `--query` imprime o material da chave privada na saída. A opção `--output` salva o material da chave privada no arquivo especificado. A extensão deve ser `.pem` ou `.ppk`, dependendo do formato da chave. O nome da chave privada pode ser diferente do nome da chave pública mas, para facilitar, use o mesmo nome.

```
aws ec2 create-key-pair \
    --key-name my-key-pair \
    --key-type rsa \
    --key-format pem \
    --query "KeyMaterial" \
    --output text > my-key-pair.pem
```

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

```
chmod 400 key-pair-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.

PowerShell

Para criar um par de chaves usando o Amazon EC2

Use o cmdlet New-EC2KeyPair como a seguir para gerar e salvar a chave em um arquivo `.pem` ou `.ppk`. O cmdlet Out-File salva o material da chave privada em um arquivo com a extensão especificada. A extensão deve ser `.pem` ou `.ppk`, dependendo do formato da chave. O nome da chave privada pode ser diferente do nome da chave pública mas, para facilitar, use o mesmo nome.

```
(New-EC2KeyPair `
    -KeyName "my-key-pair" `
    -KeyType "rsa" `
    -KeyFormat "pem").KeyMaterial | Out-File -Encoding ascii -FilePath C:\path\my-key-pair.pem
```

Criar um par de chaves usando o AWS CloudFormation

Quando você cria um novo par de chaves usando o CloudFormation, a chave privada é salva no AWS Systems Manager Parameter Store. O nome do parâmetro tem o seguinte formato:

```
/ec2/keypair/key_pair_id
```

Para obter mais informações, consulte o Armazenamento de parâmetros do AWS Systems Manager, no Guia do usuário do AWS Systems Manager.

Para criar um par de chaves usando o CloudFormation

1. Especifique o recurso AWS::EC2::KeyPair em seu modelo.

```
Resources:
  NewKeyPair:
    Type: 'AWS::EC2::KeyPair'
    Properties:
      KeyName: new-key-pair
```

2. Use o comando describe-key-pairs da seguinte forma para obter o ID do par de chaves.

```
aws ec2 describe-key-pairs --filters Name=key-name,Values=new-key-pair --query
 KeyPairs[*].KeyPairId --output text
```

O seguinte é um exemplo de saída.

```
key-05abb699beEXAMPLE
```

3. Use o comando get-parameter da seguinte forma para obter o parâmetro para sua chave e salvar o material da chave em um arquivo `.pem`.

```
aws ssm get-parameter --name /ec2/keypair/key-05abb699beEXAMPLE --with-decryption
 --query Parameter.Value --output text > new-key-pair.pem
```

Permissões obrigatórias do IAM

Para habilitar o CloudFormation a gerenciar parâmetros da Parameter Store em seu nome, o perfil do IAM assumido pelo CloudFormation ou seu usuário devem ter as permissões a seguir:

- `ssm:PutParameter`: concede permissão para criar um parâmetro para o material da chave privada.
- `ssm:DeleteParameter`: concede permissão para excluir o parâmetro que armazenou o material da chave privada. Essa permissão é necessária independentemente de o par de chaves ter sido importado ou criado pelo CloudFormation.

Quando o CloudFormation exclui um par de chaves criado ou importado por uma pilha, ele realiza uma verificação de permissões para determinar se você tem permissão para excluir os parâmetros, embora o CloudFormation só crie um parâmetro quando cria um par de chaves, não quando importa um par de chaves. O CloudFormation testa a permissão necessária usando um nome de parâmetro fabricado que não corresponde a nenhum parâmetro em sua conta. Portanto, você pode ver um nome de parâmetro fabricado na mensagem de erro `AccessDeniedException`.

Criar um par de chaves usando uma ferramenta de terceiros e importe a chave pública para o Amazon EC2

Em vez de usar o Amazon EC2 para criar um par de chaves, você pode criar um par de chaves RSA ou ED25519 usando uma ferramenta de terceiros e, então, importar a chave pública para o Amazon EC2.

Requisitos para pares de chaves

- Tipos compatíveis:
  - (Linux e Windows) RSA

  - (Somente Linux) ED25519

    > **Note**
    >
    > As chaves ED25519 não são compatíveis com as instâncias do Windows.

  - O Amazon EC2 não aceita chaves DSA.
- Formatos com suporte
  - Formato de chave pública OpenSSH (para Linux, o formato em `~/.ssh/authorized_keys`)
  - (Somente Linux) Se você se conectar usando SSH enquanto usa a API do EC2 Instance Connect, o formato do SSH2 também será compatível.
  - O formato de arquivo de chave privada SSH deve ser PEM ou PPK
  - (Apenas RSA) Formato DER codificado em Base64
  - (Apenas RSA) Formato de arquivo de chave pública SSH, conforme especificado em RFC 4716
- Tamanhos compatíveis:
  - 1024, 2048 e 4096.
  - (Somente Linux) Se você se conectar usando SSH enquanto usa a API do EC2 Instance Connect, os tamanhos compatíveis serão 2048 e 4096.

Para criar um par de chaves usando uma ferramenta de terceiros

1. Gere um par de chaves com uma ferramenta de terceiros de sua escolha. Por exemplo, é possível usar ssh-keygen (uma ferramenta fornecida com a instalação padrão de OpenSSH). Como alternativa, Java, Ruby, Python e muitas outras linguagens de programação fornecem bibliotecas padrão que podem ser usadas para criar um par de chaves.

   > **Important**
   >
   > A chave privada deve estar no formato PEM ou PPK. Por exemplo, use `ssh-keygen -m PEM` para gerar a chave OpenSSH no formato PEM.

2. Salve a chave pública em um arquivo local. Por exemplo, `~/.ssh/my-key-pair.pub` (Linux, macOS) 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 que tenha a extensão `.pem` ou `.ppk`. Por exemplo, `~/.ssh/my-key-pair.pem` ou `~/.ssh/my-key-pair.ppk` (Linux, macOS) ou `C:\keys\my-key-pair.pem` ou `C:\keys\my-key-pair.ppk` (Windows). A extensão do arquivo é importante porque, dependendo da ferramenta usada para se conectar à instância, você precisará de um formato de arquivo específico. O OpenSSH requer um arquivo `.pem`, enquanto o PuTTY requer um arquivo `.ppk`.

> **Important**
>
> Salve o arquivo de chave privada em um lugar seguro. Você precisará fornecer o nome da chave pública ao iniciar uma instância e a chave privada correspondente sempre que se conectar à instância.

Depois de criar o par de chaves, use um dos seguintes métodos para importar o par de chaves para Amazon EC2.

Console

Para importar a chave pública para o Amazon EC2

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Key Pairs (Pares de chaves).
3. Selecione Import key pair (Importar par de chaves).
4. Em Name (Nome), insira um nome descritivo para a chave pública. O nome pode incluir até 255 caracteres ASCII. Não pode incluir espaços no início nem no final.

> **Note**
>
> Quando você se conecta à instância pelo console do EC2, o console sugere esse nome para o arquivo de chave privada.

5. Escolha Browse (Procurar) para navegar e selecionar a chave pública ou cole o conteúdo da chave pública no campo Public key contents (Conteúdo da chave pública).
6. Selecione Import key pair (Importar par de chaves).
7. Verifique se a chave pública que você importou aparece na lista de pares de chaves.

AWS CLI

Para importar a chave pública para o Amazon EC2

Use o comando import-key-pair.

```
aws ec2 import-key-pair \
    --key-name my-key-pair \
    --public-key-material fileb://path/my-key-pair.pub
```

Como verificar se o par de chaves foi importado com êxito

Use o comando describe-key-pairs.

```
aws ec2 describe-key-pairs --key-names my-key-pair
```

PowerShell

Para importar a chave pública para o Amazon EC2

Use o cmdlet Import-EC2KeyPair.

```
$publickey=[Io.File]::ReadAllText("C:\Users\TestUser\.ssh\id_rsa.pub")
Import-EC2KeyPair `
    -KeyName my-key-pair `
    -PublicKey $publickey
```

Como verificar se o par de chaves foi importado com êxito

Use o cmdlet Get-EC2KeyPair.

```
Get-EC2KeyPair -KeyName my-key-pair
```

Descrever seus pares de chaves

É possível descrever os pares de chaves que você armazenou no Amazon EC2. Também é possível recuperar o material da chave pública e identificar a chave pública especificada na inicialização.

Tarefas

- Descrever seus pares de chaves
- Recuperar o material da chave pública
- Identifique a chave pública que foi especificada na inicialização

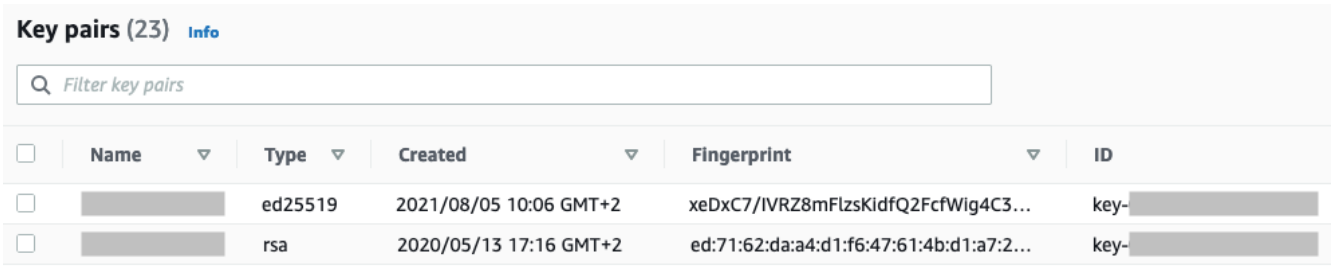
Descrever seus pares de chaves

É possível visualizar as seguintes informações sobre suas chaves públicas armazenadas no Amazon EC2: nome da chave pública, ID, tipo de chave, impressão digital, material da chave pública, a data e a hora (no fuso horário UTC) em que a chave foi criada pelo Amazon EC2 (se a chave foi criada por uma ferramenta de terceiros, será mostrado a data e a hora em que a chave foi importada para o Amazon EC2) e todas as etiquetas associadas à chave pública.

Console

Para visualizar informações sobre seus pares de chave

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação à esquerda, escolha Key Pairs (Pares de chaves).
3. É possível visualizar as informações sobre cada chave pública na tabela Key pairs (Pares de chaves).



4. Para visualizar as tags de uma chave pública, marque a caixa de seleção ao lado da chave e escolha Ações, Gerenciar tags.

AWS CLI

Para visualizar informações sobre um par de chaves

Use o comando describe-key-pairs.

```
aws ec2 describe-key-pairs --key-names key-pair-name
```

PowerShell

Para visualizar informações sobre um par de chaves

Use o cmdlet Get-EC2KeyPair.

```
Get-EC2KeyPair -KeyName key-pair-name
```

Recuperar o material da chave pública

É possível obter o material de chave pública para seus pares de chaves. Veja a seguir um exemplo de chave pública. Observe que as quebras de linha estão presentes para facilitar a legibilidade.

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQClKsfkNkuSevGj3eYhCe53pcjqP3maAhDFcvBS7O6V
hz2ItxCih+PnDSUaw+WNQn/mZphTk/a/gU8jEzoOWbkM4yxyb/wB96xbiFveSFJuOp/d6RJhJOI0iBXr
lsLnBItntckiJ7FbtxJMXLvvwJryDUilBMTjYtwB+QhYXUMOzce5Pjz5/i8SeJtjnV3iAoG/cQk+0FzZ
qaeJAAHco+CY/5WrUBkrHmFJr6HcXkvJdWPkYQS3xqC0+FmUZofz221CBt5IMucxXPkX4rWi+z7wB3Rb
BQoQzd8v7yeb7OzlPnWOyN0qFU0XA246RA8QFYiCNYwI3f05p6KLxEXAMPLE
```

Private key

Para recuperar o material de chave pública usando ssh-keygen (Linux)

No computador Linux ou macOS local, use o comando ssh-keygen. 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
```

Se esse comando do ssh-keygen falhar, execute o seguinte comando chmod para garantir que o arquivo de chave privada tenha as permissões necessárias.

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

Para recuperar o material de chave pública usando PuTTYgen (Windows)

Em seu computador Windows local, inicie o PuTTYgen. Escolha Load. Selecione o arquivo `.ppk` ou `.pem` de chave privada. O PuTTYgen exibe a chave pública em Public key for pasting into OpenSSH authorized_keys file (Chave pública para colar no arquivo authorized_keys do OpenSSH). Também é possível visualizar a chave pública selecionando Save public key (Salvar a chave pública), especificando um nome para o arquivo, salvando-o e abrindo-o.

AWS CLI

Para recuperar o material de chave pública

Use o seguinte comando describe-key-pairs e especifique a opção `--include-public-key`.

```
aws ec2 describe-key-pairs \
    --key-names key-pair-name \
    --include-public-key \
    --query "KeyPairs[].PublicKey"
```

PowerShell

Para recuperar o material de chave pública

Use o cmdlet Get-EC2KeyPair.

```
(Get-EC2KeyPair -KeyName key-pair-name -IncludePublicKey $true).PublicKey
```

IMDSv2

Linux

Execute os seguintes comandos em sua instância Linux.

```
TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-
token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-
data/public-keys/0/openssh-key
```

Windows

Execute os seguintes cmdlets na sua instância Windows.

```
[string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds"
 = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method GET -Uri
 http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
```

IMDSv1

Linux

Execute o seguinte comando em sua instância Linux.

```
curl http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
```

Windows

Execute o seguinte cmdlet na sua instância Windows.

```
Invoke-RestMethod -uri  http://169.254.169.254/latest/meta-data/public-keys/0/
openssh-key
```

Identifique a chave pública que foi especificada na inicialização

Se você especificar uma chave pública ao iniciar uma instância, o nome da chave pública será registrado pela instância. O nome de chave pública relatado para uma instância não muda mesmo que você altere a chave pública na instância ou adicione chaves públicas.

Console

Para identificar a chave pública especificada na inicialização 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.
4. Na guia Detalhes, em Detalhes da instância, encontre Par de chaves atribuído na inicialização.

AWS CLI

Para identificar a chave pública especificada na inicialização da instância

Use o seguinte comando describe-instances.

```
aws ec2 describe-instances \
    --instance-id i-1234567890abcdef0 \
    --query "Reservations[].Instances[].KeyName" \
    --output text
```

O seguinte é um exemplo de saída.

```
key-pair-name
```

PowerShell

Para identificar a chave pública especificada na inicialização da instância

Use o cmdlet Get-EC2Instance.

```
(Get-EC2Instance -InstanceId i-1234567890abcdef0).Instances | Select KeyName
```

O seguinte é um exemplo de saída.

```
KeyName
-------
key-pair-name
```

Excluir o par de chaves

É possível excluir um par de chaves, o que remove a chave pública armazenada no Amazon EC2. A exclusão de um par de chaves não exclui a chave privada correspondente.

Ao excluir uma chave pública usando os métodos a seguir, você só exclui a chave pública que foi armazenada no Amazon EC2 quando você criou ou importou o par de chaves. A exclusão de uma chave pública não a remove de nenhuma instância às quais você a adicionou, seja quando você iniciou a instância ou mais tarde. Também não exclui a chave privada do computador local. É possível continuar a se conectar a instâncias iniciadas usando um par de chaves excluído do Amazon EC2, desde que ainda tenha o arquivo (`.pem`) da chave privada.

> **Important**
>
> Se você estiver usando um grupo do Auto Scaling (por exemplo, em um ambiente do Elastic Beanstalk), verifique se a chave pública que você está excluindo não está especificada em um modelo de inicialização associado ou configuração de execução. Se o Amazon EC2 Auto Scaling detectar uma instância não íntegra, executará uma instância de substituição. No entanto, a inicialização da instância falhará se o par de chaves públicas não for encontrado. Para obter mais informações, consulte Modelos de execução no Manual do usuário do Amazon EC2 Auto Scaling.

Console

Exclua sua chave pública no Amazon EC2

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Key Pairs (Pares de chaves).
3. Selecione o par de chaves a ser excluído e escolha Actions (Ações), Delete (Excluir).
4. No campo de confirmação, insira `Delete` e escolha Delete (Excluir).

AWS CLI

Exclua sua chave pública no Amazon EC2

Use o comando delete-key-pair.

```
aws ec2 delete-key-pair --key-name my-key-pair
```

PowerShell

Exclua sua chave pública no Amazon EC2

Use o cmdlet Remove-EC2KeyPair.

```
Remove-EC2KeyPair -KeyName my-key-pair
```

Adicionar ou substituir uma chave pública na instância do Linux

Se você perder uma chave privada, perderá o acesso a todas as instâncias que usam o par de chaves. Para obter mais informações sobre como se conectar a uma instância usando um par de chaves diferente daquele que você especificou ao iniciar a execução, consulte Eu perdi minha chave privada.

Ao iniciar uma instância, é possível especificar um par de chaves. Quando a instância é iniciada pela primeira vez, a chave pública especificada no lançamento é colocada na instância do Linux em uma entrada dentro de `~/.ssh/authorized_keys`. Ao conectar-se pela primeira vez à instância do

Linux usando SSH, você especifica o usuário padrão e a chave privada que corresponde à chave pública que está armazenada na instância do Linux.

Depois de se conectar à instância, você pode alterar o par de chaves usado para acessar a conta padrão do sistema da instância adicionando uma nova chave pública na instância ou substituindo a chave pública (excluindo a chave pública existente e adicionando uma nova) na instância. Também é possível remover todas as chaves públicas de uma instância.

É possível adicionar ou substituir um par de chaves pelos seguintes motivos:

- Se um usuário da sua organização requisitar acesso ao usuário no sistema usando um par de chaves separado, será possível adicionar a chave pública à sua instância.
- Se alguém tiver uma cópia da chave privada (arquivo `.pem`) e você quiser impedir que essa pessoa se conecte à sua instância (por exemplo, se tiver saído da organização), poderá excluir a chave pública na instância e substituí-la por uma nova.
- Se você criar uma AMI do Linux a partir de uma instância, o material da chave pública será copiado da instância para a AMI. Se você executar uma instância da AMI, a nova instância incluirá a chave pública da instância original. Para impedir que alguém com a chave privada se conecte à nova instância, remova a chave pública da instância original antes de criar a AMI.

Use os procedimentos a seguir para modificar o par de chaves para o usuário padrão, como `ec2-user`. Para obter informações sobre como adicionar usuários à sua instância, consulte a documentação do sistema operacional utilizado na instância.

Para adicionar ou substituir um par de chaves

1. Crie um par de chaves usando o console do Amazon EC2 ou uma ferramenta de terceiros.
2. Recupere a chave pública do seu novo par de chaves. Para obter mais informações, consulte Recuperar o material da chave pública.
3. Conecte-se à sua instância.
4. Na instância, usando o editor de texto de sua escolha, abra o arquivo `.ssh/authorized_keys`. Cole as informações de chave pública do novo par de chaves abaixo das informações de chave pública existentes e salve o arquivo.
5. Desconecte-se da instância. Teste se é possível se conectar à instância usando o arquivo de chave privada do novo par de chaves.
6. Se você estiver usando o Auto Scaling, a frota do EC2 ou um modelo de inicialização para iniciar as instâncias, verifique se o par de chaves sendo substituído está especificado no

modelo de inicialização ou na configuração de inicialização. Caso contrário, ocorrerá falha nas inicializações de instâncias

7. (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`.

Para remover uma chave pública de uma instância

1. Conecte-se à sua instância.
2. Usando um editor de texto à sua escolha, abra o arquivo `.ssh/authorized_keys` na instância. Exclua as informações da chave pública e salve o arquivo.

> **Warning**
>
> Se você remover todas as chaves públicas e se desconectar de uma instância, não poderá se reconectar a menos que tenha configurado uma maneira alternativa de fazer login.

Verificar a impressão digital do par de chaves

Para verificar a impressão digital do seu par de chaves, compare a impressão digital exibida na página Pares de chaves no console do Amazon EC2 ou a impressão digital retornada pelo comando describe-key-pairs com a impressão digital gerada usando a chave privada em seu computador local. Essas impressões digitais devem coincidir.

Quando o Amazon EC2 calcula uma impressão digital, ele pode incluir preenchimento na impressão digital com caracteres =. Outras ferramentas, como ssh-keygen, podem omitir esse preenchimento.

Se você estiver tentando verificar a impressão digital da instância do Linux do EC2 em vez da impressão digital do par de chaves, consulte Obter a impressão digital da instância.

Como as impressões digitais são calculadas

O Amazon EC2 usa diferentes funções de hash para calcular as impressões digitais de pares de chaves RSA e ED25519. Além disso, para pares de chaves RSA, o Amazon EC2 calcula as impressões digitais de maneira diferente. O serviço usa funções diferentes de hash dependendo de o par de chaves ter sido criado pelo Amazon EC2 ou importado para o Amazon EC2.

A tabela a seguir lista as funções de hash usadas para calcular as impressões digitais para pares de chaves RSA e ED25519 que são criados pelo Amazon EC2 e importados para o Amazon EC2.

(Instâncias do Linux) Funções de hash usadas para calcular impressões digitais

Fonte do par de chaves	Pares de chaves RSA (Windows e Linux)	Pares de chaves ED25519 (Linux)
Criado pelo Amazon EC2	SHA-1	SHA-256
Importado para o Amazon EC2	MD5[1]	SHA-256

[1] Se você importar uma chave RSA pública para o Amazon EC2, a impressão digital será calculada usando uma função hash MD5. Isso continua sendo verdadeiro independentemente de como você tenha criado o par de chaves. Por exemplo, usando uma ferramenta de terceiros ou gerando uma nova chave pública com base em uma chave privada existente criada usando o Amazon EC2.

Ao usar o mesmo par de chaves em regiões diferentes

Se você planeja usar o mesmo par de chaves para se conectar a instâncias em diferentes Regiões da AWS, é necessário importar a chave pública para todas as regiões nas quais você a usará. Se usar o Amazon EC2 para criar o key pair, será possível Recuperar o material da chave pública de forma que você possa importar a chave pública para as outras regiões.

> **Note**
>
> - Se você criar um par de chaves RSA usando o Amazon EC2 e gerar uma chave pública com base na chave privada do Amazon EC2, as chaves públicas importadas terão uma impressão digital diferente da chave pública original. Isso ocorre porque a impressão digital da chave RSA original criada usando o Amazon EC2 é calculada usando uma função de hash SHA-1, enquanto a impressão digital das chaves RSA importadas é calculada usando uma função de hash MD5.
> - Para pares de chaves ED25519, as impressões digitais serão as mesmas, independentemente de terem sido criadas pelo Amazon EC2 ou importadas para o Amazon EC2, porque a mesma função hash SHA-256 é usada para calcular a impressão digital.

Gerar uma impressão digital com base em uma chave privada

Use um dos seguintes comandos para gerar uma impressão digital com base na chave privada em sua máquina local.

Se estiver usando uma máquina local do Windows, poderá executar os comandos a seguir usando o Subsistema do Windows para Linux (WSL). Instale o WSL e uma distribuição do Linux usando as instruções em Como instalar Linux no Windows com WSL. O exemplo fornecido nas instruções instala a distribuição Ubuntu do Linux, mas é possível instalar qualquer distribuição. Você é solicitado a reiniciar o computador para que as alterações sejam implementadas.

- Se tiver criado o par de chaves usando o Amazon EC2

  Use as ferramentas OpenSSL para gerar uma impressão digital como apresentado nos exemplos a seguir.

  Para pares de chaves do RSA:

  ```
  openssl pkcs8 -in path_to_private_key -inform PEM -outform DER -topk8 -nocrypt |
   openssl sha1 -c
  ```

  (Instâncias do Linux) Para pares de chaves ED25519:

  ```
  ssh-keygen -l -f path_to_private_key
  ```

- (Somente pares de chaves RSA) Se você tiver importado a chave pública para o Amazon EC2

  É possível seguir este procedimento independentemente de como criou o par de chaves, usando, por exemplo, uma ferramenta de terceiros ou gerando uma nova chave pública a partir de uma chave privada existente criada usando o Amazon EC2

  Use as ferramentas OpenSSL para gerar a impressão digital como apresentado no exemplo a seguir.

  ```
  openssl rsa -in path_to_private_key -pubout -outform DER | openssl md5 -c
  ```

- Se tiver criado um par de chaves OpenSSH usando o OpenSSH 7.8 ou posterior e importado a chave pública para o Amazon EC2

  Use o ssh-keygen para gerar uma impressão digital como apresentado nos exemplos a seguir.

Para pares de chaves do RSA:

```
ssh-keygen -ef path_to_private_key -m PEM | openssl rsa -RSAPublicKey_in -outform DER
 | openssl md5 -c
```

(Instâncias do Linux) Para pares de chaves ED25519:

```
ssh-keygen -l -f path_to_private_key
```

Grupos de segurança do Amazon EC2 para as instâncias do EC2

Um grupo de segurança atua como firewall virtual para as instâncias do EC2 visando controlar o tráfego de entrada e de saída. As regras de entrada controlam o tráfego de entrada para a instância e as regras de saída controlam o tráfego de saída da instância. Ao executar sua instância, é possível especificar um ou mais grupos de segurança. Se você não especificar um grupo de segurança, o Amazon EC2 usará o grupo de segurança padrão para a VPC. Depois de executar uma instância, é possível alterar seus grupos de segurança.

A segurança é uma responsabilidade compartilhada entre a AWS e você. Para obter mais informações, consulte Segurança no Amazon EC2. A AWS fornece grupos de segurança como uma das ferramentas para proteger as instâncias, e você precisa configurá-los para atender às suas necessidades de segurança. Se houver requisitos que não sejam totalmente atendidos pelos grupos de segurança, é possível manter seu próprio firewall em qualquer uma das instâncias além de usar grupos de segurança.

Preços

Não há cobrança adicional pelo uso de grupos de segurança.

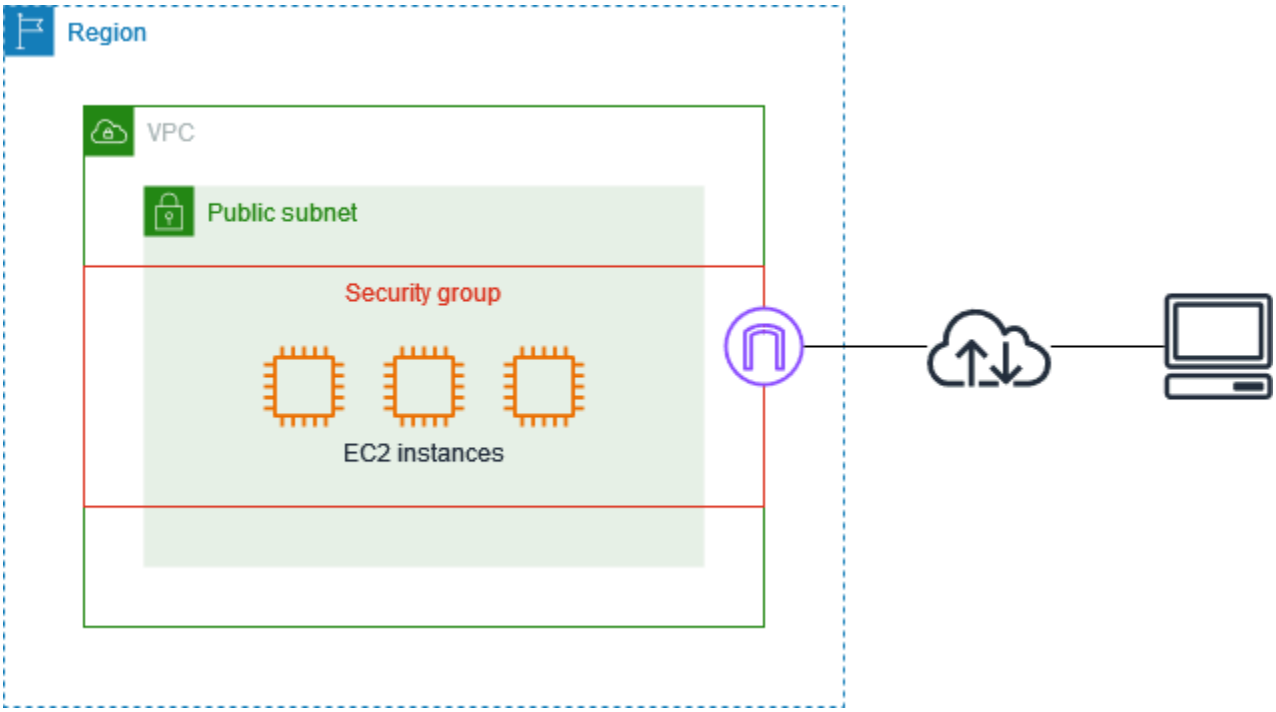
Conteúdo

- Visão geral
- Criar um grupo de segurança para a instância do Amazon EC2
- Alterar os grupos de segurança da instância do Amazon EC2
- Excluir um grupo de segurança do Amazon EC2
- Rastreamento de conexão de grupo de segurança do Amazon EC2
- Regras de grupo de segurança para diferentes casos de uso

Visão geral

É possível associar cada instância a vários grupos de segurança e associar cada grupo de segurança a várias instâncias. Você adiciona regras a cada security group que permite tráfego de entrada ou de saída das instâncias associadas. É possível modificar as regras de um grupo de segurança a qualquer momento. As regras novas e modificadas são aplicadas automaticamente para todas as instâncias que estão associados ao grupo de segurança. Quando o Amazon EC2 decide se deve permitir que o tráfego atinja uma instância, ele avalia todas as regras de todos os grupos de segurança associados à instância. Para ter mais informações, consulte Security group rules no Guia do usuário da Amazon VPC.

O diagrama a seguir mostra uma VPC com uma sub-rede, um gateway da Internet e um grupo de segurança. A sub-rede contém instâncias do EC2. O grupo de segurança está associado às instâncias. O único tráfego que chega à instância é aquele permitido pelas regras do grupo de segurança. Por exemplo, se o grupo de segurança contiver uma regra que permita o tráfego SSH da rede, será possível realizar a conexão com a instância com o computador ao usar SSH. Se o grupo de segurança contiver uma regra que permita todo o tráfego dos recursos associados a ele, cada instância poderá receber qualquer tráfego enviado das outras instâncias.



Os grupos de segurança são stateful — se você enviar uma solicitação da instância, o tráfego da resposta dessa solicitação terá permissão para fluir, independentemente das regras de entrada do grupo de segurança. Além disso, as respostas ao tráfego de entrada autorizado são permitidas

para fluir, independentemente das regras de saída. Para obter mais informações, consulte Acompanhamento da conexão.

Criar um grupo de segurança para a instância do Amazon EC2

Os grupos de segurança atuam como firewall para instâncias associadas, controlando o tráfego de entrada e de saída no nível da instância. É possível adicionar regras a um grupo de segurança que permitam que você se conecte à instância usando SSH (instâncias do Linux) ou RDP (instâncias do Windows). Você também pode adicionar regras que permitam o tráfego do cliente, por exemplo, o tráfego HTTP e HTTPS destinado a um servidor Web.

É possível associar um grupo de segurança a uma instância quando a inicia. Quando você adiciona ou remove regras de grupos de segurança associados, essas alterações são aplicadas automaticamente a todas as instâncias às quais você associou o grupo de segurança.

Depois de iniciar uma instância, você pode associar grupos de segurança adicionais. Para obter mais informações, consulte Alterar os grupos de segurança da instância do Amazon EC2.

É possível adicionar regras de grupo de segurança de entrada e saída quando criar um grupo de segurança ou pode adicioná-las mais tarde. Para obter mais informações, consulte Configurar regras de grupos de segurança. Para obter exemplos de regras que você pode adicionar a um grupo de segurança, consulte Regras de grupo de segurança para diferentes casos de uso.

Considerações

- Novos grupos de segurança começam com apenas uma regra de saída que permite que todo o tráfego deixe as instâncias. Adicione regras para permitir qualquer tráfego de entrada ou para restringir o tráfego de saída.
- Ao configurar uma fonte para uma regra que permita acesso SSH ou RDP às instâncias, não autorize acesso de qualquer lugar, pois isso concederia acesso à instância de todos os endereços IP da Internet. Isso é aceitável por um período curto em um ambiente de teste, mas não é seguro em ambientes de produção.
- Se houver mais de uma regra para uma porta específica, o Amazon EC2 aplicará a regra mais permissiva. Por exemplo, se você tiver uma regra que permita o acesso à porta TCP 22 (SSH) do endereço IP 203.0.113.1 e outra regra que permita o acesso à porta TCP 22 de qualquer lugar, todos terão acesso à porta TCP 22.
- É possível associar vários grupos de segurança a uma instância. Portanto, uma instância pode ter centenas de regras aplicáveis. Isso pode causar problemas quando você acessar a instância. Recomendamos que você condense suas regras o máximo possível.

- Quando você especifica um grupo de segurança como a origem ou o destino de uma regra, a regra afeta todas as instâncias associadas ao grupo de segurança. O tráfego de entrada é permitido com base nos endereços IP privados das instâncias associadas ao grupo de segurança 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.
- O Amazon EC2 bloqueia o tráfego na porta 25 por padrão. Para obter mais informações, consulte Restrição para e-mails enviados usando a porta 25.

Console

Para criar um security group

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Grupos de segurança.
3. Escolha Criar grupo de segurança.
4. Insira um nome descritivo e uma breve descrição para o grupo de segurança. Você não pode alterar o nome e a descrição de um grupo de segurança depois que ele é criado.
5. Em VPC, escolha a VPC na qual você executará suas instâncias do Amazon EC2.
6. (Opcional) Para adicionar regras de entrada, escolha Regras de entrada. Em cada regra, escolha Adicionar regra e especifique o protocolo, a porta e a origem. Por exemplo, para permitir tráfego SSH, escolha SSH em Tipo e especifique o endereço IPv4 público do seu computador ou rede em Origem.
7. (Opcional) Para adicionar regras de saída, escolha Regras de saída. Em cada regra, escolha Adicionar regra e especifique o protocolo, a porta e o destino. Caso contrário, você pode manter a regra padrão, o que permite todo o tráfego de saída.
8. (Opcional) Para adicionar uma tag, escolha Add new tag (Adicionar nova tag) e insira a chave e o valor da tag.
9. Escolha Create security group (Criar grupo de segurança).

AWS CLI

Como criar um grupo de segurança

Use o seguinte comando create-security-group.

```
aws ec2 create-security-group \
```

```
    --group-name my-security-group \
    --description "my security group" \
    --vpc-id vpc-1234567890abcdef0
```

Para exemplos que adicionam regras, consulte the section called “Configurar regras de grupos de segurança”.

PowerShell

Como criar um grupo de segurança

Use o cmdlet New-EC2SecurityGroup.

```
New-EC2SecurityGroup `
    -GroupName my-security-group `
    -Description "my security group" `
    -VpcId vpc-1234567890abcdef0
```

Para exemplos que adicionam regras, consulte the section called “Configurar regras de grupos de segurança”.

Alterar os grupos de segurança da instância do Amazon EC2

É possível especificar grupos de segurança para instâncias do Amazon EC2 quando iniciá-las. Depois de iniciar uma instância, você pode adicionar ou remover grupos de segurança. Você também pode adicionar, remover ou editar regras de grupos de segurança para grupos de segurança associados a qualquer momento.

Os grupos de segurança estão associados a interfaces de rede. Adicionar ou remover grupos de segurança altera os grupos de segurança associados à interface de rede primária. Também é possível alterar os grupos de segurança associados a interfaces de rede secundárias. Para obter mais informações, consulte Modificar atributos da interface de rede.

Tarefas

- Adicionar ou remover grupos de segurança
- Configurar regras de grupos de segurança

Adicionar ou remover grupos de segurança

Após iniciar uma instância, você pode adicionar ou remover grupos de segurança da lista de grupos de segurança associados. Quando você associa vários grupos de segurança a uma instância, as regras de cada security group são efetivamente agregadas para criar um conjunto de regras. O Amazon EC2 usa esse conjunto de regras para determinar se deve permitir tráfego.

Requisitos

- A instância deve estar no estado `running` ou `stopped`.

Console

Para modificar os grupos de segurança 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, em seguida, escolha Actions (Ações), Security (Segurança), Change security groups (Alterar grupos de segurança).
4. Em Associated security groups (Grupos de segurança associados), selecione um grupo de segurança na lista e escolha Add security group (Adicionar grupo de segurança).

   Para remover um grupo de segurança já associado, escolha Remove (Remover) para esse grupo de segurança.
5. Escolha Salvar.

AWS CLI

Para modificar os grupos de segurança de uma instância

Use o seguinte comando modify-instance-attribute.

```
aws ec2 modify-instance-attribute \
    --instance-id i-1234567890abcdef0 \
    --groups sg-1234567890abcdef0
```

PowerShell

Para modificar os grupos de segurança de uma instância

Use o cmdlet Edit-EC2InstanceAttribute.

```
Edit-EC2InstanceAttribute `
    -InstanceId i-1234567890abcdef0 `
    -Group sg-1234567890abcdef0
```

Configurar regras de grupos de segurança

Depois de criar um grupo de segurança, você pode adicionar, atualizar e excluir as regras dele. Quando você adiciona, atualiza ou exclui uma regra, a alteração é aplicada automaticamente aos recursos associados ao grupo de segurança.

Para obter exemplos de regras que você pode adicionar a um grupo de segurança, consulte Regras de grupo de segurança para diferentes casos de uso.

Permissões obrigatórias

Antes de começar, verifique se você tem as permissões necessárias. Para obter mais informações, consulte Exemplo: trabalhar com grupos de segurança.

Protocolos e portas

- Com o console, quando você seleciona um tipo predefinido, Protocolo e Intervalo de portas são especificados para você. Para inserir um intervalo de portas, você deve selecionar um dos seguintes tipos personalizados: TCP personalizado ou UDP personalizado .
- Com a AWS CLI, você pode adicionar uma única regra com uma única porta usando as opções `--protocol` e `--port`. Para adicionar várias regras ou uma regra com um intervalo de portas, use a opção `--ip-permissions`.

Origens e destinos

- Com o console, você pode especificar o seguinte como origens para as regras de entrada ou destinos para as regras de saída.
  - Personalizado: um bloco CIDR IPv4 e um bloco CIDR IPv6, um grupo de segurança ou uma lista de prefixos.
  - Anywhere-IPv4: o bloco CIDR IPv4 0.0.0.0/0.
  - Anywhere-IPv6: o bloco CIDR IPv6 ::/0.

  - Meu IP: o endereço IPv4 público do computador local.
- Com a AWS CLI, você pode especificar um bloco CIDR IPv4 usando a opção `--cidr` ou um grupo de segurança usando a opção `--source-group`. Para especificar uma lista de prefixos ou um bloco CIDR IPv6, use a opção `--ip-permissions`.

> **Warning**
>
> Se você adicionar regras de entrada para as portas 22 (SSH) ou 3389 (RDP), recomendamos enfaticamente que você autorize somente o endereço IP específico ou um intervalo de endereços que precisem de acesso às instâncias. Caso escolha Anywhere-IPv4, você permitirá que o tráfego de todos os endereços IPv4 acessem as instâncias usando o protocolo especificado. Caso escolha Anywhere-IPv6, você permitirá que o tráfego de todos os endereços IPv6 acessem as instâncias usando o protocolo especificado.

Console

Para configurar regras do grupo de segurança

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Grupos de segurança.
3. Selecione o grupo de segurança.
4. Para editar as regras de entrada, escolha Editar regras de entrada em Ações ou na guia Regras de entrada.

   a. Para adicionar uma regra, escolha Adicionar regra e insira o tipo, o protocolo, a porta e a origem da regra.

      Se o tipo for TCP ou UDP, será necessário inserir o intervalo de portas a ser permitido. Para ICMP personalizado, você deverá escolher o nome do tipo ICMP em Protocol (Protocolo) e, se aplicável, o nome do código em Port range (Intervalo de portas). Para qualquer outro tipo, o protocolo e o intervalo de portas serão configurados para você.

   b. Para atualizar uma regra, altere o protocolo, a descrição e a origem da regra, conforme necessário. Porém, você não pode alterar o tipo de origem. Por exemplo, se a origem for um bloco CIDR IPv4, você não poderá especificar um bloco CIDR IPv6, uma lista de prefixos ou um grupo de segurança.

c. Para excluir uma regra, escolha seu botão Excluir.

5. Para editar as regras de saída, escolha Editar regras de saída em Ações ou na guia Regras de saída.

   a. Para adicionar uma regra, escolha Adicionar regra e insira o tipo, o protocolo, a porta e o destino da regra. Você também pode inserir uma descrição opcional.

      Se o tipo for TCP ou UDP, será necessário inserir o intervalo de portas a ser permitido. Para ICMP personalizado, você deverá escolher o nome do tipo ICMP em Protocol (Protocolo) e, se aplicável, o nome do código em Port range (Intervalo de portas). Para qualquer outro tipo, o protocolo e o intervalo de portas serão configurados para você.

   b. Para atualizar uma regra, altere o protocolo, a descrição e a origem da regra, conforme necessário. Porém, você não pode alterar o tipo de origem. Por exemplo, se a origem for um bloco CIDR IPv4, você não poderá especificar um bloco CIDR IPv6, uma lista de prefixos ou um grupo de segurança.

   c. Para excluir uma regra, escolha seu botão Excluir.

6. Selecione Salvar regras.

AWS CLI

Para adicionar regras de grupo de segurança

Use o comando authorize-security-group-ingress para adicionar regras de entrada. O exemplo a seguir permite tráfego SSH de entrada proveniente dos blocos CIDR na lista de prefixos especificada.

```
aws ec2 authorize-security-group-ingress \
    --group-id sg-1234567890abcdef0 \
    --ip-permissions
 'IpProtocol=tcp,FromPort=22,ToPort=22,PrefixListIds=[{PrefixListId=pl-
f8a6439156EXAMPLE}]'
```

Use o comando authorize-security-group-egress para adicionar regras de saída. O exemplo a seguir permite tráfego TCP de saída na porta 80 para instâncias com o grupo de segurança especificado.

```
aws ec2 authorize-security-group-egress \
    --group-id sg-1234567890abcdef0 \
```

```
    --ip-permissions
 'IpProtocol=tcp,FromPort=80,ToPort=80,UserIdGroupPairs=[{GroupId=sg-0aad1c26bb6EXAMPLE}]'
```

Para remover regras de grupo de segurança

Use o seguinte comando revoke-security-group-ingress para remover uma regra de entrada.

```
aws ec2 revoke-security-group-egress \
    --group id sg-1234567890abcdef0 \
    --security-group-rule-ids sgr-09ed298024EXAMPLE
```

Use o seguinte comando revoke-security-group-egress para remover uma regra de saída.

```
aws ec2 revoke-security-group-ingress \
    --group id sg-1234567890abcdef0 \
    --security-group-rule-ids sgr-0352250c1aEXAMPLE
```

Para modificar regras do grupo de segurança

Use o comando modify-security-group-rules. O exemplo a seguir altera o bloco CIDR IPv4 da regra do grupo de segurança especificado.

```
aws ec2 modify-security-group-rules \
    --group id sg-1234567890abcdef0 \
    --security-group-rules
 'SecurityGroupRuleId=sgr-09ed298024EXAMPLE,SecurityGroupRule={IpProtocol=tcp,FromPort=80,To
```

PowerShell

Para adicionar regras de grupo de segurança

Use o cmdlet Grant-EC2SecurityGroupIngress para adicionar regras de entrada. O exemplo a seguir permite tráfego SSH de entrada proveniente dos blocos CIDR na lista de prefixos especificada.

```
$plid = New-Object -TypeName Amazon.EC2.Model.PrefixListId
$plid.Id = "pl-f8a6439156EXAMPLE"
Grant-EC2SecurityGroupIngress `
    -GroupId sg-1234567890abcdef0 `
    -IpPermission @{IpProtocol="tcp"; FromPort=22; ToPort=22; PrefixListIds=$plid}
```

Use o cmdlet Grant-EC2SecurityGroupEgress para adicionar regras de saída. O exemplo a seguir permite tráfego TCP de saída na porta 80 para instâncias com o grupo de segurança especificado.

```
$uigp = New-Object -TypeName Amazon.EC2.Model.UserIdGroupPair
$uigp.GroupId = "sg-0aad1c26bb6EXAMPLE"
Grant-EC2SecurityGroupEgress `
    -GroupId sg-1234567890abcdef0 `
    -IpPermission @{IpProtocol="tcp"; FromPort=80; ToPort=80; UserIdGroupPairs=
$uigp}
```

Para remover regras de grupo de segurança

Use o cmdlet Revoke-EC2SecurityGroupIngress para remover regras de entrada.

```
Revoke-EC2SecurityGroupIngress `
    -GroupId sg-1234567890abcdef0 `
    -SecurityGroupRuleId sgr-09ed298024EXAMPLE
```

Use o cmdlet Revoke-EC2SecurityGroupEgress para remover regras de saída.

```
Revoke-EC2SecurityGroupEgress `
    -GroupId sg-1234567890abcdef0 `
    -SecurityGroupRuleId sgr-0352250c1aEXAMPLE
```

Para modificar regras do grupo de segurança

Use o cmdlet Edit-EC2SecurityGroupRule. O exemplo a seguir altera o bloco CIDR IPv4 da regra do grupo de segurança especificado.

```
$sgrr = New-Object -TypeName Amazon.EC2.Model.SecurityGroupRuleRequest
$sgrr.IpProtocol = "tcp"
$sgrr.FromPort = 80
$sgrr.ToPort = 80
$sgrr.CidrIpv4 = "0.0.0.0/0"
$sgr = New-Object -TypeName Amazon.EC2.Model.SecurityGroupRuleUpdate
$sgr.SecurityGroupRuleId = "sgr-09ed298024EXAMPLE"
$sgr.SecurityGroupRule = $sgrr
Edit-EC2SecurityGroupRule  `
    -GroupId sg-1234567890abcdef0 `
    -SecurityGroupRule $sgr
```

Excluir um grupo de segurança do Amazon EC2

Quando você não precisar mais de um grupo de segurança que criou para usar com instâncias do Amazon EC2, poderá excluí-lo.

Requisitos

- O grupo de segurança não pode ser associado a uma instância ou a uma interface de rede.
- O grupo de segurança não pode ser referenciado por uma regra de outro grupo de segurança.

Console

Para excluir um security group

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. (Opcional) Para verificar se o grupo de segurança não está associado a uma instância, faça o seguinte:
   a. No painel de navegação, escolha Security Groups (Grupos de segurança).
   b. Copie o ID do grupo de segurança a ser excluído.
   c. No painel de navegação, escolha Instâncias.
   d. Na barra de pesquisa, adicione o filtro IDs do grupo de segurança que são iguais a e cole o ID do grupo de segurança. Se não houver resultados, então o grupo de segurança não está associado a uma instância. Caso contrário, você deverá desassociar o grupo de segurança antes de poder excluí-lo.
3. No painel de navegação, escolha Security Groups (Grupos de segurança).
4. Selecione o grupo de segurança e escolha Ações, Excluir grupos de segurança.
5. Caso tenha selecionado mais de um grupo de segurança, será solicitada sua confirmação. Se alguns dos grupos de segurança não puderem ser excluídos, exibiremos o status de cada grupo de segurança, que indicará se ele será ou não excluído. Para confirmar a exclusão, insira Excluir.
6. Escolha Excluir.

AWS CLI

Para excluir um security group

Use o seguinte comando delete-security-group.

```
aws ec2 delete-security-group --group-id sg-1234567890abcdef0
```

PowerShell

Para excluir um security group

Use o cmdlet Remove-EC2SecurityGroup.

```
Remove-EC2SecurityGroup -GroupId sg-1234567890abcdef0
```

Rastreamento de conexão de grupo de segurança do Amazon EC2

Os grupos de segurança usam o acompanhamento da conexão para acompanhar as informações sobre o tráfego de entrada e saída da instância. As regras são aplicadas com base no estado da conexão do tráfego para determinar se o tráfego é permitido ou negado. Com essa abordagem, os grupos de segurança são tipo com estado. Isso significa que as respostas ao tráfego de entrada têm permissão para sair da instância independentemente das regras do grupo de segurança de saída e vice-versa.

Por exemplo, suponha que você inicie um comando como netcat ou similar para instâncias de seu computador doméstico, e as regras de grupo de segurança de entrada permitam tráfego ICMP. As informações sobre a conexão (inclusive as informações da porta) são rastreadas. O tráfego de resposta da instância para o comando não é monitorado como uma nova solicitação, mas sim como uma conexão estabelecida e tem permissão para sair da instância, mesmo que as regras de seu grupo de segurança restrinjam o tráfego de saída ICMP.

Para protocolos diferentes de TCP, UDP ou ICMP, somente o endereço IP e o número do protocolo são acompanhados. Se a instância enviar tráfego para outro host e esse host iniciar o mesmo tipo de tráfego para a instância em 600 segundos, o grupo de segurança para a instância o aceitará independentemente das regras de entrada do grupo de segurança. O grupo de segurança aceitará isso, pois será considerado como tráfego de resposta para o tráfego original.

Quando você altera uma regra do grupo de segurança, suas conexões monitoradas não são imediatamente interrompidas. O grupo de segurança continua a permitir pacotes até o tempo limite das conexões existentes. Para garantir que o tráfego seja interrompido imediatamente, ou que todo o tráfego esteja sujeito às regras do firewall, independentemente do estado de monitoramento, será possível usar uma Network ACL para a sub-rede. As Network ACLs são stateless e, portanto, não

permitem automaticamente o tráfego de resposta. A adição de uma ACL de rede que bloqueia o tráfego em qualquer direção quebra as conexões existentes. Para saber mais, consulte Network ACLs no Guia do usuário da Amazon VPC.

> **Note**
>
> Os grupos de segurança não têm efeito sobre o tráfego de DNS de ou para o Route 53 Resolver, às vezes chamadas de "endereço IP VPC+2" (consulte O que é o Amazon Route 53 Resolver? no Guia do desenvolvedor do Amazon Route 53) ou o "AmazonProvidedDNS" (consulte Trabalhar com conjuntos de opções de DHCP no Guia do usuário do Amazon Virtual Private Cloud). Se você quiser filtrar solicitações de DNS por meio do Route 53 Resolver, é possível habilitar o Route 53 Resolver DNS Firewall (consulte Route 53 Resolver DNS Firewall no Guia do desenvolvedor do Amazon Route 53).

Conexões não rastreadas

Nem todos os fluxos de tráfego são acompanhados. Se uma regra do grupo de segurança permitir fluxos TCP ou UDP para todo o tráfego (0.0.0.0/0 ou ::/0) e houver uma regra correspondente na outra direção que permita todo o tráfego de resposta (0.0.0.0/0 ou ::/0) para qualquer porta (0-65535), esse fluxo de tráfego não será monitorado, a menos que faça parte de uma conexão monitorada automaticamente. O tráfego de resposta para um fluxo não monitorado é permitido com base na regra de entrada ou de saída que permite o tráfego de resposta, e não é baseado nas informações de monitoramento.

Um fluxo de tráfego não acompanhado será interrompido imediatamente se a regra que permite o fluxo for removida ou alterada. Por exemplo, se você tiver uma regra de saída aberta (0.0.0.0/0) e remover uma regra que permita todo tráfego (porta TCP 22) SSH de entrada (0.0.0.0/0) para a instância (ou modificá-la de forma que a conexão não seja mais permitida), suas conexões SSH existentes na instância serão imediatamente descartadas. A conexão não estava sendo rastreada anteriormente, então a alteração interromperá a conexão. Por outro lado, se você tiver uma regra de entrada mais restrita que inicialmente permita uma conexão SSH (o que significa que a conexão foi monitorada), mas altere essa regra para não permitir mais novas conexões do endereço do cliente SSH atual, a conexão existente não será interrompida pela alteração da regra.

Conexões rastreadas automaticamente

As conexões feitas a seguir são monitoradas automaticamente, mesmo que a configuração do grupo de segurança não exija monitoramento:

- Gateways da Internet apenas de saída
- Aceleradoras do Global Accelerator
- Gateways NAT
- Endpoints do Network Firewall
- Network Load Balancers
- AWS PrivateLink (endpoints da VPC de interface)
- AWS Lambda (Interfaces de rede elástica hiperplanas)
- Endpoints de gateway do DynamoDB: cada conexão com o DynamoDB consome duas entradas da funcionalidade conntrack.

Subsídios para monitoramento de conexão

O Amazon EC2 define um número máximo de conexões que podem ser rastreadas por instância. Depois que o máximo é atingido, todos os pacotes enviados ou recebidos são descartados, porque não é possível estabelecer uma nova conexão. Quando isso acontece, as aplicações que enviam e recebem pacotes não podem se comunicar corretamente. Use a métrica de desempenho da rede `conntrack_allowance_available` para determinar o número de conexões rastreadas ainda disponíveis para esse tipo de instância.

Para determinar se os pacotes foram descartados porque o tráfego de rede para sua instância excedeu o número máximo de conexões que podem ser rastreadas, use a métrica `conntrack_allowance_exceeded` de performance de rede. Para obter mais informações, consulte Monitorar o desempenho de rede de instâncias do EC2.

Com o Elastic Load Balancing, se você exceder o número máximo de conexões que podem ser rastreadas por instância, recomendamos que escale o número de instâncias registradas com o balanceador de carga ou o tamanho das instâncias registradas com o balanceador de carga.

Práticas recomendadas para monitoramento de conexões

O roteamento assimétrico, em que o tráfego entra em uma instância por meio de uma interface de rede e sai por meio de uma interface de rede diferente, pode reduzir a performance máxima que uma instância poderá alcançar se os fluxos forem rastreados.

Para manter a performance máxima e otimizar o gerenciamento de conexões quando o monitoramento de conexões estiver habilitado para os grupos de segurança, recomendamos a seguinte configuração:

- Evite topologias de roteamento assimétrico, se possível.
- Em vez de usar grupos de segurança para filtragem, use ACLs de rede.
- Se você precisar usar grupos de segurança com rastreamento de conexão, configure o menor possível de tempo limite do rastreio de conexões inativas. Para obter mais informações sobre o tempo limite do rastreio de conexões inativas, consulte a seção a seguir.
- Para conexões de longa duração, configure os keep alives do TCP para enviar pacotes de verificação em intervalos de menos de 5 minutos para garantir que as conexões permaneçam abertas e mantenham seu estado rastreado. Isso ajuda a evitar que as conexões sejam interrompidas devido ao tempo limite de inatividade e reduz a sobrecarga do restabelecimento da conexão, especialmente nos casos em que os tempos limite de conexão podem ser reduzidos devido à atividade mínima.

Para obter mais informações sobre a performance do ajuste no sistema Nitro, consulte Considerações sobre o Nitro System para ajuste de performance.

Tempo limite de rastreamento de conexão ociosa

O grupo de segurança monitora cada conexão estabelecida para garantir que os pacotes de retorno sejam entregues como esperado. Há um número máximo de conexões que podem ser rastreadas por instância. As conexões que permanecem ociosas podem levar à exaustão do rastreamento da conexão e fazer com que as conexões não sejam rastreadas e os pacotes sejam descartados. É possível definir o tempo limite de rastreamento de conexões em uma interface de rede do Elastic.

> **Note**
>
> Esse recurso só está disponível para instâncias baseadas em Nitro.

Há três tempos limite configuráveis:

- Tempo limite para TCP estabelecido: tempo limite (em segundos) para conexões TCP ociosas em um estado estabelecido.
  - Mín: `60` segundos
  - Máx: `432000` segundos
  - Padrão: `350` segundos para tipos de instância Nitrov6, excluindo P6e-GB200. E `432000` segundos para outros tipos de instâncias, incluindo P6e-GB200.

  - Recomendado: menos de `432000` segundos
- Tempo limite de UDP: tempo limite (em segundos) para fluxos UDP ociosos que só tiverem tráfego em uma única direção ou uma única transação de solicitação-resposta.
  - Mín: `30` segundos
  - Máx: `60` segundos
  - Padrão: `30` segundos
- Tempo limite de fluxo UDP: tempo limite (em segundos) para fluxos UDP ociosos classificados como fluxos que tiveram mais de uma transação de solicitação-resposta.
  - Mín: `60` segundos
  - Máx: `180` segundos
  - Padrão: `180` segundos

Talvez você queira modificar os tempos limite padrão para algum dos seguintes casos:

- Se você estiver monitorando conexões rastreadas usando as métricas de performance de rede do Amazon EC2, as métricas conntrack_allowance_exceeded e conntrack_allowance_available permitem monitorar os pacotes descartados e a utilização da conexão rastreada para gerenciar proativamente a capacidade da instância do EC2 com ações de aumento ou redução de escala para ajudar a atender à demanda de conexões de rede antes de descartar pacotes. Se você estiver observando quedas de conntrack_allowance_exceeded nas instâncias do EC2, pode ser benéfico definir um tempo limite de TCP estabelecido mais baixo para levar em conta sessões TCP/UDP paralisadas devido a clientes ou caixas intermediárias de rede inadequados.
- Normalmente, os balanceadores de carga ou os firewalls têm um tempo limite de ociosidade de TCP estabelecido na faixa de 60 a 90 minutos. Se você estiver executando workloads que devem lidar com um número muito alto de conexões (mais de 100 mil) de dispositivos como firewalls de rede, é recomendável configurar um tempo limite semelhante em uma interface de rede do EC2.
- Se você estiver executando uma workload que utiliza uma topologia de roteamento assimétrico, recomendamos que você configure um tempo limite de inatividade estabelecido por TCP de 60 segundos.
- Se você estiver executando workloads com um grande número de conexões, como DNS, SIP, SNMP, Syslog, Radius e outros serviços que usam principalmente UDP para atender a solicitações, definir o tempo limite do ‘fluxo UDP’ como 60 segundos proporciona maior escala/performance para a capacidade existente e evita falhas cinzentas.

- Em conexões TCP/UDP por Network Load Balancers (NLBs), todas as conexões são rastreadas. O valor do tempo limite de ociosidade para fluxos TCP é de 350 segundos e para fluxos UDP é de 120 segundos e difere dos valores de tempo limite do nível da interface. Talvez você queira configurar limites de tempos no nível da interface de rede para permitir mais flexibilidade de limite de tempo do que os padrões para o balanceador de carga.

Você tem a opção de configurar os tempos limite de rastreamento de conexão ao fazer o seguinte:

- Criar uma interface de rede
- Modificar atributos da interface de rede
- Iniciar uma instância do EC2
- Criar um modelo de inicialização de instância do EC2

Exemplo

No exemplo a seguir, o grupo de segurança tem regras de entrada específicas para tráfego TCP e ICMP, e uma regra de saída que permite todo o tráfego de saída.

Entrada

Tipo de protocolo	Número da porta	Origem
TCP	22 (SSH)	203.0.113.1/32
TCP	80 (HTTP)	0.0.0.0/0
TCP	80 (HTTP)	::/0
ICMP	Todos	0.0.0.0/0

Saída

Tipo de protocolo	Número da porta	Destino
Todos	Tudo	0.0.0.0/0
Tudo	Tudo	::/0

Com uma conexão de rede direta com a instância ou interface de rede, o comportamento de rastreamento é o seguinte:

- O tráfego TCP de entrada e saída na porta 22 (SSH) é monitorado porque a regra de entrada permite o tráfego somente de 203.0.113.1/32, e não de todos os endereços IP (0.0.0.0/0).
- O tráfego TCP de entrada e de saída na porta 80 (HTTP) não é monitorado porque as regras de entrada e saída permitem o tráfego de todos os endereços IP.
- O tráfego ICMP é sempre monitorado.

Se você remover a regra de saída para o tráfego IPv4, todo o tráfego IPv4 de entrada e saída será monitorado, incluindo o tráfego na porta 80 (HTTP). O mesmo se aplica ao tráfego IPv6 se você remover a regra de saída para o tráfego IPv6.

Regras de grupo de segurança para diferentes casos de uso

É possível criar um grupo de segurança e adicionar regras que reflitam a função da instância associada ao grupo de segurança. Por exemplo, uma instância configurada como servidor Web precisa de regras de grupo de segurança que permitam acesso HTTP e HTTPS de entrada. Da mesma forma, uma instância de banco de dados precisa de regras que permitam o acesso para o tipo de banco de dados, como acesso pela porta 3306 para MySQL.

Os seguintes são exemplos de tipos de regras que é possível adicionar aos grupos de segurança para tipos específicos de acesso.

Exemplos

- Regras do servidor da Web
- Regras do servidor de banco de dados
- Regras para se conectar a instâncias pelo computador
- Regras para se conectar a instâncias por uma instâncias com o mesmo grupo de segurança
- Regras de ping/ICMP
- Regras do servidor DNS
- Regras do Amazon EFS
- Regras do Elastic Load Balancing

Para obter instruções, consulte Criar um grupo de segurança e the section called “Configurar regras de grupos de segurança”.

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, será possível adicionar regras para controlar o tráfego de entrada HTTP e HTTPS em endereços IPv6.

Tipo de protocolo	Número do protocolo	Porta	IP de origem	Observações
TCP	6	80 (HTTP)	0.0.0.0/0	Permite acesso HTTP de entrada em qualquer endereço IPv4
TCP	6	443 (HTTPS)	0.0.0.0/0	Permite acesso HTTPS de entrada em qualquer endereço IPv4
TCP	6	80 (HTTP)	::/0	Permite acesso HTTP de entrada em qualquer endereço IPv6
TCP	6	443 (HTTPS)	::/0	Permite acesso HTTPS de entrada em qualquer endereço IPv6

Regras do servidor de banco de dados

As seguintes regras de entrada são exemplos de regras que é possível adicionar para acesso ao banco de dados, dependendo do tipo de banco de dados que você está executando na instância. Para obter mais informações sobre instâncias do Amazon RDS, consulte o Manual do usuário do Amazon RDS.

Para o IP de origem, especifique um dos seguintes:

- Um endereço IP específico ou um intervalo de endereços IP (na notação de bloco CIDR) em sua rede local
- Um ID de grupo de segurança para um grupo de instâncias que acessa o banco de dados

Tipo de protocolo	Número do protocolo	Porta	Observações
TCP	6	1433 (MS SQL)	A porta padrão para acessar um banco de dados Microsoft SQL Server, por exemplo, em uma instância do Amazon RDS
TCP	6	3306 (MYSQL/ Aurora)	A porta padrão para acessar um banco de dados MySQL ou Aurora, por exemplo, em uma instância do Amazon RDS
TCP	6	5439 (Redshift)	A porta padrão para acessar um banco de dados de cluster do Amazon Redshift.
TCP	6	5432 (PostgreSQL)	A porta padrão para acessar um banco de dados PostgreSQL, por exemplo, em uma instância do Amazon RDS
TCP	6	1521 (Oracle)	A porta padrão para acessar um banco de dados Oracle, por exemplo, em uma instância do Amazon RDS

Também é possível restringir o tráfego de saída de seus servidores de banco de dados. Por exemplo, talvez você queira permitir o acesso à Internet para atualizações de software, mas restringir todos os outros tipos de tráfego. Primeiro, remova a regra de saída padrão que permite todo o tráfego de saída.

Tipo de protocolo	Número do protocolo	Porta	IP de destino	Observações
TCP	6	80 (HTTP)	0.0.0.0/0	Permite acesso HTTP de saída a qualquer endereço IPv4

Tipo de protocolo	Número do protocolo	Porta	IP de destino	Observações
TCP	6	443 (HTTPS)	0.0.0.0/0	Permite acesso HTTPS de saída a qualquer endereço IPv4
TCP	6	80 (HTTP)	::/0	(VPC habilitada para IPv6 somente) Permite acesso de saída HTTP a qualquer endereço IPv6
TCP	6	443 (HTTPS)	::/0	(VPC habilitada para IPv6 somente) Permite acesso de saída HTTPS a qualquer endereço IPv6

Regras para se conectar a instâncias pelo computador

Para se conectar à instância, seu grupo de segurança deve ter regras de entrada que permitam acesso SSH (para instâncias do Linux) ou acesso RDP (para instâncias do Windows).

Tipo de protocolo	Número do protocolo	Porta	IP de origem
TCP	6	22 (SSH)	O endereço IPv4 público de seu computador ou um intervalo de endereços IP na rede local. Se a VPC estiver habilitada para IPv6 e sua instância tiver um endereço IPv6, será possível 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

Tipo de protocolo	Número do protocolo	Porta	IP de origem
			sua instância tiver um endereço IPv6, será possível digitar um endereço IPv6 ou um intervalo.

Regras para se conectar a instâncias por uma instâncias com o mesmo grupo de segurança

Para permitir que as instâncias associadas ao mesmo grupo de segurança se comuniquem entre si, adicione regras explícitas para isso.

> **Note**
>
> Se você configurar rotas para encaminhar o tráfego entre duas instâncias em sub-redes diferentes por meio de um dispositivo middlebox, deverá garantir que os grupos de segurança de ambas as instâncias permitam o fluxo de tráfego entre as instâncias. O grupo de segurança para cada instância deve fazer referência ao endereço IP privado da outra instância ou ao intervalo CIDR da sub-rede que contém a outra instância, como a origem. Se você fizer referência ao grupo de segurança da outra instância como a origem, isso não permitirá que o tráfego flua entre as instâncias.

A tabela a seguir descreve a regra de entrada para um grupo de segurança 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 grupo de segurança ou o intervalo CIDR da sub-rede que contém a outra instância (consulte a observação).

Regras de ping/ICMP

O comando ping é um tipo de tráfego ICMP. Para emitir um ping para a instância,você deve adicionar uma das seguintes regras de entrada ICMP.

Tipo	Protocolo	Origem		
ICMP personalizado: IPv4	Solicitação de eco	O endereço IPv4 público do computador, um endereço IPv4 específico ou um endereço IPv4 ou IPv6 de qualquer lugar.		
Todos os ICMP - IPv4	ICMP IPv4 (1)	O endereço IPv4 público do computador, um endereço IPv4 específico ou um endereço IPv4 ou IPv6 de qualquer lugar.		

Para usar o comando ping6 para fazer ping no endereço IPv6 da instância, adicione a seguinte regra ICMPv6 de entrada.

Tipo	Protocolo	Origem		
Todos os ICMP: IPv6	ICMP Pv6 (58)	O endereço IPv6 do computador, um endereço IPv4 específico ou um endereço		

Tipo	Protocolo	Origem		
		IPv4 ou IPv6 de qualquer lugar.		

Regras do servidor DNS

Se tiver configurado a instância do EC2 como um servidor DNS, você deverá garantir que o tráfego TCP e UDP possa atingir seu servidor DNS pela porta 53.

Para o IP de origem, especifique um dos seguintes:

- Um endereço IP ou um intervalo de endereços IP (na notação de bloco CIDR) em uma rede
- O ID de um grupo de segurança de um conjunto de instâncias na rede que requer acesso ao servidor DNS

Tipo de protocolo	Número do protocolo	Porta
TCP	6	53
UDP	17	53

Regras do Amazon EFS

Se estiver usando um sistema de arquivos do Amazon EFS com instâncias do Amazon EC2, o grupo de segurança que você associa a seus destinos de montagem do Amazon EFS deve permitir tráfego por meio do protocolo NFS.

Tipo de protocolo	Número do protocolo	Portas	IP de origem	Observações
TCP	6	2049 (NFS)	O ID do grupo de segurança	Permite acesso NFS de entrada de recursos (incluindo o destino de montagem) associados a esse grupo de segurança

Para montar um sistema de arquivos do Amazon EFS na instância do Amazon EC2, conecte-se à instância. Portanto, o grupo de segurança associado à instância deve ter regras que permitam SSH de entrada do computador local ou da rede local.

Tipo de protocolo	Número do protocolo	Portas	IP de origem	Observações
TCP	6	22 (SSH)	O intervalo de endereços IP do computador local ou o intervalo de endereços IP (na notação de bloco CIDR) da rede.	Permite acesso SSH de entrada no computador local.

Regras do Elastic Load Balancing

Se você registrar as instâncias do EC2 com um balanceador de carga, o grupo de segurança associado ao balanceador de carga deverá permitir comunicação com as instâncias. Para obter mais informações, consulte os tópicos a seguir na documentação do Elastic Load Balancing.

- Grupos de segurança para o Application Load Balancer
- Grupos de segurança para o Network Load Balancer
- Configurar grupos de segurança para o Classic Load Balancer

NitroTPM para instâncias do Amazon EC2

O Nitro Trusted Platform Module (NitroTPM) é um dispositivo virtual fornecido pelo AWS Nitro System que está em conformidade com a especificação TPM 2.0. Armazena, com segurança, artefatos (como senhas, certificados ou chaves de criptografia) que são usados para autenticar a instância. O NitroTPM pode gerar chaves e usá-las em funções criptográficas (como hash, assinatura, criptografia e descriptografia).

O NitroTPM fornece inicialização medida, um processo em que o carregador de inicialização e o sistema operacional criam hashes criptográficos de cada binário de inicialização e os combinam aos valores anteriores nos registros de configuração de plataforma (PCRs) internos do NitroTPM. Com a inicialização medida, é possível obter valores de PCR assinados do NitroTPM e usá-los para provar

às entidades remotas a integridade do software de inicialização da instância. Isto é conhecido como atestado remoto.

Com o NitroTPM, chaves e segredos podem ser marcados com um valor de PCR específico de modo que nunca possam ser acessados se houver alteração no valor da PCR e, portanto, na integridade da instância. Essa forma especial de acesso condicional é chamada de selagem e desselagem. Tecnologias de sistema operacional, como BitLocker, podem usar o NitroTPM para selar uma chave de descriptografia da unidade, de modo que a unidade só possa ser descriptografada quando o sistema operacional for inicializado corretamente e estiver em bom estado.

Para usar o NitroTPM, é necessário selecionar uma imagem de máquina da Amazon (AMI) que foi configurada para ser compatível com o NitroTPM e depois usá-la para executar instâncias baseadas em Nitro. É possível selecionar uma das AMIs pré-criadas da Amazon ou criar a sua própria.

Preços

Não há custo adicional para usar o NitroTPM. Você paga apenas pelos recursos adjacentes que usar.

Conteúdo

- Requisitos para usar o NitroTPM com instâncias do Amazon EC2
- Habilitar uma AMI do Linux para NitroTPM
- Certifique-se de que uma AMI esteja habilitada para o NitroTPM
- Habilitar ou interromper o uso do NitroTPM em uma instância do Amazon EC2
- Verificar se uma instância do Amazon EC2 está habilitada para o NitroTPM
- Recuperar a chave pública de endosso de uma instância do EC2

Requisitos para usar o NitroTPM com instâncias do Amazon EC2

Para iniciar uma instância com o NitroTPM habilitado, você deve atender aos pré-requisitos a seguir.

Tópicos

- AMIs
- Tipos de instância
- Considerações

AMIs

A AMI deve ter o NitroTPM habilitado.

AMIs do Linux

Não há nenhuma AMI pré-configurada. Você deve configurar sua própria AMI. Para obter mais informações, consulte Habilitar uma AMI do Linux para NitroTPM.

AMIs Windows

Para encontrar uma AMI do AWS Windows pré-configurada para NitroTPM e UEFI Secure Boot com chaves da Microsoft, consulte Encontrar AMIs do Windows Server configuradas com NitroTPM e UEFI Secure Boot na Referência de AMIs do AWS Windows.

> **Note**
>
> Sistema operacional: a AMI deve incluir um sistema operacional com um driver TPM 2.0 Command Response Buffer (CRB). A maioria dos sistemas operacionais atuais contém um driver TPM 2.0 CRB.
> Modo de inicialização da UEFI: a AMI deve ser configurada para o modo de inicialização da UEFI. Para obter mais informações, consulte UEFI Secure Boot para instâncias do Amazon EC2.

Tipos de instância

Você deve usar um dos seguintes tipos de instância virtualizada:

- Uso geral: M5, M5a, M5ad, M5d, M5dn, M5n, M5zn, M6a, M6g, M6gd, M6i, M6id, M6idn, M6in, M7a, M7g, M7gd, M7i, M7i-flex, M8a, M8azn, M8g, M8gb, M8gd, M8gn, M8i, M8id, M8i-flex, T3, T3a, T4g
- Otimizadas para computação: C5, C5a, C5ad, C5d, C5n, C6a, C6g, C6gd, C6gn, C6i, C6id, C6in, C7a, C7g, C7gd, C7gn, C7i, C7i-flex, C8a, C8g, C8gb, C8gd, C8gn, C8i, C8id, C8i-flex
- Otimizadas para memória: R5, R5a, R5ad, R5b, R5d, R5dn, R5n, R6a, R6g, R6gd, R6i, R6id, R6idn, R6in, R7a, R7g, R7gd, R7i, R7iz, R8a, R8g, R8gb, R8gd, R8gn, R8i, R8id, R8i-flex, U7i-6tb, U7i-8tb, U7i-12tb, U7in-16tb, U7in-24tb, U7in-32tb, X2idn, X2iedn, X2iezn, X8g, X8aedz, X8i, z1d
- Otimizadas para armazenamento: D3, D3en, I3en, I4i, I7i, I7ie, I8g, I8ge, Im4gn

- Computação acelerada: F2, G4dn, G5, G6, G6e, G6f, Gr6, Gr6f, G7e, Inf1, Inf2, P5, P5e, P5en, P6-B200, P6-B300, Trn2, Trn2u
- Computação de alta performance: Hpc6a, Hpc6id, Hpc8a

Considerações

As seguintes considerações se aplicam ao usar o NitroTPM:

- Depois de iniciar uma instância usando uma AMI com o NitroTPM habilitado, se você quiser alterar o tipo de instância, o novo tipo de instância escolhido também deverá ser compatível com o NitroTPM.
- Os volumes BitLocker criptografados com chaves baseadas no NitroTPM só podem ser usados na instância original.
- O estado do NitroTPM não é exibido no console do Amazon EC2.
- O estado do NitroTPM não está incluído nos snapshots do Amazon EBS.
- O estado do NitroTPM não está incluído nas imagens do VM Import/Export.
- O NitroTPM não é compatível com o AWS Outposts, em zonas locais ou em zonas do Wavelength.

Habilitar uma AMI do Linux para NitroTPM

Para habilitar o NitroTPM para uma instância, você deve iniciar a instância usando uma AMI com o NitroTPM habilitado. Será possível configurar a AMI do Linux com suporte do NitroTPM quando registrá-la. Você não pode configurar o suporte ao NitroTPM posteriormente.

Para obter a lista de AMIs do Windows que são configuradas previamente para oferecer suporte ao NitroTPM, consulte Requisitos para usar o NitroTPM com instâncias do Amazon EC2.

Você deve criar uma AMI com o NitroTPM configurado usando a API RegisterImage. Você não pode usar o console do Amazon EC2 ou o VM Import/Export.

Habilitar uma AMI do Linux para NitroTPM

1. Inicie uma instância temporária com a AMI do Linux necessária. Observe o ID do volume raiz, que você pode encontrar no console na guia Armazenamento da instância.
2. Depois que a instância atingir o estado `running`, crie um snapshot do volume raiz da instância. Para obter mais informações, consulte Criar um snapshot de um volume do EBS.

3. Registre o snapshot que você criou como uma AMI. No mapeamento de dispositivos de blocos, especifique o snapshot que você criou para o volume raiz.

   Um exemplo do comando register-image é mostrado a seguir. Para `--tpm-support`, especifique `v2.0`. Para `--boot-mode`, especifique `uefi`.

```
aws ec2 register-image \
    --name my-image \
    --boot-mode uefi \
    --architecture x86_64 \
    --root-device-name /dev/xvda \
    --block-device-mappings DeviceName=/dev/
xvda,Ebs={SnapshotId=snap-0abcdef1234567890} \
    --tpm-support v2.0
```

   Um exemplo do cmdlet Register-EC2Image é mostrado a seguir.

```
$block = @{SnapshotId=snap-0abcdef1234567890}
Register-EC2Image `
    -Name my-image `
    -Architecture "x86_64" `
    -RootDeviceName /dev/xvda `
    -BlockDeviceMapping @{DeviceName="/dev/xvda";Ebs=$block} `
    -BootMode Uefi `
    -TpmSupport V20
```

4. Encerre a instância temporária que você iniciou na etapa 1.

Certifique-se de que uma AMI esteja habilitada para o NitroTPM

Para habilitar o NitroTPM para uma instância, você deve iniciar a instância usando uma AMI com o NitroTPM habilitado. É possível descrever uma imagem para verificar se ela está habilitada para o NitroTPM. Se você for o proprietário da AMI, poderá descrever o atributo da imagem `tpmSupport`.

O console do Amazon EC2 não exibe `TpmSupport`.

AWS CLI

Para verificar se o NitroTPM está habilitado

Use o comando describe-images.

```
aws ec2 describe-images \
    --image-ids ami-0abcdef1234567890 \
    --query Images[*].TpmSupport
```

Se o NitroTPM estiver habilitado para a AMI, a saída será como a seguir. Se o TPM não estiver habilitado, a saída será vazia.

```
[
    "v2.0"
]
```

Como alternativa, se você for o proprietário da AMI, poderá usar o comando describe-image-attribute com o atributo `tpmSupport`.

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

O seguinte é um exemplo de saída.

```
{
    "ImageId": "ami-0abcdef1234567890",
    "TpmSupport": {
        "Value": "v2.0"
    }
}
```

Para encontrar AMIs com o NitroTPM habilitado

O exemplo a seguir lista os IDs das AMIs pertencentes a você que possuem o NitroTPM habilitado.

```
aws ec2 describe-images \
    --owners self \
    --filters Name=tpm-support,Values=v2.0 \
    --query Images[].ImageId
```

PowerShell

Para verificar se o NitroTPM está habilitado

Use o cmdlet Get-EC2Image.

```
Get-EC2Image `
    -ImageId ami-0abcdef1234567890 | Select TpmSupport
```

Se o NitroTPM estiver habilitado para a AMI, a saída será como a seguir. Se o TPM não estiver habilitado, a saída será vazia.

```
TpmSupport
----------
v2.0
```

Como alternativa, se você for o proprietário da AMI, poderá usar o cmdlet Get-EC2ImageAttribute com o atributo `tpmSupport`.

```
Get-EC2ImageAttribute `
    -ImageId ami-0abcdef1234567890 `
    -Attribute tpmSupport
```

Para encontrar AMIs com o NitroTPM habilitado

O exemplo a seguir lista os IDs das AMIs pertencentes a você que possuem o NitroTPM habilitado.

```
Get-EC2Image `
    -Owner self `
    -Filter @{Name="tpm-support; Values="v2.0"} | Select ImageId
```

Habilitar ou interromper o uso do NitroTPM em uma instância do Amazon EC2

Você só pode habilitar uma instância do Amazon EC2 para o NitroTPM no momento da execução. Depois que uma instância está habilitada para o NitroTPM, não é possível desabilitá-la. Se você não precisar mais usar o NitroTPM, é necessário configurar o sistema operacional para interromper o uso.

Tópicos

- Iniciar uma instância com o NitroTPM habilitado

- Interromper o uso do NitroTPM em uma instância

Iniciar uma instância com o NitroTPM habilitado

Quando você inicia uma instância com os pré-requisitos, o NitroTPM é habilitado automaticamente na instância. Você só pode habilitar o NitroTPM em uma instância no momento da execução. Para obter mais informações sobre como iniciar uma instância, consulte Iniciar uma instância do Amazon EC2.

Interromper o uso do NitroTPM em uma instância

Após executar uma instância com o NitroTPM habilitado, não será possível desabilitar o NitroTPM para a instância. No entanto, é possível configurar o sistema operacional para interromper o uso do NitroTPM desabilitando o driver do dispositivo TPM 2.0 na instância com as seguintes ferramentas:

- Para Instâncias do Linux, use tpm-tools.
- Para Instâncias do Windows, use o console de gerenciamento do TPM (tpm.msc).

Para obter mais informações sobre como desabilitar o driver do dispositivo, consulte a documentação do sistema operacional.

Verificar se uma instância do Amazon EC2 está habilitada para o NitroTPM

É possível verificar se a instância do Amazon EC2 está habilitada para o NitroTPM. Se o suporte ao NitroTPM estiver habilitado na instância, o comando retornará `"v2.0"`. Caso contrário, o campo `TpmSupport` não estará presente na saída.

O console do Amazon EC2 não exibe o campo `TpmSupport`.

AWS CLI

Para verificar se uma instância está habilitada para o NitroTPM

Use o comando describe-instances.

```
aws ec2 describe-instances \
    --instance-ids i-1234567890abcdef0 \
    --query Reservations[].Instances[].TpmSupport
```

PowerShell

Para verificar se uma instância está habilitada para o NitroTPM

Use o cmdlet Get-EC2Instance.

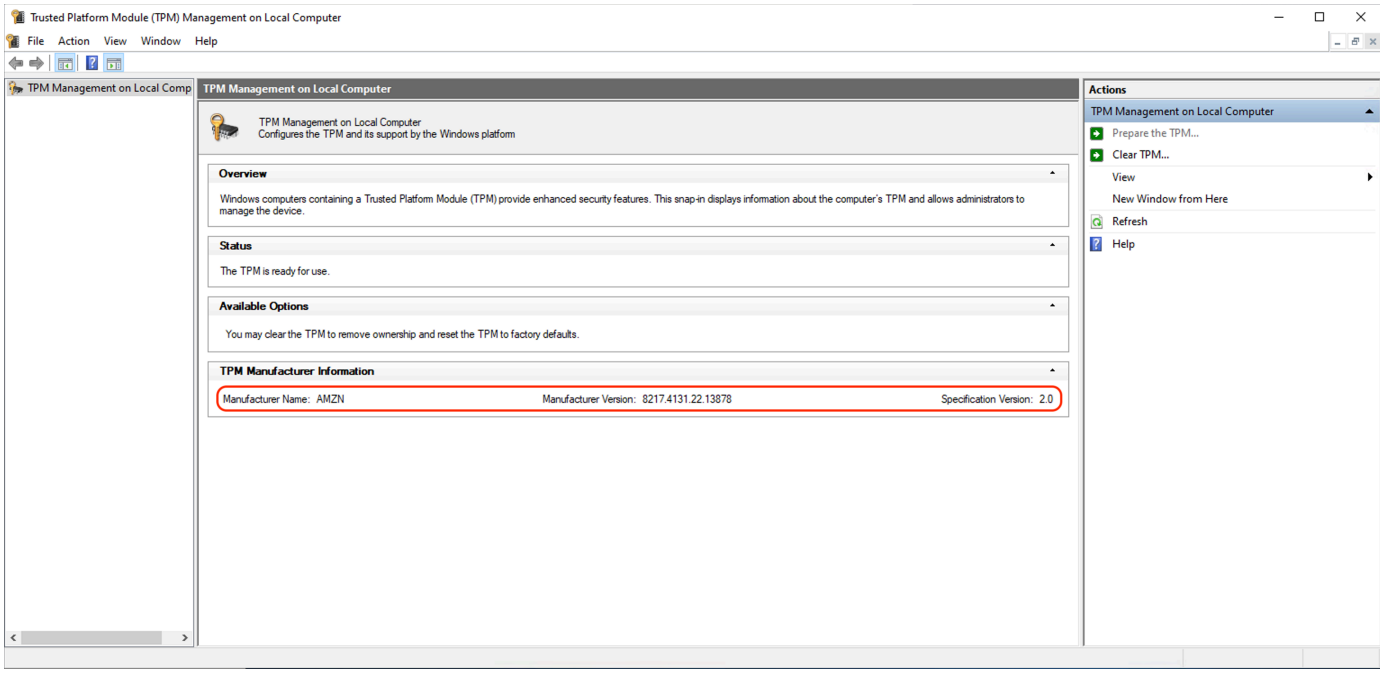
```
(Get-EC2Instance `
    -InstanceId i-1234567890abcdef0).Instances.TpmSupport
```

Verifique o acesso ao NitroTPM na sua instância do Windows

(Somente instâncias do Windows) Para verificar se o NitroTPM está acessível para Windows

1. Conecte-se à instância do Windows do EC2.
2. Na instância, execute o programa tpm.msc.

   Será aberta a janela TPM Management on Local Computer (Gerenciamento do TPM no computador local).
3. Confira o campo TPM Manufacturer Information (Informações do fabricante do TPM). Contém o nome do fabricante e a versão do NitroTPM na instância.



Recuperar a chave pública de endosso de uma instância do EC2

É possível recuperar com segurança a chave pública de endosso de uma instância a qualquer momento.

AWS CLI

Para recuperar a chave pública de endosso de uma instância

Use o comando get-instance-tpm-ek-pub.

Exemplo 1

O exemplo a seguir obtém a chave pública de endosso `rsa-2048` no formato `tpmt` para a instância especificada.

```
aws ec2 get-instance-tpm-ek-pub \
    --instance-id i-1234567890abcdef0 \
    --key-format tpmt \
    --key-type rsa-2048
```

A seguir está um exemplo de saída.

```
{
    "InstanceId": "i-01234567890abcdef",
    "KeyFormat": "tpmt",
    "KeyType": "rsa-2048",
    "KeyValue": "AAEACwADALIAIINxl2dEhLEXAMPLEUal1yT9UtduBlILZPKh2hszFGmqAAYAgABDA
    EXAMPLEAAABAOiRd7WmgtdGNoV1h/AxmW+CXExblG8pEUfNm0LOLiYnEXAMPLERqApiFa/UhvEYqN4
    Z7jKMD/usbhsQaAB1gKA5RmzuhSazHQkax7EXAMPLEzDthlS7HNGuYn5eG7qnJndRcakS+iNxT8Hvf
    0S1ZtNuItMs+Yp4SO6aU28MT/JZkOKsXIdMerY3GdWbNQz9AvYbMEXAMPLEPyHfzgVO0QTTJVGdDxh
    vxtXCOu9GYf0crbjEXAMPLEd4YTbWdDdgOKWF9fjzDytJSDhrLAOUctNzHPCd/92l5zEXAMPLEOIFA
    Ss50C0/802c17W2pMSVHvCCa9lYCiAfxH/vYKovAAE="
}
```

Exemplo 2

O exemplo a seguir obtém a chave pública de endosso `rsa-2048` no formato `der` para a instância especificada.

```
aws ec2 get-instance-tpm-ek-pub \
```

```
    --instance-id i-1234567890abcdef0 \
    --key-format der \
    --key-type rsa-2048
```

A seguir está um exemplo de saída.

```
{
    "InstanceId": "i-1234567890abcdef0",
    "KeyFormat": "der",
    "KeyType": "rsa-2048",
    "KeyValue": "MIIBIjANBgEXAMPLEw0BAQEFAAOCAQ8AMIIBCgKCAQEA6JF3taEXAMPLEXWH8DGZb4
    JcTFuUbykRR82bQs4uJifaKSOv5NGoEXAMPLEG8Rio3hnuMowP+6xuGxBoAHWAoDlGbO6FJrMdEXAMP
    LEnYUHvMO2GVLsc0a5ifl4buqcmd1FxqRL6I3FPwe9/REXAMPLE0yz5inhI7ppTbwxP8lmQ4qxch0x6
    tjcZ1Zs1DP0EXAMPLERUYLQ/Id/OBU7RBNMlUZ0PGG/G1cI670Zh/RytuOdx9iEXAMPLEtZ0N2A4pYX
    1+PMPK0lIOGssA5Ry03Mc8J3/3aXnOD2/ASRQ4gUBKznQLT/zTZEXAMPLEJUe8IJr2VgKIB/Ef+9gqi
    8AAQIDAQAB"
}
```

PowerShell

Para recuperar a chave pública de endosso de uma instância

Use o cmdlet Get-EC2InstanceTpmEkPub.

Exemplo 1

O exemplo a seguir obtém a chave pública de endosso `rsa-2048` no formato `tpmt` para a instância especificada.

```
Get-EC2InstanceTpmEkPub `
    -InstanceId i-1234567890abcdef0 `
    -KeyFormat tpmt `
    -KeyType rsa-2048
```

Exemplo 2

O exemplo a seguir obtém a chave pública de endosso `rsa-2048` no formato `der` para a instância especificada.

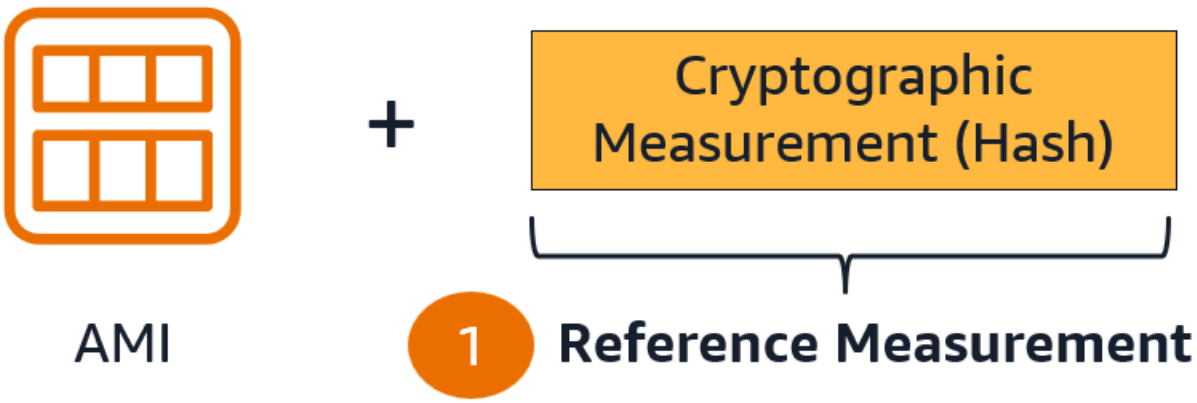
```
Get-EC2InstanceTpmEkPub `
    -InstanceId i-1234567890abcdef0 `
```

```
    -KeyFormat der `
    -KeyType rsa-2048
```

Atestação de instância do Amazon EC2

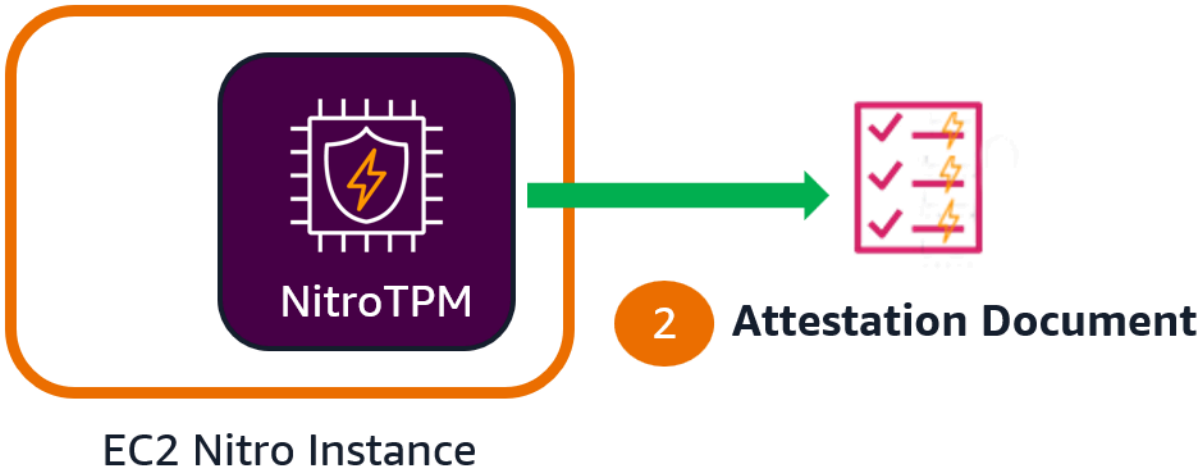
A atestação é um processo que permite que você prove criptograficamente para qualquer parte que somente software, drivers e processos de inicialização confiáveis estão sendo executados em uma instância do Amazon EC2. A atestação de instâncias do Amazon EC2 é habilitada pelo Nitro Trusted Platform Module (NitroTPM) e por AMIs atestáveis.

A primeira etapa da atestação é compilar uma AMI atestável e determinar as medidas de referência dessa AMI. Uma AMI atestável é uma AMI compilada do zero para atestação. As medidas de referência são medidas de todo o software e de todas as configurações que você incluiu na AMI. Para obter mais informações sobre como você pode obter as medidas de referência, consulte Criar o exemplo de descrição da imagem.



A próxima etapa é iniciar uma instância do EC2 habilitada para Nitro-TPM com a AMI atestável. Depois de iniciar a instância, você pode usar as ferramentas do NitroTPM para gerar o atestado. Depois, você pode comparar as medidas reais da instância do EC2 que se encontram no atestado com as medidas de referência para verificar se a instância tem o software e as configurações em que você confia.

Comparando as medidas de referência geradas durante o processo de criação da AMI atestável com as medidas incluídas no atestado de uma instância, é possível validar que somente software e código confiáveis estão sendo executados na instância.



Integração com AWS KMS

Para facilitar o processo de comparação de medidas, é possível usar o AWS Key Management Service (AWS KMS) como um verificador de atestados. Com o AWS KMS, você pode criar políticas de chave do KMS baseadas em atestação que permitem operações específicas com a chave KMS somente se você fornecer um atestado com medidas que correspondam às medidas de referência. Para isso, você adiciona chaves de condições específicas às suas políticas de chaves do KMS que usam as medidas de referência como os valores das chaves de condições e depois especifica quais operações do KMS serão permitidas se a chave de condição for satisfeita.

Ao realizar operações do KMS usando a chave KMS, você deve anexar um atestado à solicitação do KMS. O AWS KMS valida as medidas do atestado em relação às medidas de referência da política de chave do KMS e permite acesso à chave somente se as medidas corresponderem.

Além disso, ao gerar o atestado para uma instância, você deve especificar uma chave pública para um par de chaves que possui. A chave pública especificada é incluída no atestado. Quando o AWS KMS valida o atestado e permite uma operação de descriptografia, ele criptografa automaticamente a resposta com a chave pública incluída no atestado antes de devolvê-la. Isso garante que a resposta possa ser descriptografada e usada somente com a chave privada correspondente à chave pública incluída no atestado.

Isso garante que somente instâncias que executam software e código confiáveis possam realizar operações criptográficas usando uma chave do KMS.

Atestação de ambientes de computação isolados

Em geral, você pode criar e configurar uma instância do EC2 para ser um ambiente computacional isolado, que não fornece acesso interativo nem um mecanismo para que os administradores e usuários acessem os dados que estão sendo processados na instância do EC2. Com a atestação de instâncias do EC2, você pode provar para um terceiro ou outro serviço que a instância está sendo executada como um ambiente computacional isolado. Para obter mais informações, consulte Isolar dados de seus próprios operadores.

Para ter um exemplo, veja o exemplo de descrição de imagem do Amazon Linux 2023 que cria um ambiente computacional isolado. É possível usar esse exemplo de descrição de imagem como ponto de partida e personalizá-lo para atender aos seus requisitos.

Modelo de Responsabilidade Compartilhada da AWS

O NitroTPM e as AMIS atestáveis são os elementos que podem ajudar você a instalar e configurar atestação nas instâncias do EC2. Você é responsável por configurar a AMI para atender ao seu respectivo caso de uso. Para obter mais informações, consulte Modelo de responsabilidade compartilhada da AWS.

Tópicos

- AMIs atestáveis
- Preparar o AWS KMS para atestação
- Obter o atestado do NitroTPM
- Integração com o AWS KMS
- Isolar dados de seus próprios operadores

AMIs atestáveis

Uma AMI atestável é uma imagem de máquina da Amazon (AMI) com um hash criptográfico correspondente que representa todo o seu conteúdo. O hash é gerado durante o processo de criação da AMI e é calculado com base em todo o conteúdo dessa AMI, incluindo as aplicações, o código e o processo de inicialização.

Manter um estado atestável

As medidas de uma instância são baseadas em seu estado inicial de inicialização. Qualquer alteração de software ou código feita na instância após a inicialização que persista após as

reinicializações alterará a medida da instância após as reinicializações. Se as medidas forem alteradas, elas se desviarão das medidas de referência da AMI atestável, e a instância não poderá mais atestar para o AWS KMS com sucesso após a reinicialização. Assim sendo, para que as AMIs atestáveis sejam úteis, as instâncias precisam voltar ao estado original de inicialização após a reinicialização.

Voltar sempre ao estado original de inicialização garante que uma instância possa atestar com sucesso após a reinicialização. Os seguintes utilitários podem ser usados para garantir que as instâncias permaneçam atestáveis após as reinicializações:

- `erofs`: Enhanced Read-Only File System. Esse utilitário garante que o sistema de arquivos raiz seja somente leitura. Com esse utilitário, as gravações no sistema de arquivos, incluindo `/etc`, `/run` e `/var`, são armazenadas na memória e perdidas quando a instância é reiniciada, deixando o sistema de arquivos raiz em seu estado original de inicialização. Para obter mais informações, consulte a documentação do erofs.
- `dm-verity`: fornece proteção de integridade para o sistema de arquivos raiz somente leitura. O utilitário calcula um hash dos blocos do sistema de arquivos e o armazena na linha de comando do kernel. Isso permite que o kernel verifique a integridade do sistema de arquivos durante a inicialização. Para obter mais informações, consulte a documentação do dm-verity.

Requisitos para a criação de AMIs atestáveis

AMIs atestáveis têm os seguintes requisitos:

- Sistema operacional básico: Amazon Linux 2023 e NixOS
- Arquitetura: arquitetura `x86_64` ou `arm64`
- Compatibilidade com TPM: o NitroTPM deve estar habilitado. Para obter mais informações, consulte Requisitos para usar o NitroTPM com instâncias do Amazon EC2.
- Modo de inicialização: o modo de inicialização UEFI deve estar habilitado.

Tópicos

- Criar AMIs atestáveis
- Criar o exemplo de descrição de imagem do Amazon Linux 2023
- Exemplo de descrição de imagem do Amazon Linux 2023
- Personalize o exemplo de descrição de imagem do Amazon Linux 2023 para a workload

- Calcular medidas de PCR para uma AMI personalizada

Criar AMIs atestáveis

Para criar uma AMI atestável, você precisará usar o Amazon Linux 2023 com o KIWI Next Generation (KIWI NG). O Amazon Linux 2023 fornece o software e os utilitários necessários para compilar uma AMI atestável usando o KIWI NG.

O KIWI NG é uma ferramenta de código aberto para a criação de imagens baseadas no Linux pré-configuradas. O KIWI NG usa descrições de imagem XML que definem o conteúdo de uma imagem. A descrição da imagem especifica o sistema operacional básico, o software, a configuração do kernel e os scripts a serem executados para compilar uma AMI pronta para uso para um caso de uso específico.

Durante a compilação da AMI, você precisa usar o utilitário `nitro-tpm-pcr-compute` para gerar as medidas de referência com base na Unified Kernel Image (UKI) gerada pelo KIWI NG. Para obter mais informações sobre o uso do utilitário `nitro-tpm-pcr-compute`, consulte Calcular medidas de PCR para uma AMI personalizada.

A AWS fornece um exemplo de descrição de imagem do Amazon Linux 2023 que inclui todas as configurações necessárias para configurar uma instância do EC2 em um ambiente computacional isolado. Para obter mais informações, consulte Criar o exemplo de descrição de imagem do Amazon Linux 2023.

Criar o exemplo de descrição de imagem do Amazon Linux 2023

A AWS fornece um exemplo de descrição de imagem do Amazon Linux 2023 que você pode usar como ponto de partida para criar suas próprias AMIs atestáveis personalizadas para suas workloads. O exemplo de descrição de imagem inclui o Amazon Linux 2023 como sistema operacional básico, as configurações `dm-verity` e `erofs`, para garantir a imutabilidade do sistema de arquivos, e remove todo acesso interativo (como SSH, conexão de instância do EC2 e console serial) para criar um ambiente computacional isolado. Para obter mais informações sobre o exemplo de descrição de imagem, consulte o repositório do Github.

O exemplo de descrição de imagem instala automaticamente as ferramentas do NitroTPM (`nitro-tpm-pcr-compute` e `nitro-tpm-attest`) na imagem gerada no diretório `/usr/bin/`. Isso garante que as ferramentas sejam pré-instaladas nas instâncias iniciadas na AMI.

O exemplo de descrição de imagem inclui um script, `edit_boot_install.sh`, que inclui os comandos necessários para gerar as medidas de referência. O script monta o arquivo da imagem de disco bruta (`.raw`) criada pelo KIWI NG em um dispositivo de loopback, localiza a UKI, que tem a extensão de arquivo `.efi`, e executa o utilitário `nitro-tpm-pcr-compute` para gerar as medidas de referência para a AMI. O script é executado automaticamente pelo KIWI NG durante a compilação.

Este tutorial mostra como compilar o exemplo de descrição de imagem para criar uma AMI atestável.

Para obter mais informações sobre como criar suas próprias descrições de imagem, consulte a seguinte documentação do KIWI NG:

- Início rápido
- Descrição de imagem
- Exemplo de descrição de imagem do Amazon Linux 2023

Para compilar o exemplo de descrição de imagem do Amazon Linux 2023 usando o KIWI NG

1. Inicie uma instância do Amazon EC2 usando a AMI AL2023 mais recente. Para garantir que a instância tenha espaço de armazenamento suficiente para compilar a AMI, provisione pelo menos 12 GB de armazenamento.
2. Instale as dependências necessárias. O seguinte comando instala estes utilitários:

   - `kiwi-cli`
   - `veritysetup`
   - `erofs-utils`
   - `aws-nitro-tpm-tools`

   ```
   sudo dnf install -y kiwi-cli python3-kiwi kiwi-systemdeps-core python3-poetry-core
    qemu-img veritysetup erofs-utils git cargo aws-nitro-tpm-tools
   ```

3. Instale o utilitário `coldsnap`. Esse utilitário permite que você crie snapshots do Amazon EBS a partir de dados de imagem brutos. Você usará esse utilitário para criar um snapshot do EBS a partir do arquivo da imagem de disco bruta criada pelo KIWI NG.

   ```
   git clone https://github.com/awslabs/coldsnap.git
   cd coldsnap
   ```

```
cargo install --locked coldsnap
cd ..
```

4. Obtenha os arquivos de exemplos de descrição de imagem.

```
sudo dnf install kiwi-image-descriptions-examples
```

Os arquivos de exemplos de descrição de imagem são baixados para o seguinte diretório: `/usr/share/kiwi-image-descriptions-examples/al2023/attestable-image-example`

5. Compile o exemplo de descrição de imagem usando o comando `system build` do KIWI NG. O comando a seguir cria um arquivo da imagem de disco bruta no diretório `./image`.

```
sudo kiwi-ng \
--color-output \
--loglevel 0 \
system build \
--description /usr/share/kiwi-image-descriptions-examples/al2023/attestable-image-example \
--target-dir ./image
```

Para obter mais informações, consulte a documentação do kiwi-ng system build.

6. Obtenha as medidas de referência da AMI. As medidas são geradas pelo utilitário `nitro-tpm-pcr-compute` durante a criação da imagem na etapa anterior. É possível localizar as medidas de referência no seguinte arquivo: `./image/pcr_measurements.json`.

As medidas são fornecidas no seguinte formato JSON:

```
{
  "Measurements": {
    "HashAlgorithm": "SHA384 { ... }",
    "PCR4": "PCR4_measurement",
    "PCR7": "PCR7_measurement",
    "PCR12": "PCR12_measurement"
  }
}
```

7. Use o utilitário `coldsnap` para carregar a imagem de disco bruta criada pelo KIWI NG em um snapshot do EBS. O comando retorna o ID do snapshot. Anote o valor do ID, pois vai precisar dele na próxima etapa.

```
SNAPSHOT=$(.cargo/bin/coldsnap upload ./image/kiwi*.raw)
echo "Created snapshot: $SNAPSHOT"
```

Para obter mais informações sobre o utilitário `coldsnap`, consulte o repositório do coldsnap no GitHub.

8. Registre uma AMI habilitada para o TPM 2.0 com o modo de inicialização UEFI usando o snapshot da etapa anterior. Para `--architecture`, especifique `x86_64` para Intel ou `arm64` para Graviton.

```
aws ec2 register-image \
--name "attestable_isolated_al2023_ami" \
--virtualization-type hvm \
--boot-mode uefi \
--architecture x86_64|arm64 \
--root-device-name /dev/xvda \
--block-device-mappings DeviceName=/dev/xvda,Ebs={SnapshotId=${SNAPSHOT}} \
--tpm-support v2.0 \
--ena-support
```

Exemplo de descrição de imagem do Amazon Linux 2023

O exemplo de descrição de imagem do Amazon Linux 2023 tem as seguintes características:

1. Inicialização da Unified Kernel Image (UKI): inicialize usando um único binário assinado que combine o kernel `initrd` e os parâmetros de inicialização em uma única imagem imutável.
2. Sistema de arquivos-raiz somente leitura: use o Enhanced Read-Only File System (`erofs`) com proteção dm-verity para garantir que o sistema de arquivos-raiz não possa ser modificado e mantenha a verificação da integridade criptográfica.
3. Sistema de arquivos de sobreposição efêmera: crie um sistema de arquivos de sobreposição temporário que permita gravações temporárias em diretórios como `/etc`, `/run` e `/var`. Como esse sistema de arquivos de sobreposição existe somente na memória, todas as alterações são perdidas automaticamente quando a instância é reinicializada, garantindo que o sistema retorne ao estado confiável original.
4. Métodos de acesso remoto desabilitados: remova os seguintes mecanismos de acesso remoto para evitar acesso remoto:

Método de acesso	Descrição	Implementação da descrição da imagem
SSH	Exclui o servidor OpenSSH. Torna a instância inerentemente incapaz de lidar com tráfego SSH.	Ignorar o pacote `openssh-server *`
Dados do usuário	Remove o Cloud-init. Elimina a capacidade dos operadores de fornecer dados de usuários às instâncias e executar scripts de inicialização.	Ignorar os pacotes `cloud-init e cloud-init-cfg-ec2 *`
Chrony	Desabilita a porta de comando chrony. Evita que os operadores executem comandos chrony em instâncias em execução.	Ignorar o pacote `amazon-chrony-config *`
MOTD	Remove o pacote MOTD. Elimina a capacidade dos operadores de alterar mensagens ou funcionalidades nas instâncias em execução.	Ignorar o pacote `update-motd *`
AWS SSM	Remove o agente do AWS SSM. Evita o acesso remoto às instâncias em execução usando o AWS SSM.	Ignorar o pacote `amazon-ssm-agent *`
EC2 Instance Connect	Remove o pacote do EC2 Instance Connect. Desabilita o acesso SSH usando essa ferramenta.	Ignorar o pacote `ec2-instance-connect *`
Console de série	Desabilita o console de série. Garante que o acesso ao console não esteja disponível para instâncias em execução e elimina a capacidade dos operadores de fazer login no console de série.	Desabilitado pelo parâmetro da linha de comando do kernel

* Para obter mais informações, consulte Elementos da descrição de imagem.

Personalize o exemplo de descrição de imagem do Amazon Linux 2023 para a workload

É possível personalizar o exemplo de descrição de imagem do Amazon Linux 2023 e incluir os pacotes de software, os scripts e os arquivos necessários para a workload específica. As personalizações são realizadas adicionando ou modificando vários elementos da descrição de imagem do KIWI NG.

Tópicos

- Gerenciamento de repositórios
- Gerenciamento de pacotes
- Adicionar arquivos e diretórios
- Adicionar scripts personalizados

Gerenciamento de repositórios

Por padrão, o exemplo de descrição de imagem inclui um único elemento `<repository>` que aponta para um endpoint-espelho para os principais repositórios do Amazon Linux 2023. Se necessário, você pode adicionar referências a outros repositórios a partir dos quais o software necessário será instalado.

O exemplo de descrição de imagem usa o gerenciador de pacotes `dnf`, conforme definido no elemento `<packagemanager>`.

Para obter mais informações sobre a adição de repositórios, consulte Setting up Repositories.

Gerenciamento de pacotes

Por padrão, o exemplo de descrição de imagem inclui todos os pacotes necessários para criar uma AMI atestável do Amazon Linux 2023 para um ambiente computacional isolado com um sistema de arquivos somente leitura `erofs`.

É possível incluir pacotes de software adicionais na descrição da imagem adicionando-os ao elemento `<packages>` da descrição da imagem. O elemento `<packages>` define todo o software que deve estar instalado na AMI.

Você também pode usar o elemento <packages> para desinstalar ou excluir pacotes de software específicos.

Para obter mais informações sobre como adicionar ou remover pacotes da descrição de imagem, consulte Adding and Removing Packages.

Adicionar arquivos e diretórios

O exemplo de descrição de imagem inclui um diretório de árvore de sobreposição (/root/). O diretório da árvore de sobreposição é um diretório que contém arquivos e diretórios que serão copiados na imagem durante o processo de criação da imagem. Todos os arquivos e diretórios que você colocar no diretório da árvore de sobreposição serão copiados diretamente no sistema de arquivos raiz da imagem durante o processo de criação da imagem.

O diretório da árvore de sobreposição é copiado na imagem após todos os pacotes serem instalados. Os arquivos novos são adicionados e os arquivos existentes são sobrescritos.

Adicionar scripts personalizados

O exemplo de descrição de imagem inclui um único script personalizado, edit_boot_install.sh. Esse script inclui os comandos necessários para executar o utilitário nitro-tpm-pcr-compute, que gera as medidas de referência com base no conteúdo da imagem. Esse script é chamado imediatamente após a instalação do bootloader.

Se necessário, você pode incluir seus próprios scripts personalizados na descrição da imagem para realizar tarefas ou configurações durante o processo de criação da imagem ou na sua primeira inicialização. O uso de scripts permite que você personalize as imagens de maneiras que não são possíveis usando apenas a descrição da imagem.

Para incluir scripts personalizados na descrição da imagem, você precisa nomeá-los corretamente segundo o tipo de script e adicioná-los ao mesmo diretório em que está o arquivo appliance.kiwi. O KIWI NG detectará e executará os scripts automaticamente se eles forem nomeados corretamente e colocados no local correto, sem ser necessário referenciá-los explicitamente no arquivo da descrição da imagem.

Para obter mais informações sobre os scripts compatíveis com o KIWI NG, consulte User-Defined Scripts.

Calcular medidas de PCR para uma AMI personalizada

O utilitário `nitro-tpm-pcr-compute` permite gerar as medidas de referência para uma AMI atestável durante a compilação com base na Unified Kernel Image (UKI).

O exemplo de descrição de imagem do Amazon Linux 2023 instala automaticamente o utilitário na imagem compilada no diretório `/usr/bin/`. O exemplo de descrição de imagem também inclui um script com os comandos necessários para executar o utilitário e gerar as medidas de referência durante a criação da imagem. Se você estiver usando o exemplo de descrição de imagem, não precisará instalar ou executar o utilitário manualmente. Para obter mais informações, consulte Criar o exemplo de descrição de imagem do Amazon Linux 2023.

Instalar o utilitário **`nitro-tpm-pcr-compute`**

Se você estiver usando o Amazon Linux 2023, poderá instalar o utilitário `nitro-tpm-pcr-compute` a partir do repositório Amazon Linux como se segue.

```
sudo yum install aws-nitro-tpm-tools
```

As ferramentas são instaladas no diretório `/usr/bin`.

Usar o utilitário **`nitro-tpm-pcr-compute`**

O utilitário fornece um único comando, `nitro-tpm-pcr-compute`, para gerar as medidas de referência.

Ao executar o comando, você deve especificar o seguinte:

- Unified Kernel Image (`UKI.efi`): necessária para inicialização padrão e UEFI.

Para gerar as medidas de referência para uma AMI atestável:

Use o seguinte comando e os seguintes parâmetros:

```
/usr/bin/nitro-tpm-pcr-compute \
--image UKI.efi
```

O utilitário retorna as medidas de referência no seguinte formato JSON:

```
{
  "Measurements": {
```

```
    "HashAlgorithm": "SHA384 { ... }",
    "PCR4": "PCR4_measurement",
    "PCR7": "PCR7_measurement",
    "PCR12": "PCR12_measurement"
  }
}
```

Para obter um exemplo prático de como usar o utilitário `nitro-tpm-pcr-compute`, consulte o script `edit_boot_install.sh` incluído no exemplo de descrição de imagem do Amazon Linux 2023.

Preparar o AWS KMS para atestação

> **Note**
>
> Se você estiver atestando para um serviço de terceiros, deverá criar seus próprios mecanismos personalizados para receber, analisar e validar atestados. Para obter mais informações, consulte Validar um atestado do NitroTPM.

Depois de criar a AMI atestável, você deve ter as medidas de referência que pode usar para validar as solicitações de uma instância do Amazon EC2. A AWS KMS tem compatibilidade integrada com atestação com o NitroTPM.

Para a chave AWS KMS que você usou para criptografar seus dados secretos, adicione uma política de chave que permita acesso à chave somente se as solicitações de API incluírem um atestado com medidas que correspondam às medidas de referência geradas durante o processo de criação da AMI atestável. Use medidas PCR4 e PCR12 para inicialização padrão ou medidas PCR7 para inicialização segura. Isso garante que somente as solicitações de instâncias iniciadas usando a AMI atestável possam realizar operações criptográficas usando a chave AWS KMS.

O AWS KMS fornece as chaves de condição `kms:RecipientAttestation:NitroTPMPCR4`, `kms:RecipientAttestation:NitroTPMPCR7` e `kms:RecipientAttestation:NitroTPMPCR12`, que permitem criar condições baseadas em atestação para políticas de chave KMS do NitroTPM. Para obter mais informações, consulte Condition keys for NitroTPM.

Por exemplo, a política de chave AWS KMS a seguir permitirá acesso à chave somente se a solicitação for originária de uma instância com o perfil de instância `MyEC2InstanceRole` anexado e se a solicitação incluir um atestado com valores específicos de PCR 4 e PCR 12.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Allow requests from instances with attested AMI only",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/MyEC2InstanceRole"
      },
      "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey",
        "kms:GenerateRandom"
      ],
      "Resource": "*",
      "Condition": {
        "StringEqualsIgnoreCase": {

 "kms:RecipientAttestation:NitroTPMPCR4":"EXAMPLE6b9b3d89a53b13f5dfd14a1049ec0b80a9ae4b159adde4

 "kms:RecipientAttestation:NitroTPMPCR12":"000000000000000000000000000000000000000000000000000
        }
      }
    }
  ]
}
```

Obter o atestado do NitroTPM

O atestado é um componente essencial do processo de atestação do NitroTPM. Ele contém uma série de medidas criptográficas que podem ser usadas para verificar a identidade da instância e provar que ela está executando somente software confiável. É possível usar o atestado com o AWS KMS, que tem compatibilidade integrada com a atestação do NitroTPM, ou criar seus próprios mecanismos criptográficos de atestação.

O utilitário `nitro-tpm-attest` permite que você recupere um atestado assinado do NitroTPM para uma instância do Amazon EC2 durante o runtime

O exemplo de descrição de imagem do Amazon Linux 2023 instala automaticamente o utilitário na imagem compilada no diretório `/usr/bin/`. Isso garante que o utilitário seja pré-instalado nas

instâncias iniciadas usando a AMI. Não é necessário instalar o utilitário manualmente. Para obter mais informações, consulte Criar o exemplo de descrição de imagem do Amazon Linux 2023.

Tópicos

- Instalar o utilitário nitro-tpm-attest
- Usar o utilitário nitro-tpm-attest
- Conteúdo do atestado do NitroTPM
- Validar um atestado do NitroTPM

Instalar o utilitário `nitro-tpm-attest`

Se você estiver usando o Amazon Linux 2023, poderá instalar o utilitário `nitro-tpm-attest` a partir do repositório Amazon Linux como se segue.

```
sudo yum install aws-nitro-tpm-tools
```

Usar o utilitário `nitro-tpm-attest`

O utilitário fornece um único comando, `nitro-tpm-attest`, para recuperar o atestado. O comando retorna o atestado codificado em Concise Binary Object Representation (CBOR) e assinado usando CBOR Object Signing and Encryption (COSE).

Ao executar o comando, você pode especificar os seguintes parâmetros opcionais:

- `public-key`: uma chave pública que pode ser usada pelo AWS KMS ou por um serviço externo para criptografar dados de resposta antes de serem retornados. Isso garante que somente o destinatário pretendido, que possui a chave privada, possa descriptografar os dados. Por exemplo, se você estiver atestando com o AWS KMS, o serviço criptografa os dados de texto simples com a chave pública no atestado e retorna o texto cifrado resultante no campo `CiphertextForRecipient` da resposta. Compatível somente com chaves RSA.
- `user-data`: os dados do usuário podem ser usados para entregar dados assinados adicionais a um serviço externo. Esses dados do usuário podem ser usados para concluir um protocolo acordado entre a instância solicitante e o serviço externo. Não usado para atestação com o AWS KMS.
- `nonce`: o nonce pode ser usado para configurar a autenticação de desafio-resposta entre a instância e o serviço externo para ajudar a evitar ataques de falsificação de identidade. Usar um

nonce permite que o serviço externo verifique se está interagindo com uma instância ao vivo e não com um impostor que está reutilizando um atestado antigo. Não usado para atestação com o AWS KMS.

Para recuperar o atestado

Use o seguinte comando e os seguintes parâmetros opcionais:

```
/usr/bin/nitro-tpm-attest \
--public-key rsa_public_key \
--user-data user_data \
--nonce nonce
```

Para ver um exemplo completo que mostra como gerar um par de chaves RSA e como solicitar um atestado com a chave pública, consulte o repositório nitro-tpm-attest do GitHub.

Conteúdo do atestado do NitroTPM

Um atestado é gerado pelo NitroTPM e assinado pelo Hipervisor Nitro. Ele inclui uma série de valores de registros de configuração de plataforma (PCR) relativos a uma instância do Amazon EC2. Os seguintes PCRs são incluídos no atestado:

> **Important**
>
> PCR0 e PCR1 geralmente são usados para medir o código de inicialização inicial, que é controlado pela AWS Para permitir atualizações seguras do código de inicialização inicial, esses PCRs sempre conterão valores constantes.

- `PCR0`: código executável do firmware do sistema principal
- `PCR1`: dados do firmware do sistema principal
- `PCR2`: código executável estendido ou conectável
- `PCR3`: dados de firmware estendidos ou conectáveis
- `PCR4`: código do gerenciador de inicialização
- `PCR5`: configuração de código e dados do gerenciador de inicialização e tabela de partição do GPT
- `PCR6`: especificações do fabricante da plataforma host
- `PCR7`: política de Secure Boot

- PCR8 – 15: definido para uso pelo sistema operacional estático
- PCR16: depuração
- PCR23: compatibilidade com aplicação

PCR4, PCR7 e PCR12 são usados especificamente para validar se uma instância foi iniciada usando uma AMI atestável. O PCR4 e o PCR12 pode ser usado para validar com uma inicialização padrão e o PCR7 pode ser usado para validar com Secure Boot.

- PCR4 (código do gerenciador de inicialização): quando uma instância é iniciada, o NitroTPM cria hashes criptográficos de todos os binários executados pelo ambiente UEFI. Com as AMIs atestáveis, esses binários de inicialização incorporam hashes que evitam o carregamento futuro de binários que não tenham os hashes correspondentes. Dessa forma, o hash binário de inicialização única pode descrever exatamente qual código uma instância executará.
- PCR7 (política de inicialização segura): os binários de inicialização UEFI podem ser assinados com uma chave de assinatura de inicialização segura UEFI. Quando a Secure Boot UEFI está habilitada, a UEFI impede a execução de binários de inicialização UEFI que não atendam à política configurada. O PCR7 contém um hash da política de Secure Boot UEFI da instância.

  Se precisar manter uma política única do KMS que persista nas atualizações da instância, será possível criar uma política que seja validada em relação ao PCR7 para validar um certificado de Secure Boot UEFI. Durante a criação de uma AMI atestável, você pode assinar o binário de inicialização com seu certificado e instalá-lo como o único certificado permitido nos dados UEFI da AMI. Lembre-se de que esse modelo exige que você ainda gere um novo certificado, instale-o em sua política e atualize as AMIs se quiser evitar que instâncias iniciadas de AMIs antigas (não confiáveis) passem pela política do KMS.
- PCR12 — Contém o hash da linha de comando passado para o binário de inicialização UEFI. Necessário em conjunto com o PCR4 para inicialização padrão, para validar que a linha de comando não sofreu alterações.

Validar um atestado do NitroTPM

> **Note**
>
> Este tópico se destina aos usuários que estão usando um serviço de gerenciamento de chaves terceirizado e precisam criar seus próprios mecanismos de validação de atestado.

Este tópico fornece uma visão geral detalhada de todo o fluxo de atestação do NitroTPM. Também discute o que é gerado pelo sistema AWS Nitro quando um atestado é solicitado e explica como um serviço de gerenciamento de chaves deve processar um atestado.

Tópicos

- O atestado
- Validação do atestado

O objetivo do atestado é provar que uma instância é uma entidade confiável, com base no código e na configuração que está sendo executada. A raiz de confiança da instância reside no sistema AWS Nitro, que fornece os atestados.

Os atestados são assinados pela Public Key Infrastructure (PKI) da atestação do AWS Nitro, que inclui uma autoridade de certificação publicada que pode ser incorporada a qualquer serviço.

O atestado

Os atestados são codificados em Concise Binary Object Representation (CBOR) e assinados usando CBOR Object Signing and Encryption (COSE).

Para obter mais informações sobre CBOR, consulte RFC 8949: Concise Binary Object Representation (CBOR).

Especificação do atestado

O exemplo a seguir mostra a estrutura de um atestado.

```
AttestationDocument = {
    module_id: text,                    ; issuing Nitro hypervisor module ID
    timestamp: uint .size 8,            ; UTC time when document was created, in
                                        ; milliseconds since UNIX epoch
    digest: digest,                     ; the digest function used for calculating the
                                        ; register values
    nitrotpm_pcrs: { + index => pcr },  ; map of PCRs at the moment the Attestation
 Document was generated
    certificate: cert,                  ; the public key certificate for the public
 key
                                        ; that was used to sign the Attestation
 Document
    cabundle: [* cert],                 ; issuing CA bundle for infrastructure
 certificate
```

```
    ? public_key: user_data,             ; an optional DER-encoded key the attestation
                                         ; consumer can use to encrypt data with
    ? user_data: user_data,              ; additional signed user data, defined by
 protocol
    ? nonce: user_data,                  ; an optional cryptographic nonce provided by
 the
                                         ; attestation consumer as a proof of
 authenticity
}

cert = bytes .size (1..1024)       ; DER encoded certificate
user_data = bytes .size (0..1024)
pcr = bytes .size (32/48/64)       ; PCR content
index = 0..31
digest = "SHA384"
```

Os parâmetros opcionais do atestado (`public_key`, `user_data` e `nonce`) podem ser usados para estabelecer um protocolo de validação personalizado entre uma instância de atestado e o serviço externo.

Validação do atestado

Ao solicitar um atestado do Hipervisor Nitro, você recebe um blob binário que contém o atestado assinado. O atestado assinado é um objeto codificado em CBOR e assinado com COSE (usando o objeto de estrutura de assinatura COSE_Sign1). O processo de validação inclui as seguintes etapas:

1. Decodifique o objeto CBOR e mapeie-o para uma estrutura COSE_Sign1.
2. Extraia o atestado da estrutura COSE_Sign1.
3. Verifique a cadeia do certificado.
4. Certifique-se de que o atestado esteja devidamente assinado.

Os atestados são assinados pela PKI da atestação do AWS Nitro, que inclui um certificado raiz para as partições comerciais AWS. O certificado-raiz pode ser baixado de https://aws-nitro-enclaves.amazonaws.com/AWS_NitroEnclaves_Root-G1.zip e pode ser verificado usando a impressão digital a seguir.

```
64:1A:03:21:A3:E2:44:EF:E4:56:46:31:95:D6:06:31:7E:D7:CD:CC:3C:17:56:E0:98:93:F3:C6:8F:79:BB:5B
```

O certificado raiz é baseado em uma chave privada da autoridade privada de certificação (AWS Private CA) do AWS Certificate Manager e tem vida útil de 30 anos. O assunto da PCA tem o seguinte formato:

```
CN=aws.nitro-enclaves, C=US, O=Amazon, OU=AWS
```

Tópicos

- COSE e CBOR
- Validação semântica
- Validade de certificado
- Validade da cadeia de certificados

COSE e CBOR

Normalmente, a estrutura de assinatura COSE_Sign1 é usada quando apenas uma assinatura vai ser colocada em uma mensagem. Os parâmetros que lidam com o conteúdo e a assinatura são colocados no cabeçalho protegido em vez de ter a separação da COSE_Sign. A estrutura pode ser codificada como marcada ou não marcada, dependendo do contexto em que será usada. Uma estrutura marcada COSE_Sign1 é identificada pela tag CBOR 18.

O objeto CBOR que traz o corpo, a assinatura e as informações sobre o corpo e a assinatura é chamado de estrutura COSE_Sign1. A estrutura COSE_Sign1 é uma matriz CBOR. A matriz inclui os campos a seguir.

```
[
  protected:   Header,
  unprotected: Header,
  payload:     This field contains the serialized content to be signed,
  signature:   This field contains the computed signature value.
]
```

No contexto de um atestado, a matriz inclui o que se segue.

```
18(/* COSE_Sign1 CBOR tag is 18 */
    {1: -35}, /* This is equivalent with {algorithm: ECDS 384} */
    {}, /* We have nothing in unprotected */
    $ATTESTATION_DOCUMENT_CONTENT /* Attestation Document */,
```

```
    signature /* This is the signature */
)
```

Para obter mais informações sobre CBOR, consulte RFC 8949: Concise Binary Object Representation (CBOR).

Validação semântica

Um atestado sempre tem o pacote da CA na ordem a seguir.

```
[ ROOT_CERT - INTERM_1 - INTERM_2 .... - INTERM_N]
      0          1          2             N - 1
```

Lembre-se dessa ordem, pois algumas ferramentas existentes, como o CertPath do Java do Java PKI API Programmer's Guide, podem exigir uma ordem diferente.

Para validar os certificados, comece com o pacote da CA do atestado e gere a cadeia necessária, na qual `TARGET_CERT` é o certificado no atestado.

```
[TARGET_CERT, INTERM_N, ..... , INTERM_2, INTERM_1, ROOT_CERT]
```

Validade de certificado

Para todos os certificados da cadeia, você deve garantir que a data atual esteja dentro do período de validade especificado no certificado.

Validade da cadeia de certificados

Em geral, uma cadeia de vários certificados pode ser necessária, incluindo um certificado do proprietário da chave pública assinado por uma CA e zero ou mais certificados adicionais de CAs assinados por outras CAs. Essas cadeias, chamadas de caminhos de certificação, são necessárias porque um usuário de chave pública é inicializado apenas com um número limitado de chaves públicas garantidas da CA. Os procedimentos de validação do caminho de certificação para a PKI da Internet são baseados no algoritmo fornecido no X.509. O processamento do caminho de certificação verifica a associação entre o nome distinto do sujeito e/ou o nome alternativo do sujeito e a chave pública do sujeito. A vinculação é limitada pelas restrições especificadas nos certificados que compõem o caminho e as entradas que são especificadas pela parte que vai confiar. As restrições básicas e as extensões das restrições das políticas permitem que a lógica de processamento do caminho de certificação automatize o processo de tomada de decisão.

> **Note**
>
> A CRL deve estar desabilitada ao fazer a validação.

Usando Java, partindo do caminho raiz e da cadeia de certificados gerada, a validação da cadeia se dá como se segue.

```
validateCertsPath(certChain, rootCertficate) {
    /* The trust anchor is the root CA to trust */
    trustAnchors.add(rootCertificate);

    /* We need PKIX parameters to specify the trust anchors
     * and disable the CRL validation
     */
    validationParameters = new PKIXParameters(trustAnchors);
    certPathValidator = CertPathValidator.getInstance(PKIX);
    validationParameters.setRevocationEnabled(false);

    /* We are ensuring that certificates are chained correctly */
    certPathValidator.validate(certPath, validationParameters);
}
```

Integração com o AWS KMS

A instância deve ter uma aplicação que possa fazer solicitações de API do AWS KMS com atestado recuperado do NitroTPM. Quando você faz uma solicitação com um atestado, o AWS KMS valida as medidas no atestado fornecido em relação às medidas de referência na política de chave do KMS. Solicitações são permitidas somente se as medidas no atestado corresponderem às medidas de referência na política de chave do KMS.

Quando você chama as operações de API Decrypt, DeriveSharedSecret, GenerateDataKey, GenerateDataKeyPair ou GenerateRandom com um documento assinado, essas APIs criptografam o texto sem formatação na resposta com a chave pública do Atestado e retornam texto cifrado em vez de texto sem formatação. Esse texto cifrado pode ser descriptografado somente com a chave privada correspondente que foi gerada na instância.

Para obter mais informações, consulte o Cryptographic attestation for NitroTPM no AWS Key Management Service Developer Guide.

> **Note**
>
> Se você estiver atestando para um serviço de terceiros, deverá criar seus próprios mecanismos personalizados para receber, analisar e validar atestados. Para obter mais informações, consulte Validar um atestado do NitroTPM.

Isolar dados de seus próprios operadores

O Sistema AWS Nitro tem zero acesso do operador. Não existe nenhum mecanismo para que qualquer sistema da AWS ou pessoa faça login nos hosts do Amazon EC2 Nitro, acesse a memória das instâncias do EC2 ou acesse dados de clientes mantidos no armazenamento de instâncias criptografadas locais ou volumes criptografados remotos do Amazon EBS.

Ao processar dados altamente sensíveis, pode ser aconselhável restringir o acesso a esses dados evitando que até seus próprios operadores acessem a instância do EC2.

É possível criar AMIs atestáveis personalizadas, configuradas para fornecer um ambiente computacional isolado. A configuração da AMI depende da workload e dos requisitos da aplicação. Leve em conta essas práticas recomendáveis ao compilar a AMI para criar um ambiente computacional isolado.

- Remova todo acesso interativo para evitar que os operadores ou usuários acessem a instância.
- Certifique-se de que somente software e código confiáveis estejam incluídos na AMI.
- Configure um firewall de rede dentro da instância para bloquear o acesso.
- Garanta estados somente leitura e imutáveis para todos os sistemas de armazenamento e de arquivos.
- Restrinja o acesso à instância a chamadas de API autenticadas, autorizadas e registradas em log.

Atualizar AMIs atestáveis que não têm acesso interativo

Quando você inicia uma instância usando uma AMI de ambiente computacional isolado, não há como nenhum usuário ou operador se conectar à instância. Isso significa que não existe nenhuma maneira de instalar ou atualizar software na instância após a inicialização.

Se for necessário um novo software ou uma atualização de software, será necessário uma nova AMI atestável que inclua o software ou as atualizações de software requeridas. Depois, use essa AMI

para iniciar uma nova instância ou para realizar uma substituição do volume raiz na instância original. Qualquer alteração de software feita na AMI resultará na geração de um novo hash.

As ações a seguir resultarão em uma alteração nas medidas de referência do atestado do NitroTPM:

- Interromper e iniciar uma instância iniciada com uma AMI atestável
- Realizar uma substituição de volume raiz por uma AMI diferente

Se você realizar qualquer uma dessas ações, deverá atualizar o serviço de atestado com as novas medidas de referência. Por exemplo, você deverá atualizar a política de chaves do KMS com as novas medidas de referência se estiver usando o AWS KMS para atestação.

Uma instância retém o material de chave do NitroTPM durante todo o seu ciclo de vida e persiste durante interrupções/inícios e operações de substituição de volume raiz.

Credential Guard para instâncias do Windows

O AWS Nitro System é compatível com instâncias do Credential Guard para Amazon Elastic Compute Cloud (Amazon EC2) no Windows. O Credential Guard é um recurso de segurança baseada em virtualização (VBS) do Windows que permite a criação de ambientes isolados para proteger ativos de segurança, como credenciais de usuário do Windows e imposição da integridade de código, além das proteções do kernel do Windows. Quando você executa instâncias do Windows no EC2, o Credential Guard usa o AWS Nitro System para impedir que as credenciais de login do Windows sejam extraídas da memória do sistema operacional.

Conteúdos

- Pré-requisitos
- Inicialização de uma instância compatível
- Desabilitação da integridade da memória
- Ativação do Credential Guard
- Verificação se o Credential Guard está em execução

Pré-requisitos

Sua instância do Windows deve cumprir os pré-requisitos a seguir para utilizar o Credential Guard.

Imagens de máquina da Amazon (AMIs)

A AMI deve ser pré-configurada para habilitar o NitroTPM e o UEFI Secure Boot. Para obter mais informações sobre as AMIs compatíveis, consulte the section called “Requisitos”.

Integridade da memória

Não há suporte à integridade da memória, também conhecida como integridade de código protegida por hipervisor (HVCI) ou integridade de código imposta pelo hipervisor. Antes de ativar o Credential Guard, você deve garantir que esse atributo esteja desabilitado. Para obter mais informações, consulte Desabilitação da integridade da memória.

Tipos de instância

Os seguintes tipos de instância são compatíveis com o Credential Guard em todos os tamanhos, exceto se indicado de outra forma: `C5`, `C5d`, `C5n`, `C6i`, `C6id`, `C6in`, `C7i`, `C7i-flex`, `M5`, `M5d`, `M5dn`, `M5n`, `M5zn`, `M6i`, `M6id`, `M6idn`, `M6in`, `M7i`, `M7i-flex`, `R5`, `R5b`, `R5d`, `R5dn`, `R5n`, `R6i`, `R6id`, `R6idn`, `R6in` `R7i`, `R7iz`, `T3`.

> **Note**
>
> - Embora o NitroTPM tenha alguns tipos de instância obrigatórios em comum, o tipo de instância deve ser um dos tipos de instância anteriores para ser compatível com o Credential Guard.
> - O Credential Guard não é compatível com:
>   - Instâncias bare metal
>   - Os seguintes tipos de instância: `C7i.48xlarge`, `M7i.48xlarge` e `R7i.48xlarge`.

Para obter mais informações sobre tipos de instância, consulte o Guia de tipos de instância do Amazon EC2.

Inicialização de uma instância compatível

Agora é possível usar o console do Amazon EC2 ou AWS Command Line Interface (AWS CLI) para iniciar uma instância que é compatível com o Credential Guard. Você precisará de um ID de AMI compatível para iniciar sua instância, que seja exclusivo para cada Região da AWS.

> **Tip**
>
> É possível usar o link a seguir para descobrir e iniciar instâncias com AMIs compatíveis fornecidas pela Amazon no console do Amazon EC2: https://console.aws.amazon.com/ec2/v2/home?#Images:visibility=public-images;v=3;search=:TPM-Windows_Server;ownerAlias=amazon

Console

Como iniciar uma instância

Siga as etapas para iniciar uma instância, especificando um tipo de instância compatível e uma AMI do Windows configurada previamente.

AWS CLI

Como iniciar uma instância

Use o comando run-instances para iniciar uma instância usando um tipo de instância compatível e a AMI do Windows pré-configurada.

```
aws ec2 run-instances \
    --image-id resolve:ssm:/aws/service/ami-windows-latest/TPM-Windows_Server-2022-English-Full-Base \
    --instance-type c6i.large \
    --region us-east-1 \
    --subnet-id subnet-0abcdef1234567890
    --key-name key-name
```

PowerShell

Como iniciar uma instância

Use o comando New-EC2Instance para iniciar uma instância usando um tipo de instância compatível e a AMI do Windows pré-configurada.

```
New-EC2Instance `
    -ImageId resolve:ssm:/aws/service/ami-windows-latest/TPM-Windows_Server-2022-English-Full-Base `
    -InstanceType c6i.large `
    -Region us-east-1 `
```

```
    -SubnetId subnet-0abcdef1234567890 `
    -KeyName key-name
```

Desabilitação da integridade da memória

É possível usar o Editor de Política de Grupo Local para desativar a integridade da memória em cenários compatíveis. A seguinte orientação pode ser aplicada para cada configuração em Proteção da integridade do código baseada em virtualização:

- Habilitada sem bloqueio: modifique a configuração para Desabilitada para desabilitar a integridade da memória.
- Habilitada com bloqueio de UEFI: a integridade da memória foi habilitada com o bloqueio de UEFI. A integridade da memória não pode ser desabilitada depois de habilitada com o bloqueio de UEFI. Recomendamos criar uma nova instância com a integridade da memória desabilitada e encerrar a instância sem suporte se ela não estiver em uso.

Para desabilitar a integridade da memória com o Editor de Política de Grupo Local

1. Conecte-se à sua instância como uma conta de usuário com privilégios de administrador usando o protocolo do Desktop Remoto (RDP). Para obter mais informações, consulte the section called “Conectar-se usando um cliente RDP”.
2. Abra o menu Iniciar e pesquise **`cmd`** para iniciar um prompt de comando.
3. Execute os comandos a seguir para abrir o Editor de Política de Grupo Local: `gpedit.msc`
4. No Editor de Política de Grupo Local, selecione Configuração do Computador, Modelos Administrativos, Sistema, Device Guard.
5. Selecione Ativar Segurança Baseada em Virtualização e, em seguida, selecione Editar configuração de política.
6. Abra o menu suspenso de configurações para Proteção da integridade do código baseada em virtualização, escolha Desabilitada e, em seguida, escolha Aplicar.
7. Reinicie a instância para aplicar as alterações.

Ativação do Credential Guard

Depois de iniciar uma instância do Windows com um tipo de instância e uma AMI compatíveis e confirmar que a integridade da memória está desabilitada, será possível habilitar o Credential Guard.

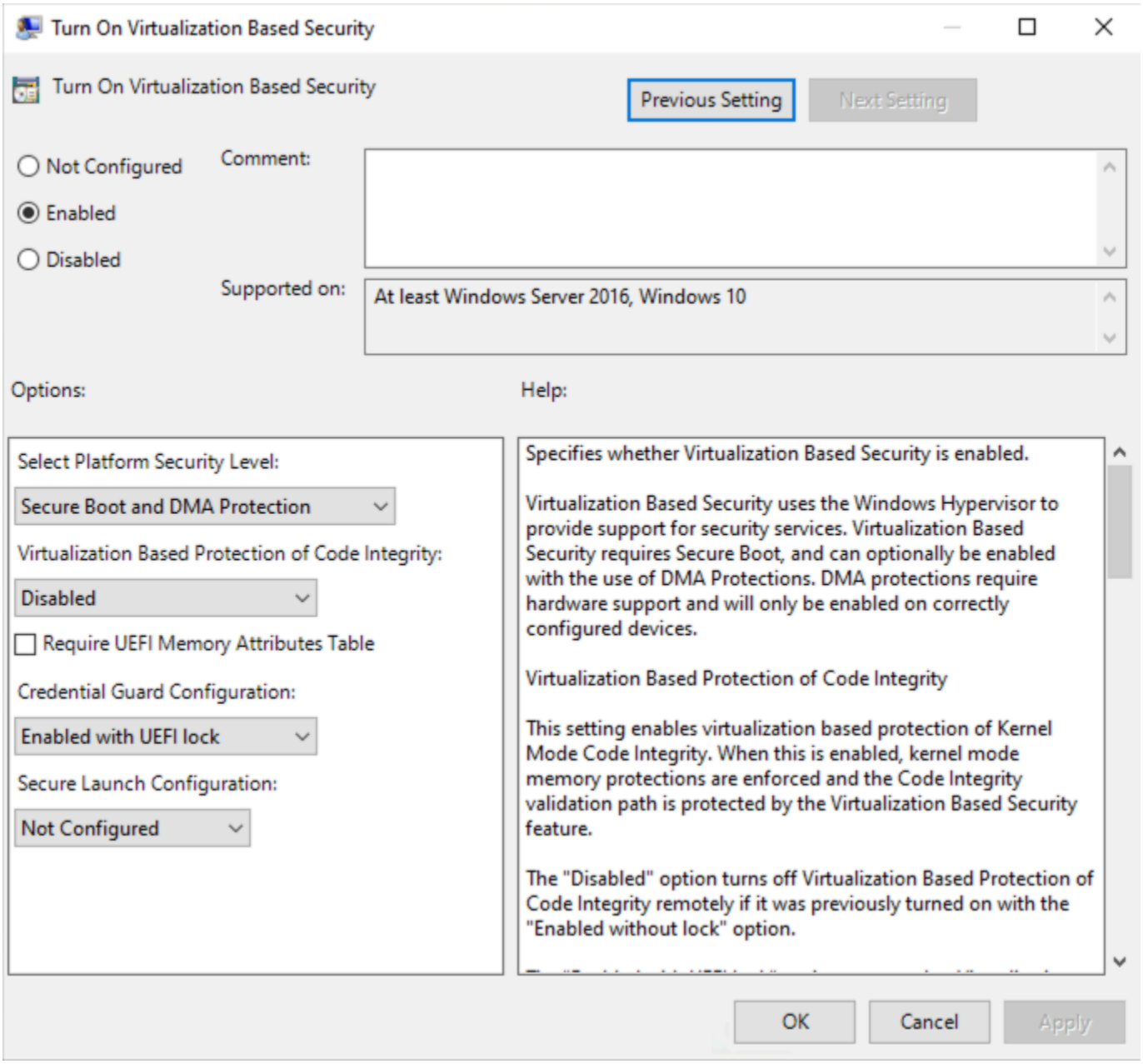
> **Important**
>
> São necessários privilégios de administrador para executar as seguintes etapas para ativar o Credential Guard.

Para ativar o Credential Guard

1. Conecte-se à sua instância como uma conta de usuário com privilégios de administrador usando o protocolo do Desktop Remoto (RDP). Para obter mais informações, consulte the section called “Conectar-se usando um cliente RDP”.
2. Abra o menu Iniciar e pesquise **`cmd`** para iniciar um prompt de comando.
3. Execute os comandos a seguir para abrir o Editor de Política de Grupo Local: `gpedit.msc`
4. No Editor de Política de Grupo Local, selecione Configuração do Computador, Modelos Administrativos, Sistema, Device Guard.
5. Selecione Ativar Segurança Baseada em Virtualização e, em seguida, selecione Editar configuração de política.
6. Escolha Ativado no menu Ativar Segurança Baseada em Virtualização.
7. Em Selecione o Nível de Segurança da Plataforma, escolha Inicialização segura e a proteção de DMA.
8. Em Configuração do Credential Guard, escolha Habilitada com bloqueio de UEFI.

   > **Note**
   >
   > As configurações de política restantes não são necessárias para ativar o Credential Guard e podem ser deixadas como Não configuradas.

   A imagem a seguir exibe as configurações de VBS definidas conforme descrito anteriormente:



9. Reinicie a instância para aplicar as configurações.

Verificação se o Credential Guard está em execução

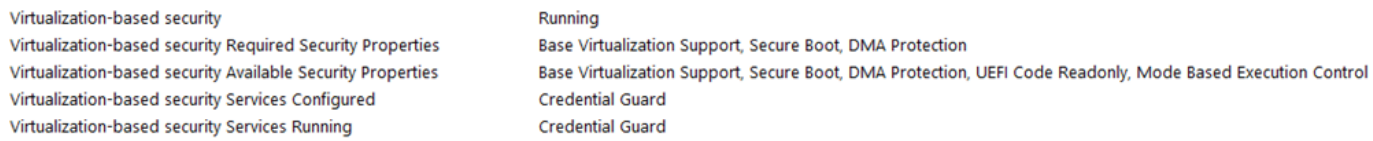
É possível usar a ferramenta Informações do sistema Microsoft (`Msinfo32.exe`) para confirmar se o Credential Guard está em execução.

> **Important**
>
> Você deve primeiro reinicializar a instância para concluir a aplicação das configurações de política necessárias para ativar o Credential Guard.

Para verificar se o Credential Guard está em execução

1. Conecte-se à sua instância usando o Remote Desktop Protocol (RDP). Para obter mais informações, consulte the section called “Conectar-se usando um cliente RDP”.
2. Na sessão RDP da sua instância, abra o menu Iniciar e pesquise **`cmd`** para iniciar um prompt de comando.
3. Abra as informações do sistema ao executar o comando a seguir: `msinfo32.exe`
4. A ferramenta Informações do sistema Microsoft lista os detalhes da configuração do VBS. Ao lado de Serviços de segurança baseados em virtualização, confirme se o Credential Guard aparece como em execução.

   A imagem a seguir mostra que o VBS está sendo executado conforme descrito anteriormente:



Acessar o Amazon EC2 usando um endpoint da VPC de interface

É possível melhorar a postura de segurança da sua VPC criando uma conexão privada entre os recursos da sua VPC e a API do Amazon EC2. É possível acessar a API do Amazon EC2 como se estivesse em sua VPC, sem usar um gateway da Internet, um dispositivo NAT, uma conexão VPN ou uma conexão Direct Connect. As instâncias do EC2 na VPC não precisam de endereços IP públicos para acessar a API do Amazon EC2.

Para obter mais informações, consulte Acessar os Serviços da AWS pelo AWS PrivateLink no Guia do AWS PrivateLink.

Conteúdo

- Criar um VPC endpoint de interface
- Criar uma política de endpoint

Criar um VPC endpoint de interface

Crie um endpoint de interface para o Amazon EC2 usando o seguinte nome de serviço:

- com.amazonaws.*região*.ec2: cria um endpoint para as ações da API do Amazon EC2.

Para obter mais informações, consulte Acessar um AWS service (Serviço da AWS) usando um endpoint de VPC de interface, no Guia do AWS PrivateLink.

Criar uma política de endpoint

Uma política de endpoint é um recurso do IAM que você pode anexar ao endpoint de interface. A política de endpoint padrão permite acesso total à API do Amazon EC2 por meio do endpoint de interface. Para controlar o acesso permitido à API do Amazon EC2 pela VPC, anexe uma política de endpoint personalizada ao endpoint de interface.

Uma política de endpoint especifica as seguintes informações:

- As entidades principais que podem executar ações.
- As ações que podem ser executadas.
- O recurso no qual as ações podem ser executadas.

> **Important**
>
> Quando uma política não padrão é aplicada a um endpoint da VPC de interface para o Amazon EC2, determinadas solicitações de API com falha, como as com falha de `RequestLimitExceeded`, podem não ser registradas no AWS CloudTrail nem no Amazon CloudWatch.

Para obter mais informações, consulte Control access to services using endpoint policies (Controlar o acesso a serviços usando políticas de endpoint) no Guia do AWS PrivateLink.

O exemplo a seguir mostra uma política de VPC endpoint que nega permissão para criar volumes não criptografados ou executar instâncias com volumes não criptografados. O exemplo de política também concede permissão para executar todas as outras ações do Amazon EC2.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
    {
        "Action": "ec2:*",
        "Effect": "Allow",
        "Resource": "*",
        "Principal": "*"
    },
    {
        "Action": [
            "ec2:CreateVolume"
        ],
        "Effect": "Deny",
        "Resource": "*",
        "Principal": "*",
        "Condition": {
            "Bool": {
                "ec2:Encrypted": "false"
            }
        }
    },
    {
        "Action": [
            "ec2:RunInstances"
        ],
        "Effect": "Deny",
        "Resource": "*",
        "Principal": "*",
        "Condition": {
            "Bool": {
                "ec2:Encrypted": "false"
            }
        }
    }]
}
```

Opções de armazenamento para as instâncias do Amazon EC2

O Amazon EC2 fornece opções de armazenamento físico de dados flexíveis, econômicas e fáceis de usar para suas instâncias. Cada opção tem uma combinação exclusiva de performance e durabilidade. Essas opções de armazenamento podem ser usadas independentemente ou em conjunto para atender às suas necessidades.

Armazenamento em bloco

- Amazon EBS: o Amazon EBS fornece volumes duráveis de armazenamento ao nível do bloco que podem ser anexados e desanexados das instâncias. É possível anexar vários volumes do EBS a uma única instância. Um volume do EBS persiste independentemente da vida útil da instância associada a ele. Você pode criptografar os volumes do EBS. Para manter uma cópia de backup dos dados, você pode criar snapshots dos volumes do EBS. Os snapshots são armazenados no Amazon S3. Você pode criar um volume do EBS a partir de um snapshot.
- Armazenamento em bloco temporário do armazenamento de instância para instâncias do EC2: o armazenamento de instância fornece armazenamento temporário ao nível do bloco para as instâncias. O número, o tamanho e o tipo dos volumes de armazenamento de instâncias são determinados pelo tipo e tamanho da instância. Os dados em um volume de armazenamento de instâncias só são mantidos durante a vida da instância associada; se você interromper, hibernar ou encerrar uma instância, todos os dados em volumes de armazenamento de instâncias serão perdidos.

Armazenamento de objetos

- Amazon S3: o Amazon S3 fornece acesso a uma infraestrutura de armazenamento 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, é possível usar o Amazon S3 para armazenar cópias de backup de seus dados e aplicações. O Amazon EC2 usa o Amazon S3 para armazenar snapshots do EBS e AMIs baseadas no Amazon S3.

Armazenamento de arquivos

- Amazon EFS (Somente instâncias do Linux): o Amazon EFS fornece armazenamento de arquivos escalável para uso com o Amazon EC2. É possível criar um sistema de arquivos de EFS e configurar suas instâncias para montar o sistema de arquivos. É possível usar um

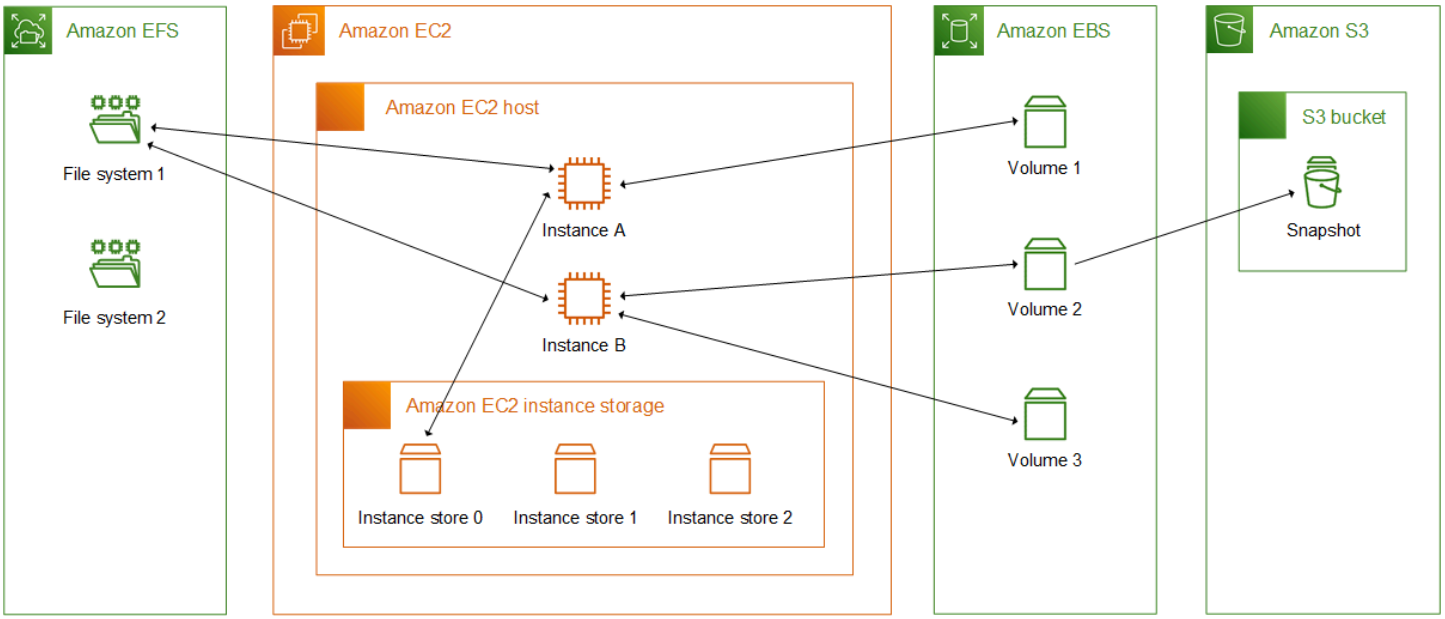
sistema de arquivos EFS como uma fonte de dados comum para workloads e aplicações em execução em várias instâncias.

- Amazon FSx: com o Amazon FSx, você pode inicializar, executar e escalar sistemas de arquivos com muitos recursos e de alto desempenho na nuvem. O Amazon FSx é um serviço totalmente gerenciado que é compatível com uma ampla variedade de workloads. Você pode escolher entre esses sistemas de arquivos amplamente usados: Lustre, NetApp ONTAP, OpenZFS e Windows File Server.

Armazenamento em cache de arquivos

- Usar o Amazon File Cache com instâncias do Amazon EC2: o Amazon File Cache fornece cache temporário de alto desempenho na AWS para processamento de dados de arquivos. O cache fornece acesso a dados de leitura e gravação para as workloads de computação no Amazon EC2 com latências inferiores a um milissegundo, até centenas de GB/s de throughput e até milhões de IOPS.

A figura a seguir mostra a relação entre essas opções de armazenamento e sua instância.



Preço de armazenamento da AWS

Abra Preços da AWS, vá até Preços de produtos da AWS e selecione Armazenamento. Escolha o produto de armazenamento para abrir sua página de preços.

Armazenamento em blocos persistente do Amazon EBS para instâncias do Amazon EC2

O Amazon Elastic Block Store (Amazon EBS) oferece recursos de armazenamento em bloco escaláveis e de alta performance que podem ser usados com instâncias do Amazon EC2. Com o Amazon EBS, é possível criar e gerenciar os seguintes recursos de armazenamento em blocos:

- Volumes do Amazon EBS: volumes de armazenamento que são anexados a instâncias do Amazon EC2. Após anexar um volume a uma instância, será possível usá-lo da mesma forma como usaria o armazenamento em bloco. A instância pode interagir com o volume da mesma forma que faria com uma unidade local.
- Snapshots do Amazon EBS: esses são backups pontuais dos volumes do Amazon EBS que persistem independentemente do volume em si. É possível criar snapshots para fazer backup dos dados nos volumes do Amazon EBS. Em seguida, será possível restaurar novos volumes desses snapshots a qualquer momento.

É possível criar e anexar volumes do EBS a uma instância durante a execução, e também pode criar e anexar volumes do EBS a uma instância a qualquer momento após a execução. Você também pode aumentar o tamanho ou a performance dos seus volumes do EBS sem desanexar o volume ou reiniciar a instância.

Você também pode criar snapshots do EBS de um volume do EBS a qualquer momento após a criação. É possível usar snapshots do EBS para fazer backup dos dados armazenados nos volumes. É possível então usar esses snapshots para restaurar volumes instantaneamente ou migrar dados entre Contas da AWS, regiões da AWS ou zonas de disponibilidade. É possível usar o Amazon Data Lifecycle Manager ou o AWS Backup para automatizar a criação, a retenção e a exclusão de snapshots do EBS.

Um volume gerenciado do EBS é gerenciado por um provedor de serviços, como o Modo automático do Amazon EKS. Você não pode modificar diretamente as configurações de um volume gerenciado do EBS. Os volumes gerenciados do EBS são identificados por um valor true no campo Gerenciado. Para obter mais informações, consulte Instâncias gerenciadas do Amazon EC2.

Para obter mais informações sobre como trabalhar com volumes e snapshots, consulte o Guia do usuário do Amazon EBS.

Limites de volume do Amazon EBS para instâncias do Amazon EC2

O número máximo de volumes do Amazon EBS que é possível anexar a uma instância depende do tipo e do tamanho da instância. Se o limite de associações de volume para uma instância for excedido, a solicitação de associação falhará com o erro `AttachmentLimitExceeded`.

Ao considerar quantos volumes adicionar à sua instância, é necessário avaliar se uma maior largura de banda de E/S ou maior capacidade de armazenamento são necessárias.

Largura de banda x capacidade

Para casos de uso de largura de banda consistentes e previsíveis, use instâncias otimizadas para Amazon EBS com volumes SSD de finalidade geral ou volumes SSD com IOPS provisionadas. Para obter o máximo de performance, faça a correspondência entre as IOPS provisionadas para seus volumes e a largura de banda disponível para o tipo da instância.

Para configurações de RAID, talvez você ache que matrizes com mais de 8 volumes prejudicam a performance devido à maior sobrecarga de E/S. Teste a performance de aplicações individuais e ajuste, se necessário.

Sumário

- Limites de volume para instâncias criadas no Nitro System
  - Limite de volume dedicado do EBS
  - Limite de volume compartilhado do EBS
- Limites de volume para instâncias baseadas em Xen
  - Instâncias do Linux
  - Instâncias do Windows

Limites de volume para instâncias criadas no Nitro System

Os limites de volumes para instâncias criadas no Nitro System dependem do tipo de instância. Alguns tipos de instância do Nitro contam com um limite de volume dedicado do EBS, enquanto a maioria tem um limite de volume compartilhado. Para visualizar os limites para anexação de volumes em cada tipo de instância, veja o seguinte:

- Amazon EBS specifications – General purpose
- Amazon EBS specifications – Compute optimized

- Amazon EBS specifications – Memory optimized
- Amazon EBS specifications – Storage optimized
- Amazon EBS specifications – Accelerated computing
- Amazon EBS specifications – High-performance computing
- Amazon EBS specifications – Previous generation

Limite de volume dedicado do EBS

Os tipos de instância do Nitro, apresentados a seguir, têm um limite de volume dedicado do EBS que varia dependendo do tamanho da instância. O limite não é compartilhado com outros anexos do dispositivo. Em outras palavras, você pode anexar qualquer número de volumes do EBS até o limite de anexação de volume, independentemente do número de dispositivos anexados, como volumes de armazenamento de instância NVMe e interfaces de rede.

- Uso geral: M7a | M7i | M7i-flex | M8a | M8azn | M8g | M8gb | M8gd | M8gn | M8i | M8id | M8i-flex
- Otimizadas para computação: C7a | C7i | C7i-flex | C8a | C8g | C8gb | C8gd | C8gn | C8i | C8id | C8i-flex
- Otimizadas para memória: R7a | R7i | R7iz | R8a | R8g | R8gb | R8gd | R8gn | R8i | R8id | R8i-flex | U7i-6tb | U7i-8tb | U7i-12tb | U7in-16tb | U7in-24tb | U7in-32tb | U7inh-32tb | X8g | X8aedz | X8i
- Otimizadas para armazenamento: I7i | I7ie | I8g | I8ge
- Computação acelerada: F2 | G6 | G6e | G6f | Gr6 | Gr6f | G7e | P4d | P4de | P5 | P5e | P5en | P6-B200 | P6-B300 | P6e-GB200 | Trn2 | Trn2u
- Computação de alta performance Hpc7a | Hpc8a

Limite de volume compartilhado do EBS

Todos os outros tipos de instância do Nitro (não listados em Limite de volume dedicado do EBS) têm um limite de anexo de volume que é compartilhado entre os volumes do Amazon EBS, as interfaces de rede e os volumes de armazenamento de instância para NVMe. É possível anexar qualquer número de volumes do Amazon EBS até esse limite, menos o número de interfaces de rede conectadas e os volumes de armazenamento de instâncias NVMe. Lembre-se de que cada instância deve ter pelo menos uma interface de rede e que os volumes de armazenamento de instâncias NVMe são anexados automaticamente na inicialização.

A maioria das instâncias do Nitro suporta um máximo de 28 anexos. Os exemplos a seguir demonstram como calcular quantos volumes do EBS você pode anexar.

Exemplos

- Com uma instância `m5.xlarge` com apenas a interface de rede principal, você pode anexar 27 volumes do EBS.

  28 volumes - 1 interface de rede = 27
- Com uma instância `m5.xlarge` com duas interfaces de rede adicionais, você pode anexar 25 volumes do EBS.

  28 volumes - 3 interfaces de rede = 25
- Com uma instância `m5d.xlarge` com duas interfaces de rede adicionais, você pode anexar 24 volumes do EBS.

  28 volumes - 3 interfaces de rede - 1 volume de armazenamento de instância NVMe = 24

Limites de volume para instâncias baseadas em Xen

Os limites de volumes para instâncias baseadas em Xen, como T2, dependem do sistema operacional.

Para obter mais informações, consulte Instâncias baseadas em Xen.

Instâncias do Linux

Anexar mais de 40 volumes a uma instância do Linux baseada em Xen pode causar falhas na inicialização. Esse número inclui o volume raiz, mais os volumes do Amazon EBS e os volumes de armazenamento de instâncias anexados.

Em caso de 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, inicie a instância e anexe novamente os volumes depois que a instância estiver em execução.

> **Important**
>
> A anexação de mais de 40 volumes a uma instância do Linux baseada em Xen ocorre somente em uma base de melhor esforço e não é garantida.

Instâncias do Windows

A tabela a seguir mostra os limites de volumes para instâncias do Windows baseadas em Xen em função do driver usado. Esses números incluem o volume raiz, mais quaisquer volumes do Amazon EBS e volumes de armazenamento de instâncias anexados.

Driver	Solicitação de volume
AWS PV	26
Citrix PV	26
Red Hat PV	17

Não recomendamos anexar mais de 26 volumes a uma instância do Windows baseada em Xen com drivers AWS PV ou Citrix PV, pois é provável que isso cause problemas de performance. Para determinar quais drivers PV sua instância está usando ou atualizar sua instância do Windows do Red Hat para drivers Citrix PV, consulte the section called “Atualizar drivers de PV”.

> **Important**
>
> A anexação de um número de volumes superior ao a seguir a uma instância do Windows baseada em Xen ocorre somente em uma base de melhor esforço e não é garantida.

Para obter mais informações sobre como os nomes dos dispositivos estão relacionados a volumes, consulte Como os volumes são anexados e mapeados para instâncias Windows do Amazon EC2.

Cartões EBS

A maioria dos tipos de instância é compatível com um cartão EBS. Os tipos de instância compatíveis com vários cartões EBS oferecem maior desempenho otimizado para EBS, tanto no throughput como IOPS do EBS. O desempenho máximo da sua instância Amazon EC2 é distribuído igualmente em cada cartão EBS. Por exemplo, em uma instância EC2 com capacidade total de `1,000,000` IOPS com 2 cartões EBS, cada cartão EBS pode suportar até `500,000` IOPS. Para obter informações sobre o desempenho do Amazon EBS compatível com sua instância do Amazon EC2, consulte Tipos de instância otimizados para o Amazon EBS.

Ao anexar um volume do Amazon EBS a uma instância compatível com vários cartões EBS, você pode selecionar o cartão EBS para o volume especificando o índice do cartão EBS. O volume raiz deve ser anexado ao índice 0 do cartão EBS.

Tipos de instância com vários cartões EBS

Os tipos de instância a seguir são compatíveis com vários cartões EBS. Para obter informações sobre a quantidade de volumes do Amazon EBS compatíveis com um tipo de instância, consulte Limites de volume do Amazon EBS para instâncias do Amazon EC2.

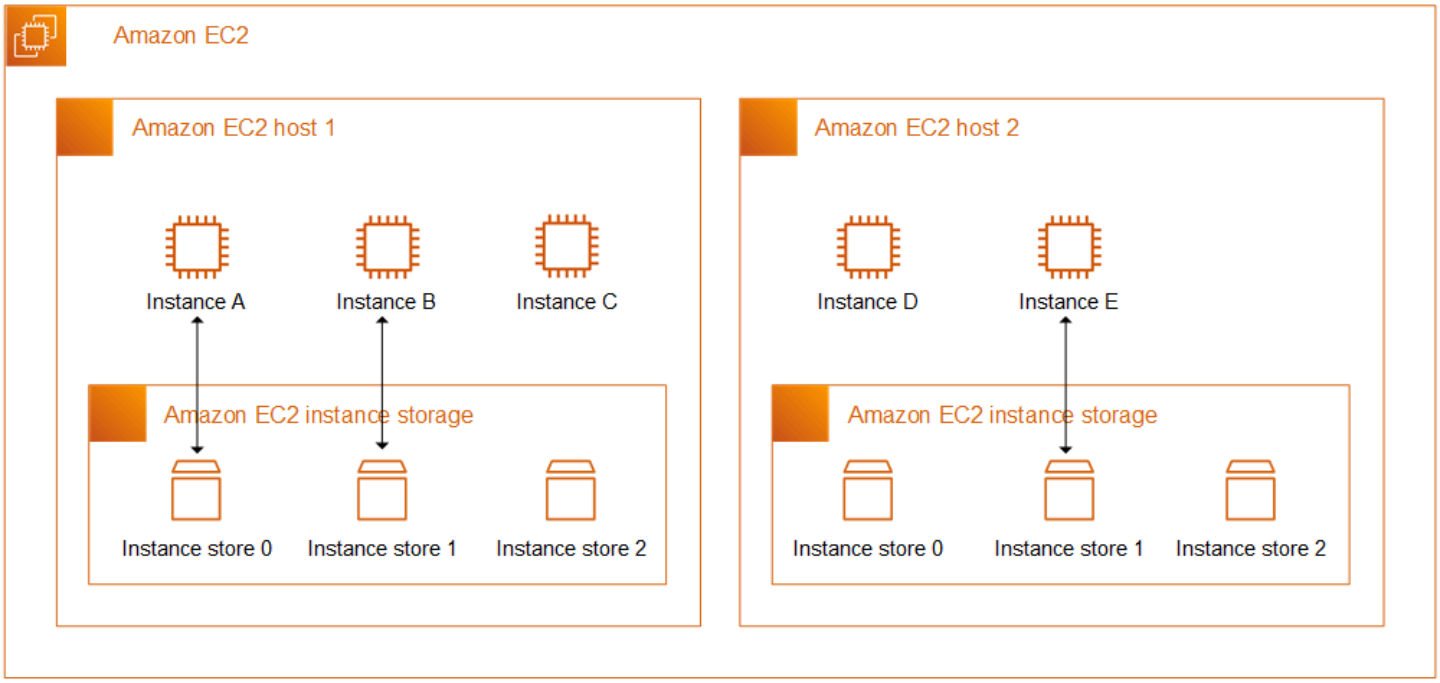
Tipo de instância	Quantidade de cartões EBS
c8gb.48xlarge	2
c8gb.metal-48xl	2
m8gb.48xlarge	2
r8gb.48xlarge	2
r8gb.metal-48xl	2

Armazenamento em bloco temporário do armazenamento de instância para instâncias do EC2

Um armazenamento de instância fornece armazenamento temporário ao nível do bloco para a instância do EC2. Esse armazenamento é fornecido por discos que estão anexados fisicamente ao computador host. O armazenamento de instância é ideal para armazenamento temporário de informações que mudam com frequência, como buffers, caches, dados temporários e outros conteúdos temporários. Ele também pode ser usado para o armazenamento de dados temporários replicados em toda a frota de instâncias, como um grupo com balanceamento de carga de servidores Web.

Um armazenamento de instâncias consiste em um ou mais volumes de armazenamento de instâncias expostos como dispositivos de bloco. O tamanho de um armazenamento de instâncias e o número de dispositivos disponíveis variam por tipo e tamanho de instância. Por exemplo, nem todo tipo de instância fornece volumes de armazenamento de instância. Para obter mais informações, consulte Limites de volume de armazenamento de instância para instâncias do EC2.

Os dispositivos virtuais para volumes de armazenamento de instância recebem nomes de dispositivos virtuais na ordem de `ephemeral0` a `ephemeral23`. Por exemplo, com um tipo de instância compatível com um volume de armazenamento de instância, o nome do dispositivo virtual desse volume é `ephemeral0`. Com um tipo de instância compatível com quatro volumes de armazenamento de instância, os nomes dos dispositivos virtuais dos quatro volumes são os seguintes: `ephemeral0`, `ephemeral1`, `ephemeral2` e `ephemeral3`.



Preço de armazenamento de instância

Não há cobrança adicional para usar os volumes de armazenamento de instância fornecidos para a instância. Os volumes do armazenamento de instância são incluídos como parte do custo de uso da instância.

Conteúdo

- Persistência de dados para volumes de armazenamento de instância do Amazon EC2
- Limites de volume de armazenamento de instância para instâncias do EC2
- Volumes de armazenamento de instância SSD para instâncias do EC2
- Adicionar volumes de armazenamento de instâncias a uma instância do EC2
- Habilitar volume de troca do armazenamento de instância para instâncias M1 e C1 do EC2
- Inicializar volumes de armazenamento de instância em instâncias do EC2
- Estatísticas de performance detalhadas para os volumes de armazenamento de instância do Amazon EC2

Persistência de dados para volumes de armazenamento de instância do Amazon EC2

Os volumes de armazenamento de instâncias são anexados somente na execução da instância. Você não pode anexar volumes de armazenamento de instâncias depois de executar. Você não pode desanexar um volume de armazenamento de instâncias de uma instância e anexá-lo a outra instância.

Um volume de armazenamento de instâncias existe somente durante a vida útil da instância à qual está anexado. Você não pode configurar um volume de armazenamento de instâncias para persistir além da vida útil da instância associada.

Os dados em um volume de armazenamento de instâncias persistem mesmo que a instância seja reinicializada. No entanto, os dados não persistem se a instância for interrompida, hibernada ou encerrada. Quando a instância for interrompida, hibernada ou encerrada, todos os blocos do volume de armazenamento de instâncias serão apagados criptograficamente.

Portanto, não dependa dos volumes de armazenamento de instâncias para dados valiosos e de longo prazo. Se você precisar reter os dados armazenados em um volume de armazenamento de instâncias além da vida útil da instância, você precisará copiar manualmente esses dados para um armazenamento mais persistente, como um volume do Amazon EBS, um bucket do Amazon S3 ou um sistema de arquivos do Amazon EFS.

Há alguns eventos que podem fazer com que seus dados não persistam durante toda a vida útil da instância. A tabela a seguir indica se os dados nos volumes de armazenamento de instâncias persistem durante eventos específicos, tanto para instâncias virtualizadas quanto para instâncias bare metal.

Event	O que acontece com seus dados?
Eventos do ciclo de vida da instância iniciados pelo usuário	
A instância foi reinicializada	The data persists
A instância foi interrompida	The data does not persist
A instância está em hibernação	The data does not persist
A instância foi encerrada	The data does not persist

Event	O que acontece com seus dados?
O tipo da instância foi alterado	The data does not persist *
Uma AMI baseada em EBS é criada na instância	The data does not persist in the created AMI **
Uma AMI baseada no Amazon S3 é criada usando a instância (Linux instances)	The data persists in the AMI bundle uploaded to Amazon S3 ***
Eventos do sistema operacional iniciados pelo usuário	
A shutdown is initiated	The data does not persist †
A restart is initiated	The data persists
AWS Eventos agendados da	
Interrupção da instância	The data does not persist
Reinicialização da instância	The data persists
Reinicialização do sistema	The data persists
Desativação da instância	The data does not persist
Eventos não planejados	
Recuperação automática simplificada	The data does not persist
Recuperação baseada em ações do CloudWatch	The data does not persist
The underlying disk fails	The data on the failed disk does not persist
Power failure	The data persists upon reboot

* Se o novo tipo de instância for compatível com o armazenamento de instâncias, a instância receberá o número de volumes de armazenamento de instâncias compatível com o novo tipo de instância, mas os dados não serão transferidos para a nova instância. Se o novo tipo de instância

não for compatível com o armazenamento de instâncias, a instância não receberá os volumes de armazenamento de instâncias.

** Os dados não estão incluídos na AMI baseada em EBS e não estão incluídos nos volumes de armazenamento de instâncias anexados às instâncias executadas nessa AMI.

*** Os dados estão incluídos no pacote de AMIs que é carregado no Amazon S3. Quando você executa uma instância nessa AMI, a instância obtém os volumes de armazenamento de instâncias agrupados na AMI com os dados que eles continham no momento em que a AMI foi criada.

† As proteções contra encerramento e interrupção não protegem as instâncias contra interrupções ou encerramentos de instâncias como resultado de desligamentos iniciados por meio do sistema operacional na instância. Os dados armazenados nos volumes de armazenamento de instâncias não persistem nos eventos de interrupção e encerramento de instâncias.

Limites de volume de armazenamento de instância para instâncias do EC2

O número, o tamanho e o tipo dos volumes de armazenamento de instância são determinados pelo tipo da instância. Alguns tipos de instância, como M6, C6 e R6, não são compatíveis com volumes de armazenamento de instâncias, enquanto outros tipos de instância, como M5d, C6gd e R6gd, são compatíveis com volumes de armazenamento de instâncias. Você não pode anexar mais volumes de armazenamento de instâncias a uma instância do que o compatível com o tipo de instância. Para os tipos de instâncias compatíveis com volumes de armazenamento de instâncias, o número e o tamanho dos volumes de armazenamento de instâncias variam de acordo com o tamanho da instância. Por exemplo, `m5d.large` é compatível com um volume de armazenamento de instâncias de 75 GB, enquanto `m5d.24xlarge` é compatível com quatro volumes de armazenamento de instâncias de 900 GB.

Para tipos de instância com volumes de armazenamento de instâncias NVMe, todos os volumes de armazenamento de instâncias compatíveis são automaticamente anexados à instância na execução. Para tipos de instância com volumes de armazenamento de instância que não tem a especificação NVMe, como C1, C3, M1, M2, M3, R3, D2, H1, I2, X1 e X1e, é necessário especificar manualmente os mapeamentos de dispositivos de blocos para os volumes de armazenamento de instância que você deseja anexar na inicialização. Depois que a instância for iniciada, você deverá formatar e montar os volumes de armazenamento de instâncias anexados antes de poder usá-los. Você não pode anexar um volume de armazenamento de instâncias depois de executar a instância.

Alguns tipos de instância usam unidades de estado sólido (SSD) NVMe ou SATA, enquanto outros usam unidades de disco rígido (HDD) SATA. SDDs entregam alta performance e aleatória de E/

S com latência muito baixa, mas você não precisa que os dados persistam quando a instância é terminada ou você pode tirar proveito de arquiteturas tolerantes a falhas. Para obter mais informações, consulte Volumes de armazenamento de instância SSD para instâncias do EC2.

Os dados nos volumes de armazenamento de instâncias do NVMe e alguns volumes de armazenamento de instâncias de HDD são criptografados em repouso. Para obter mais informações, consulte Proteção de dados no Amazon EC2.

Volumes de armazenamento de instâncias disponíveis

O Guia de tipos de instância do Amazon EC2 fornece otimizações de quantidade, de tamanho, de tipo e de performance de volumes de armazenamento de instância disponíveis em cada tipo de instância compatível. Para obter mais informações, consulte:

- Instance store specifications: General purpose
- Instance store specifications: Compute optimized
- Instance store specifications: Memory optimized
- Instance store specifications: Storage optimized
- Instance store specifications: Accelerated computing
- Instance store specifications: High-performance computing
- Instance store specifications: Previous generation

Console

Como recuperar informações de volume de armazenamento de instância

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Instance Types (Tipos de instância).
3. Adicione o filtro Local instance storage = true. A coluna Armazenamento indica o tamanho total do armazenamento da instância para o tipo de instância.
4. (Opcional) Clique no ícone Preferências e ative a Contagem de discos de armazenamento. Essa coluna indica o número de volumes de armazenamento de instâncias.
5. (Opcional) Adicione filtros para ampliar o escopo de tipos específicos de instância de interesse.

AWS CLI

Como recuperar informações de volume de armazenamento de instância

Use o comando describe-instance-types. O exemplo a seguir mostra o tamanho total do armazenamento de instância para cada tipo de instância nas famílias de instâncias R6i com volumes de armazenamento de instância.

```
aws ec2 describe-instance-types \
    --filters "Name=instance-type,Values=r6i*" "Name=instance-storage-
supported,Values=true" \
    --query "InstanceTypes[].[InstanceType, InstanceStorageInfo.TotalSizeInGB]" \
    --output table
```

O seguinte é um exemplo de saída.

```
----------------------------
|  DescribeInstanceTypes   |
+----------------+---------+
|  r6id.16xlarge  |  3800  |
|  r6idn.16xlarge |  3800  |
|  r6idn.8xlarge  |  1900  |
|  r6id.2xlarge   |  474   |
|  r6idn.xlarge   |  237   |
|  r6id.12xlarge  |  2850  |
|  r6idn.2xlarge  |  474   |
|  r6id.xlarge    |  237   |
|  r6idn.24xlarge |  5700  |
|  r6id.4xlarge   |  950   |
|  r6id.32xlarge  |  7600  |
|  r6id.24xlarge  |  5700  |
|  r6idn.large    |  118   |
|  r6idn.4xlarge  |  950   |
|  r6id.large     |  118   |
|  r6id.8xlarge   |  1900  |
|  r6idn.32xlarge |  7600  |
|  r6idn.metal    |  7600  |
|  r6id.metal     |  7600  |
|  r6idn.12xlarge |  2850  |
+----------------+--------+
```

Para obter detalhes completos de armazenamento de instâncias para um tipo de instância

Use o comando describe-instance-types.

```
aws ec2 describe-instance-types \
    --filters "Name=instance-type,Values=r6id.16xlarge" \
    --query "InstanceTypes[].InstanceStorageInfo"
```

O exemplo de resultado mostra que esse tipo de instância tem 2 volumes SSD NVMe de 1.900 GB, para um total de 3.800 GB de armazenamento de instância.

```
[
    {
        "TotalSizeInGB": 3800,
        "Disks": [
            {
                "SizeInGB": 1900,
                "Count": 2,
                "Type": "ssd"
            }
        ],
        "NvmeSupport": "required",
        "EncryptionSupport": "required"
    }
]
```

PowerShell

Como recuperar informações de volume de armazenamento de instância

Use o cmdlet Get-EC2InstanceType. O exemplo a seguir mostra o tamanho total do armazenamento de instância para cada tipo de instância nas famílias de instâncias R6i com volumes de armazenamento de instância.

```
(Get-EC2InstanceType -Filter @{Name="instance-type";
 Values="r6i*"},@{Name="instance-storage-supported"; Values="true"})
 | Format-Table @{Name="InstanceType";Expression={$_.InstanceType}},
 @{Name="TotalSize";Expression={$_.InstanceStorageInfo.TotalSizeInGB}}
```

O seguinte é um exemplo de saída.

```
InstanceType   TotalSize
```

```
------------   ---------
r6idn.16xlarge      3800
r6id.16xlarge       3800
r6id.xlarge          237
r6idn.8xlarge       1900
r6idn.2xlarge        474
r6id.12xlarge       2850
r6idn.xlarge         237
r6id.2xlarge         474
r6id.4xlarge         950
r6idn.24xlarge      5700
r6id.32xlarge       7600
r6id.24xlarge       5700
r6idn.large          118
r6id.large           118
r6idn.4xlarge        950
r6id.8xlarge        1900
r6id.metal          7600
r6idn.32xlarge      7600
r6idn.metal         7600
r6idn.12xlarge      2850
```

Para obter detalhes completos de armazenamento de instâncias para um tipo de instância

Use o cmdlet Get-EC2InstanceType. A saída é convertida para o formato JSON.

```
(Get-EC2InstanceType -Filter @{Name="instance-type";
 Values="r6id.16xlarge"}).InstanceStorageInfo | ConvertTo-Json
```

O exemplo de resultado mostra que esse tipo de instância tem 2 volumes SSD NVMe de 1.900 GB, para um total de 3.800 GB de armazenamento de instância.

```
{
  "Disks": [
    {
      "Count": 2,
      "SizeInGB": 1900,
      "Type": "ssd"
    }
  ],
  "EncryptionSupport": {
    "Value": "required"
```

```
  },
  "NvmeSupport": {
    "Value": "required"
  },
  "TotalSizeInGB": 3800
}
```

Volumes de armazenamento de instância SSD para instâncias do EC2

Como outros volumes de armazenamento de instâncias, é necessário 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 a uma instância do EC2.

Volumes SSD de NVMe

Algumas instâncias oferecem volumes de armazenamento de instâncias de unidades de estado sólido (SSD) de memória expressa não volátil (NVMe). Para obter mais informações sobre o tipo de volume de armazenamento de instâncias compatível com cada tipo de instância, consulte Limites de volume de armazenamento de instância para instâncias do EC2.

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.

Instâncias do Linux

Para acessar os volumes de NVMe, os drivers de NVMe devem ser instalados. As AMIs a seguir atendem a este requisito:

- AL2023
- Amazon Linux 2
- Amazon Linux AMI 2018.03 e posteriores
- Ubuntu 14.04 ou posterior com kernel `linux-aws`

> **Note**
>
> Os tipos de instância baseados no AWS Graviton requerem o Ubuntu 18.04 ou posterior com kernel `linux-aws`

- Red Hat Enterprise Linux 7.4 ou posterior
- SUSE Linux Enterprise Server 12 SP2 ou posterior
- CentOS 7.4.1708 ou posterior
- FreeBSD 11.1 ou posterior
- Debian GNU/Linux 9 ou posterior

- Bottlerocket

Depois de se conectar à instância, é possível listar os dispositivos de NVMe usando o comando lspci O seguinte é um exemplo da saída de uma instância `i3.8xlarge` compatível com quatro dispositivos de NVMe.

```
[ec2-user ~]$ lspci
00:00.0 Host bridge: Intel Corporation 440FX - 82441FX PMC [Natoma] (rev 02)
00:01.0 ISA bridge: Intel Corporation 82371SB PIIX3 ISA [Natoma/Triton II]
00:01.1 IDE interface: Intel Corporation 82371SB PIIX3 IDE [Natoma/Triton II]
00:01.3 Bridge: Intel Corporation 82371AB/EB/MB PIIX4 ACPI (rev 01)
00:02.0 VGA compatible controller: Cirrus Logic GD 5446
00:03.0 Ethernet controller: Device 1d0f:ec20
00:17.0 Non-Volatile memory controller: Device 1d0f:cd01
00:18.0 Non-Volatile memory controller: Device 1d0f:cd01
00:19.0 Non-Volatile memory controller: Device 1d0f:cd01
00:1a.0 Non-Volatile memory controller: Device 1d0f:cd01
00:1f.0 Unassigned class [ff80]: XenSource, Inc. Xen Platform Device (rev 01)
```

Se você está usando um sistema operacional compatível mas os dispositivos de NVMe não estão sendo exibidos, verifique se o módulo de NVMe está carregado usando o comando a seguir.

- Amazon Linux, Amazon Linux 2, Ubuntu 14/16, Red Hat Enterprise Linux, SUSE Linux Enterprise Server, CentOS 7

```
$ lsmod | grep nvme
```

```
nvme           48813  0
```

- Ubuntu 18

```
$ cat /lib/modules/$(uname -r)/modules.builtin | grep nvme
s/nvme/host/nvme-core.ko
kernel/drivers/nvme/host/nvme.ko
kernel/drivers/nvmem/nvmem_core.ko
```

Os volumes de NVMe estão em conformidade com a especificação NVMe 1.0e. É possível usar os comandos de NVMe com os volumes de NVMe. Com o Amazon Linux, é possível instalar o pacote `nvme-cli` no repositório usando o comando yum install. Com outras versões compatíveis do Linux, é possível fazer download do pacote `nvme-cli` se ele não estiver disponível na imagem.

Instâncias do Windows

As AMIs do Windows da AWS mais recentes dos seguintes sistemas operacionais contêm os drivers do AWS NVMe usados para interagir com volumes de armazenamento de instâncias SSD que são expostos como dispositivos de bloco de NVMe para melhor performance:

- Windows Server 2025
- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2

Depois de se conectar à instância, é possível verificar se você vê os volumes de NVMe no Gerenciador de Disco. Na barra de ferramentas, abra o menu de contexto (clique com o botão direito do mouse) no logotipo do Windows e escolha Disk Management.

As AMIs do Windows da AWS fornecidas pela Amazon incluem o driver do AWS NVMe. Se você não estiver usando as AMIs do Windows da AWS mais recentes, instale o driver atual do AWS NVMe.

Volumes SSD não NVMe

As instâncias apresentadas a seguir oferecem suporte a volumes de armazenamento de instância que usam SSDs não NVMe para fornecer alta performance de E/S randômica: C3, I2, M3, R3 e

X1. Para obter mais informações sobre o suporte a volumes de armazenamento de instâncias com suporte de cada tipo de instância, consulte Limites de volume de armazenamento de instância para instâncias do EC2.

Performance de E/S de volume de armazenamento de instância baseada em SSD

Ao preencher os volumes de armazenamento de instâncias baseados em SSD, o número de IOPS de gravação que é possível atingir diminui. Isso se deve ao trabalho extra que o controlador SSD deve fazer para encontrar espaço disponível, regravar os dados existentes e apagar o espaço não utilizado para que possa ser regravado. Esse processo de coleta de lixo resulta em uma amplificação da gravação interna no SSD, expressa como uma proporção entre as operações de gravação SSD e as operações de gravação do usuário. Essa redução na performance será ainda maior se as operações de gravação não ocorrerem em múltiplos de 4.096 bytes ou não estiverem alinhadas com um limite de 4.096 bytes. Se você gravar uma quantidade menor de bytes ou os bytes que não estejam alinhados, o controlador SSD deverá ler os dados adjacentes e armazenar o resultado em um novo local. Esse padrão resulta em uma amplificação da gravação muito maior, maior latência e uma performance de E/S drasticamente reduzida.

Os controladores SSD podem usar várias estratégias para reduzir o impacto da amplificação da gravação. Uma dessas estratégias é reservar espaço no armazenamento de instâncias SSD para que o controlador possa gerenciar, com mais eficiência, o espaço disponível para operações de gravação. Isso é denominado superprovisionamento. Os volumes de armazenamento de instância baseados em SSD fornecidos a uma instância não têm espaço reservado para o provisionamento em excesso. Para reduzir a amplificação da gravação, recomendamos reservar 10% do volume como não particionado, de modo que o controlador SSD possa usá-lo para provisionamento em excesso. Isso diminui o armazenamento que é possível usar, mas aumenta a performance mesmo se o disco estiver próximo da capacidade total.

Para volumes de armazenamento de instância compatíveis com TRIM, é possível usar o comando TRIM para notificar o controlador de SSD sempre que você não precisa mais dos dados que gravou. Isso fornece ao controlador mais espaço livre, o que pode reduzir a amplificação da gravação e aumentar a performance. Para obter mais informações, consulte Suporte a TRIM do volume de armazenamento de instâncias.

Suporte a TRIM do volume de armazenamento de instâncias

Alguns tipos de instâncias oferecem suporte a volumes SSD com TRIM. Para obter mais informações, consulte Limites de volume de armazenamento de instância para instâncias do EC2.

> **Note**
>
> (Somente para instâncias do Windows) As instâncias que executam o Windows Server 2012 R2 são compatíveis com a função TRIM a partir da versão 7.3.0 do driver PV da AWS. As instâncias que executam versões anteriores do Windows Server não são compatíveis com TRIM.

Os volumes de armazenamento de instâncias que oferecem suporte ao TRIM são aparados completamente antes de serem alocados à instância. Esses volumes não estão formatados com um sistema de arquivos quando uma instância é iniciada, portanto, é necessário formatá-los para que possam ser montados e usados. Para obter acesso mais rápido a esses volumes, é necessário ignorar a operação TRIM ao formatá-los.

(Instâncias do Windows) Para desabilitar temporariamente o suporte para a função TRIM durante a formatação inicial, use o comando `fsutil behavior set DisableDeleteNotify 1`. Após a conclusão da formatação, habilite novamente o suporte para a função TRIM ao usar `fsutil behavior set DisableDeleteNotify 0`.

Com volumes de armazenamento de instâncias que oferecem suporte ao TRIM, é possível usar o comando TRIM para notificar o controlador de SSD quando você não precisa mais dos dados que gravou. Isso fornece ao controlador mais espaço livre, o que pode reduzir a amplificação da gravação e aumentar a performance. Em instâncias do Linux, use o comando `fstrim` para habilitar a função TRIM periódica. Em instâncias do Windows, use o comando `fsutil behavior set DisableDeleteNotify 0` para garantir que o suporte para a função TRIM esteja habilitado durante a operação normal.

Adicionar volumes de armazenamento de instâncias a uma instância do EC2

Para tipos de instância com volumes de armazenamento de instâncias NVMe, todos os volumes de armazenamento de instâncias compatíveis são automaticamente anexados à instância na execução. Eles são automaticamente enumerados e atribuídos a um nome de dispositivo na execução da instância.

Para tipos de instância com volumes de armazenamento de instância que não tem a especificação NVMe, como C1, C3, M1, M2, M3, R3, D2, H1, I2, X1 e X1e, é necessário especificar manualmente os mapeamentos de dispositivos de blocos para os volumes de armazenamento de instância

que você deseja anexar na inicialização. Os mapeamentos de dispositivos de blocos podem ser especificados na solicitação de execução da instância ou na AMI usada para executar a instância. O mapeamento de dispositivos de blocos inclui um nome de dispositivo e o volume para o qual ele é mapeado. Para obter mais informações, consulte . Mapeamento de dispositivos de blocos para volumes em instâncias do Amazon EC2

> **Important**
>
> Volumes de armazenamento de instâncias podem ser anexados a uma instância somente quando você executá-la. Você não pode anexar volumes de armazenamento de instâncias depois de executar a instância.

Depois de executar uma instância, verifique se os volumes de armazenamento de instâncias da instância estão formatados e montados para poderem ser usados. O volume raiz do armazenamento de instância é configurado automaticamente ao ser montado.

Consideração dos volumes raiz

Um mapeamento de dispositivos de blocos sempre especifica o volume raiz da instância. O volume raiz é sempre montado automaticamente.

Instâncias do Linux: o volume raiz corresponde a um volume do Amazon EBS ou a um volume de armazenamento de instância. 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. Para obter mais informações, consulte Tipo do volume de raiz.

Instâncias do Windows: o volume raiz deve ser um volume do Amazon EBS. O armazenamento de instância não é compatível com o volume raiz.

Conteúdo

- Adicionar volumes de armazenamento de instância a uma AMI do Amazon EC2
- Adicionar volumes de armazenamento de instância a uma instância do EC2 durante a execução
- Disponibilizar o volume de armazenamento de instância para uso em uma instância do EC2

Adicionar volumes de armazenamento de instância a uma AMI do Amazon EC2

É possível criar uma AMI com um mapeamento de dispositivos de blocos que inclua volumes de armazenamento de instâncias.

Se você executar uma instância compatível com volumes de armazenamento de instâncias não NVMe usando uma AMI que especifique mapeamentos de dispositivos de blocos de volumes de armazenamento de instâncias, a instância incluirá esses volumes de armazenamento de instâncias. Se o número de mapeamentos de dispositivos de blocos de volumes de armazenamento de instâncias na AMI exceder o número de volumes de armazenamento de instâncias disponíveis para a instância, os mapeamentos de dispositivos de blocos de volumes de armazenamento de instâncias adicionais serão ignorados.

Se você executar uma instância compatível com volumes de armazenamento de instâncias NVMe usando uma AMI que especifique mapeamentos de dispositivos de blocos de volume de armazenamento de instâncias, eles serão ignorados. As instâncias compatíveis com volumes de armazenamento de instâncias NVMe recebem todos os volumes de armazenamento de instâncias compatíveis, independentemente dos mapeamentos de dispositivos de blocos especificados na solicitação de execução da instância e na AMI. O mapeamento de dispositivos desses volumes depende da ordem na qual o sistema operacional enumera os volumes.

Considerações

- O número de volumes de armazenamento de instâncias disponíveis depende do tipo de instância. Para obter mais informações, consulte the section called “Volumes de armazenamento de instâncias disponíveis”.
- Você precisa especificar um nome de dispositivo para cada dispositivo de blocos. Para obter mais informações, consulte Nomes de dispositivos para volumes em instâncias do Amazon EC2.
- Ao executar uma instância, será possível omitir volumes de armazenamento de instâncias não NVMe especificados no mapeamento de dispositivos de blocos da AMI ou adicionar volumes de armazenamentos de instâncias.
- Para instâncias M3, especifique volumes de armazenamento de instância no mapeamento de dispositivos de blocos da instância, não na AMI. O Amazon EC2 pode ignorar mapeamentos de dispositivos de blocos de volumes de armazenamento de instância na AMI.

Console

Para adicionar volumes de armazenamento de instância a uma AMI baseada no Amazon EBS

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances e selecione a instância.

3. Escolha Actions (Ações), Image and templates (Imagem e modelos), Create image (Criar imagem).
4. Na página diálogo Create Image (Criar imagem), adicione um nome e uma descrição significativos para imagem.
5. Para cada volume de armazenamento de instâncias a ser adicionado, selecione Add volume (Adicionar volume), em Volume type (Tipo de volume) selecione um volume de armazenamento de instâncias, e em Device (Dispositivo), selecione um nome de dispositivo.
6. Escolha Criar imagem.

AWS CLI

Para adicionar volumes de armazenamento de instância a uma AMI

Use o comando create-image com a opção `--block-device-mappings` para especificar um mapeamento de dispositivos de blocos para uma AMI baseada no EBS. Use o comando register-image com a opção `--block-device-mappings` para especificar um mapeamento de dispositivo de blocos para uma AMI baseada no Amazon S3.

```
--block-device-mappings file://mapping.json
```

O mapeamento de dispositivos de blocos a seguir adiciona dois volumes de armazenamento de instâncias.

```
[
    {
        "DeviceName": "/dev/sdc",
        "VirtualName": "ephemeral0"
    },
    {
        "DeviceName": "/dev/sdd",
        "VirtualName": "ephemeral1"
    }
]
```

PowerShell

Para adicionar volumes de armazenamento de instância a uma AMI

Use o cmdlet New-EC2Image com o parâmetro `-BlockDeviceMapping` para especificar um mapeamento de dispositivos de blocos para uma AMI baseada no EBS. Use o cmdlet Register-

EC2Image com o parâmetro `-BlockDeviceMapping` para especificar um mapeamento de dispositivos de blocos para uma AMI baseada no Amazon S3.

```
-BlockDeviceMapping $bdm
```

O mapeamento de dispositivos de blocos a seguir adiciona dois volumes de armazenamento de instâncias.

```
$bdm = @()

$sdc = New-Object -TypeName Amazon.EC2.Model.BlockDeviceMapping
$sdc.DeviceName = "/dev/sdc"
$sdc.VirtualName = "ephemeral0"
$bdm += $sdc

$sdd = New-Object -TypeName Amazon.EC2.Model.BlockDeviceMapping
$sdd.DeviceName = "/dev/sdd"
$sdd.VirtualName = "ephemeral1"
$bdm += $sdd
```

Adicionar volumes de armazenamento de instância a uma instância do EC2 durante a execução

Ao executar um tipo de instância com volumes de armazenamento de instância não NVMe, como C1, C3, M1, M2, M3, R3, D2, H1, I2, X1 e X1e, é necessário especificar os mapeamentos de dispositivos de blocos para os volumes de armazenamento de instância que você deseja anexar na execução. Os mapeamentos de dispositivos de blocos devem ser especificados na solicitação de execução da instância ou na AMI usada para executar a instância.

Se a AMI incluir mapeamentos de dispositivos de bloco para os volumes de armazenamento de instâncias, você não precisará especificar mapeamentos de dispositivos de blocos na solicitação de execução da instância, a menos que precise de mais volumes de armazenamento de instâncias do que os incluídos na AMI.

Se a AMI não incluir mapeamentos de dispositivos de blocos para volumes de armazenamento de instâncias, você deverá especificar os mapeamentos de dispositivos de bloco na solicitação de execução da instância.

Para tipos de instância com volumes de armazenamento de instâncias NVMe, todos os volumes de armazenamento de instâncias compatíveis são automaticamente anexados à instância na execução.

Considerações

- O número de volumes de armazenamento de instâncias disponíveis depende do tipo de instância. Para obter mais informações, consulte the section called “Volumes de armazenamento de instâncias disponíveis”.
- Você precisa especificar um nome de dispositivo para cada dispositivo de blocos. Para obter mais informações, consulte Nomes de dispositivos para volumes em instâncias do Amazon EC2.
- Para instâncias do M3, é possível receber volumes de armazenamento de instâncias mesmo que você não os especifique no mapeamento de dispositivos de blocos da instância.

Console

Para especificar um mapeamento de dispositivos de blocos em uma solicitação de inicialização de instância

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel, escolha Executar instância.
3. Na seção Application and OS Images (Imagens de aplicações e SO), selecione a AMI a ser usada.
4. Na seção Configurar armazenamento, a seção Volumes de armazenamento de instâncias lista os volumes de armazenamento de instâncias que podem ser anexados à instância.
5. Para cada volume de armazenamento de instância a ser anexado, em Nome do dispositivo, selecione o nome do dispositivo a ser usado.
6. Defina as configurações de instância restantes conforme necessário e, em seguida, escolha Iniciar instância.

AWS CLI

Para especificar um mapeamento de dispositivos de blocos em uma solicitação de inicialização de instância

Use o comando run-instances com a opção `--block-device-mappings`.

```
--block-device-mappings file://mapping.json
```

O mapeamento de dispositivos de blocos a seguir adiciona dois volumes de armazenamento de instâncias.

```
[
    {
        "DeviceName": "/dev/sdc",
        "VirtualName": "ephemeral0"
    },
    {
        "DeviceName": "/dev/sdd",
        "VirtualName": "ephemeral1"
    }
]
```

PowerShell

Para especificar um mapeamento de dispositivos de blocos em uma solicitação de inicialização de instância

Use o cmdlet New-EC2Instance com a opção `-BlockDeviceMapping`.

```
-BlockDeviceMapping $bdm
```

O mapeamento de dispositivos de blocos a seguir adiciona dois volumes de armazenamento de instâncias.

```
$bdm = @()

$sdc = New-Object -TypeName Amazon.EC2.Model.BlockDeviceMapping
$sdc.DeviceName = "/dev/sdc"
$sdc.VirtualName = "ephemeral0"
$bdm += $sdc

$sdd = New-Object -TypeName Amazon.EC2.Model.BlockDeviceMapping
$sdd.DeviceName = "/dev/sdd"
$sdd.VirtualName = "ephemeral1"
$bdm += $sdd
```

Disponibilizar o volume de armazenamento de instância para uso em uma instância do EC2

Depois de iniciar uma instância com volumes de armazenamento de instâncias anexados, você deverá montar os volumes antes de poder acessá-los.

Instâncias do Linux

É possível formatar volumes com o sistema de arquivos de sua escolha depois de iniciar a instância.

Para disponibilizar um volume de armazenamento de instâncias no Linux

1. Conecte-se à instância usando um cliente SSH. Para obter mais informações, consulte Conectar-se à instância do Linux usando SSH.
2. Use o comando `df -h` para visualizar os volumes formatados e montados.

```
$ df -h
Filesystem      Size  Used Avail Use% Mounted on
devtmpfs        3.8G   72K  3.8G   1% /dev
tmpfs           3.8G     0  3.8G   0% /dev/shm
/dev/nvme0n1p1  7.9G  1.2G  6.6G  15% /
```

3. Use o `lsblk` para visualizar todos os volumes que foram mapeados na inicialização, mas não formatados e montados.

```
$ lsblk
NAME          MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
nvme0n1       259:1    0    8G  0 disk
##nvme0n1p1   259:2    0    8G  0 part /
##nvme0n1p128 259:3    0    1M  0 part
nvme1n1       259:0    0 69.9G  0 disk
```

4. Para formatar e montar um volume de armazenamento de instâncias que foi apenas mapeado, faça o seguinte:

   a. Crie um sistema de arquivos no dispositivo usando o comando `mkfs`.

   ```
   $ sudo mkfs -t xfs /dev/nvme1n1
   ```

   b. Crie um diretório no qual montar o dispositivo usando o comando `mkdir`.

```
$ sudo mkdir /data
```

c. Monte o dispositivo no diretório recém-criado usando o comando `mount`.

```
$ sudo mount /dev/nvme1n1 /data
```

Instâncias do Windows

Em instâncias do Windows, reformatamos os volumes de armazenamento de instâncias com o sistema de arquivos NTFS.

É possível visualizar os volumes do armazenamento de instância usando o Gerenciamento de Disco do Windows. Para obter mais informações, consulte Listar discos não NVMe.

Como montar manualmente um volume de armazenamento de instâncias

1. Escolha Iniciar, insira Gerenciamento de computador e pressione Enter.
2. No painel esquerdo, escolha Gerenciamento de disco.
3. Se você for solicitado a inicializar o volume, escolha o volume a ser inicializado, selecione o tipo de partição necessário dependendo do seu caso de uso e escolha OK.
4. Na lista de volumes, clique com o botão direito do mouse no volume a ser montado e escolha Novo volume simples.
5. No assistente, escolha Avançar.
6. Na tela Especificar tamanho do volume, escolha Avançar para usar o tamanho máximo do volume. Como alternativa, escolha um tamanho de volume que esteja entre o espaço mínimo e o máximo em disco.
7. Na tela Atribuir uma letra ou um caminho de unidade, siga um destes procedimentos e escolha Avançar.

   - Para montar o volume com uma letra de unidade, escolha Atribuir a seguinte letra de unidade e escolha a letra da unidade a ser usada.
   - Para montar o volume como uma pasta, escolha Montar na seguinte pasta NTFS vazia e escolha Procurar para criar ou selecionar a pasta a ser usada.
   - Para montar o volume sem uma letra ou um caminho de unidade, escolha Não atribuir uma letra ou um caminho de unidade.

8. Na tela Formatar partição, especifique se deseja ou não formatar o volume. Se você optar por formatar o volume, escolha o sistema de arquivos e o tamanho da unidade necessários e especifique um rótulo de volume.
9. Escolha Avançar e Concluir.

Habilitar volume de troca do armazenamento de instância para instâncias M1 e C1 do EC2

> **Note**
>
> Este tópico se aplica somente às instâncias `c1.medium` e `m1.small` do Linux.

Os tipos de instância `c1.medium` e `m1.small` têm uma quantidade limitada de memória física. Portanto, elas recebem um volume de troca de 900 MiB no momento da inicialização para atuar como memória virtual ou espaço de troca para o sistema Linux. O espaço de troca no Linux pode ser usado quando um sistema precisa de mais memória que a que foi alocada fisicamente. Quando o espaço de troca está habilitado, os sistemas Linux podem mudar páginas da memória física usadas infrequentemente para espaço de troca (uma partição dedicada ou um arquivo de troca em um sistema de arquivos existente) e liberar esse espaço para páginas de memória que exigem acesso de alta velocidade.

> **Note**
>
> - O uso do espaço de troca para paginação de memória não é tão rápido ou eficiente quanto usar a RAM. Se a workload estiver paginando a memória regularmente no espaço de troca, é necessário considerar migrar para um tipo de instância maior com mais memória RAM. Para obter mais informações, consulte Alterações no tipo de instância do Amazon EC2.
> - Apesar de o kernel do Linux considerar esse espaço de troca uma partição do volume raiz, ele é, na realidade, um volume de armazenamento de instância separado, independentemente do tipo de volume raiz usado.

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, é possível 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, será possível 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). É possível 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), será possível 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 Limites de volume de armazenamento de instância para instâncias do EC2.

1. Liste os dispositivos de blocos anexados à instância para obter o nome do dispositivo de seu volume de armazenamento de instâncias.

   ```
   [ec2-user ~]$ lsblk -p
   NAME       MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
   /dev/xvdb  202:16   0   4G  0 disk /media/ephemeral0
   /dev/xvda1 202:1    0   8G  0 disk /
   ```

   Neste exemplo, o volume de armazenamento de instâncias é `/dev/xvdb`. Como essa é uma instância do Amazon Linux, o volume de armazenamento de instâncias está formatado e montado em `/media/ephemeral0`. Nem todos os sistemas operacionais Linux fazem isso automaticamente.

2. (Opcional) Se o volume de armazenamento de instâncias está montado (ele é listado como um `MOUNTPOINT` na saída do comando lsblk), você precisa desmontá-lo com o comando a seguir.

```
[ec2-user ~]$ sudo umount /dev/xvdb
```

3. Configure uma área de troca do Linux no dispositivo com o comando mkswap.

```
[ec2-user ~]$ sudo mkswap /dev/xvdb
mkswap: /dev/xvdb: warning: wiping old ext3 signature.
Setting up swapspace version 1, size = 4188668 KiB
no label, UUID=b4f63d28-67ed-46f0-b5e5-6928319e620b
```

4. Habilite o novo espaço de troca.

```
[ec2-user ~]$ sudo swapon /dev/xvdb
```

5. Verifique se o novo espaço de troca está sendo usado.

```
[ec2-user ~]$ swapon -s
Filename    Type  Size Used Priority
/dev/xvdb                               partition 4188668 0 -1
```

6. Edite o arquivo `/etc/fstab` para que esse espaço de troca seja habilitado automaticamente em cada inicialização do sistema.

```
[ec2-user ~]$ sudo vim /etc/fstab
```

Se o arquivo `/etc/fstab` tiver uma entrada para `/dev/xvdb` (ou para`/dev/sdb`) altere-o para que corresponda à linha abaixo. Se ele não tiver uma entrada para esse dispositivo, adicione a linha a seguir no arquivo `/etc/fstab` (usando o nome do dispositivo de troca de seu sistema):

```
/dev/xvdb       none    swap    sw  0       0
```

> **Important**
>
> Os dados do volume de armazenamento de instâncias são perdidos quando uma instância é interrompida ou hibernada. Isso inclui a formatação do espaço de troca do armazenamento de instâncias criadas em Step 3. 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 até a Step 5 no novo volume de armazenamento de instâncias.

Inicializar volumes de armazenamento de instância em instâncias do EC2

Por causa do modo como o Amazon EC2 virtualiza os discos, a primeira gravação em qualquer local em alguns volumes de armazenamento de instâncias ocorre mais lentamente que as gravações subsequentes. Para a maioria das aplicações, a amortização desse custo ao longo da vida útil da instância é aceitável. Entretanto, se você precisar de alta performance de disco, recomendamos inicializar suas unidades gravando uma vez em todos os locais da unidade antes do uso em produção.

> **Note**
>
> Tipos de instância com unidades de estado sólido (SSD) anexadas diretamente e compatíveis com TRIM fornecem performance máxima no momento da inicialização, sem inicialização. Para obter informações sobre o armazenamento de instâncias para cada tipo de instância, consulte Limites de volume de armazenamento de instância para instâncias do EC2.

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
```

Estatísticas de performance detalhadas para os volumes de armazenamento de instância do Amazon EC2

O Amazon EC2 fornece, em tempo real, estatísticas de performance de alta resolução para os volumes de armazenamento de instância NVMe anexados às instâncias do Amazon EC2 baseadas no Nitro. Essas estatísticas são apresentadas como contadores agregados que são retidos durante a toda a vida útil da instância. As estatísticas fornecem detalhes sobre o número cumulativo de operações, bytes enviados e recebidos, tempo gasto em operações de E/S de leitura e gravação e histogramas de operações de E/S de leitura e gravação. Embora essas estatísticas mantenham consistência com as estatísticas de performance detalhadas do Amazon EBS, elas também incluem histogramas de latência detalhados, categorizados por tamanho de E/S, que podem fornecer insights mais granulares sobre os padrões de performance do armazenamento. Essa maior visibilidade permite identificar precisamente quais são os tamanhos específicos de E/S que estão tendo problemas de latência, permitindo otimizar a performance das aplicações e solucionar os problemas com mais eficiência.

Você pode coletar essas estatísticas em uma granularidade de intervalos de até um segundo. Se solicitações forem feitas em uma frequência maior que a intervalos de um segundo, o driver NVMe poderá enfileirar as solicitações juntamente com outros comandos administrativos para processamento posterior.

Considerações

- As estatísticas são compatíveis apenas com volumes de armazenamento de instância NVMe anexados a instâncias baseadas no Nitro.

- Os contadores não persistem durante interrupções e reinicializações da instância.
- As estatísticas estão disponíveis sem custo adicional.

Statistics

O dispositivo de blocos NVMe fornece as seguintes estatísticas:

Nome da estatística	Nome completo	Tipo	Descrição
`total_rea d_ops`	Total de operações de leitura	Contador	O número total de operações de leitura concluídas.
`total_wri te_ops`	Total de operações de gravação	Contador	O número total de operações de gravação concluídas.
`total_rea d_bytes`	Total de bytes de leitura	Contador	O número total de bytes de leitura transferidos.
`total_wri te_bytes`	Total de bytes de gravação	Contador	O número total de bytes de gravação transferidos.
`total_rea d_time`	Tempo total de leitura	Contador	O tempo total gasto, em microssegundos, por todas as operações de leitura concluídas.
`total_wri te_time`	Tempo total de gravação	Contador	O tempo total gasto, em microssegundos, por todas as operações de gravação concluídas.
`instance_ store_vol ume_perfo rmance_ex ceeded_io ps`	A demanda de tempo total excedeu o IOPS máximo do volume	Contador	O tempo total em microssegundos que o IOPS demanda excedeu o máximo de IOPS do volume. Qualquer valor acima de `0` indica que a workload demandou mais IOPS do que o volume podia fornecer. Idealmente, a contagem incremental dessa métrica, entre os horários de dois snapshots, deve ser mínima.

Nome da estatística	Nome completo	Tipo	Descrição
`instance_store_volume_performance_exceeded_tp`	A demanda de tempo total excedeu o throughput máximo do volume	Contador	O tempo total em microssegundos que o throughput demanda excedeu o throughput máximo do volume. Qualquer valor acima de `0` indica que a workload exigia mais throughput do que o volume poderia fornecer. Idealmente, a contagem incremental dessa métrica, entre as horas de dois snapshots, deve ser mínima.
`volume_queue_length`	Tamanho de fila do volume	Ponto de tempo	O número de solicitações de operação de leitura e gravação aguardando conclusão.
`read_io_latency_histogram`	Histograma de E/S de leitura	Histograma *	O número de operações de leitura concluídas em cada compartimento de latência, em microssegundos.
`write_io_latency_histogram`	Histograma de E/S de gravação	Histograma *	O número de operações de gravação concluídas em cada compartimento de latência, em microssegundos.

> **Note**
>
> * As estatísticas do histograma representam apenas as operações de E/S que foram concluídas com êxito. As operações de E/S paralisadas ou prejudicadas não foram incluídas, mas ficarão aparentes nas estatísticas de `volume_queue_length`, que são apresentadas como estatísticas pontuais.

Acessar as estatísticas

As estatísticas devem ser acessadas diretamente na instância à qual os volumes de armazenamento de instância estão anexados. Você pode acessar as estatísticas usando um dos métodos a seguir.

Instâncias do Linux

Amazon CloudWatch

Você pode configurar o agente do Amazon CloudWatch para coletar as estatísticas da instância e disponibilizá-las como métricas personalizadas no CloudWatch. Você pode, então, usar as métricas do CloudWatch para analisar padrões de E/S, acompanhar tendências de performance, criar painéis personalizados e configurar alarmes automatizados baseados em limites de performance.

Para obter mais informações sobre a configuração do agente CloudWatch, consulte Collect Amazon EC2 instance store volume metrics.

nvme-cli tool

Para acessar as estatísticas

1. Conecte-se à instância a que o volume está anexado.
2. As AMIs do Amazon Linux 2023 lançadas após 15 de setembro de 2025 incluem a versão mais recente da ferramenta `nvme-cli`. Se você estiver usando uma AMI do Amazon Linux mais antiga, atualize a ferramenta `nvme-cli`.

   ```
   sudo yum install nvme-cli
   ```

3. Execute o comando a seguir e especifique o nome do dispositivo para o volume.

   ```
   sudo nvme amzn stats /dev/nvme0n1
   ```

As estatísticas também fornecem histogramas de latência detalhados, categorizados por tamanho de E/S. Para ver as estatísticas categorizadas por tamanho de E/S, inclua a opção `--details`. Por exemplo:

```
sudo nvme amzn stats --details /dev/nvme0n1
```

Você pode obter mais informações sobre como usar a ferramenta especificando a opção `--help`. Por exemplo:

```
sudo nvme amzn stats --help
```

Instâncias do Windows

nvme_amzn.exe tool

Para acessar as estatísticas

1. Conecte-se à instância a que o volume está anexado.
2. Certifique-se de estar usando o driver AWSNVMe versão `1.7.0` ou posterior. Para obter mais informações sobre a atualização do driver AWSNVMe, consulte Drivers AWS NVMe.
3. Obtenha o número do disco para o volume. Para obter mais informações, consulte Mapear discos NVMe em uma instância Amazon EC2 Windows para volumes.
4. Execute o comando a seguir como administrador e especifique o número do disco para o volume.

```
.\nvme_amzn.exe stats disk_number
```

As estatísticas também fornecem histogramas de latência detalhados, categorizados por tamanho de E/S. Para ver as estatísticas categorizadas por tamanho de E/S, inclua a opção `--details`. Por exemplo:

```
.\nvme_amzn.exe stats --details disk_number
```

Volumes raiz para as instâncias do Amazon EC2

Quando você inicia uma instância, um volume raiz é criado para ela. O volume raiz contém a imagem usada para inicializar a instância. Cada instância tem um único volume raiz. É possível adicionar volumes de armazenamento às instâncias durante ou após a inicialização.

A AMI usada para iniciar uma instância determina o tipo de volume raiz. É possível iniciar uma instância usando uma AMI baseada no Amazon EBS (para instâncias do Linux e do Windows) ou uma AMI baseada no Amazon S3 (somente para instâncias do Linux). Existem diferenças significativas quanto ao que é possível fazer com cada tipo de AMI. Para obter mais informações sobre essas diferenças, consulte Tipo do volume de raiz.

Recomendamos que você use AMIs baseadas no Amazon EBS, pois elas são iniciadas mais rapidamente e usam armazenamento persistente.

Reservamos nomes de dispositivos específicos para os volumes raízes. Para obter mais informações, consulte Nomes de dispositivos para volumes em instâncias do Amazon EC2.

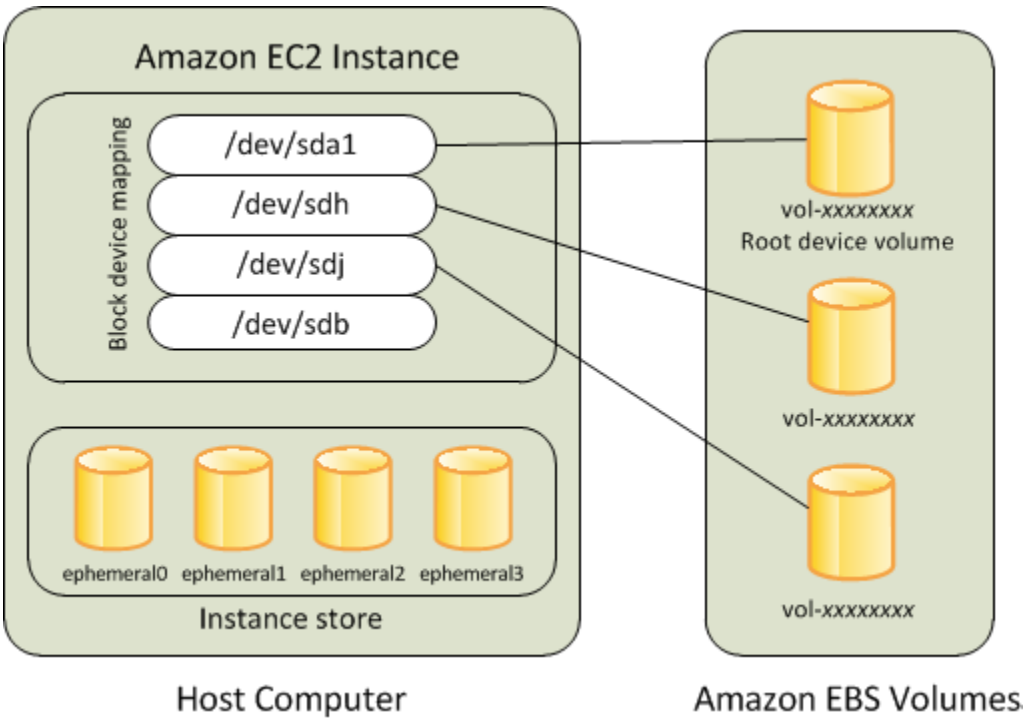
Conteúdo

- Instâncias com um volume raiz do Amazon EBS
- Instâncias com um volume raiz de armazenamento de instância (somente para instâncias do Linux)
- Manter um volume raiz do Amazon EBS após o encerramento de uma instância do Amazon EC2
- Substituir o volume raiz de uma instância do Amazon EC2 sem interrompê-la

Instâncias com um volume raiz do Amazon EBS

As instâncias que usam o Amazon EBS para o volume raiz automaticamente têm um volume do Amazon EBS associado. Quando você inicia uma instância com uma AMI baseada no Amazon EBS, criamos um volume do Amazon EBS para cada snapshot do Amazon EBS referenciado pela AMI. Também é possível usar outros volumes do Amazon EBS ou volumes de armazenamento de instâncias, dependendo do tipo de instância.

Uma instância com volume raiz do EBS pode ser interrompida e reiniciada posteriormente sem afetar os dados armazenados nos volumes anexados. Você pode executar diversas operações envolvendo instâncias e volumes enquanto a instância com volume raiz do EBS estiver no estado interrompido. Por exemplo, é possível modificar as propriedades da instância, alterar o tamanho ou atualizar o kernel que está usando, ou ainda anexar o volume raiz a outra instância em execução para depuração ou para qualquer outro propósito. Para obter mais informações, consulte Volumes do Amazon EBS.



Limitação

Você não pode usar os volumes `st1` ou `sc1` do EBS como volumes raízes.

Falha de instância

Caso uma instância cujo volume raiz é do EBS apresente falha, é possível recuperar a sessão usando um dos seguintes métodos:

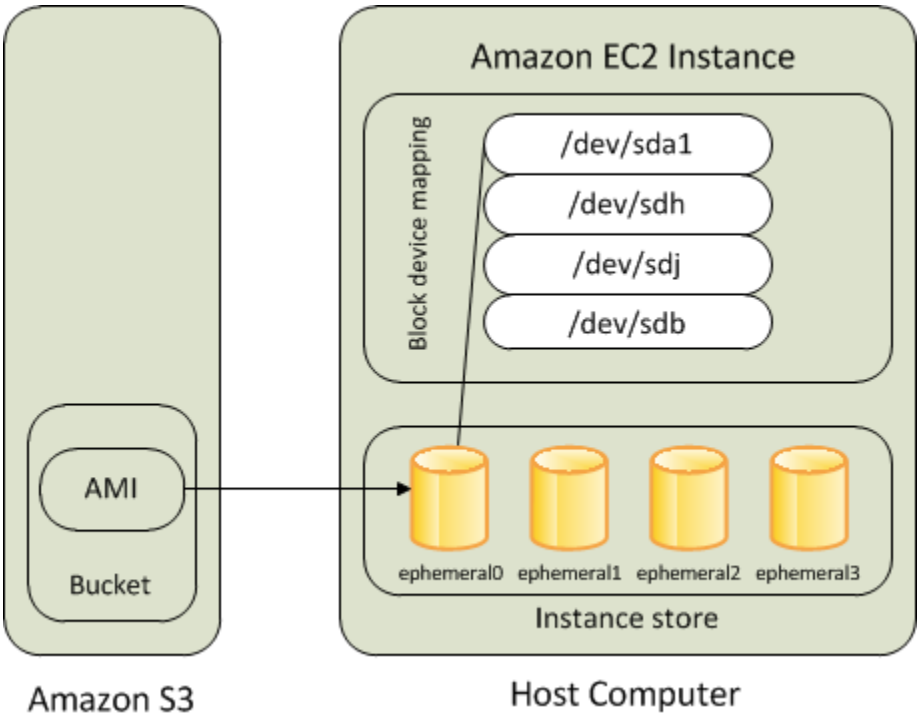
- Pare e reinicie (teste esse método primeiro).
- Faça automaticamente o snapshot de todos os volumes relevantes e crie uma nova AMI. Para obter mais informações, consulte Criação de uma AMI baseada no Amazon EBS.
- Associe o volume à nova instância seguindo estas etapas:
  1. Crie um snapshot de novo 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.

Instâncias com um volume raiz de armazenamento de instância (somente para instâncias do Linux)

> **Note**
>
> Os volumes raiz baseados no armazenamento de instância não são compatíveis com instâncias do Windows.

As instâncias que usam armazenamento de instância como volume raiz têm automaticamente um ou mais volumes de armazenamento de instância disponíveis, sendo que um deles funciona como volume raiz. Ao iniciar uma instância usando uma AMI baseada no Amazon S3, a AMI é copiada para o volume raiz. Observe que você também usar volumes adicionais de armazenamento de instâncias, dependendo do tipo de instância.

Todos os dados presentes nos volumes de armazenamento de instância permanecem enquanto a instância estiver em execução, mas são excluídos no encerramento da instância (instâncias com volume raiz de armazenamento de instância não permitem a ação Interromper) ou em caso de falha, por exemplo, se houver problemas no drive subjacente. Para obter mais informações, consulte Armazenamento em bloco temporário do armazenamento de instância para instâncias do EC2.



Tipos de instâncias compatíveis

Somente os seguintes tipos de instância são compatíveis com um volume de armazenamento de instância como o dispositivo raiz: C1, C3, D2, I2, M1, M2, M3, R3 e X1.

Falha de instância

Após uma instância com volume raiz do tipo armazenamento de instância falhar ou ser encerrada, ela não pode ser restaurada. Se você planeja usar instâncias com volume raiz do tipo armazenamento de instância, recomendamos que distribua os dados dos volumes de instância entre várias zonas de disponibilidade. Você também deve fazer backup dos dados críticos dos volumes de armazenamento de instâncias para o armazenamento persistente regularmente.

Manter um volume raiz do Amazon EBS após o encerramento de uma instância do Amazon EC2

Por padrão, o volume raiz do Amazon EBS para uma instância é excluído quando a instância é terminada. Você pode alterar o comportamento padrão para garantir que o volume raiz do Amazon EBS persista após a instância ser terminada. Para alterar o comportamento padrão, defina o atributo `DeleteOnTermination` como `false`. Você pode fazer isso ao iniciar a instância ou posteriormente.

Tarefas

- Configurar o volume raiz para persistir durante a execução da instância
- Configurar o volume raiz para persistir em uma instância existente
- Confirmar que um volume raiz está configurado para persistir

Configurar o volume raiz para persistir durante a execução da instância

Você pode configurar o volume raiz para persistir quando a instância for iniciada.

Console

Para configurar o volume raiz para persistir ao inicializar uma instância

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias) e Launch instances (Executar instâncias).
3. Escolha uma imagem de máquina da Amazon (AMI), um tipo de instância e um par de chaves e defina suas configurações de rede.

4. Em Configurar armazenamento, escolha Avançado.
5. Expanda o volume raiz.
6. Em Excluir no encerramento, escolha Não.
7. Ao concluir a configuração da instância, escolha Executar instância.

AWS CLI

Para configurar o volume raiz para persistir ao inicializar uma instância

Use o comando run-instances e inclua a seguinte opção.

```
--block-device-mappings file://mapping.json
```

Em `mapping.json`, especifique um mapeamento de dispositivos de blocos que defina o atributo `DeleteOnTermination` como `false`.

```
[
    {
        "DeviceName": "/dev/sda1",
        "Ebs": {
            "DeleteOnTermination": false
        }
    }
]
```

PowerShell

Para configurar o volume raiz para persistir ao inicializar uma instância

Use o cmdlet New-EC2Instance e inclua o seguinte parâmetro.

```
-BlockDeviceMapping $bdm
```

Crie um mapeamento de dispositivos de blocos que defina o atributo `DeleteOnTermination` como `$false`.

```
$ebs = New-Object Amazon.EC2.Model.EbsBlockDevice
$ebs.DeleteOnTermination = $false
```

```
$bdm = New-Object Amazon.EC2.Model.BlockDeviceMapping
$bdm.DeviceName = "dev/xvda"
$bdm.Ebs = $ebs
```

Configurar o volume raiz para persistir em uma instância existente

Você pode configurar o volume raiz para persistir para uma instância em execução. Observe que não é possível realizar essa tarefa usando o console do Amazon EC2.

AWS CLI

Para configurar o volume raiz para persistir para uma instância existente

Use o comando modify-instance-attribute com um mapeamento de dispositivo de blocos que define o atributo `DeleteOnTermination` como `false`.

```
aws ec2 modify-instance-attribute \
    --instance-id i-1234567890abcdef0 \
    --block-device-mappings file://mapping.json
```

Especifique o seguinte em `mapping.json`.

```
[
    {
        "DeviceName": "/dev/xvda",
        "Ebs": {
            "DeleteOnTermination": false
        }
    }
]
```

PowerShell

Para configurar o volume raiz para persistir para uma instância existente

Use o cmdlet Edit-EC2InstanceAttribute com um mapeamento de dispositivos de blocos que define o atributo `DeleteOnTermination` como `$false`.

```
$ebs = New-Object Amazon.EC2.Model.EbsInstanceBlockDeviceSpecification
$ebs.DeleteOnTermination = $false
```

```
$bdm = New-Object Amazon.EC2.Model.InstanceBlockDeviceMappingSpecification
$bdm.DeviceName = "/dev/xvda"
$bdm.Ebs = $ebs
Edit-EC2InstanceAttribute `
    -InstanceId i-1234567890abcdef0 `
    -BlockDeviceMapping $bdm
```

Confirmar que um volume raiz está configurado para persistir

Confirme que um volume raiz está configurado para persistir.

Console

Para confirmar que um volume raiz está configurado para persistir

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias) e selecione a instância.
3. Na guia Storage (Armazenamento), em Block devices (Dispositivos de blocos), localize a entrada do volume raiz. Se a opção Delete on termination (Excluir ao encerrar) for No, o volume será configurado para persistir.

AWS CLI

Para confirmar que um volume raiz está configurado para persistir

Use o comando describe-instances e verifique se o atributo `DeleteOnTermination` está definido como `false`.

```
aws ec2 describe-instances \
    --instance-id i-1234567890abcdef0 \
    --query "Reservations[].Instances[].BlockDeviceMappings"
```

O seguinte é um exemplo de saída.

```
[
    [
        {
            "DeviceName": "/dev/xvda",
            "Ebs": {
```

```
                "AttachTime": "2024-07-12T04:05:33.000Z",
                "DeleteOnTermination": false,
                "Status": "attached",
                "VolumeId": "vol-1234567890abcdef0"

        }
    ]
]
```

PowerShell

Para confirmar que um volume raiz está configurado para persistir

Use o cmdlet Get-EC2Instance e verifique se o atributo `DeleteOnTermination` está definido como `False`.

```
(Get-EC2Instance -InstanceId i-
i-1234567890abcdef0).Instances.BlockDeviceMappings.Ebs
```

O seguinte é um exemplo de saída.

```
AssociatedResource  :
AttachTime          : 7/12/2024 4:05:33 AM
DeleteOnTermination : False
Operator            :
Status              : attached
VolumeId            : vol-1234567890abcdef0
```

Substituir o volume raiz de uma instância do Amazon EC2 sem interrompê-la

O Amazon EC2 permite que você substitua o volume raiz do Amazon EBS por uma instância em execução retendo o seguinte:

- Dados armazenados em volumes de armazenamento de instâncias: os volumes de armazenamento de instâncias permanecem anexados à instância após a restauração do volume raiz.
- Dados armazenados em volumes de dados (não raiz) do Amazon EBS: os volumes não raiz do Amazon EBS permanecem anexados à instância após a restauração do volume raiz.

- Configuração de rede — Todas as interfaces de rede permanecem conectadas à instância e mantêm seus endereços IP, identificadores e IDs de anexo. Quando a instância fica disponível, todo o tráfego de rede pendente é liberado. Além disso, a instância permanece no mesmo host físico, portanto, mantém seus endereços IP públicos e privados e o nome DNS.
- Políticas do IAM — IAM os perfis e as políticas (como políticas baseadas em tags) associados à instância são mantidos e impostos.

Conteúdo

- Como funciona a substituição de volume raiz
- Considerações
- Substituir um volume raiz

Como funciona a substituição de volume raiz

Quando você substitui o volume raiz de uma instância, uma tarefa de substituição do volume raiz é criada. O volume raiz original é desvinculado da instância e o novo volume raiz é anexado à instância em seu lugar. O mapeamento de dispositivos de blocos da instância é atualizado para refletir a ID do volume raiz substituto.

Quando você substituir o volume raiz de uma instância, deverá especificar a origem do snapshot para o novo volume. As opções a seguir são possíveis.

Restaurar um volume raiz ao seu estado original

Essa opção substitui o volume raiz atual por um volume baseado no snapshot usado para criá-lo.

Considerações sobre o uso do estado de inicialização

O volume raiz substituto obtém o mesmo tipo, tamanho e exclusão nos atributos de encerramento do volume raiz original.

Substituir um volume raiz usando um snapshot

Essa opção substitui o volume raiz atual por um volume substituto baseado no snapshot que você especifica. Por exemplo, um snapshot específico que você criou antes usando esse volume raiz. Isso é útil se você precisar fazer uma recuperação depois de problemas causados porque o volume raiz foi corrompido por ou erros de configuração de rede no sistema operacional convidado.

O volume raiz substituto obtém o mesmo tipo, tamanho e exclusão nos atributos de encerramento do volume raiz original.

Considerações sobre o uso de um snapshot

- Só é possível usar snapshots criados diretamente dos volumes raiz atuais ou anteriores da instância.
- Não é possível usar cópias de snapshots criadas de snapshots que foram tirados do volume raiz.
- Após substituir o volume raiz com sucesso, você ainda pode usar os snapshots obtidos do volume raiz original para substituir o novo volume raiz (substituto).

Substituir o volume raiz usando uma AMI

Essa opção substitui o volume raiz atual usando uma AMI que você especifica. Isso é útil se você precisar realizar correções ou atualizações de sistemas operacionais e aplicações. A AMI deve ter o mesmo código de produto, informações de cobrança, tipo de arquitetura e tipo de virtualização que a instância.

Se a instância estiver habilitada para ENA ou sriov-net, você deverá usar uma AMI que ofereça suporte a esses recursos. Se a instância não estiver habilitada para ENA ou sriov-net, você poderá selecionar uma AMI que não inclua suporte para esses recursos ou adicionar suporte automaticamente se selecionar uma AMI compatível com ENA ou sriov-net.

Se a instância estiver habilitada para o NitroTPM, você deverá usar uma AMI que tenha o NitroTPM habilitado. O suporte ao NitroTPM não será habilitado se a instância não tiver sido configurada para ele, independentemente da AMI que você selecionar.

Você pode selecionar uma AMI com um modo de inicialização diferente do modo da instância, desde que a instância seja compatível com o modo de inicialização da AMI. Se a instância não for compatível com o modo de inicialização, a solicitação falhará. Se a instância for compatível com o modo de inicialização, o novo modo de inicialização será propagado para a instância e seus dados UEFI serão atualizados adequadamente. Se você tiver modificado a ordem de inicialização manualmente ou adicionado uma chave UEFI Secure Boot privada para carregar módulos privados do kernel, as alterações serão perdidas durante a substituição do volume raiz.

O volume raiz substituto obtém o mesmo tipo de volume e o mesmo atributo de exclusão ao encerrar do volume raiz original, e obtém o tamanho do mapeamento de dispositivos de blocos do volume raiz AMI.

> **Note**
>
> O tamanho do mapeamento de dispositivos de blocos de volume raiz da AMI deve ser igual ou maior que o tamanho do volume raiz original. Se o tamanho do mapeamento de dispositivos de blocos do volume raiz da AMI for menor que o tamanho do volume raiz original, a solicitação falhará.

Após a conclusão da tarefa de substituição do volume raiz, as seguintes informações novas e atualizadas são refletidas quando você descreve a instância usando o console, a AWS CLI ou AWS SDKs:

- ID da nova AMI
- ID de novo volume para o volume raiz
- Atualização da configuração do modo de inicialização (se alterada pela AMI)
- Atualização da configuração do NitroTPM (se habilitada pela AMI)
- Atualização da configuração do ENA (se habilitada pela AMI)
- Atualização da configuração de sriov-net (se habilitada pela AMI)

A ID da nova AMI também é refletida nos metadados da instância.

Considerações sobre o uso de uma AMI:

- Se você usar uma AMI que tenha vários mapeamentos de dispositivos de blocos, somente o volume raiz da AMI será usado. Os outros volumes (não raiz) serão ignorados.
- Você só poderá usar esse recurso se tiver permissões para a AMI e o respectivo snapshot de volume raiz associado. Não é possível usar esse recurso com AMIs do AWS Marketplace.
- Você só poderá usar uma AMI sem um código de produto se a instância não tiver um código de produto.
- O tamanho do mapeamento de dispositivos de blocos de volume raiz da AMI deve ser igual ou maior que o tamanho do volume raiz original. Se o tamanho do mapeamento de dispositivos de blocos do volume raiz da AMI for menor que o tamanho do volume raiz original, a solicitação falhará.
- Os documentos de identidade da instância são atualizados automaticamente.

- Se a instância for compatível com NitroTPM, os dados do nitroTPM da instância serão redefinidos e novas chaves serão geradas.

Após a conclusão do processo de substituição do volume raiz, você pode escolher se deseja manter o volume raiz original. Se você optar por excluir o volume raiz original após a conclusão do processo de substituição, o volume raiz original será automaticamente excluído e ficará irrecuperável. Se você escolher manter o volume raiz original após a conclusão do processo, o volume permanecerá provisionado em sua conta. Você deverá excluí-lo manualmente quando não precisar mais dele.

A tarefa de substituição de volume raiz passa pelos seguintes estados durante o processo:

- `pending`: o volume substituto está sendo criado.
- `in-progress`: o volume original está sendo desanexado e o volume substituto está sendo anexado.
- `succeeded`: o volume substituto foi anexado com sucesso à instância e ela está disponível.
- `failing`: a tarefa de substituição está em processo de falha.
- `failed`: houve falha na tarefa de substituição, mas o volume raiz original ainda está anexado.
- `failing-detached`: a tarefa de substituição está em processo de falha e a instância pode não ter um volume raiz anexado.
- `failed-detached`: houve falha na tarefa de substituição e a instância não tem um volume raiz anexado.

Se a tarefa de substituição do volume raiz falhar, a instância será reinicializada e o volume raiz original permanecerá anexado à instância.

Considerações

Antes de começar, considere o seguinte:

Requisitos

- A instância deve estar no estado `running`.
- A instância é reinicializada automaticamente durante o processo. O conteúdo da memória (RAM) é apagado durante a reinicialização. Não requer reinicializações manuais.
- Não é possível substituir o volume raiz se ele for um volume de armazenamento de instâncias. Só há compatibilidade com instâncias com volumes raiz do Amazon EBS.

- Você pode substituir o volume raiz de todos os tipos de instâncias virtualizadas e instâncias bare metal do EC2 Mac. Nenhum outro tipo de instância bare metal é compatível.
- Só é possível usar snapshots criados diretamente dos volumes raiz atuais ou anteriores da instância.
- Se sua conta estiver habilitada para Criptografia do Amazon EBS por padrão na região atual, o volume raiz de substituição criado pela tarefa de substituição do volume raiz será sempre criptografado, independentemente do status de criptografia do snapshot especificado ou do volume raiz da AMI especificada.

Resultados da criptografia

A tabela a seguir resume os possíveis resultados da criptografia.

	Volume raiz original	Snapshot ou AMI especificado	Criptografia por padrão	Volume raiz substituto	Chave de criptografia usada para o volume raiz substituto
Restaurar o volume raiz substituto para o estado de execução inicial	Criptografado	Não aplicável	Não considerado	Criptografado	Mesma chave do KMS do volume raiz original
	Não criptografado	Não aplicável	Desabilitado	Não criptografado	Não aplicável
	Não criptografado	Não aplicável	Habilitada	Criptografado	Conta chave KMS padrão para criptografia do Amazon EBS
Restaurar o volume raiz	Criptografado	Não criptografado	Não considerado	Criptografado	Mesma chave do

	Volume raiz original	Snapshot ou AMI especificado	Criptografia por padrão	Volume raiz substituto	Chave de criptografia usada para o volume raiz substituto
de substituição a partir do snapshot ou da AMI					KMS do volume raiz original
	Criptografado	Criptografado	Não considerado	Criptografado	Mesma chave do KMS do volume raiz original
	Não criptografado	Não criptografado	Desabilitado	Não criptografado	Não aplicável
	Não criptografado	Não criptografado	Habilitada	Criptografado	Contachave KMS padrão para criptografia do Amazon EBS

	Volume raiz original	Snapshot ou AMI especificado	Criptografia por padrão	Volume raiz substituto	Chave de criptografia usada para o volume raiz substituto
	Não criptografado	Criptografado	Não considerado	Criptografado	Se a AMI ou o snapshot pertencer à conta, o volume de substituição será criptografado com a chave do KMS da AMI ou do snapshot. Se a AMI ou o snapshot for compartilhados com a conta, o volume de substituição será criptografado com a chave do KMS padrão para criptografia do Amazon EBS da conta.

Substituir um volume raiz

Quando você substitui o volume raiz de uma instância, uma tarefa de substituição do volume raiz é criada. É possível usar a tarefa de substituição de volume raiz para monitorar o progresso e o resultado do processo de substituição.

Console

Para substituir o volume raiz

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância que será substituída pelo volume raiz e escolha Actions (Ações), Monitor and troubleshoot (Monitorar e solucionar problemas) e Replace root volume (Substituir volume raiz).

   > **Note**
   >
   > A ação Replace root volume (Substituir volume raiz) estará desabilitada se a instância selecionada não estiver no estado `running`.

4. Em Restaurar, escolha uma das seguintes opções:

   - Estado de inicialização: restaurar o volume raiz substituto a partir do snapshot que foi usado para criar o volume raiz atual.
   - Instantâneo: restaurar o volume raiz de substituição para o instantâneo que você especificar. Em Snapshot, selecione o snapshot a ser usado.
   - Imagem: restaurar o volume raiz substituto usando a AMI que você especificar. Em Imagem, selecione a AMI a ser usada.

5. (Opcional) Em Taxa de inicialização do volume, você pode especificar, em MiB/s, a taxa provisionada do Amazon EBS para inicialização do volume (taxa de inicialização do volume) na qual os blocos de snapshot devem ser baixados do Amazon S3 para o volume. Para obter mais informações, consulte Use an Amazon EBS Provisioned Rate for Volume Initialization. Para usar a taxa de inicialização padrão ou a restauração rápida de snapshots (se habilitada para o snapshot selecionado), não especifique nenhuma taxa.
6. (Opcional) Para excluir o volume raiz que você está substituindo, selecione Excluir volume raiz substituído.

7. Escolha Criar tarefa de substituição.
8. Para monitorar a tarefa de substituição, escolha a guia Armazenamento para a instância e expanda Tarefas recentes de substituição do volume raiz.

AWS CLI

Para restaurar o volume raiz substituto para o estado de execução

Use o comando create-replace-root-volume-task. Em `--instance-id`, especifique o ID da instância para a qual deseja substituir o volume raiz. Omita os parâmetros `--snapshot-id` e `--image-id`. Para excluir o volume raiz original após ele ter sido substituído, inclua `--delete-replaced-root-volume` e especifique `true`. Para especificar a taxa de inicialização do volume na qual os blocos de snapshot são baixados do Amazon S3 para o volume, para `--volume-initialization-rate`, especifique um valor entre `100` e `300` MiB/s.

```
aws ec2 create-replace-root-volume-task \
--instance-id i-1234567890abcdef0 \
--delete-replaced-root-volume \
--volume-initialization-rate 150
```

Para restaurar o volume raiz em um snapshot específico

Use o comando create-replace-root-volume-task. Em `--instance-id`, especifique o ID da instância para a qual deseja substituir o volume raiz. Em `--snapshot-id`, especifique o ID do snapshot a ser usado. Para excluir o volume raiz original após ele ter sido substituído, inclua `--delete-replaced-root-volume` e especifique `true`. Para especificar a taxa de inicialização do volume na qual os blocos de snapshot são baixados do Amazon S3 para o volume, para `--volume-initialization-rate`, especifique um valor entre `100` e `300` MiB/s.

```
aws ec2 create-replace-root-volume-task \
--instance-id i-1234567890abcdef0 \
--snapshot-id snap-9876543210abcdef0 \
--delete-replaced-root-volume \
--volume-initialization-rate 150
```

Para restaurar o volume raiz substituto usando uma AMI

Use o comando create-replace-root-volume-task. Em `--instance-id`, especifique o ID da instância para a qual deseja substituir o volume raiz. Em `--image-id`, especifique o ID da

AMI a ser usada. Para excluir o volume raiz original após ele ter sido substituído, inclua `--delete-replaced-root-volume` e especifique `true`. Para especificar a taxa de inicialização do volume na qual os blocos de snapshot são baixados do Amazon S3 para o volume, para `--volume-initialization-rate`, especifique um valor entre `100` e `300` MiB/s.

```
aws ec2 create-replace-root-volume-task \
--instance-id i-1234567890abcdef0 \
--image-id ami-09876543210abcdef \
--delete-replaced-root-volume \
--volume-initialization-rate 150
```

Para visualizar o status de uma tarefa de substituição de volume raiz

Use o comando describe-replace-root-volume-tasks e especifique os IDs das tarefas de substituição do volume raiz a serem visualizadas.

```
aws ec2 describe-replace-root-volume-tasks \
    --replace-root-volume-task-ids replacevol-1234567890abcdef0 \
    --query ReplaceRootVolumeTasks[].TaskState
```

O seguinte é um exemplo de saída.

```
[
    "succeeded"
]
```

Como alternativa, especifique o filtro `instance-id` para filtrar os resultados por instância.

```
$ aws ec2 describe-replace-root-volume-tasks \
    --filters Name=instance-id,Values=i-1234567890abcdef0
```

PowerShell

Para restaurar o volume raiz substituto para o estado de execução

Use o comando New-EC2ReplaceRootVolumeTask. Em `-InstanceId`, especifique o ID da instância para a qual deseja substituir o volume raiz. Omita os parâmetros `-SnapshotId` e `-ImageId`. Para excluir o volume raiz original após ele ter sido substituído, inclua `-DeleteReplacedRootVolume` e especifique `$true`. Para especificar a taxa de inicialização

do volume na qual os blocos de snapshot são baixados do Amazon S3 para o volume, para `-VolumeInitializationRate`, especifique um valor entre `100` e `300` MiB/s.

```
New-EC2ReplaceRootVolumeTask `
    -InstanceId i-1234567890abcdef0 `
    -VolumeInitializationRate 150 `
    -DeleteReplacedRootVolume $true
```

Para restaurar o volume raiz em um snapshot específico

Use o comando New-EC2ReplaceRootVolumeTask. Em `--InstanceId`, especifique o ID da instância para a qual deseja substituir o volume raiz. Em `-SnapshotId`, especifique o ID do snapshot a ser usado. Para excluir o volume raiz original após ele ter sido substituído, inclua `-DeleteReplacedRootVolume` e especifique `$true`. Para especificar a taxa de inicialização do volume na qual os blocos de snapshot são baixados do Amazon S3 para o volume, para `-VolumeInitializationRate`, especifique um valor entre `100` e `300` MiB/s.

```
New-EC2ReplaceRootVolumeTask `
    -InstanceId i-1234567890abcdef0 `
    -SnapshotId snap-9876543210abcdef0 `
    -VolumeInitializationRate 150 `
    -DeleteReplacedRootVolume $true
```

Para restaurar o volume raiz substituto usando uma AMI

Use o comando New-EC2ReplaceRootVolumeTask. Em `-InstanceId`, especifique o ID da instância para a qual deseja substituir o volume raiz. Em `-ImageId`, especifique o ID da AMI a ser usada. Para excluir o volume raiz original após ele ter sido substituído, inclua `-DeleteReplacedRootVolume` e especifique `$true`. Para especificar a taxa de inicialização do volume na qual os blocos de snapshot são baixados do Amazon S3 para o volume, para `-VolumeInitializationRate`, especifique um valor entre `100` e `300` MiB/s.

```
New-EC2ReplaceRootVolumeTask `
    -InstanceId i-1234567890abcdef0 `
    -ImageId ami-0abcdef1234567890 `
    -VolumeInitializationRate 150 `
    -DeleteReplacedRootVolume $true
```

Para visualizar o status de uma tarefa de substituição de volume raiz

Use o comando Get-EC2ReplaceRootVolumeTask e especifique os IDs das tarefas de substituição do volume raiz a serem visualizadas.

```
(Get-EC2ReplaceRootVolumeTask `
    -ReplaceRootVolumeTaskIds replacevol-1234567890abcdef0).TaskState.Value
```

O seguinte é um exemplo de saída.

```
Succeeded
```

Como alternativa, especifique o filtro `instance-id` para filtrar os resultados por instância.

```
PS C:\> Get-EC2ReplaceRootVolumeTask -Filters @{Name = 'instance-id'; Values =
 'i-1234567890abcdef0'} | Format-Table
```

Nomes de dispositivos para volumes em instâncias do Amazon EC2

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 do Amazon EBS para instâncias do Amazon EC2.

Conteúdo

- Nomes de dispositivos disponíveis
- Considerações sobre nomes de dispositivos

Nomes de dispositivos disponíveis

Instâncias do Linux

Há dois tipos de virtualização disponíveis para instâncias do Linux: paravirtual (PV) e máquina virtual de hardware (HVM). O tipo de virtualização de uma instância é determinado pela AMI usada para

executar a instância. Todos os tipos de instância são compatíveis com AMIs HVM. Alguns tipos de instância da geração anterior oferecem suporte a AMIs PV. Observe o tipo de virtualização da AMI, pois os nomes de dispositivos recomendados e disponíveis que é possível usar dependem do tipo de virtualização da instância. Para obter mais informações, consulte Tipos de virtualização.

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	Available (Disponível)	Reservado para volume raiz	Recomendado para volumes de dados do EBS	Volumes de armazenamento de instâncias
Paravirtual	/dev/sd[a-z] /dev/sd[a-z][1-15] /dev/hd[a-z] /dev/hd[a-z][1-15]	/dev/sda1	/dev/sd[f-p] /dev/sd[f-p][1-6]	/dev/sd[b-e]
HVM	/dev/sd[a-z] /dev/xvd[a-c][a-z] /dev/xvdd[a-x]	Difere por AMI /dev/sda1 ou /dev/xvda	/dev/sd[b-z] /dev/xvdb[b-z] *	/dev/sd[b-e] /dev/sd [] BH (h1.16xlarge) /dev/sd[b-y] (d2.8xlarge) /dev/sd[b-i] (i2.8xlarge) **

* Os nomes de dispositivo que você especifica para volumes NVMe do EBS no mapeamento de dispositivos de blocos são renomeados usando nomes de dispositivo de NVMe (`/dev/nvme[0-26]n1`). O driver do dispositivo de blocos pode atribuir nomes de dispositivos NVMe em uma ordem diferente da especificada para os volumes no mapeamento de dispositivos de blocos.

** Os volumes de armazenamento de instâncias NVMe são automaticamente enumerados e atribuídos a um nome de dispositivo NVMe.

Instâncias do Windows

As AMIs do Windows da AWS usam um dos seguintes conjuntos de drivers para permitir acesso ao hardware virtualizado:

- AWS PV: Drivers paravirtuais para as instâncias do Windows
- AWS NVMe: AWSDrivers NVMe

Nomes de dispositivos para instâncias baseadas no Nitro

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 a uma instância baseada no Nitro.

Tipo de driver	Available (Disponível)	Reservado para volume raiz	Recomendado para volumes do EBS	Volumes de armazenamento de instâncias
AWS NVMe	xvd[a-z] xvd[a-c][a-z] xvdd[a-x] /dev/sda1	/dev/sda1	xvd[b-z] xvdb[b-z]	*

* Os volumes de armazenamento de instâncias NVMe são automaticamente enumerados e atribuídos a um letra de unidade do Windows.

Nomes de dispositivos para instâncias baseadas no Xen

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 a uma instância baseada no Xen.

Tipo de driver	Available (Disponível)	Reservado para volume raiz	Recomendado para volumes do EBS	Volumes de armazenamento de instâncias
AWS PV	xvd[b-z] xvd[b-c][a-z] /dev/sda1 /dev/sd[b-e]	/dev/sda1	xvd[f-z]	xvdc[a-x] xvd[a-e]
Citrix PV (não tem mais suporte)	xvd[b-z] xvd[b-c][a-z] /dev/sda1 /dev/sd[b-e]	/dev/sda1	xvd[f-z]	xvdc[a-x] xvd[a-e]
Red Hat PV (não tem mais suporte)	xvd[a-z] xvd[b-c][a-z] /dev/sda1 /dev/sd[b-e]	/dev/sda1	xvd[f-p]	xvdc[a-x] xvd[a-e]

Para obter mais informações sobre volumes de armazenamento de instâncias, consulte Armazenamento em bloco temporário do armazenamento de instância para instâncias do EC2. Para obter mais informações sobre volumes do EBS do NVMe (instâncias baseadas em Nitro), incluindo como identificar o dispositivo do EBS, consulte Amazon EBS e NVMe no Guia do usuário do Amazon EBS.

Considerações sobre nomes de dispositivos

Lembre-se do seguinte ao selecionar um nome de dispositivo:

- A parte final dos nomes de dispositivos que você usar não deve se sobrepor, pois isso poderia causar problemas ao iniciar a instância. Por exemplo, evite usar combinações como `/dev/xvdf` e `xvdf` para volumes anexados à mesma instância.
- 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 instância de NVMe são enumerados automaticamente e recebem um nome de dispositivo de NVMe (instâncias do Linux) ou uma letra de unidade do Windows (instâncias do Windows).
- (Instâncias do Windows) As AMIs do Windows da AWS vêm com um software adicional que prepara uma instância quando ela é inicializada pela primeira vez. Ele é o serviço EC2Config (AMIs do Windows de versões anteriores ao Windows Server 2016) ou EC2Launch (Windows Server 2016 e posterior). Após o mapeamento nas unidades, os dispositivos são inicializados e montados. A unidade raiz é inicializada e montada como `C:\`. Por padrão, quando um volume do EBS é anexado a uma instância do Windows, ele poderá ser mostrado como qualquer letra de unidade na instância. É possível alterar as configurações para definir as letras dos volumes de acordo com suas especificações. Para volumes de armazenamento de instâncias, o padrão depende do driver . AWS Os drivers PV e Citrix PV atribuem aos volumes de armazenamento de instância letras que vão de Z: a A: Os drivers do Red Hat atribuem aos volumes de armazenamento da instância letras de unidades que vão de D: a Z:. Para obter mais informações, consulte Agentes de inicialização do Windows em instâncias do Windows do Amazon EC2 e Como os volumes são anexados e mapeados para instâncias Windows do Amazon EC2.
- (Instâncias do Linux) Dependendo do driver de dispositivo de blocos do kernel, o dispositivo pode ser anexado com um nome diferente do especificado. Por exemplo, se você especificar um nome de dispositivo de `/dev/sdh`, o dispositivo poderá ser renomeado como `/dev/xvdh` ou `/dev/hdh`. Na maioria dos casos, a letra à direita permanece a mesma. Em algumas versões do Red Hat Enterprise Linux (e suas variantes, como o CentOS), a letra à direita pode ser alterada (`/dev/sda` pode se tornar `/dev/xvde`). Nesses casos, a letra à direita de cada nome de dispositivo é aumentada no mesmo número de vezes. Por exemplo, se `/dev/sdb` é renomeado `/dev/xvdf`, então `/dev/sdc` é renomeado `/dev/xvdg`. O Amazon Linux cria um link simbólico para o nome que você especificou no dispositivo renomeado. Outros sistemas operacionais podem se comportar de maneira diferente.
- (Instâncias do Linux) As AMIs de HVM não oferecem suporte ao uso de números finais em nomes de dispositivos, com exceção de `/dev/sda1`, que é destinado ao volume raiz, e `/dev/sda2`.

Embora o uso de /dev/sda2 seja possível, não recomendamos o uso desse mapeamento de dispositivo com instâncias HVM.

- (Instâncias do Linux) Ao usar as AMIs PV, não é possível anexar volumes que compartilhem as mesmas letras de dispositivo com e sem dígitos finais. 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, use dígitos à direita em todos os nomes de dispositivos que compartilham as mesmas letras base (como /dev/sdc1, /dev/sdc2, /dev/sdc3).
- (Instâncias do Linux) Alguns kernels personalizados podem ter restrições que limitam o uso a /dev/sd[f-p] ou a /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].

Antes de especificar o nome do dispositivo selecionado, verifique se ele está disponível. Caso contrário, você receberá um erro informando que o nome de dispositivo já está em uso. Para visualizar os dispositivos de disco e seus pontos de montagem, use o comando lsblk (instâncias do Linux), ou o utilitário Gerenciamento de Disco ou o comando diskpart (instâncias do Windows).

Mapeamento de dispositivos de blocos para volumes em instâncias do Amazon EC2

Cada instância que você inicia conta com um volume raiz associado, que pode ser um volume do Amazon EBS ou um volume de armazenamento de instância. Use mapeamentos 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. É possível associar volumes adicionais do EBS a uma instância em execução. Contudo, a única forma de associar volumes de armazenamento de instâncias a uma instância é usar mapeamentos de dispositivos de blocos para anexá-los à medida que a instância é executada.

Conteúdo

- Conceitos de mapeamento de dispositivos de blocos
- Adicionar mapeamentos de dispositivos de blocos a uma AMI
- Adicionar mapeamentos de dispositivos de blocos a uma instância do Amazon EC2

Conceitos de mapeamento de dispositivos de blocos

Um dispositivo de blocos é um dispositivo de armazenamento que move dados em sequências de bytes ou de bits (blocos). Esses dispositivos oferecem suporte ao acesso aleatório e geralmente usam E/S em buffer. Os exemplos incluem discos rígidos, unidades de CD-ROM e pen-drives. Um dispositivo de blocos pode ser fisicamente ligado a um computador ou acessado remotamente, como se estivesse ligado fisicamente ao computador.

O Amazon EC2 oferece suporte a dois tipos de dispositivo de blocos:

- Volumes de armazenamento de instâncias (dispositivos virtuais cujo hardware subjacente é ligado fisicamente ao computador host da instância)
- Volumes EBS (dispositivos de armazenamento remoto)

Um mapeamento de dispositivos de blocos define os dispositivos de blocos (volumes de armazenamento de instâncias e volumes do EBS) para anexar a uma instância. É possível 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, é possível 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
- Advertências do armazenamento de instâncias de mapeamento de dispositivos de blocos
- Exemplo de mapeamento de dispositivos de blocos
- Como os dispositivos são disponibilizados no sistema operacional

Entradas do mapeamento de dispositivos de blocos

Ao criar um mapeamento de dispositivos de blocos, é preciso especificar as informações a seguir para cada dispositivo de blocos que você precisa associar à instância:

- O nome de dispositivo usado no Amazon EC2. O driver de dispositivo de blocos da instância atribui o nome real do volume ao montar o volume. O nome atribuído pode ser diferente do nome

recomendado pelo Amazon EC2. Para obter mais informações, consulte Nomes de dispositivos para volumes em instâncias do Amazon EC2.

Para volumes de armazenamento de instâncias, você também especifica as seguintes informações:

- O dispositivo virtual: `ephemeral[0-23]`. Observe que o número e o tamanho de volumes de armazenamento de instâncias disponíveis variam por tipo de instância.

Para volumes de armazenamento de instâncias NVMe, as seguintes informações também se aplicam:

- Esses volumes são automaticamente enumerados e atribuídos a um nome de dispositivo; incluí-los no mapeamento de dispositivos de blocos não surtirá nenhum efeito.

Para volumes do EBS, você também especifica as seguintes informações:

- O ID do snapshot a ser usado para criar o dispositivo de blocos (snap-xxxxxxxx). Esse valor é opcional, desde que você especifique um tamanho do volume. Você não pode especificar a ID de snapshots arquivados.
- O tamanho do volume em GiB. O tamanho especificado deve ser maior que ou igual ao tamanho do snapshot especificado.
- Se o volume deve ser excluído no encerramento da instância (`true` ou `false`). Por padrão, o volume raiz tem o valor `true`, enquanto os volumes anexados têm o valor `false`. Quando você cria a AMI, o mapeamento de dispositivos de blocos dele herda essa configuração da instância. Quando você executa uma instância, ela herda essa configuração da AMI.
- O tipo de volume, que pode ser `gp2` e `gp3` para SSD de uso geral, `io1` e `io2` para SSD de IOPS provisionadas, `st1` para HDD otimizado para throughput, `sc1` para HDD a frio ou `standard` para magnético.
- O número de operações de entrada/saída por segundo (IOPS) que o volume é capaz de suportar. (Usado apenas com volumes `io1` e `io2`.)
- Alguns tipos de instância oferecem suporte a mais de um cartão EBS. Você pode selecionar o cartão EBS para o volume a ser anexado especificando o índice do cartão EBS. Para obter mais informações, consulte Cartões EBS.

Advertências do armazenamento de instâncias de mapeamento de dispositivos de blocos

Há várias advertências a serem consideradas ao executar instâncias com os AMIs que têm volumes de armazenamento de instâncias em seus mapeamentos de dispositivos de blocos.

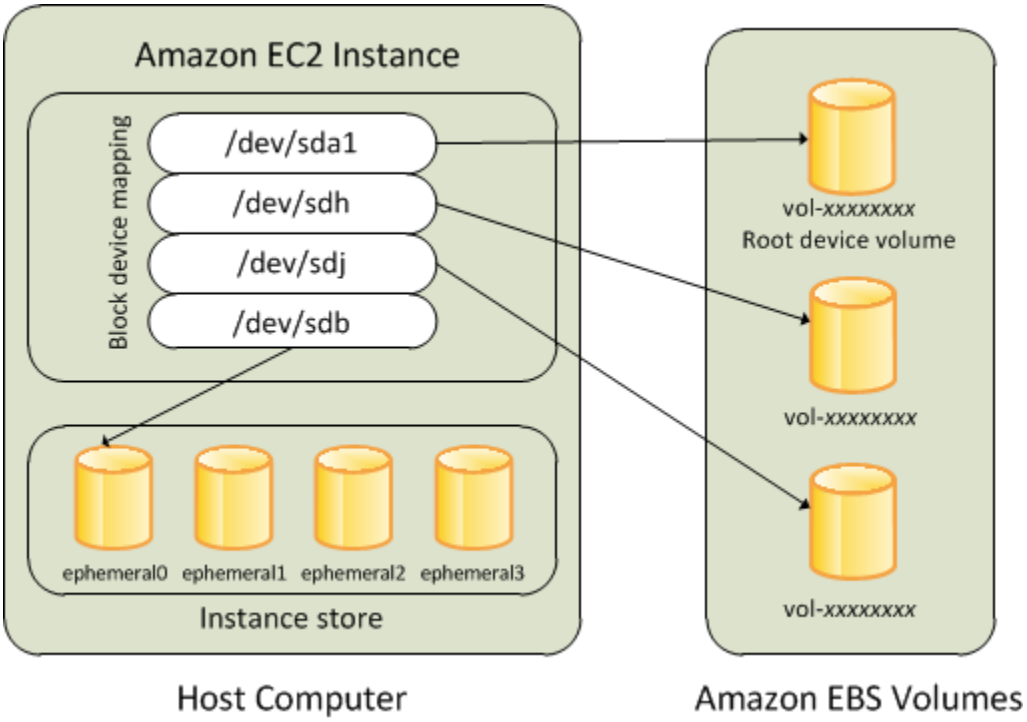
- Alguns tipos de instância incluem mais volumes de armazenamento de instâncias que outros, e alguns tipos de instância não contêm nenhum volume de armazenamento de instâncias. Se seu tipo de instância for compatível com um volume de armazenamento de instâncias e o AMI tiver mapeamentos para dois volumes de armazenamento de instâncias, a instância será executada com um volume de armazenamento de instâncias.
- Volumes de armazenamento de instâncias só podem ser mapeados no momento da execução. Você não pode interromper uma instância sem volumes de armazenamento de instâncias (como `t2.micro`), alterar a instância para um tipo que suporte os volumes de armazenamento de instâncias e reiniciem a instância com volumes de armazenamento de instâncias. No entanto, é possível 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 aceito 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. Especifique 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`. Além disso, isso indica qual volume do EBS é o volume raiz, identificado como `/dev/sda1`.



Observe que esse exemplo de mapeamento de dispositivos de blocos é utilizado em exemplos de comandos e APIs neste tópico. É possível encontrar os exemplos de comandos e APIs que criam mapeamentos de dispositivos de blocos em Especificar um mapeamento de dispositivos de blocos para uma AMI e Atualizar o mapeamento de dispositivos de blocos ao executar uma instância.

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.

Instâncias do Linux: os nomes de dispositivos especificados no mapeamento de dispositivos de blocos são mapeados para os dispositivos de blocos correspondentes quando a instância é inicializada pela primeira vez. O tipo de instância determina quais volumes de armazenamento de instâncias são formatados e montados por padrão. É possível 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 em bloco temporário do armazenamento de instância para instâncias do EC2. O driver do dispositivo de blocos para a instância determina quais dispositivos são usados quando os volumes são formatados e montados.

Instâncias do Windows: os nomes de dispositivos especificados no mapeamento de dispositivos de blocos são mapeados para os dispositivos de bloco correspondentes quando a instância é inicializada pela primeira vez e, em seguida, o serviço Ec2Config inicializa e monta as unidades. O volume raiz está configurado para ser montado como `C:\`. Os volumes de armazenamento de instâncias são montados como `Z:\`, `Y:\`, etc. Quando um volume do EBS é montado, isso pode acontecer usando qualquer letra de unidade disponível. No entanto, é possível configurar como as letras de unidade são atribuídas aos volumes do EBS. Para obter mais informações, consulte the section called “Agentes de inicialização do Windows”.

Adicionar mapeamentos de dispositivos de blocos a uma 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. Para adicionar mais dispositivos de blocos a uma AMI, crie sua própria AMI.

Tópicos

- Especificar um mapeamento de dispositivos de blocos para uma AMI
- Visualizar os volumes do EBS em um mapeamento de dispositivo de blocos da AMI

Especificar um mapeamento de dispositivos de blocos para uma AMI

Há duas maneiras de especificar volumes além do volume do dispositivo raiz ao criar uma AMI. Se você já tiver associado volumes a uma instância em execução antes de criar uma AMI pela instância, o mapeamento de dispositivos de blocos para a AMI incluirá os mesmos volumes. Para volumes do EBS, os dados existentes são salvos em um novo snapshot, e é esse novo snapshot que é especificado no mapeamento de dispositivos de blocos. Para volumes de armazenamento de instâncias, os dados não são preservados.

Para AMI baseados em EBS, é possível adicionar volumes do EBS e volumes de armazenamento de instâncias usando um mapeamento de dispositivos de blocos. Em uma AMI baseada no Amazon S3, é possível adicionar volumes de armazenamento de instância apenas alterando as entradas do mapeamento de dispositivos de blocos no arquivo de manifesto da imagem durante o registro da AMI.

> **Note**
>
> Para instâncias M3, especifique 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.

Console

Para adicionar volumes a uma AMI

1. Abra o console do Amazon EC2.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione uma instância e escolha Actions (Ações), Image and templates (Imagem e modelos), Create image (Criar imagem).
4. Insira um nome e uma descrição para a imagem.
5. Os volumes de instância aparecem em Volumes de instância (Volumes de instância). Para adicionar outro volume, escolha Add volume (Adicionar volume).
6. Em Volume type (Tipo de volume), escolha o tipo de volume. Para Device (Dispositivo), escolha o nome do dispositivo. Para um volume do EBS, é possível especificar detalhes adicionais, como um snapshot, o tamanho do volume, o tipo de volume, IOPS e estado de criptografia.
7. Escolha Create Image (Criar imagem).

AWS CLI

Para adicionar volumes a uma AMI

Use o comando create-image para especificar um mapeamento de dispositivos de blocos para uma AMI com EBS. Use o comando register-image para especificar um mapeamento de dispositivos de blocos para uma AMI baseada no Amazon S3.

Especifique o mapeamento de dispositivos de blocos usando o parâmetro `--block-device-mappings`. Você pode especificar argumentos codificados em JSON diretamente na linha de comando ou referenciando um arquivo JSON, como mostrado aqui.

```
--block-device-mappings file://mapping.json
```

Para adicionar um volume de armazenamento de instâncias, use o mapeamento a seguir. Observe que os volumes de armazenamento de instância NVMe são adicionados automaticamente.

```
{
    "DeviceName": "device_name",
    "VirtualName": "ephemeral0"
}
```

Para adicionar um volume vazio do de 100 GiB, use o mapeamento a seguir.

```
{
    "DeviceName": "device_name",
    "Ebs": {
      "VolumeSize": 100
    }
}
```

Para adicionar um volume do EBS com base em um snapshot, use o mapeamento a seguir.

```
{
    "DeviceName": "device_name",
    "Ebs": {
      "SnapshotId": "snap-1234567890abcdef0"
    }
}
```

Para omitir um mapeamento de um dispositivo, use o mapeamento a seguir:

```
{
```

```
    "DeviceName": "device_name",
    "NoDevice": ""
}
```

PowerShell

Use o cmdlet New-EC2Image para especificar um mapeamento de dispositivos de blocos para uma AMI baseada no EBS. Use o cmdlet Register-EC2Image para especificar um mapeamento de dispositivos de blocos para uma AMI baseada no Amazon S3.

Adicione a opção `-BlockDeviceMapping`, especificando as atualizações em `bdm`:

```
-BlockDeviceMapping $bdm
```

O exemplo a seguir adiciona um volume com base em um snapshot.

```
$ebd = New-Object -TypeName Amazon.EC2.Model.EbsBlockDevice
$ebd.SnapshotId = "snap-1234567890abcdef0"
$bdm = New-Object -TypeName Amazon.EC2.Model.BlockDeviceMapping
$bdm.DeviceName = "device_name"
$bdm.Ebs = $ebd
```

O mapeamento a seguir adiciona um volume vazio de 100 GB.

```
$ebd = New-Object -TypeName Amazon.EC2.Model.EbsBlockDevice
$ebd.VolumeSize = 100
$bdm = New-Object -TypeName Amazon.EC2.Model.BlockDeviceMapping
$bdm.DeviceName = "device_name"
$bdm.Ebs = $ebd
```

Visualizar os volumes do EBS em um mapeamento de dispositivo de blocos da AMI

É possível facilmente enumerar volumes do EBS no mapeamento de dispositivos de blocos para AMI.

Console

Para visualizar os volumes do EBS de uma AMI

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, você pode acessar as seguintes informações sobre o volume raiz, sendo que o termo dispositivo raiz tem o mesmo significado de volume raiz:

   - Root Device Type (Tipo de dispositivo raiz (`ebs`)
   - Root Device Name (Nome do dispositivo raiz) (por exemplo, `/dev/sda1`)
   - Block Devices (Dispositivos de blocos) (por exemplo, `/dev/sda1=snap-1234567890abcdef0:8:true`)

   Se a AMI tiver sido criada com volumes do EBS adicionais usando um mapeamento de dispositivos de blocos, o campo Block Devices (Dispositivos de blocos) exibirá o mapeamento desses volumes adicionais também. (Essa tela não exibe volumes de armazenamento de instâncias.)

AWS CLI

Para visualizar os volumes do EBS de uma AMI

Use o comando describe-images.

```
aws ec2 describe-images \
    --image-ids ami-0abcdef1234567890 \
    --query Image[0].BlockDeviceMappings
```

PowerShell

Para visualizar os volumes do EBS de uma AMI

Use o cmdlet Get-EC2Image.

```
(Get-EC2Image -ImageId ami-0abcdef1234567890).BlockDeviceMappings
```

Adicionar mapeamentos de dispositivos de blocos a uma instância do Amazon EC2

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. É possível 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.

Limitações

- 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, especifique um snapshot cujo tamanho seja igual ou maior que o tamanho do snapshot especificado no mapeamento de dispositivos de blocos da AMI.

Tarefas

- Atualizar o mapeamento de dispositivos de blocos ao executar uma instância
- Atualizar o mapeamento de dispositivos de blocos de uma instância em execução
- Visualizar os volumes do EBS em um mapeamento de dispositivos de blocos de instância
- Visualizar o mapeamento de dispositivos de blocos de instância para volumes de armazenamento de instâncias

Atualizar o mapeamento de dispositivos de blocos ao executar uma instância

É possível adicionar volumes do EBS e volumes de armazenamento de instâncias a uma instância quando iniciá-la. Observe que atualizar o mapeamento de dispositivos de blocos para uma instância não cria uma alteração permanente no mapeamento de dispositivos de blocos da AMI do qual ela foi executada.

Console

Para atualizar os volumes para uma instância na inicialização

1. Siga o procedimento para inicializar uma instância, mas não inicialize a instância até concluir as etapas a seguir para atualizar os volumes.

2. (Opcional) Para adicionar um volume, escolha Configurar armazenamento, Adicionar novo volume. Selecione o tamanho e o tipo de volume.
3. (Opcional) Para suprimir um volume que foi especificado pelo mapeamento de dispositivos de blocos da AMI, escolha Configurar armazenamento, Remover.
4. (Opcional) Para modificar a configuração de um volume do EBS, no painel Configurar armazenamento, escolha Avançado. Expanda as informações do volume e faça as alterações necessárias.
5. No painel Resumo, analise a configuração da instância e selecione Iniciar instância. Para obter mais informações, consulte Executar uma instância do EC2 usando o assistente de inicialização de instâncias no console.

AWS CLI

Para atualizar os volumes para uma instância na inicialização

Use o comando run-instances com a opção `--block-device-mappings`.

```
--block-device-mappings file://mapping.json
```

Por exemplo, vamos supor que o mapeamento de dispositivos de blocos de uma AMI especifique o seguinte:

- `/dev/xvda`: volume raiz do EBS
- `/dev/sdh`: volume do EBS criado de `snap-1234567890abcdef0`
- `/dev/sdj`: volume vazio do EBS com um tamanho de `100`
- `/dev/sdb`: volume de armazenamento de instância `ephemeral0`

Suponha que o seguinte seja o mapeamento de dispositivos de blocos da instância em `mapping.json`.

```
[
    {
        "DeviceName": "/dev/xvda",
        "Ebs": {
            "VolumeSize": 100
        }
    },
```

```
    {
        "DeviceName": "/dev/sdj",
        "NoDevice": ""
    },
    {
        "DeviceName": "/dev/sdh",
        "Ebs": {
            "VolumeSize": 300
        }
    },
    {
        "DeviceName": "/dev/sdc",
        "VirtualName": "ephemeral1"
    }
]
```

O mapeamento de dispositivos de blocos da instância faz o seguinte:

- Substitui o tamanho do volume raiz (`/dev/xvda`) para 100 GiB.
- Impede que `/dev/sdj` se vincule à instância.
- Substitui o tamanho de `/dev/sdh` para 300 GiB. Observe que você não precisa especificar o ID de snapshot novamente.
- Adiciona um volume efêmero, `/dev/sdc`. Se o tipo de instância não for compatível com múltiplos volumes de armazenamento de instância, esse mapeamento não surtirá efeito. Se o tipo de instância for compatível com volumes NVMe de armazenamento de instância, eles serão enumerados automaticamente e incluídos no mapeamento de dispositivos de blocos da instância e não poderão ser substituídos.

PowerShell

Para atualizar os volumes para uma instância na inicialização

Use o parâmetro `-BlockDeviceMapping` com o cmdlet New-EC2Instance com o parâmetro `-BlockDeviceMapping`.

```
-BlockDeviceMapping $bdm
```

Suponha que o seguinte seja o mapeamento de dispositivos de blocos da instância em `$bdm`.

```
$bdm = @()
```

```
$root = New-Object -TypeName Amazon.EC2.Model.BlockDeviceMapping
$root.DeviceName = "/dev/xvda"
$ebs1 = New-Object -TypeName Amazon.EC2.Model.EbsBlockDevice
$ebs1.VolumeSize = 100
$root.Ebs = $ebs1
$bdm += $root

$sdj = New-Object -TypeName Amazon.EC2.Model.BlockDeviceMapping
$sdj.DeviceName = "/dev/sdj"
$sdj.NoDevice = ""
$bdm += $sdj

$sdh = New-Object -TypeName Amazon.EC2.Model.BlockDeviceMapping
$sdh.DeviceName = "/dev/sdh"
$ebs2 = New-Object -TypeName Amazon.EC2.Model.EbsBlockDevice
$ebs2.VolumeSize = 300
$sdh.Ebs = $ebs2
$bdm += $sdh

$sdc = New-Object -TypeName Amazon.EC2.Model.BlockDeviceMapping
$sdc.DeviceName = "/dev/sdc"
$sdc.VirtualName = "ephemeral1"
$bdm += $sdc
```

O mapeamento de dispositivos de blocos da instância faz o seguinte:

- Substitui o tamanho do volume raiz (`/dev/xvda`) para 100 GiB.
- Impede que `/dev/sdj` se vincule à instância.
- Substitui o tamanho de `/dev/sdh` para 300 GiB. Observe que você não precisa especificar o ID de snapshot novamente.
- Adiciona um volume efêmero, `/dev/sdc`. Se o tipo de instância não for compatível com múltiplos volumes de armazenamento de instância, esse mapeamento não surtirá efeito. Se o tipo de instância for compatível com volumes NVMe de armazenamento de instância, eles serão enumerados automaticamente e incluídos no mapeamento de dispositivos de blocos da instância e não poderão ser substituídos.

Atualizar o mapeamento de dispositivos de blocos de uma instância em execução

Você não precisa parar a instância para alterar esse atributo.

AWS CLI

Para atualizar o mapeamento de dispositivos de blocos de uma instância em execução

Use o comando modify-instance-attribute.

Adicione a opção `--block-device-mappings`:

```
--block-device-mappings file://mapping.json
```

Em `mapping.json`, especifique as atualizações. Por exemplo, a atualização a seguir atualiza o volume raiz para que os dados sejam mantidos de forma persistente.

```
[
  {
    "DeviceName": "/dev/sda1",
    "Ebs": {
      "DeleteOnTermination": false
    }
  }
]
```

PowerShell

Para atualizar o mapeamento de dispositivos de blocos de uma instância em execução

Use o cmdlet Edit-EC2InstanceAttribute.

Adicione a opção `-BlockDeviceMapping`:

```
-BlockDeviceMapping $bdm
```

Em `bdm`, especifique as atualizações. Por exemplo, a atualização a seguir atualiza o volume raiz para que os dados sejam mantidos de forma persistente.

```
$ebd = New-Object -TypeName Amazon.EC2.Model.EbsBlockDevice
$ebd.DeleteOnTermination = false
$bdm = New-Object -TypeName Amazon.EC2.Model.BlockDeviceMapping
$bdm.DeviceName = "/dev/sda1"
$bdm.Ebs = $ebd
```

Visualizar os volumes do EBS em um mapeamento de dispositivos de blocos de instância

É possível facilmente enumerar volumes do EBS para a instância.

Console

Para visualizar os volumes do EBS de uma instância

1. Abra o console do Amazon EC2.
2. No painel de navegação, escolha Instâncias.
3. Selecione a instância e veja os detalhes exibidos na guia Armazenamento. No mínimo, você pode acessar as seguintes informações sobre o volume raiz, sendo que o termo dispositivo raiz tem o mesmo significado de volume raiz:

   - Root device type (Tipo de dispositivo raiz) (por exemplo, EBS)
   - Root Device Name (Nome do dispositivo raiz) (por exemplo, `/dev/xvda`)
   - Dispositivos de blocos (por exemplo, `/dev/xvda`, `/dev/sdf` e `/dev/sdj`)

   Se a instância tiver sido executada com volumes adicionais do EBS usando um mapeamento de dispositivo de bloco, eles aparecerão em Block devices (Dispositivos de bloco). Nenhum dos volumes de armazenamento de instâncias aparece nesta guia.
4. Para exibir informações adicionais sobre um volume do EBS, escolha seu ID de volume para ir para a página de volume.

AWS CLI

Para visualizar os volumes do EBS de uma instância

Use o comando describe-instances.

```
aws ec2 describe-instances \
    --instance-ids i-1234567890abcdef0 \
    --query Reservations[*].Instances[0].BlockDeviceMappings
```

PowerShell

Para visualizar os volumes do EBS de uma instância

Use o cmdlet Get-EC2Instance.

```
(Get-EC2Instance -InstanceId i-0bac57d7472c89bac).Instances.BlockDeviceMappings
```

Visualizar o mapeamento de dispositivos de blocos de instância para volumes de armazenamento de instâncias

O tipo de instância determina o número e o tipo de volumes de armazenamento de instância que estão disponíveis para a instância. Se o número de volumes de armazenamento de instâncias em um mapeamento de dispositivos de blocos exceder o número de volumes de armazenamento de instâncias disponível para uma instância, os volumes adicionais serão ignorados. Para visualizar os volumes de armazenamento de instância da instância, execute o comando lsblk (instâncias do Linux) ou abra o Gerenciamento de Disco do Windows (instâncias do Windows). Para saber a quantidade de volumes de armazenamento de instância que são compatíveis com cada tipo de instância, consulte Amazon EC2 instance type specifications.

Quando você vir o mapeamento de dispositivos de blocos para sua instância, verá somente os volumes do EBS, não os volumes de armazenamento de instâncias. O método a ser usado para visualizar os volumes de armazenamento de instâncias para a instância depende do tipo de volume.

Volumes de armazenamento de instâncias do NVMe

Instâncias do Linux

É possível usar o pacote de linha de comando do NVMe, nvme-cli, para consultar os volumes de armazenamento de instâncias do NVMe no mapeamento de dispositivos de blocos. Faça download e instale o pacote de sua instância e execute o seguinte comando.

```
[ec2-user ~]$ sudo nvme list
```

Este é um exemplo de saída de uma instância. O texto na coluna Modelo indica se o volume é um volume do EBS ou um volume do armazenamento de instâncias. Neste exemplo, tanto `/dev/nvme1n1` como `/dev/nvme2n1` são volumes de armazenamento de instâncias.

```
Node             SN                   Model
 Namespace
---------------- -------------------- ----------------------------------------
 ---------
```

```
/dev/nvme0n1     vol06afc3f8715b7a597 Amazon Elastic Block Store             1

/dev/nvme1n1     AWS2C1436F5159EB6614 Amazon EC2 NVMe Instance Storage       1

/dev/nvme2n1     AWSB1F4FF0C0A6C281EA Amazon EC2 NVMe Instance Storage       1
  ...
```

Instâncias do Windows

É possível utilizar o Gerenciamento de disco ou o PowerShell para listar volumes NVMe do EBS e do armazenamento de instâncias. Para obter mais informações, consulte the section called “Mapear discos NVMe para volumes”.

Volumes de armazenamento de instâncias HDD ou SSD

É possível usar os metadados da instância para consultar os volumes de armazenamento de instâncias HDD ou SSD no mapeamento de dispositivos de blocos. Os volumes de armazenamento de instâncias NVMe não estão incluídos.

O URI de base de todas as solicitações de metadados da instância é `http://169.254.169.254/latest/`. Para obter mais informações, consulte Usar metadados da instância para gerenciar a instância do EC2.

Instâncias do Linux

Primeiro, conecte-se à instância em execução. Com base na instância, use esta consulta para obter o mapeamento de dispositivos de blocos.

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/block-device-mapping/
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/block-device-mapping/
```

A resposta inclui o nome dos dispositivo de blocos para a instância. Por exemplo, a saída de uma instância `m1.small` com armazenamento de instância é semelhante a esta:

```
ami
ephemeral0
root
swap
```

O dispositivo `ami` corresponde ao volume raiz do ponto de vista da instância. Os volumes de armazenamento de instâncias têm o nome `ephemeral[0-23]`. O dispositivo `swap` é para o arquivo da página. Se você também tiver mapeado os volumes do EBS, eles serão exibidos como `ebs1`, `ebs2`, etc.

Para obter detalhes sobre um dispositivo de blocos individual no mapeamento de dispositivos de blocos, coloque o nome dele na consulta anterior, como mostrado aqui.

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/block-device-mapping/ephemeral0
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/block-device-mapping/ephemeral0
```

Instâncias do Windows

Primeiro, conecte-se à instância em execução. Com base na instância, use esta consulta para obter o mapeamento de dispositivos de blocos.

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/block-device-mapping/
```

A resposta inclui o nome dos dispositivo de blocos para a instância. Por exemplo, a saída de uma instância `m1.small` com armazenamento de instância é semelhante a esta:

```
ami
ephemeral0
root
```

```
swap
```

O dispositivo `ami` corresponde ao volume raiz do ponto de vista da 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.

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/block-device-mapping/ephemeral0
```

Como os volumes são anexados e mapeados para instâncias Windows do Amazon EC2

> **Note**
>
> Este tópico se aplica somente a instâncias do Windows.

Sua instância do Windows vem com um volume do EBS que serve como o volume raiz. Se sua instância do Windows usar os drivers AWS PV ou Citrix PV, é possível adicionar até 25 volumes, contabilizando um total de 26 volumes. Para obter mais informações, consulte Limites de volume do Amazon EBS para instâncias do Amazon EC2.

Dependendo do tipo de sua instância, você terá de 0 a 24 volumes de armazenamento de instâncias possíveis disponíveis para a instância. Para usar qualquer um dos volumes de armazenamento de instâncias que estão disponíveis para a instância, você deverá especificá-los ao criar sua AMI ou executar a instância. Também é possível adicionar volumes do EBS ao criar sua AMI ou executar a instância ou anexá-los enquanto a instância estiver em execução.

Quando você adicionar um volume à sua instância, especifique o nome do dispositivo que o Amazon EC2 usa. Para ter mais informações, consulte Nomes de dispositivos para volumes em instâncias do Amazon EC2. AWS As imagens de máquina da Amazon (AMIs) do Windows contêm um conjunto de drivers que são usados pelo Amazon EC2 para mapear o armazenamento de instância e os volumes do EBS aos discos e a letras de unidade do Windows.

Métodos para mapear discos para volumes do EBS

- Mapear discos NVMe em uma instância Amazon EC2 Windows para volumes
- Mapear discos não NVMe em uma instância Amazon EC2 Windows para volumes

Mapear discos NVMe em uma instância Amazon EC2 Windows para volumes

Com instâncias baseadas em Nitro, os volumes do EBS são expostos como dispositivos NVMe. Este tópico explica como visualizar os discos NVMe que estão disponíveis para o sistema operacional Windows na sua instância. Também mostra como mapear esses discos NVMe para os volumes subjacentes do Amazon EBS e os nomes de dispositivos especificados para os mapeamentos de dispositivos de blocos usados pelo Amazon EC2.

Tópicos

- Listar discos NVMe
- Mapear discos NVMe para volumes

Listar discos NVMe

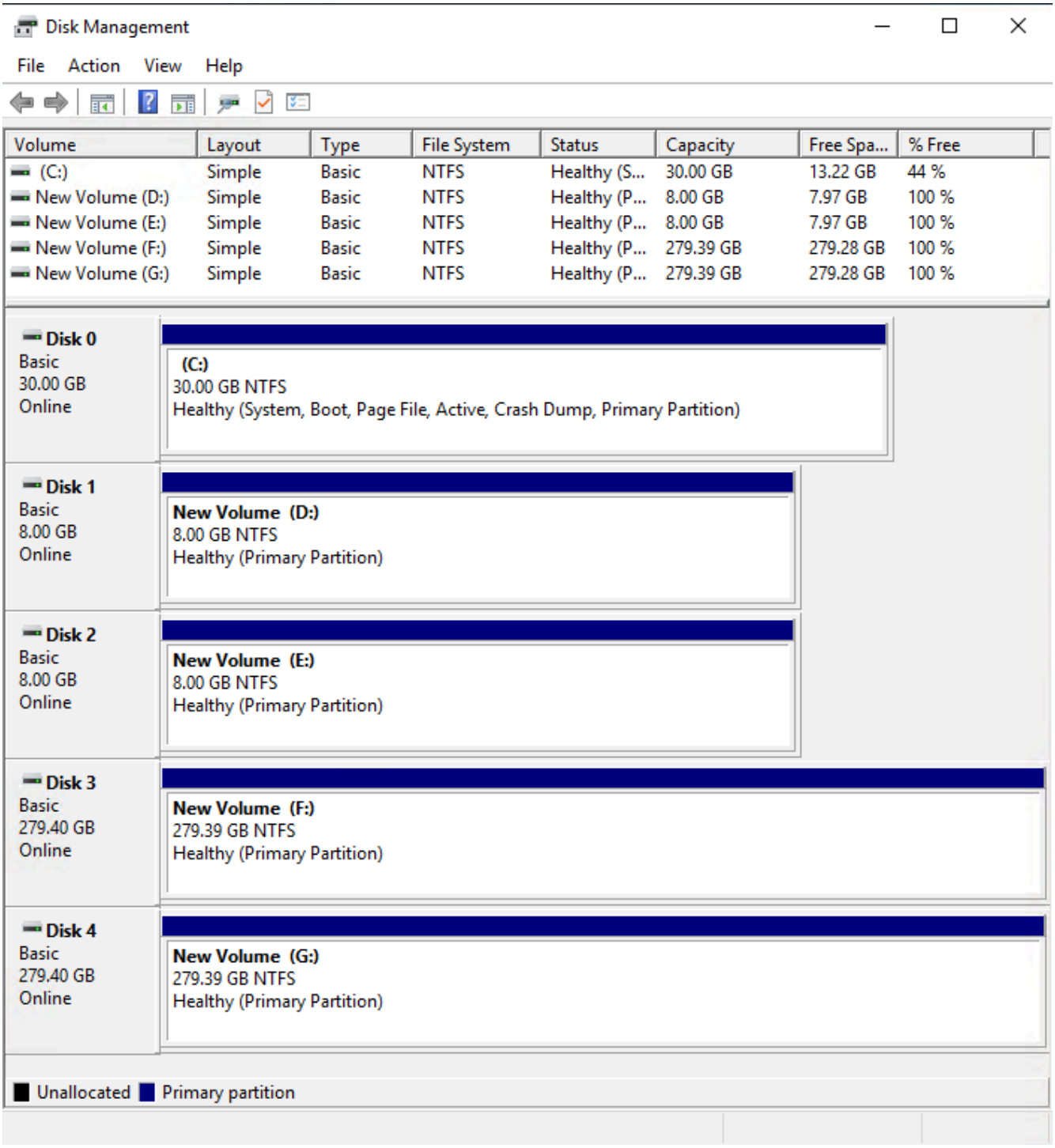
É possível encontrar os discos na instância do Windows usando Gerenciamento de disco ou Powershell.

Disk Management

Para localizar os discos em sua instância do Windows

1. Execute a sessão da sua instância do Windows usando o Desktop Remoto. Para obter mais informações, consulte Conectar-se à instância do Windows no usando RDP.
2. Inicie o utilitário de Gerenciamento de Disco.
3. Revise os discos. O volume raiz é um volume do EBS montado como `C:\`. Se não houver nenhum outro disco mostrado, você não especificou volumes adicionais quando criou a AMI ou executou a instância.

   Veja a seguir um exemplo que mostra os discos disponíveis se você executar uma instância `r5d.4xlarge` com dois volumes adicionais do EBS.



PowerShell

O script do PowerShell a seguir lista cada disco e seu nome de dispositivo e volume correspondentes. Destina-se ao uso com instâncias baseadas em Nitro, que usam volumes de armazenamento de instância e do EBS de NVMe.

Conecte-se à sua instância do Windows e execute o seguinte comando para habilitar a execução de script do PowerShell.

```
Set-ExecutionPolicy RemoteSigned
```

Copie o script a seguir e salve-o como `mapping.ps1` na instância do Windows.

```
# List the disks for NVMe volumes

function Get-EC2InstanceMetadata {
    param([string]$Path)
    (Invoke-WebRequest -Uri "http://169.254.169.254/latest/$Path").Content
}

function GetEBSVolumeId {
    param($Path)
    $SerialNumber = (Get-Disk -Path $Path).SerialNumber
    if($SerialNumber -clike 'vol*'){
        $EbsVolumeId = $SerialNumber.Substring(0,20).Replace("vol","vol-")
    }
    else {
       $EbsVolumeId = $SerialNumber.Substring(0,20).Replace("AWS","AWS-")
    }
    return $EbsVolumeId
}

function GetDeviceName{
    param($EbsVolumeId)
    if($EbsVolumeId -clike 'vol*'){

        $Device  = ((Get-EC2Volume -VolumeId $EbsVolumeId ).Attachment).Device
        $VolumeName = ""
    }
     else {
        $Device = "Ephemeral"
        $VolumeName = "Temporary Storage"
    }
    Return $Device,$VolumeName
}

function GetDriveLetter{
    param($Path)
    $DiskNumber =  (Get-Disk -Path $Path).Number
```

```
    if($DiskNumber -eq 0){
        $VirtualDevice = "root"
        $DriveLetter = "C"
        $PartitionNumber = (Get-Partition -DriveLetter C).PartitionNumber
    }
    else
    {
        $VirtualDevice = "N/A"
        $DriveLetter = (Get-Partition -DiskNumber $DiskNumber).DriveLetter
        if(!$DriveLetter)
        {
            $DriveLetter = ((Get-Partition -DiskId $Path).AccessPaths).Split(",")[0]
        }
        $PartitionNumber = (Get-Partition -DiskId $Path).PartitionNumber
    }

    return $DriveLetter,$VirtualDevice,$PartitionNumber

}

$Report = @()
foreach($Path in (Get-Disk).Path)
{
    $Disk_ID = ( Get-Partition -DiskId $Path).DiskId
    $Disk = ( Get-Disk -Path $Path).Number
    $EbsVolumeId  = GetEBSVolumeId($Path)
    $Size =(Get-Disk -Path $Path).Size
    $DriveLetter,$VirtualDevice, $Partition = (GetDriveLetter($Path))
    $Device,$VolumeName = GetDeviceName($EbsVolumeId)
    $Disk = New-Object PSObject -Property @{
      Disk          = $Disk
      Partitions    = $Partition
      DriveLetter   = $DriveLetter
      EbsVolumeId   = $EbsVolumeId
      Device        = $Device
      VirtualDevice = $VirtualDevice
      VolumeName= $VolumeName
    }
 $Report += $Disk
}

$Report | Sort-Object Disk | Format-Table -AutoSize -Property Disk, Partitions,
 DriveLetter, EbsVolumeId, Device, VirtualDevice, VolumeName
```

Execute o script da seguinte forma:

```
PS C:\> .\mapping.ps1
```

Veja a seguir um exemplo de saída para uma instância com um volume raiz, dois volumes do EBS e dois volumes de armazenamento de instâncias.

```
Disk Partitions DriveLetter EbsVolumeId           Device    VirtualDevice VolumeName
---- ---------- ----------- -----------           ------    ------------- ----------
   0          1 C           vol-03683f1d861744bc7 /dev/sda1 root
   1          1 D           vol-082b07051043174b9 xvdb      N/A
   2          1 E           vol-0a4064b39e5f534a2 xvdc      N/A
   3          1 F           AWS-6AAD8C2AEEE1193F0 Ephemeral N/A           Temporary
 Storage
   4          1 G           AWS-13E7299C2BD031A28 Ephemeral N/A           Temporary
 Storage
```

Se você não tiver fornecido suas credenciais do Tools for Windows PowerShell na instância do Windows, o script não poderá obter o ID de volume do EBS e usará N/A na coluna `EbsVolumeId`.

Mapear discos NVMe para volumes

Você pode usar o comando Get-Disk para mapear os números de disco do Windows para volumes do Amazon EBS e volumes de armazenamento de instância do Amazon EC2.

```
PS C:\> Get-Disk
Number Friendly Name Serial Number                    HealthStatus
 OperationalStatus      Total Size Partition

                      Style
------ ------------- -------------                    ------------
 -----------------      ---------- ----------
3      NVMe Amazo... AWS6AAD8C2AEEE1193F0_00000001.   Healthy              Online
              279.4 GB MBR
4      NVMe Amazo... AWS13E7299C2BD031A28_00000001.   Healthy              Online
              279.4 GB MBR
2      NVMe Amazo... vol0a4064b39e5f534a2_00000001.   Healthy              Online
                  8 GB MBR
0      NVMe Amazo... vol03683f1d861744bc7_00000001.   Healthy              Online
                 30 GB MBR
```

```
1      NVMe Amazo... vol082b07051043174b9_00000001.   Healthy              Online
                8 GB MBR
```

Também é possível executar o comando ebsnvme-id para mapear números de disco do NVMe para IDs de volume do EBS e nomes de dispositivos.

```
PS C:\> C:\PROGRAMDATA\Amazon\Tools\ebsnvme-id.exe
Disk Number: 0
Volume ID: vol-03683f1d861744bc7
Device Name: sda1

Disk Number: 1
Volume ID: vol-082b07051043174b9
Device Name: xvdb

Disk Number: 2
Volume ID: vol-0a4064b39e5f534a2
Device Name: xvdc
```

Mapear discos não NVMe em uma instância Amazon EC2 Windows para volumes

Para instâncias executadas com uma AMI do Windows que use drivers AWS PV ou Citrix PV, será possível usar as relações descritas nesta página para mapear os discos do Windows ao seu armazenamento de instâncias e volumes do EBS. Este tópico explica como visualizar os discos não NVMe que estão disponíveis para o sistema operacional Windows na sua instância. Também mostra como mapear esses discos não NVMe para os volumes subjacentes do Amazon EBS e os nomes de dispositivos especificados para os mapeamentos de dispositivos de blocos usados pelo Amazon EC2.

> **Note**
>
> Se você executar uma instância Se sua AMI da Windows usar drivers Red Hat PV, é possível atualizar sua instância para usar os drivers Citrix. Para obter mais informações, consulte the section called “Atualizar drivers de PV”.

Tópicos

- Listar discos não NVMe

- Mapear discos não NVMe para volumes

Listar discos não NVMe

É possível encontrar os discos na instância do Windows usando o Gerenciamento de disco ou o Powershell.

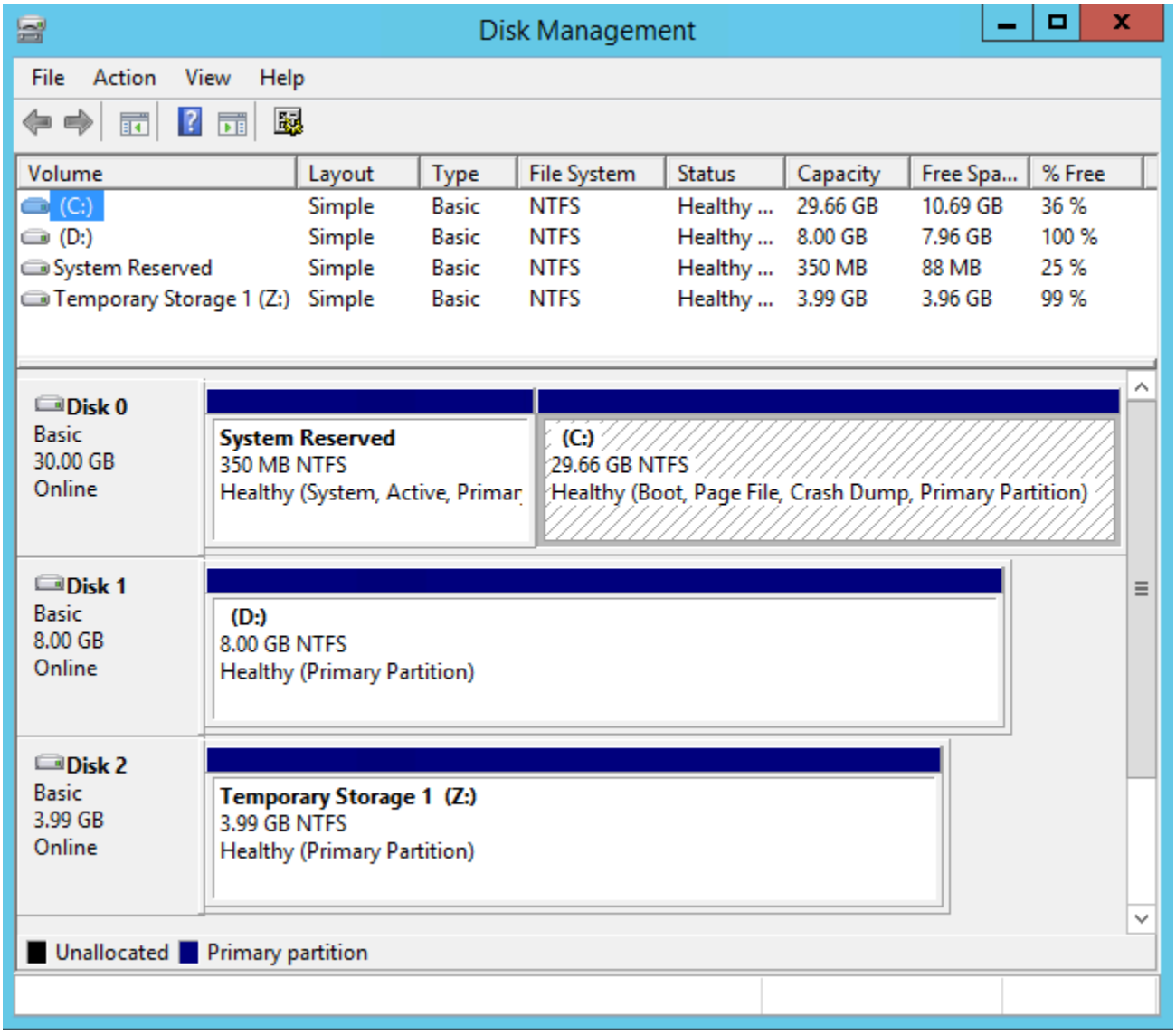
Disk Management

Para localizar os discos em sua instância do Windows

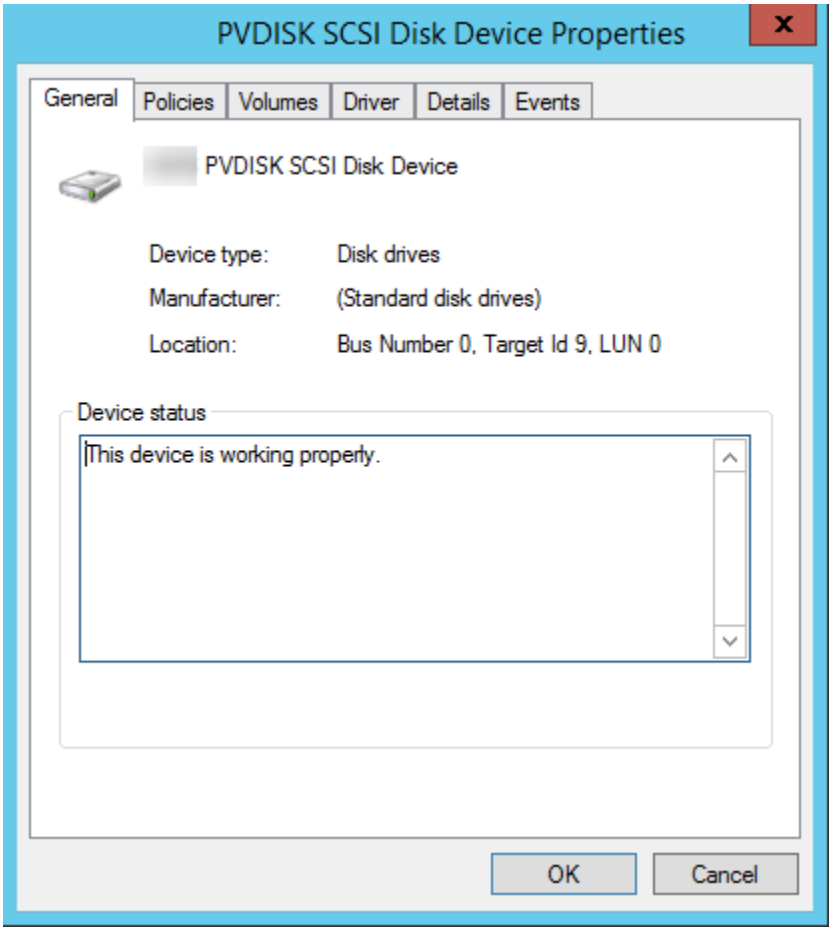
1. Execute a sessão da sua instância do Windows usando o Desktop Remoto. Para obter mais informações, consulte Conectar-se à instância do Windows no usando RDP.
2. Inicie o utilitário de Gerenciamento de Disco.

   Na barra de tarefas, clique com o botão direito do mouse no logotipo do Windows e escolha Gerenciamento de disco.
3. Revise os discos. O volume raiz é um volume do EBS montado como `C:\`. Se não houver nenhum outro disco mostrado, você não especificou volumes adicionais quando criou a AMI ou executou a instância.

   Veja a seguir um exemplo que mostra os discos que estão disponíveis se você executar uma instância `m3.medium` com um volume de armazenamento de instâncias (disco 2) e um volume do EBS adicional (disco 1).



4. Clique com o botão direito no painel cinza identificado como Disco 1 e selecione Properties (Propriedades). Observe o valor de Location (Local) e procure-o nas tabelas em Mapear discos não NVMe para volumes. Por exemplo, o seguinte disco tem o Número de barramento de local 0, ID de destino 9, LUN 0. De acordo com a tabela de volumes do EBS, o nome do dispositivo para esse local é `xvdj`.



PowerShell

O script do PowerShell a seguir lista cada disco e seu nome de dispositivo e volume correspondentes.

Requisitos e limitações

- Requer o Windows Server 2012 ou posterior.
- Requer credenciais para obter o ID de volume do EBS. É possível configurar um perfil usando o Tools for PowerShell, ou anexar uma função do IAM à instância.
- Não suporta volumes NVMe.
- Não suporta discos dinâmicos.

Conecte-se à sua instância do Windows e execute o seguinte comando para habilitar a execução de script do PowerShell.

```
Set-ExecutionPolicy RemoteSigned
```

Copie o script a seguir e salve-o como `mapping.ps1` na instância do Windows.

```
# List the disks
function Convert-SCSITargetIdToDeviceName {
  param([int]$SCSITargetId)
  If ($SCSITargetId -eq 0) {
    return "sda1"
  }
  $deviceName = "xvd"
  If ($SCSITargetId -gt 25) {
    $deviceName += [char](0x60 + [int]($SCSITargetId / 26))
  }
  $deviceName += [char](0x61 + $SCSITargetId % 26)
  return $deviceName
}

[string[]]$array1 = @()
[string[]]$array2 = @()
[string[]]$array3 = @()
[string[]]$array4 = @()

Get-WmiObject Win32_Volume | Select-Object Name, DeviceID | ForEach-Object {
  $array1 += $_.Name
  $array2 += $_.DeviceID
}

$i = 0
While ($i -ne ($array2.Count)) {
  $array3 += ((Get-Volume -Path $array2[$i] | Get-Partition | Get-
Disk).SerialNumber) -replace "_[^ ]*$" -replace "vol", "vol-"
  $array4 += ((Get-Volume -Path $array2[$i] | Get-Partition | Get-
Disk).FriendlyName)
  $i ++
}

[array[]]$array = $array1, $array2, $array3, $array4

Try {
  $InstanceId = Get-EC2InstanceMetadata -Category "InstanceId"
  $Region = Get-EC2InstanceMetadata -Category "Region" | Select-Object -
ExpandProperty SystemName
```

```
}
Catch {
  Write-Host "Could not access the instance Metadata using AWS Get-
EC2InstanceMetadata CMDLet.
Verify you have AWSPowershell SDK version '3.1.73.0' or greater installed and
 Metadata is enabled for this instance." -ForegroundColor Yellow
}
Try {
  $BlockDeviceMappings = (Get-EC2Instance -Region $Region -Instance
 $InstanceId).Instances.BlockDeviceMappings
  $VirtualDeviceMap = (Get-EC2InstanceMetadata -Category
 "BlockDeviceMapping").GetEnumerator() | Where-Object { $_.Key -ne "ami" }
}
Catch {
  Write-Host "Could not access the AWS API, therefore, VolumeId is not available.
Verify that you provided your access keys or assigned an IAM role with adequate
 permissions." -ForegroundColor Yellow
}

Get-disk | ForEach-Object {
  $DriveLetter = $null
  $VolumeName = $null
  $VirtualDevice = $null
  $DeviceName = $_.FriendlyName

  $DiskDrive = $_
  $Disk = $_.Number
  $Partitions = $_.NumberOfPartitions
  $EbsVolumeID = $_.SerialNumber -replace "_[^ ]*$" -replace "vol", "vol-"
  if ($Partitions -ge 1) {
    $PartitionsData = Get-Partition -DiskId $_.Path
    $DriveLetter = $PartitionsData.DriveLetter | Where-object { $_ -notin @("",
 $null) }
    $VolumeName = (Get-PSDrive | Where-Object { $_.Name -in
 @($DriveLetter) }).Description | Where-object { $_ -notin @("", $null) }
  }
  If ($DiskDrive.path -like "*PROD_PVDISK*") {
    $BlockDeviceName = Convert-SCSITargetIdToDeviceName((Get-WmiObject -Class
 Win32_Diskdrive | Where-Object { $_.DeviceID -eq ("\\.\PHYSICALDRIVE" +
 $DiskDrive.Number) }).SCSITargetId)
    $BlockDeviceName = "/dev/" + $BlockDeviceName
    $BlockDevice = $BlockDeviceMappings | Where-Object { $BlockDeviceName -like "*"
 + $_.DeviceName + "*" }
    $EbsVolumeID = $BlockDevice.Ebs.VolumeId
```

```
    $VirtualDevice = ($VirtualDeviceMap.GetEnumerator() | Where-Object { $_.Value -
eq $BlockDeviceName }).Key | Select-Object -First 1
  }
  ElseIf ($DiskDrive.path -like "*PROD_AMAZON_EC2_NVME*") {
    $BlockDeviceName = (Get-EC2InstanceMetadata -Category
 "BlockDeviceMapping")."ephemeral$((Get-WmiObject -Class Win32_Diskdrive | Where-
Object { $_.DeviceID -eq ("\\.\PHYSICALDRIVE" + $DiskDrive.Number) }).SCSIPort - 2)"
    $BlockDevice = $null
    $VirtualDevice = ($VirtualDeviceMap.GetEnumerator() | Where-Object { $_.Value -
eq $BlockDeviceName }).Key | Select-Object -First 1
  }
  ElseIf ($DiskDrive.path -like "*PROD_AMAZON*") {
    if ($DriveLetter -match '[^a-zA-Z0-9]') {
      $i = 0
      While ($i -ne ($array3.Count)) {
        if ($array[2][$i] -eq $EbsVolumeID) {
          $DriveLetter = $array[0][$i]
          $DeviceName = $array[3][$i]
        }
        $i ++
      }
    }
    $BlockDevice = ""
    $BlockDeviceName = ($BlockDeviceMappings | Where-Object { $_.ebs.VolumeId -eq
 $EbsVolumeID }).DeviceName
  }
  ElseIf ($DiskDrive.path -like "*NETAPP*") {
    if ($DriveLetter -match '[^a-zA-Z0-9]') {
      $i = 0
      While ($i -ne ($array3.Count)) {
        if ($array[2][$i] -eq $EbsVolumeID) {
          $DriveLetter = $array[0][$i]
          $DeviceName = $array[3][$i]
        }
        $i ++
      }
    }
    $EbsVolumeID = "FSxN Volume"
    $BlockDevice = ""
    $BlockDeviceName = ($BlockDeviceMappings | Where-Object { $_.ebs.VolumeId -eq
 $EbsVolumeID }).DeviceName
  }
  Else {
    $BlockDeviceName = $null
```

```
    $BlockDevice = $null
  }
  New-Object PSObject -Property @{
    Disk          = $Disk;
    Partitions    = $Partitions;
    DriveLetter   = If ($DriveLetter -eq $null) { "N/A" } Else { $DriveLetter };
    EbsVolumeId   = If ($EbsVolumeID -eq $null) { "N/A" } Else { $EbsVolumeID };
    Device        = If ($BlockDeviceName -eq $null) { "N/A" } Else
 { $BlockDeviceName };
    VirtualDevice = If ($VirtualDevice -eq $null) { "N/A" } Else { $VirtualDevice };
    VolumeName    = If ($VolumeName -eq $null) { "N/A" } Else { $VolumeName };
    DeviceName    = If ($DeviceName -eq $null) { "N/A" } Else { $DeviceName };
  }
} | Sort-Object Disk | Format-Table -AutoSize -Property Disk, Partitions,
 DriveLetter, EbsVolumeId, Device, VirtualDevice, DeviceName, VolumeName
```

Execute o script da seguinte forma:

```
PS C:\> .\mapping.ps1
```

A seguir está um exemplo de saída.

```
Disk  Partitions  DriveLetter   EbsVolumeId            Device      VirtualDevice
 DeviceName              VolumeName
----  ----------  -----------   -----------            ------      -------------
 ----------              ----------
   0           1            C   vol-0561f1783298efedd   /dev/sda1   N/A
 NVMe Amazon Elastic B   N/A
   1           1            D   vol-002a9488504c5e35a   xvdb        N/A
 NVMe Amazon Elastic B   N/A
   2           1            E   vol-0de9d46fcc907925d   xvdc        N/A
 NVMe Amazon Elastic B   N/A
```

Se você não tiver fornecido suas credenciais na instância do Windows, o script não poderá obter o ID de volume do EBS e usará N/A na coluna `EbsVolumeId`.

Mapear discos não NVMe para volumes

O driver de dispositivo de blocos da instância distribui os nomes de volume reais ao montar volumes.

Mapeamentos

- Volumes de armazenamento de instâncias
- Volumes do EBS

Volumes de armazenamento de instâncias

A tabela a seguir descreve como os drivers Citrix PV e AWS PV mapeiam volumes de armazenamento de instâncias não NVMe a volumes do Windows. O número de volumes de armazenamento de instâncias disponíveis é determinado pelo tipo de instância. Para obter mais informações, consulte Limites de volume de armazenamento de instância para instâncias do EC2.

Local	Nome do dispositivo
Barramento número 0, ID de destino 78, LUN 0	xvdca
Barramento número 0, ID de destino 79, LUN 0	xvdcb
Barramento número 0, ID de destino 80, LUN 0	xvdcc
Barramento número 0, ID de destino 81, LUN 0	xvdcd
Barramento número 0, ID de destino 82, LUN 0	xvdce
Barramento número 0, ID de destino 83, LUN 0	xvdcf
Barramento número 0, ID de destino 84, LUN 0	xvdcg
Barramento número 0, ID de destino 85, LUN 0	xvdch
Barramento número 0, ID de destino 86, LUN 0	xvdci
Barramento número 0, ID de destino 87, LUN 0	xvdcj
Barramento número 0, ID de destino 88, LUN 0	xvdck
Barramento número 0, ID de destino 89, LUN 0	xvdcl

Volumes do EBS

A tabela a seguir descreve como os drivers Citrix PV e AWS PV mapeiam volumes do EBS não NVME a volumes do Windows.

Local	Nome do dispositivo
Barramento número 0, ID de destino 0, LUN 0	/dev/sda1
Barramento número 0, ID de destino 1, LUN 0	xvdb
Barramento número 0, ID de destino 2, LUN 0	xvdc
Barramento número 0, ID de destino 3, LUN 0	xvdd
Barramento número 0, ID de destino 4, LUN 0	xvde
Barramento número 0, ID de destino 5, LUN 0	xvdf
Barramento número 0, ID de destino 6, LUN 0	xvdg
Barramento número 0, ID de destino 7, LUN 0	xvdh
Barramento número 0, ID de destino 8, LUN 0	xvdi
Barramento número 0, ID de destino 9, LUN 0	xvdj
Barramento número 0, ID de destino 10, LUN 0	xvdk
Barramento número 0, ID de destino 11, LUN 0	xvdl
Barramento número 0, ID de destino 12, LUN 0	xvdm
Barramento número 0, ID de destino 13, LUN 0	xvdn
Barramento número 0, ID de destino 14, LUN 0	xvdo
Barramento número 0, ID de destino 15, LUN 0	xvdp
Barramento número 0, ID de destino 16, LUN 0	xvdq
Barramento número 0, ID de destino 17, LUN 0	xvdr

Local	Nome do dispositivo
Barramento número 0, ID de destino 18, LUN 0	xvds
Barramento número 0, ID de destino 19, LUN 0	xvdt
Barramento número 0, ID de destino 20, LUN 0	xvdu
Barramento número 0, ID de destino 21, LUN 0	xvdv
Barramento número 0, ID de destino 22, LUN 0	xvdw
Barramento número 0, ID de destino 23, LUN 0	xvdx
Barramento número 0, ID de destino 24, LUN 0	xvdy
Barramento número 0, ID de destino 25, LUN 0	xvdz

Prevenção contra gravação interrompida nas instâncias do Linux do Amazon EC2

> **Note**
>
> A prevenção de gravação interrompida é compatível somente com as instâncias do Linux.

A prevenção de gravação interrompida é um recurso de armazenamento em blocos desenvolvido pela AWS para melhorar a performance das workloads de banco de dados relacional com uso intenso de E/S e reduzir a latência sem afetar negativamente a resiliência dos dados. Bancos de dados relacionais que usam InnoDB ou XtraDB como mecanismo de banco de dados, como MySQL e MariaDB, se beneficiarão da prevenção de gravações interrompidas.

Normalmente, bancos de dados relacionais que usam páginas maiores do que a atomicidade de falha de energia do dispositivo de armazenamento usam mecanismos de log de dados para proteger contra gravações interrompidas. O MariaDB e o MySQL usam um arquivo buffer de gravação dupla para registrar dados em log antes de gravá-los nas tabelas de dados. No caso de gravações incompletas ou interrompidas, como resultado de falhas no sistema operacional ou perda de energia durante transações de gravação, o banco de dados pode recuperar os dados do buffer de gravação

dupla. A sobrecarga adicional de E/S associada à gravação no buffer de gravação dupla afeta a performance do banco de dados e a latência da aplicação, além de reduzir o número de transações que podem ser processadas por segundo. Para obter mais informações sobre o buffer de gravação dupla, consulte a documentação do MariaDB e do MySQL.

Com a prevenção de gravações interrompidas, os dados são gravados no armazenamento em transações de gravação do tipo tudo ou nada, o que elimina a necessidade de usar o buffer de gravação dupla. Isso evita que dados parciais ou interrompidos sejam gravados no armazenamento em caso de falhas no sistema operacional ou perda de energia durante transações de gravação. O número de transações processadas por segundo pode ser aumentado em até 30%, e a latência de gravação pode ser reduzida em até 50%, sem comprometer a resiliência das workloads.

Preços

Não há custos adicionais para o uso da prevenção de gravação interrompida.

Conteúdo

- Tamanhos de blocos para prevenção contra gravação interrompida no Amazon EC2
- Requisitos para usar prevenção contra gravação interrompida no Amazon EC2
- Verificar a compatibilidade das instâncias do Amazon EC2 com a prevenção contra gravação interrompida
- Configurar a workload no Amazon EC2 para prevenção contra gravação interrompida

Tamanhos de blocos para prevenção contra gravação interrompida no Amazon EC2

A prevenção de gravação interrompida é compatível com operações de gravação para blocos de dados de 4 KiB, 8 KiB e 16 KiB. O endereço do bloco lógico inicial (LBA) do bloco de dados deve estar alinhado ao respectivo tamanho do limite do bloco de 4 KiB, 8 KiB ou 16 KiB. Por exemplo, para operações de gravação de 16 KiB, o LBA inicial do bloco de dados deve estar alinhado a um tamanho limite de bloco de 16 KiB.

A tabela a seguir mostra a compatibilidade de tipos de armazenamento e instância.

	Blocos de 4 KiB	Blocos de 8 KiB	Blocos de 16 KiB
Volumes de armazenamento de instâncias	Todos os volumes de armazenamento de instância NVMe vinculados às instâncias da família I da geração atual.	As instâncias I4i, Im4gn, Is4gen, I7i, I7ie, I8g e I8ge são compatíveis com o AWS Nitro SSD.	
Volumes do Amazon EBS	Todos os volumes do Amazon EBS anexados a instâncias baseadas em Nitro.		

Para confirmar se sua instância e seu volume são compatíveis com prevenção de gravação interrompida, consulte se a instância é compatível com prevenção de gravação interrompida e outros detalhes, como tamanhos de blocos e limites compatíveis. Para obter mais informações, consulte Verificar a compatibilidade das instâncias do Amazon EC2 com a prevenção contra gravação interrompida.

Requisitos para usar prevenção contra gravação interrompida no Amazon EC2

Para que a prevenção de gravação interrompida funcione adequadamente, uma operação de E/S deve atender aos requisitos de tamanho, alinhamento e limite, conforme especificado nos campos `NTWPU`, `NTWGU` e `NTWBU`. Você deve configurar seu sistema operacional para garantir que o subsistema de armazenamento específico (sistema de arquivos, LVM, RAID etc.) não modifique as propriedades de E/S na pilha de armazenamento, incluindo mesclagens de blocos, divisões ou realocação de endereços de blocos, antes de ser enviada ao dispositivo.

A prevenção de gravação interrompida foi testada com a seguinte configuração:

- Um tipo de instância e tipo de armazenamento que são compatíveis com o tamanho de bloco necessário.
- Amazon Linux 2 com a versão de kernel 5.10 ou posterior.
- ext4 com `bigalloc` habilitado e um tamanho de cluster de 16 KiB, e os utilitários ext4 mais recentes (e2fsprogs 1.46.5 ou posterior).
- Modo de acesso a arquivos `O_DIRECT` para ignorar o cache do buffer do kernel Linux.

> **Note**
>
> Você não precisa desativar a mesclagem de E/S para workloads do MySQL e do MariaDB.

Verificar a compatibilidade das instâncias do Amazon EC2 com a prevenção contra gravação interrompida

Para confirmar se sua instância e volume são compatíveis com prevenção de gravação interrompida e para visualizar os dados específicos do fornecedor do namespace NVMe que contém informações de prevenção de gravação interrompida, use o comando a seguir.

```
$ sudo nvme id-ns -v device_name
```

> **Note**
>
> O comando retorna as informações específicas do fornecedor em hexadecimal com interpretação ASCII. Talvez seja necessário criar uma ferramenta, semelhante à `ebsnvme-id`, nas aplicações, que possa ler e analisar a saída.

Por exemplo, o comando a seguir retorna os dados específicos do fornecedor do namespace NVMe que contêm informações de prevenção de gravação interrompida para `/dev/nvme1n1`.

```
$ sudo nvme id-ns -v /dev/nvme1n1
```

Se sua instância e seu volume oferecerem suporte à prevenção de gravação interrompida, eles retornarão as seguintes informações de prevenção de gravação interrompida da AWS nos dados específicos do fornecedor do namespace NVMe.

> **Note**
>
> Os bytes na tabela a seguir representam a diferença em bytes do início dos dados específicos do fornecedor do namespace NVMe.

Bytes	Descrição
0:31	O nome do ponto de montagem da conexão do dispositivo, por exemplo /dev/xvda . Você fornece isso durante a solicitação de anexo de volume e ele pode ser usado pela instância do Amazon EC2 para criar um link simbólico para o dispositivo de blocos NVMe (nvmeXn1).
32:63	O ID do volume. Por exemplo, .vol01234567890abcdef Esse campo pode ser usado para mapear o dispositivo NVMe para o volume anexado.
64:255	Reservado para uso futuro.
256:257	Tamanho da unidade de prevenção de gravação interrompida do namespace (NTWPU). Esse campo indica o tamanho específico do namespace da operação de gravação garantida para ser gravada atomicamente no NVM durante uma falha de energia ou condição de erro. Esse campo é especificado em blocos lógicos representados em valores baseados em zero.
258:259	Tamanho da granularidade de prevenção de gravação interrompida do namespace (NTWPG). Esse campo indica os incrementos de tamanho específico do namespace abaixo de NTWPU da operação de gravação garantida para ser gravada atomicamente no NVM durante uma falha de energia ou condição de erro. Ou seja, o tamanho deve ser NTWPG * n <= NTWPU onde n é um número inteiro positivo. O deslocamento do LBA da operação de gravação também deve estar alinhado com esse campo. Esse campo é especificado em blocos lógicos representados em valores baseados em zero.
260:263	Tamanho do limite de prevenção de gravação interrompida do namespace (NTWPU). Esse campo indica o tamanho do limite atômico desse namespace para o valor de NTWPU. Gravações nesse namespace que cruzam os limites atômicos não teê garantia de serem gravadas atomicamente no NVM durante uma falha de energia ou condição de erro. Um valor de 0h indica que não há limites atômicos para condições de falha ou erro de energia. Todos os outros valores especificam um

Bytes	Descrição
	tamanho em termos de blocos lógicos usando a mesma codificação do campo NTWPU.

Configurar a workload no Amazon EC2 para prevenção contra gravação interrompida

A prevenção de gravações interrompidas é habilitada por padrão em tipos de instância compatíveis com volumes compatíveis. Você não precisa habilitar nenhuma configuração adicional para habilitar seu volume ou instância para evitar gravações interrompidas.

> **Note**
>
> Não há impacto no performance em workloads que não são compatíveis com a prevenção de gravações interrompidas. Você não precisa fazer nenhuma alteração nessas workloads
> As workloads que são compatíveis com prevenção de gravação interrompida, mas não estão configuradas para usá-la, continuam usando o buffer de gravação dupla e não recebem nenhum benefício de performance.

Para configurar sua pilha de software MySQL ou MariaDB para desativar o buffer de gravação dupla e usar a prevenção de gravação interrompida, conclua as seguintes etapas:

1. Configure seu volume para usar o sistema de arquivos ext4 com a opção BigAlloc e defina o tamanho do cluster como 4 KiB, 8 KiB ou 16 KiB. O uso do BigAlloc com um tamanho de cluster de 4 KiB, 8 KiB ou 16 KiB garante que o sistema de arquivos aloque arquivos alinhados com o respectivo limite.

   ```
   $  mkfs.ext4 -O bigalloc -C 4096|8192|16384 device_name
   ```

   > **Note**
   >
   > Para MySQL e MariaDB, você deve usar `-C 16384` para corresponder ao tamanho da página do banco de dados. Definir a granularidade da alocação para um valor diferente de um múltiplo do tamanho da página pode resultar em alocações que podem ser

incompatíveis com os limites de prevenção de gravação interrompida do dispositivo de armazenamento.

Por exemplo:

```
$  mkfs.ext4 -O bigalloc -C 16384 /dev/nvme1n1
```

2. Configure o InnoDB para usar o método `O_DIRECT` de descarga e desative a gravação dupla do InnoDB. Use seu editor de texto preferido para abrir `/etc/my.cnf` e atualize os parâmetros `innodb_flush_method` e `innodb_doublewrite` da seguinte forma:

```
innodb_flush_method=O_DIRECT
innodb_doublewrite=0
```

Important

Se você estiver usando o Logical Volume Manager (LVM) ou outra camada de virtualização de armazenamento, certifique-se de que os deslocamentos iniciais dos volumes estejam alinhados em múltiplos de 16 KiB. Isso é relativo ao armazenamento NVMe subjacente para contabilizar os cabeçalhos de metadados e superblocos usados pela camada de virtualização de armazenamento. Se você adicionar um deslocamento ao volume físico do LVM, isso poderá causar desalinhamento entre as alocações do sistema de arquivos e os deslocamentos do dispositivo NVMe, o que invalidaria a prevenção de gravação interrompida. Para obter mais informações, consulte `--dataalignmentoffset` na página do manual do Linux.

Snapshots do Amazon EBS baseados no Windows VSS consistentes com a aplicação

É possível obter snapshots consistentes com a aplicação de todos os volumes do Amazon EBS anexados às instâncias do Windows do Amazon EC2 usando o Run Command do AWS Systems Manager. O processo de snapshot usa o Serviço de Cópias de Snapshot de Volume (VSS) do Windows para fazer backups no nível do volume do EBS de aplicações habilitadas para VSS. Os snapshots incluem dados das transações pendentes entre essas aplicações e o disco. Além disso,

você não precisa desligar as instâncias ou desconectá-las quando precisar fazer backup de todos os volumes anexados.

Não há custos adicionais pelo uso de snapshots do EBS baseados no VSS. Você paga apenas pelos snapshots do EBS criados pelo processo de backup. Para obter mais informações, consulte Como é a cobrança pelos snapshots do Amazon EBS?

> **Note**
>
> Os snapshots baseados em VSS do Windows e consistentes com a aplicação são compatíveis somente com as instâncias do Windows.

Conteúdo

- O que é o VSS?
- Como funciona a solução de snapshots do Amazon EBS baseada no VSS
- Pré-requisitos para criar snapshots do EBS baseados no VSS do Windows
- Criar snapshots do EBS baseados no VSS para a instância EC2 Windows
- Solucionar problemas de snapshots do EBS baseados no Windows VSS
- Usar a solução AWS VSS para restaurar os dados da sua instância
- Histórico de versões da solução AWS VSS

O que é o VSS?

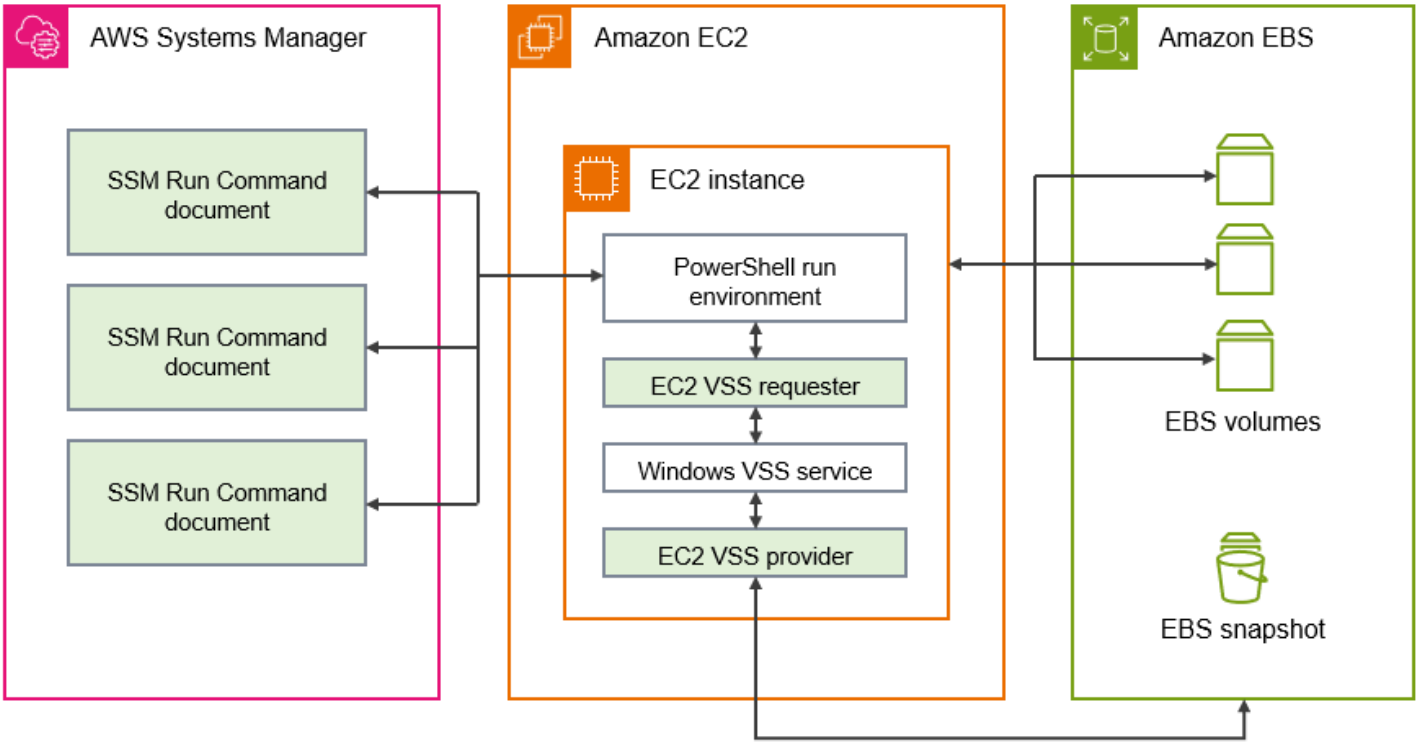
O Volume Shadow Copy Service (VSS) é uma tecnologia de backup e recuperação incluída no Microsoft Windows. Ele poderá criar cópias de backup, ou snapshots, de arquivos ou volumes do computador enquanto estiverem em uso. Para obter mais informações, consulte Serviço de Cópias de Snapshot de Volume.

Para criar um snapshot consistente com aplicações, os componentes do software a seguir são necessários.

- Serviço de VSS: parte do sistema operacional Windows
- Solicitante de VSS: o software que solicita a criação de cópias de sombra
- Gravador de VSS: normalmente fornecido como parte de uma aplicação, como o SQL Server, para garantir um conjunto de dados consistente para backup

- Provedor de VSS: o componente que cria as cópias de sombra dos volumes subjacentes

A solução de snapshots do Amazon EBS baseados no Windows VSS consiste em vários documentos do Run Command do Systems Manager (SSM) que facilitam a criação de backup e um pacote do Systems Manager Distributor, denominado `AwsVssComponents` que inclui um solicitante de VSS do EC2 e um provedor de VSS do EC2. O pacote `AwsVssComponents` deve ser instalado em instâncias do Windows do EC2 para obter snapshots dos volumes do EBS de maneira consistente com as aplicações. O diagrama a seguir ilustra a relação entre esses componentes de software.



Como funciona a solução de snapshots do Amazon EBS baseada no VSS

O processo para gerar scripts de snapshots do EBS baseados no VSS consistentes com a aplicação consiste nas etapas a seguir.

1. Preencha os do Pré-requisitos para criar snapshots do EBS baseados no VSS do Windows.
2. Insira os parâmetros para o documento do SSM `AWSEC2-VssInstallAndSnapshot` e execute esse documento usando o Run Command. Para obter mais informações, consulte Execução do documento de comando AWSEC2-VssInstallAndSnapshot (recomendado).

3. O serviço VSS do Windows na sua instância coordena todas as operações de E/S em andamento para a execução de aplicações.
4. O sistema libera todos os buffers de E/S e temporariamente todas as operações de E/S. A pausa dura no máximo dez segundos.
5. Durante essa pausa, o sistema cria snapshots de todos os volumes anexados à instância.
6. A pausa é suspensa e as operações de E/S são retomadas.
7. O sistema adiciona todos os snapshots recém-criados à lista de snapshots do EBS. O sistema marca todos os snapshots do EBS baseados no VSS que foram criados com êxito por esse processo com AppConsistent:true.
8. Se for necessário restaurar usando um snapshot, será possível usar o processo padrão do EBS de criação de um volume por meio de um snapshot ou restaurar todos os volumes para uma instância usando um script de exemplo, conforme descrito em Usar a solução AWS VSS para restaurar os dados da sua instância.

Pré-requisitos para criar snapshots do EBS baseados no VSS do Windows

É possível criar snapshots do EBS baseados no VSS com o Run Command do Systems Manager, o AWS Backup ou o Amazon Data Lifecycle Manager. Os pré-requisitos a seguir se aplicam a todas as soluções.

Requisitos do sistema

Certifique-se de que sua instância EC2 Windows atenda a todos os requisitos do sistema para criar snapshots baseados no VSS, incluindo versões compatíveis do sistema operacional Windows, .NET framework, PowerShell, AWS Tools for Windows PowerShell e AWS Systems Manager Agent.

permissões do IAM

O perfil do IAM anexado à instância do Windows do Amazon EC2 deve ter permissão para criar snapshots consistentes com aplicações ao usar o VSS. Para conceder as permissões necessárias, você pode anexar a política `AWSEC2VssSnapshotPolicy` gerenciada ao seu perfil de instância.

Componentes do VSS

Para criar snapshots consistentes com a aplicação nos sistemas operacionais Windows, o pacote `AwsVssComponents` deve estar instalado na instância. O pacote contém um VSS Agent do EC2

na instância que funciona como solicitante do VSS e um provedor do VSS do EC2 para volumes do EBS.

Requisitos do sistema

Instalar o agente do Systems Manager

O VSS é orquestrado pelo Systems Manager Agent usando o PowerShell. Verifique se a versão `3.0.502.0` ou posterior do SSM Agent está instalada em sua instância do EC2. Se você já estiver usando uma versão mais antiga do SSM Agent, poderá atualizá-la usando o Run Command. Para obter mais informações, consulte Configuração do Systems Manager para instâncias do Amazon EC2 e Trabalhar com o SSM Agent em instâncias do Amazon EC2 para Windows Server no Guia do usuário do AWS Systems Manager.

Amazon EC2 Requisitos de instância do Windows

Os snapshots do EBS baseados no VSS são compatíveis com instâncias que executam o Windows Server 2016 ou posterior.

Versão do .NET Framework

O pacote `AwsVssComponents` requer o .NET Framework versão `4.6` ou posterior. As versões do sistema operacional Windows anteriores ao Windows Server 2016 usam como padrão uma versão anterior do .NET Framework. Se a sua instância usar uma versão anterior do .NET Framework, você deverá instalar a versão `4.6` ou posterior usando o Windows Update.

AWS Tools for Windows PowerShellVersão do

Verifique se sua instância está executando a versão `3.3.48.0` ou posterior do AWS Tools for Windows PowerShell. Para verificar a versão, execute o comando a seguir na instância em um terminal do PowerShell.

```
C:\> Get-AWSPowerShellVersion
```

Para atualizar o AWS Tools for Windows PowerShell na sua instância, consulte Instalar o AWS Tools for Windows PowerShell no Guia do usuário do AWS Tools for PowerShell.

Versão Windows Powershell

Verifique se sua instância está executando o Windows PowerShell, versão principal `3`, `4` ou `5`. Para verificar a versão, execute o comando a seguir na instância em um terminal do PowerShell.

```
C:\> $PSVersionTable.PSVersion
```

Modo de linguagem do PowerShell

Certifique-se de que sua instância tenha o modo de idioma da PowerShell definido como `FullLanguage`. Para obter mais informações, consulte about_Language_Modes na documentação da Microsoft.

Usar uma política gerenciada do IAM para conceder permissões para snapshots baseados no VSS

A política gerenciada AWSEC2VssSnapshotPolicy possibilita que o Systems Manager execute as seguintes ações na instância do Windows:

- Criar e realizar a marcação de snapshots do EBS;
- Criar e realizar a marcação de imagens de máquina da Amazon (AMIs);
- Anexar metadados, como o ID do dispositivo, às etiquetas de snapshot padrão criadas pelo VSS.

Este tópico abrange os detalhes da permissão para a política gerenciada do VSS e como anexá-la ao perfil do IAM do perfil de instância do EC2.

Conteúdo

- Detalhes da política gerenciada AWSEC2VssSnapshotPolicy
- Anexar a política gerenciada de snapshot baseado no VSS ao perfil de instância

Detalhes da política gerenciada AWSEC2VssSnapshotPolicy

Uma política gerenciada pela AWS é uma política autônoma que a Amazon fornece aos clientes da AWS. As políticas gerenciadas pela AWS são projetadas para conceder permissões para casos de uso conhecidos. Não é possível alterar as permissões definidas nas políticas gerenciadas pela AWS. No entanto, você pode copiar a política e usá-la como referência para o desenvolvimento de uma política gerenciada pelo cliente específica ao seu caso de uso.

Para obter mais informações sobre as políticas gerenciadas da AWS, consulte Políticas gerenciadas da AWS no Guia do usuário do IAM.

Para usar a política gerenciada AWSEC2VssSnapshotPolicy, você pode anexá-la ao perfil do IAM anexado às instâncias EC2 Windows. Essa política possibilita que a solução VSS do EC2 crie e adicione etiquetas a imagens de máquina da Amazon (AMIs) e a snapshots do EBS. Para anexar a política, consulte Anexar a política gerenciada de snapshot baseado no VSS ao perfil de instância.

Permissões concedidas pelo AWSEC2VssSnapshotPolicy

A política AWSEC2VssSnapshotPolicy inclui as permissões a seguir do Amazon EC2 que possibilitam que o Amazon EC2 crie e gerencie snapshots do VSS em seu nome. Você pode anexar essa política gerenciada ao perfil de instância do IAM usado para as instâncias EC2 Windows.

- ec2:CreateTags: adicione etiquetas a snapshots e a AMIs do EBS para ajudar na identificação e na categorização dos recursos.
- ec2:DescribeInstanceAttribute: recupere os volumes do EBS e os mapeamentos de dispositivos de bloco correspondentes que estão anexados à instância de destino.
- ec2:CreateSnapshots: crie snapshots de volumes do EBS.
- ec2:CreateImage: crie uma AMI usando uma instância do EC2 em execução.
- ec2:DescribeImages: recupere as informações para AMIs e snapshots do EC2.
- ec2:DescribeSnapshots: defina o horário de criação e o status dos snapshots para verificar a consistência da aplicação.

> **Note**
>
> Para visualizar os detalhes da permissão para esta política, consulte AWSEC2VssSnapshotPolicy na Referência de políticas gerenciadas pela AWS.

Otimizar as permissões para casos de uso específicos (avançado)

A política gerenciada `AWSEC2VssSnapshotPolicy` inclui permissões para todas as formas pelas quais é possível criar snapshots baseados no VSS. É possível criar uma política personalizada que inclua somente as permissões de que você precisa.

Caso de uso: criar uma AMI | Caso de uso: usar o serviço AWS Backup

Caso use exclusivamente a opção `CreateAmi` ou crie snapshots baseados no VSS somente por meio do serviço do AWS Backup, você poderá otimizar as instruções de política conforme apresentado a seguir.

- Omissão das declarações de política identificadas pelos seguintes IDs de declaração (SIDs):
  - `CreateSnapshotsWithTag`
  - `CreateSnapshotsAccessInstance`
  - `CreateSnapshotsAccessVolume`
- Ajuste da instrução `CreateTagsOnResourceCreation` da seguinte maneira:
  - Remova `arn:aws:ec2:*:*:snapshot/*` dos recursos.
  - Remova `CreateSnapshots` da condição `ec2:CreateAction`.
- Ajuste da instrução `CreateTagsAfterResourceCreation` para remover `arn:aws:ec2:*:*:snapshot/*` dos recursos.
- Ajuste da instrução `DescribeImagesAndSnapshots` para remover `ec2:DescribeSnapshots` da ação da instrução.

Caso de uso: somente snapshots

Se você não usar a opção `CreateAmi`, poderá simplificar as declarações de política conforme apresentado a seguir.

- Omissão das declarações de política identificadas pelos seguintes IDs de declaração (SIDs):
  - `CreateImageAccessInstance`
  - `CreateImageWithTag`
- Ajuste da instrução `CreateTagsOnResourceCreation` da seguinte maneira:
  - Remova `arn:aws:ec2:*:*:image/*` dos recursos.
  - Remova `CreateImage` da condição `ec2:CreateAction`.
- Ajuste da instrução `CreateTagsAfterResourceCreation` para remover `arn:aws:ec2:*:*:image/*` dos recursos.
- Ajuste da instrução `DescribeImagesAndSnapshots` para remover `ec2:DescribeImages` da ação da instrução.

> **Note**
>
> Para garantir que a política personalizada funcione conforme o esperado, recomendamos analisar e incorporar atualizações regularmente à política gerenciada.

Anexar a política gerenciada de snapshot baseado no VSS ao perfil de instância

Para conceder permissões para snapshots baseados no VSS para a instância EC2 Windows, anexe a política gerenciada AWSEC2VssSnapshotPolicy ao perfil de instância conforme apresentado a seguir. É importante garantir que a instância atenda a todos os Requisitos do sistema.

> **Note**
>
> Para usar a política gerenciada, a instância deve ter o pacote `AwsVssComponents` na versão `2.3.1` ou em versões posteriores instalado. Para obter o histórico de versões, consulte Versões do pacote AwsVssComponents.

1. Abra o console do IAM, em https://console.aws.amazon.com/iam/.
2. No painel de navegação, escolha Perfis para visualizar uma lista de perfis do IAM aos quais você tem acesso.
3. Selecione o link Nome do perfil para o perfil anexado à instância. Isso abre a página de detalhes do perfil.
4. Para anexar a política gerenciada, escolha a opção Adicionar permissões, localizada no canto superior direito do painel da lista. Em seguida, selecione Anexar políticas na lista suspensa.
5. Para agilizar os resultados, insira o nome da política na barra de pesquisa (`AWSEC2VssSnapshotPolicy`).
6. Marque a caixa de seleção ao lado do nome da política a ser anexada e escolha Adicionar permissões.

Gerenciar pacote de componentes do VSS para snapshots do EBS baseados no VSS do Windows

Antes de criar snapshots do EBS baseados no VSS, verifique se você tem a versão mais recente do pacote de componentes do VSS instalada na sua instância do Windows. Existem várias maneiras possíveis de instalar o pacote `AwsVssComponents` em uma instância existente. Veja abaixo:

- (Recomendado) Execução do documento de comando AWSEC2-VssInstallAndSnapshot (recomendado). Se necessário, isso faz a instalação ou a atualização automaticamente toda vez que for executado.
- Instalar manualmente os componentes do VSS em uma instância EC2 Windows.

- Atualizar o pacote de componentes do VSS na instância EC2 Windows.

Você também pode criar uma AMI com o EC2 Image Builder que usa o componente gerenciado `aws-vss-components-windows` para instalar o pacote `AwsVssComponents` da imagem. O componente gerenciado usa o AWS Systems Manager Distributor para instalar o pacote. Depois que o Image Builder criar a imagem, toda instância que você executar na AMI associada terá o pacote VSS instalado nela. Para obter mais informações sobre como criar uma AMI com o pacote VSS instalado, consulte Componentes gerenciados do pacote do Distributor para Windows no Guia do usuário do EC2 Image Builder.

Conteúdo

- Instalar manualmente os componentes do VSS em uma instância EC2 Windows
- Atualizar o pacote de componentes do VSS na instância EC2 Windows

Instalar manualmente os componentes do VSS em uma instância EC2 Windows

Sua instância do EC2 para Windows deve ter componentes VSS instalados antes de criar snapshots consistentes com aplicações usando o Systems Manager. Se você não executar o documento do comando `AWSEC2-VssInstallAndSnapshot` para instalar ou atualizar automaticamente o pacote toda vez que criar snapshots consistentes com aplicações, deverá instalar o pacote manualmente.

Você também deve fazer a instalação manualmente se planeja usar um dos métodos a seguir para criar snapshots consistentes com aplicações usando a instância do EC2.

- Criar snapshots do VSS usando o AWS Backup
- Criar snapshots do VSS usando o Amazon Data Lifecycle Manager

Se precisar fazer uma instalação manual, recomendamos usar o pacote de componentes do AWS VSS mais recente para melhorar a confiabilidade e a performance de snapshots consistentes com aplicações nas suas instâncias do EC2 para Windows.

> **Note**
>
> Para instalar ou atualizar automaticamente o pacote `AwsVssComponents` sempre que você criar snapshots consistentes com a aplicação, recomendamos que use o Systems Manager para executar o documento `AWSEC2-VssInstallAndSnapshot`.

Para obter mais informações, consulte Execução do documento de comando AWSEC2-VssInstallAndSnapshot (recomendado).

Para instalar os componentes do VSS em uma instância do Windows do Amazon EC2, siga as etapas para o ambiente de sua preferência.

Console

Instalar os componentes do VSS usando o SSM Distributor

1. Abra o console do AWS Systems Manager em https://console.aws.amazon.com/systems-manager/.
2. No painel de navegação, selecione Executar comando.
3. Selecione Run command (Executar comando).
4. Em Command document (Documento do comando), selecione o botão ao lado de AWS-ConfigureAWSPackage.
5. Em Command parameters (Parâmetros do comando), faça o seguinte:
   a. Verifique se Action (Ação) está definida como Install (Instalar).
   b. Em Name (Nome), insira `AwsVssComponents`.
   c. Em Versão, insira uma versão ou deixe o campo vazio para que o Systems Manager instale a versão mais recente.
6. Em Targets (Destinos), identifique as instâncias nas quais você deseja executar essa operação especificando tags ou selecionando instâncias manualmente.

   > **Note**
   >
   > Se você optar por selecionar manualmente as instâncias e uma instância que você espera visualizar não estiver incluída na lista, consulte Algumas das minhas instâncias estão ausentes no Manual do usuário do AWS Systems Manager para obter dicas para solução de problemas.

7. Para Other parameters (Outros parâmetros):
   - (Opcional) Em Comment (Comentário), digite informações sobre esse comando.

- Em Timeout (seconds) (Tempo limite [segundos]), especifique o número de segundos para o sistema aguardar até a falha de execução do comando total.

8. (Opcional) Em Rate control (Controle de taxa):

   - Em Concurrency (Concorrência), especifique um número ou uma porcentagem de instâncias nas quais executar o comando ao mesmo tempo.

     > **Note**
     >
     > Se tiver selecionado destinos escolhendo tags do Amazon EC2 e não tiver certeza de quantas instâncias usam tags selecionadas, limite o número de instâncias que podem executar o documento ao mesmo tempo especificando uma porcentagem.

   - Em Error threshold (Limite de erro), especifique quando parar de executar o comando em outras instâncias depois de falhar em alguns ou em uma porcentagem de instâncias. Por exemplo, se você especificar três erros, o Systems Manager deixará de enviar o comando quando o 4° erro for recebido. As instâncias que continuam processando o comando também podem enviar erros.

9. (Opcional) Na seção Output options (Opções de saída), se você quiser salvar a saída de comando em um arquivo, selecione a caixa ao lado de Enable writing to an S3 bucket (Habilitar a gravação em um bucket do S3). Especifique o bucket e os nomes (de pastas) de prefixo (opcional).

   > **Note**
   >
   > As permissões do S3 que concedem a possibilidade de gravar os dados em um bucket do S3 são as do perfil de instância atribuído à instância, e não as do usuário que realiza essa tarefa. Para obter mais informações, consulte Configurar permissões de instância do EC2 no Guia do usuário do AWS Systems Manager.

10. (Opcional) Especifique opções para SNS notifications (Notificações do SNS).

    Para obter informações sobre como configurar notificações do Amazon SNS para o Run Command, consulte Configuração das notificações do Amazon SNS para o AWS Systems Manager.

11. Escolha Run.

AWS CLI

Use o procedimento a seguir para baixar e instalar o pacote `AwsVssComponents` em suas instâncias usando o Run Command por meio da AWS CLI. O pacote instala dois componentes: um solicitante de VSS e um fornecedor de VSS. O sistema copia esses componentes para um diretório na instância e, em seguida, registra a DLL do fornecedor como um fornecedor de VSS.

Para instalar o pacote do VSS

Execute o comando a seguir para fazer download e instalar os componentes do VSS necessários para o Systems Manager.

```
aws ssm send-command \
    --document-name "AWS-ConfigureAWSPackage" \
    --instance-ids "i-1234567890abcdef0" \
    --parameters '{"action":["Install"],"name":["AwsVssComponents"]}'
```

PowerShell

Use o procedimento a seguir para fazer baixar e instalar o pacote `AwsVssComponents` em suas instâncias usando o Run Command por meio do Tools for Windows PowerShell. O pacote instala dois componentes: um solicitante de VSS e um fornecedor de VSS. O sistema copia esses componentes para um diretório na instância e, em seguida, registra a DLL do fornecedor como um fornecedor de VSS.

Para instalar o pacote do VSS

Execute o comando a seguir para fazer download e instalar os componentes do VSS necessários para o Systems Manager.

```
Send-SSMCommand `
    -DocumentName "AWS-ConfigureAWSPackage" `
    -InstanceId "i-1234567890abcdef0" `
    -Parameter @{'action'='Install';'name'='AwsVssComponents'}
```

Verifique a assinatura nos componentes do AWS VSS

Use o procedimento a seguir para verificar a assinatura no pacote `AwsVssComponents`.

1. Conecte-se à sua instância do Windows. Para obter mais informações, consulte Conectar-se à instância do Windows no usando RDP.

2. Navegue até C:\Program Files\Amazon\AwsVssComponents.
3. Abra o menu de contexto de `ec2-vss-agent.exe` (clique com o botão direito do mouse) e escolha Propriedades.
4. Navegue até a guia Assinaturas digitais e verifique se o nome do signatário é Amazon Web Services Inc.
5. Use as etapas anteriores para verificar a assinatura em `Ec2VssInstaller` e `Ec2VssProvider.dll`.

Atualizar o pacote de componentes do VSS na instância EC2 Windows

Recomendamos que você sempre mantenha os componentes do VSS atualizados com a versão mais recente recomendada. Existem diversas maneiras diferentes de atualizar componentes quando uma nova versão do pacote `AwsVssComponents` é lançada.

Métodos de atualização

- É possível repetir as etapas descritas em Instalar manualmente os componentes do VSS em uma instância EC2 Windows quando uma nova versão dos componentes do AWS VSS é lançada.
- É possível configurar uma associação do State Manager do Systems Manager para baixar e instalar automaticamente os componentes novos ou atualizados do VSS quando o pacote `AwsVssComponents` ficar disponível.
- Para instalar ou atualizar automaticamente o pacote `AwsVssComponents` sempre que você criar snapshots consistentes com a aplicação, ao usar o Systems Manager para executar o documento `AWSEC2-VssInstallAndSnapshot`.

> **Note**
>
> Recomendamos que você use o Systems Manager para executar o documento de comando `AWSEC2-VssInstallAndSnapshot`, que instala ou atualiza automaticamente o pacote `AwsVssComponents` antes de criar snapshots consistentes com a aplicação. Para obter mais informações, consulte Execução do documento de comando AWSEC2-VssInstallAndSnapshot (recomendado).

Para criar uma associação do State Manager do Systems Manager, siga as etapas do ambiente de sua preferência.

Console

Ao configurar uma associação no Gerenciador de Estados do Systems Manager, é possível atualizar o pacote `AwsVssComponents` de duas formas, conforme abaixo:

Desinstalar e instalar novamente

Esse método faz o download e instala o pacote sem necessidade de pré-requisitos adicionais.

Atualizar no local

Este método executa uma atualização no local para o pacote e requer os seguintes pré-requisitos:

- A versão do SSM Agent instalada na instância deve ser a `3.3.808.0` ou posterior. Para obter mais informações, consulte Trabalhar com o SSM Agent em instâncias do Amazon EC2 para Windows Server no Guia do usuário do AWS Systems Manager.
- Caso seja especificado, o pacote `AwsVssComponents` deve estar na versão `2.5.0` ou posterior. As versões anteriores não são compatíveis com a atualização no local.

> **Note**
>
> Caso sua instância não cumpra esses pré-requisitos, a atualização no local não será bem-sucedida. Use a opção Desinstalar e instalar novamente em vez disso.

Para criar uma associação do State Manager

1. Abra o console AWS Systems Manager em https://console.aws.amazon.com/systems-manager/.
2. No painel de navegação, escolha State Manager.

   Ou, se a página inicial do Systems Manager abrir primeiro, abra o painel de navegação e escolha Gerenciador de Estados.
3. Selecione Criar associação.
4. No campo Association Name (Nome da associação), insira um nome descritivo.
5. Na lista Documento, escolha AWS-ConfigureAWSPackage.
6. Na seção Parameters Parâmetros), escolha Install (Instalar) na lista Action (Ação).
7. Em Tipo de instalação, escolha Desinstalar e instalar novamente ou Atualização no local.

8. No campo Name (Nome), insira `AwsVssComponents`. É possível manter os campos Version (Versão) e Additional Arguments (Argumentos adicionais) vazios.
9. Na seção Select Targets by, escolha uma opção.

> **Note**
>
> Se você optar por especificar instâncias de destino usando tags e especificar tags que são mapeadas para instâncias do Linux, a associação será bem-sucedida na instância do Windows, mas falhará nas instâncias do Linux. O status geral da associação mostra Failed.

10. Na seção Specify schedule, escolha uma opção.
11. Na seção Advanced options (Opções avançadas), em Compliance severity (Severidade de conformidade), escolha um nível de gravidade para a associação. Para obter mais informações, consulte Saiba mais sobre a conformidade de associações. Em Calendários de alteração, selecione um calendário de alterações pré-configurado. Para obter mais informações, consulte Calendário de alterações do AWS Systems Manager.
12. Em Controle de taxa, faça o seguinte:
    - Em Concurrency (Concorrência), especifique um número ou uma porcentagem de nós gerenciados nos quais executar o comando ao mesmo tempo.
    - Em Error threshold (Limite de erro), especifique quando parar de executar o comando em outros nós depois de falhar em alguns ou em uma porcentagem de nós.
13. (Opcional) Em Opções de saída, para salvar a saída de comando em um arquivo, selecione a caixa Habilitar gravação da saída no S3. Digite os nomes de bucket e prefixo (pastas) nas caixas de texto.
14. Escolha Create Association (Criar associação) e, em seguida, Close (Fechar). O sistema tenta criar a associação nas instâncias e aplicar imediatamente o estado.

> **Note**
>
> Se as instâncias do EC2 para o Windows Server mostrarem o status Com falha, verifique se o SSM Agent está sendo executado na instância e se a instância está configurada com um perfil do AWS Identity and Access Management (IAM) para o Systems Manager. Para obter mais informações, consulte Configurar o AWS Systems Manager.

AWS CLI

Use o comando create-association para atualizar um pacote do Distributor conforme uma programação sem deixar a aplicação associada offline. Somente arquivos novos ou atualizados no pacote são substituídos.

Para criar uma associação do State Manager

Execute o comando a seguir para criar uma associação. O valor de `--name`, o nome do documento, é sempre `AWS-ConfigureAWSPackage`. O comando a seguir usa a chave `InstanceIds` para especificar as instâncias de destino.

```
aws ssm create-association \
    --name "AWS-ConfigureAWSPackage" \
    --parameters action=Install,installationType="Uninstall and
 reinstall",name=AwsVssComponents \
    --targets Key=InstanceIds,Values=i-1234567890abcdef0,i-000011112222abcde
```

PowerShell

Para criar uma associação do State Manager

Use o cmdlet New-SSMAssociation.

```
New-SSMAssociation `
    -Name "AWS-ConfigureAWSPackage" `
    -Parameter  @{
        "action" = "Install"
        "installationType" = "Uninstall and reinstall"
        "name" = "AwsVssComponents"
    } `
    -Target @{
        "Key" = "InstanceIds"
        "Values" = @("i-1234567890abcdef0", "i-000011112222abcde")
    }
```

Criar snapshots do EBS baseados no VSS para a instância EC2 Windows

Depois de conhecer todos os Pré-requisitos para criar snapshots do EBS baseados no VSS do Windows, você pode usar qualquer um dos métodos a seguir para criar snapshots baseados no VSS com a instância do EC2.

Documentos de comando do AWS Systems Manager

Usar documentos de comando do Systems Manager para criar snapshots baseados no VSS.

Para automatizar os backups, você pode criar uma tarefa da janela de manutenção do AWS Systems Manager que use o documento de comando `AWSEC2-VssInstallAndSnapshot`. Para obter mais informações, consulte Trabalhar com janelas de manutenção (console) no Manual do usuário do AWS Systems Manager.

AWS Backup

Você pode criar um backup do VSS usando o AWS Backup ao habilitar o VSS no console ou na CLI. Para obter mais informações, consulte Creating Windows VSS backups no Guia do desenvolvedor do AWS Backup.

> **Note**
>
> O AWS Backup não instala automaticamente o pacote `AwsVssComponents` na instância. Você deve realizar uma instalação manual na instância. Para obter mais informações, consulte Instalar manualmente os componentes do VSS em uma instância EC2 Windows.

Amazon Data Lifecycle Manager

Você pode criar snapshots do VSS usando o Amazon Data Lifecycle Manager habilitando scripts prévios e posteriores nas políticas de ciclo de vida de snapshots. Para obter mais informações, consulte Automating application-consistent snapshots no Guia do usuário do Amazon EBS.

> **Note**
>
> O Amazon Data Lifecycle Manager não instala automaticamente o pacote `AwsVssComponents` na instância. Você deve realizar uma instalação manual na instância. Para obter mais informações, consulte Instalar manualmente os componentes do VSS em uma instância EC2 Windows.

Usar os documentos de comando do Systems Manager para criar snapshots baseados no VSS

Você pode usar documentos de comando do AWS Systems Manager para criar snapshots baseados no VSS. O conteúdo a seguir apresenta os documentos de comando disponíveis e os parâmetros de runtime que os documentos usam para criar seus snapshots.

Antes de usar qualquer um dos documentos de comando do Systems Manager, verifique se você atendeu a todos os Pré-requisitos para criar snapshots do EBS baseados no VSS do Windows.

Tópicos

- Parâmetros para documentos de snapshot de VSS do Systems Manager
- Execução de documentos de comando de snapshot de VSS do Systems Manager

Parâmetros para documentos de snapshot de VSS do Systems Manager

Todos os documentos do Systems Manager que criam snapshots de VSS usam os seguintes parâmetros, exceto onde indicado:

AmiName (string, opcional)

Se a opção CreateAmi for definida como `True`, especifique o nome da AMI que o backup criará.

description (string, opcional)

Especifique uma descrição para os snapshots ou para a imagem que esse processo vai criar.

CollectDiagnosticLogs (string, opcional)

Para coletar mais informações durante as etapas de criação de snapshots e AMIs, defina esse parâmetro como "`True`". O valor padrão desse parâmetro é "`False`". Os logs de diagnóstico consolidados são salvos como um arquivo no formato `.zip` no seguinte local em sua instância:

`C:\ProgramData\Amazon\AwsVss\Logs\`*`timestamp`*`.zip`

CopyOnly (string, opcional)

Se você estiver usando o backup nativo do SQL Server além do AWS VSS, fazer um backup somente cópia evitará que o AWS VSS rompa a cadeia nativa de backup diferencial. Para realizar uma operação de backup somente cópia, defina esse parâmetro como `True`.

O valor padrão desse parâmetro é `False`, que faz com que o AWS VSS faça uma operação de backup total.

CreateAmi (string, opcional)

Para criar uma imagem de máquina da Amazon (AMI) baseada no VSS para fazer backup da instância, defina esse parâmetro como `True`. O valor padrão desse parâmetro é `False`, que faz backup da instância com um snapshot do EBS.

Para obter mais informações sobre como criar uma AMI de uma instância, consulte Criação de uma AMI baseada no Amazon EBS.

executionTimeout (string, opcional)

Especifique o tempo máximo em segundos para executar o processo de criação de snapshots na instância ou para criar uma AMI da instância. Aumentar esse tempo limite permite que o comando aguarde mais tempo até o VSS iniciar seu congelamento e concluir a marcação dos recursos criados. Esse tempo limite só se aplica às etapas de criação de snapshot ou AMI. A etapa inicial para instalar ou atualizar o pacote `AwsVssComponents` não está incluída no tempo limite.

ExcludeBootVolume (string, opcional)

Se você criar snapshots, essa configuração excluirá os volumes de inicialização do processo de backups. Para excluir os volumes de inicialização dos snapshots, defina ExcludeBootVolume como **`True`** e CreateAmi como `False`.

Se você criar uma AMI para o backup, esse parâmetro deverá ser definido como `False`. O valor padrão desse parâmetro é `False`.

NoWriters (string, opcional)

Para excluir os gravadores do VSS do processo de snapshots, defina esse parâmetro como `True`. Excluir gravadores do VSS pode ajudar você a resolver conflitos com componentes de backup de VSS de terceiros. O valor padrão desse parâmetro é `False`.

Se `SaveVssMetadata` for `True`, esse parâmetro precisará ser definido como `False`.

SaveVSSMetadata (string, opcional)

Para salvar arquivos de metadados do VSS durante cada snapshot, defina esse parâmetro como `True`. O valor padrão é `False`. Os arquivos ajudam a fornecer insights sobre quais componentes ou gravadores foram incluídos em uma operação de backup, bem como os arquivos e volumes associados com cada snapshot. Os arquivos de metadados são usados ao restaurar um banco

de dados SQL usando a solução de restauração VSS. Para obter mais informações sobre como restaurar um banco de dados SQL a partir de snapshots do VSS, consulte Usar um runbook de automação para restaurar seu banco de dados a partir de snapshots da solução AWS VSS.

Os arquivos de metadados têm o ID do conjunto de snapshots associado em seus nomes. Você os encontrará no seguinte local na instância:

```
C:\ProgramData\Amazon\AwsVss\VssMetadata\
```

> **Warning**
>
> - Salvar arquivos de metadados do VSS requer a versão 2.4.0 ou superior do pacote de `AwsVssComponents`. Se a instância tiver uma versão anterior instalada, definir `SaveVssMetadata` como `True` fará com que a criação do snapshot falhe.
> - Os parâmetros `NoWriters` e `SaveVssMetadata` são mutuamente exclusivos. Se ambos estiverem definidos como `True`, a criação do snapshot falhará.

tags (string, opcional)

Recomendamos marcar seus snapshots e imagens com tags para facilitar a localização e o gerenciamento dos seus recursos, por exemplo, para restaurar volumes de uma lista de snapshots. O sistema adiciona a chave `Name` com um valor em branco em que você pode especificar o nome que deseja aplicar aos snapshots ou imagens de saída.

Se desejar especificar tags adicionais, separe-as com ponto e vírgulas. Por exemplo, `Key=Environment,Value=Test;Key=User,Value=TestUser1`.

> **Note**
>
> As chaves e os valores das etiquetas devem conter apenas caracteres alfanuméricos e os seguintes caracteres especiais: `( ) . /\-"'@_+:={}`.

Por padrão, o sistema adiciona as tags reservadas a seguir para imagens e snapshots baseados no VSS.

- Dispositivo: para snapshots baseados no VSS, esse é o nome do dispositivo do volume do EBS que o snapshot captura.

- AppConsistent: essa tag indica a criação com êxito de uma AMI ou um snapshot baseado no VSS.
- AwsVSSConfig: identifica snapshots e AMIs criados com o VSS habilitado. A tag inclui informações meta, como a versão de `AwsVssComponents` e o ID do conjunto de snapshots.

> **Warning**
>
> Especificar qualquer uma dessas tags reservadas na sua lista de parâmetros causará um erro.

VssVersion (string, opcional)

Somente para o documento `AWSEC2-VssInstallAndSnapshot`, você pode especificar o parâmetro `VssVersion` para instalar uma versão específica do pacote `AwsVssComponents` na instância. Deixe esse parâmetro em branco para instalar a versão padrão recomendada.

Se a versão especificada do pacote `AwsVssComponents` já estiver instalada, o script pulará a etapa de instalação e passará para a etapa de backup. Para obter uma lista das versões do pacote `AwsVssComponents` e suporte operacional, consulte Histórico de versões da solução AWS VSS.

Execução de documentos de comando de snapshot de VSS do Systems Manager

Você pode criar snapshots do EBS baseados no VSS com documentos de comando do AWS Systems Manager conforme a seguir.

Execução do documento de comando AWSEC2-VssInstallAndSnapshot (recomendado)

Quando você usa o AWS Systems Manager para executar o documento `AWSEC2-VssInstallAndSnapshot`, o script executa as etapas a seguir.

1. O script primeiro instala ou atualiza o pacote `AwsVssComponents` na instância, dependendo de ele já estar ou não instalado.
2. O script cria os snapshots consistentes com a aplicação após a conclusão da primeira etapa.

Para executar o documento `AWSEC2-VssInstallAndSnapshot`, siga as etapas para o ambiente de sua preferência.

Console

Criar snapshots do EBS baseados no VSS no console

1. Abra o console AWS Systems Manager em https://console.aws.amazon.com/systems-manager/.
2. Selecione Run Command no painel de navegação. Isso mostra uma lista dos comandos que estão sendo executados atualmente na conta, se aplicável.
3. Selecione Run command. Isso abre uma lista dos documentos de comando a que você tem acesso.
4. Selecione `AWSEC2-VssInstallAndSnapshot` na lista de documentos de comando. Para otimizar os resultados, você pode inserir todo ou parte do nome do documento. Você também pode filtrar pelo proprietário, por tipos de plataforma ou por tags.

   Quando você seleciona um documento de comando, os detalhes são preenchidos abaixo da lista.
5. Selecione `Default version at runtime` na lista Versão do documento.
6. Configure os parâmetros de comando para definir como `AWSEC2-VssInstallAndSnapshot` instalará o pacote `AwsVssComponents` e fará backup com snapshots ou com uma AMI do VSS. Para obter detalhes dos parâmetros, consulte Parâmetros para documentos de snapshot de VSS do Systems Manager.
7. Em Seleção de alvos, especifique as tags ou selecione manualmente as instâncias em que a operação deve ser executada.

   > **Note**
   >
   > Se selecionar manualmente as instâncias e uma instância que você espera ver não estiver incluída na lista, consulte Onde estão minhas instâncias? para obter dicas de solução de problemas.
8. Para obter parâmetros adicionais para definir o comportamento do Run Command do Systems Manager, como, Controle da taxa, insira os valores como descrito em Executar comandos no console.
9. Escolha Run.

   Se bem-sucedido, o comando preenche a lista de snapshots do EBS com os novos snapshots. É possível localizar esses snapshots na lista de snapshots do EBS procurando

as tags que especificou ou então `AppConsistent`. Se a execução do comando falhou, exiba a saída do comando do Systems Manager para obter detalhes do motivo da falha. Se o comando for concluído com êxito, mas houver falha no backup de um volume específico, será possível solucionar essa falha na lista de volumes do EBS.

AWS CLI

Você pode executar os comandos a seguir na AWS CLI para criar snapshots do EBS baseados no VSS e obter o status da criação do snapshot.

Criar snapshots do EBS baseados no VSS

Execute o comando a seguir para criar snapshots do EBS baseados no VSS. Para criar os snapshots, você deve identificar as instâncias com o parâmetro `--instance-ids`. Para obter mais informações sobre outros parâmetros que você pode usar, consulte Parâmetros para documentos de snapshot de VSS do Systems Manager.

```
aws ssm send-command \
 --document-name "AWSEC2-VssInstallAndSnapshot" \
 --instance-ids "i-01234567890abcdef" \
 --parameters '{"ExcludeBootVolume":["False"],"description":["Description"],"tags":
["Key=key_name,Value=tag_value"],"VssVersion":[""]}'
```

Se bem-sucedido, o documento de comando preenche a lista de snapshots do EBS com os novos snapshots. É possível localizar esses snapshots na lista de snapshots do EBS procurando as tags que especificou ou então `AppConsistent`. Se a execução do comando falhou, exiba a saída do comando para obter detalhes do motivo da falha.

Obter status do comando

Para obter o status atual dos snapshots, execute o comando a seguir usando o ID de comando retornado de send-command.

```
aws ssm get-command-invocation
 --instance-ids "i-01234567890abcdef" \
 --command-id "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" \
 --plugin-name "CreateVssSnapshot"
```

PowerShell

Execute os comandos a seguir com o AWS Tools for Windows PowerShell para criar snapshots do EBS baseados no VSS e obter o status atual do runtime da criação da saída. Especifique os parâmetros descritos na lista anterior para modificar o comportamento do processo de snapshots.

Criar snapshots do EBS baseados no VSS com o Tools for Windows PowerShell

Execute o comando a seguir para criar AMIs ou snapshots do EBS baseados no VSS.

```
Send-SSMCommand -DocumentName "AWSEC2-VssInstallAndSnapshot" -InstanceId
 "i-01234567890abcdef" -Parameter
 @{'ExcludeBootVolume'='False';'description'='a_description'
 ;'tags'='Key=key_name,Value=tag_value';'VssVersion'=''}
```

Obter status do comando

Para obter o status atual dos snapshots, execute o comando a seguir usando o ID de comando retornado de Send-SSMCommand.

```
Get-SSMCommandInvocationDetail -InstanceId "i-01234567890abcdef" -CommandId
 "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" -PluginName "CreateVssSnapshot"
```

Se bem-sucedido, o comando preenche a lista de snapshots do EBS com os novos snapshots. É possível localizar esses snapshots na lista de snapshots do EBS procurando as tags que especificou ou então `AppConsistent`. Se a execução do comando falhou, exiba a saída do comando para obter detalhes do motivo da falha.

Execução do documento de comandos AWSEC2-CreateVssSnapshot

Para executar o documento `AWSEC2-CreateVssSnapshot`, siga as etapas para o ambiente de sua preferência.

Console

Criar snapshots do EBS baseados no VSS no console

1. Abra o console AWS Systems Manager em https://console.aws.amazon.com/systems-manager/.

2. Selecione Run Command no painel de navegação. Isso mostra uma lista dos comandos que estão sendo executados atualmente na conta, se aplicável.
3. Selecione Run command. Isso abre uma lista dos documentos de comando a que você tem acesso.
4. Selecione `AWSEC2-CreateVssSnapshot` na lista de documentos de comando. Para otimizar os resultados, você pode inserir todo ou parte do nome do documento. Você também pode filtrar pelo proprietário, por tipos de plataforma ou por tags.

   Quando você seleciona um documento de comando, os detalhes são preenchidos abaixo da lista.
5. Selecione `Default version at runtime` na lista Versão do documento.
6. Configure os Parâmetros de comando para definir como `AWSEC2-CreateVssSnapshot` fará backup com snapshots ou com uma AMI do VSS. Para obter detalhes dos parâmetros, consulte Parâmetros para documentos de snapshot de VSS do Systems Manager.
7. Em Seleção de alvos, especifique as tags ou selecione manualmente as instâncias em que a operação deve ser executada.

   > **Note**
   >
   > Se selecionar manualmente as instâncias e uma instância que você espera ver não estiver incluída na lista, consulte Onde estão minhas instâncias? para obter dicas de solução de problemas.
8. Para obter parâmetros adicionais para definir o comportamento do Run Command do Systems Manager, como, Controle da taxa, insira os valores como descrito em Executar comandos no console.
9. Escolha Run.

   Se bem-sucedido, o comando preenche a lista de snapshots do EBS com os novos snapshots. É possível localizar esses snapshots na lista de snapshots do EBS procurando as tags que especificou ou então `AppConsistent`. Se a execução do comando falhou, exiba a saída do comando do Systems Manager para obter detalhes do motivo da falha. Se o comando for concluído com êxito, mas houver falha no backup de um volume específico, será possível solucionar essa falha na lista de volumes do EBS.

AWS CLI

Você pode executar o comando a seguir na AWS CLI para criar snapshots do EBS baseados no VSS.

Criar snapshots do EBS baseados no VSS

Execute o comando a seguir para criar snapshots do EBS baseados no VSS. Para criar os snapshots, você deve identificar as instâncias com o parâmetro `--instance-ids`. Para obter mais informações sobre outros parâmetros que você pode usar, consulte Parâmetros para documentos de snapshot de VSS do Systems Manager.

```
aws ssm send-command \
 --document-name "AWSEC2-CreateVssSnapshot" \
 --instance-ids "i-01234567890abcdef" \
 --parameters '{"ExcludeBootVolume":["False"],"description":["Description"],"tags":
["Key=key_name,Value=tag_value"]}'
```

Se bem-sucedido, o documento de comando preenche a lista de snapshots do EBS com os novos snapshots. É possível localizar esses snapshots na lista de snapshots do EBS procurando as tags que especificou ou então `AppConsistent`. Se a execução do comando falhou, exiba a saída do comando para obter detalhes do motivo da falha.

PowerShell

Execute o comando a seguir com o AWS Tools for Windows PowerShell para criar snapshots do EBS baseados no VSS.

Criar snapshots do EBS baseados no VSS com o Tools for Windows PowerShell

Execute o comando a seguir para criar snapshots do EBS baseados no VSS. Para criar os snapshots, você deve identificar as instâncias com o parâmetro `InstanceId`. Você pode especificar mais de uma instância para a qual criar snapshots. Para obter mais informações sobre outros parâmetros que você pode usar, consulte Parâmetros para documentos de snapshot de VSS do Systems Manager.

```
Send-SSMCommand -DocumentName AWSEC2-CreateVssSnapshot -InstanceId
 "i-01234567890abcdef" -Parameter
 @{'ExcludeBootVolume'='False';'description'='a_description'
 ;'tags'='Key=key_name,Value=tag_value'}
```

Se bem-sucedido, o comando preenche a lista de snapshots do EBS com os novos snapshots. É possível localizar esses snapshots na lista de snapshots do EBS procurando as tags que especificou ou então `AppConsistent`. Se a execução de comando for malsucedida, exiba a saída de comando do para obter detalhes sobre o motivo da falha na execução. Se o comando for concluído com êxito, mas houver falha no backup de um volume específico, será possível solucionar essa falha na lista de snapshots do EBS.

Execução de documentos de comando para um cluster de failover do Windows com armazenamento compartilhado do EBS

Você pode usar qualquer um dos procedimentos da linha de comandos descritos na seção anterior para criar um snapshot baseado no VSS. O documento de comando (`AWSEC2-VssInstallAndSnapshot` ou `AWSEC2-CreateVssSnapshot`) deve ser executado no nó primário do cluster. O documento falhará nos nós secundários, pois eles não têm acesso aos discos compartilhados. Se o primário e o secundário mudarem dinamicamente, você poderá executar o documento AWS Systems Manager Executar comando em vários nós com a expectativa de que o comando seja bem-sucedido no nó primário e falhe nos nós secundários.

> **Note**
>
> Para automatizar os backups, você pode criar uma tarefa da janela de manutenção do AWS Systems Manager que use o documento `AWSEC2-VssInstallAndSnapshot`. Para obter mais informações, consulte Trabalhar com janelas de manutenção (console) no Manual do usuário do AWS Systems Manager.

Solucionar problemas de snapshots do EBS baseados no Windows VSS

Antes de tentar qualquer outra etapa de solução de problemas, recomendamos verificar os detalhes a seguir.

- Certifique-se de que você atendeu a todos os Pré-requisitos para criar snapshots do EBS baseados no VSS do Windows.
- Verifique se está usando o Suporte para a versão do SO Windows mais recente do pacote `AwsVssComponents` para o sistema operacional. O problema observado pode ter sido resolvido em versões mais recentes.

Tópicos

- Verificar arquivos de log
- Coletar logs de diagnóstico adicionais
- Usar o VSS em instâncias com proxy configurado
- Erro: A conexão do tubo de descongelamento expirou, erro no descongelamento, tempo limite aguardando o VSS Freeze, ou outros erros de tempo limite
- Erro: não é possível invocar o método. A invocação de métodos é compatível somente em tipos principais nesse modo de linguagem.

Verificar arquivos de log

Caso tenha problemas ou receba mensagens de erro ao criar snapshots do EBS baseados no VSS, será possível visualizar a saída do comando no console do Systems Manager.

Para documentos do Systems Manager que criam snapshots do VSS, você pode definir o parâmetro `CollectDiagnosticLogs` como "`True`" no runtime. Quando o parâmetro `CollectDiagnosticLogs` é definido como "`True`", o VSS coleta logs adicionais para ajudar na depuração. Para obter mais informações, consulte Coletar logs de diagnóstico adicionais.

Se você coletar logs de diagnóstico, o documento do Systems Manager os armazena em sua instância no seguinte local: `C:\ProgramData\Amazon\AwsVss\Logs\`*`timestamp`*`.zip`. O padrão do parâmetro `CollectDiagnosticLogs` é "`False`".

> **Note**
>
> Para obter ajuda adicional com a depuração, você pode enviar o arquivo `.zip` para o Suporte.

Os seguintes logs adicionais estarão disponíveis, se você coletar ou não logs de diagnóstico:

- `%ProgramData%\Amazon\SSM\InstanceData\`*`InstanceID`*`\document\orchestration\`*`SSMCommandID`*`\awsrunPowerShellScript\runPowerShellScript\stdout`
- `%ProgramData%\Amazon\SSM\InstanceData\`*`InstanceID`*`\document\orchestration\`*`SSMCommandID`*`\awsrunPowerShellScript\runPowerShellScript\stderr`

Também é possível abrir a aplicação do Windows Event Viewer (Visualizador de Eventos) e escolher Windows Logs (Logs do Windows), Application (Aplicação) para visualizar registros adicionais. Para ver eventos especificamente do provedor VSS do EC2 do Windows e do Volume Shadow Copy Service (Serviço de Cópia de Sombra de Volume), filtre por Source (Origem) nos termos **`Ec2VssSoftwareProvider`** **`VSS`**e.

Se estiver usando o Systems Manager com endpoints da VPC e houver falha na ação da API send-command do Systems Manager (Run Command no console), verifique se configurou corretamente o endpoint a seguir: com.amazonaws.***`region`***.ec2.

Sem o endpoint do Amazon EC2 definido, ocorre falha na chamada para enumerar os volumes anexados do EBS, o que causa a falha do comando do Systems Manager. Para obter mais informações sobre como configurar endpoints da VPC com o Systems Manager, consulte Criar um endpoint da nuvem privada virtual no Manual do usuário do AWS Systems Manager.

Coletar logs de diagnóstico adicionais

Para coletar logs de diagnóstico adicionais ao usar o comando send do Systems Manager para executar o documento de snapshot do VSS, defina o parâmetro de entrada `CollectDiagnosticLogs` como "`True`" no runtime. Recomendamos que você defina esse parâmetro como "`True`" ao solucionar problemas.

Para ver um exemplo da linha de comando, selecione uma das guias a seguir.

AWS CLI

O exemplo a seguir executa o documento `AWSEC2-CreateVssSnapshot` do Systems Manager na AWS CLI:

```
aws ssm send-command \
    --document-name "AWSEC2-CreateVssSnapshot" \
    --instance-ids "i-1234567890abcdef0" \
    --parameters '{"description":["Example - create diagnostic logs at
 runtime."],"tags":["Key=tag_name,Value=tag_value"],"CollectDiagnosticLogs":
["True"]}'
```

PowerShell

O exemplo a seguir executa o documento `AWSEC2-CreateVssSnapshot` do Systems Manager no PowerShell:

```
Send-SSMCommand `
    -DocumentName "AWSEC2-CreateVssSnapshot" `
    -InstanceId "i-1234567890abcdef0" `
    -Parameter @{'description'='Example - create diagnostic logs at
 runtime.';'tags'='Key=tag_name,Value=tag_value';'CollectDiagnosticLogs'='True'}
```

Usar o VSS em instâncias com proxy configurado

Caso tenha problemas ao criar snapshots do EBS baseados no VSS em instâncias que usam um proxy para alcançar endpoints do EC2, verifique as seguintes configurações na instância:

- Certifique-se de que o proxy esteja configurado de modo que os endpoints de serviço do EC2 na região e no IMDS da instância possam ser alcançados pelo AWS Tools for Windows PowerShell em execução como SYSTEM.
- Para oferecer suporte ao uso do proxy WinHTTP configurado pelo sistema, certifique se de ter instalado a versão mais recente de `AwsVssComponents` na instância. Para obter mais informações sobre a configuração do proxy WinHTTP, consulte Netsh Commands for Windows Hypertext Transfer Protocol (WINHTTP) no site da Microsoft.

Erro: A conexão do tubo de descongelamento expirou, erro no descongelamento, tempo limite aguardando o VSS Freeze, ou outros erros de tempo limite

O provedor VSS da EC2 Windows pode atingir o tempo limite devido a atividades ou serviços na instância impedindo que snapshots baseados no VSS prossigam em tempo hábil. O Windows VSS Framework fornece uma janela de 10 segundos não configurável durante a qual a comunicação com o sistema de arquivos é pausada. Durante esse tempo, o `AWSEC2-CreateVssSnapshot` captura seus volumes.

Os seguintes problemas podem fazer com que o provedor VSS do EC2 para Windows seja executado em limites de tempo durante um snapshot:

- E/S excessiva para um volume
- Capacidade de resposta lenta da API do EC2 na instância
- Volumes fragmentados
- Incompatibilidade com algum software antivírus
- Problemas com um gravador de aplicação de VSS

- Quando o Registro de Módulos estiver habilitado para um grande número de módulos do PowerShell, os scripts do PowerShell poderão ser executados com lentidão

A maioria dos problemas de tempo limite que ocorrem ao executar o documento de comando `AWSEC2-CreateVssSnapshot` está relacionada à workload na instância ser muito alta no momento do backup. As ações a seguir podem ajudá-lo a obter um snapshot bem-sucedido:

- Tente novamente o comando `AWSEC2-CreateVssSnapshot` para ver se a tentativa do snapshot é bem-sucedida. Se a nova tentativa for bem-sucedida em alguns casos, reduzir a carga da instância poderá tornar os snapshots mais bem-sucedidos.
- Aguarde um pouco até que a workload na instância diminua e tente novamente o comando `AWSEC2-CreateVssSnapshot`. Como alternativa, é possível tentar capturar snapshots quando a instância é conhecida por estar sob baixa tensão.
- Tente snapshots do VSS quando o software antivírus no sistema estiver desativado. Se isso resolver o problema, consulte as instruções do software antivírus e configure-o para permitir snapshots do VSS.
- Se houver um grande volume de chamadas de API do Amazon EC2 na sua conta na mesma região em que estiver executando um snapshot, o controle de utilização da API pode atrasar as operações de snapshot. Para reduzir o impacto do controle de utilização, use o pacote `AwsVssComponents` mais recente. Esse pacote utiliza a ação da API `CreateSnapshots` do EC2 para reduzir o número de ações mutantes, como a criação e a marcação de snapshots por volume.
- Se você tiver vários scripts de comando `AWSEC2-CreateVssSnapshot` em execução ao mesmo tempo, siga as etapas a seguir para reduzir os problemas de simultaneidade.
  - Considere agendar snapshots durante períodos de menor atividade da API.
  - Se você usar o Run Command no console do Systems Manager (ou o SendCommand na API) para executar o script de comando, poderá usar os controles de taxa do Systems Manager para reduzir a simultaneidade.

    Você também pode usar os controles de taxa do Systems Manager para reduzir a simultaneidade em serviços como o AWS Backup, que usam o Systems Manager para executar o script de comando.
- Execute o comando `vssadmin list writers` em um shell e veja se ele relata quaisquer erros no campo Last error (Último erro) para qualquer gravador no sistema. Se algum gravador relatar um erro de tempo esgotado, tente novamente capturar snapshots quando a instância estiver com menos carga.

- Ao usar tipos de instância menores, como *t2 | t3 | t3a*.nano ou *t2 | t3 | t3a*.micro, podem ocorrer tempos limite devido a restrições de memória e CPU. As ações a seguir podem ajudar a reduzir os problemas de tempo limite.
  - Tente fechar aplicações que consomem muita memória ou CPU antes de tirar snapshots.
  - Tente tirar snapshots durante períodos de menor atividade das instâncias.

Erro: não é possível invocar o método. A invocação de métodos é compatível somente em tipos principais nesse modo de linguagem.

Você receberá esse erro quando o modo de idioma da PowerShell não estiver definido como `FullLanguage`. O documento do SSM `AWSEC2-CreateVssSnapshot` exige que o PowerShell seja configurado no modo `FullLanguage`.

Para verificar o modo de idioma, execute o comando a seguir na instância em um console da PowerShell:

```
$ExecutionContext.SessionState.LanguageMode
```

Para obter mais informações sobre os modos de idioma, consulte about_Language_Modes na documentação da Microsoft.

Usar a solução AWS VSS para restaurar os dados da sua instância

Você pode restaurar volumes do EBS para uma instância Windows a partir de snapshots baseados em VSS criados pela solução AWS VSS. Se os snapshots da solução AWS VSS incluírem backups de um banco de dados Microsoft SQL Server, será possível restaurar esse banco de dados usando o runbook do `AWSEC2-RestoreSqlServerDatabaseWithVss` AWS Systems Manager Automation.

O runbook de restauração de banco de dados automatiza o processo de restauração inteiro, incluindo a criação de volumes a partir dos snapshots e a anexação desses volumes à instância. A automação aproveita a tecnologia do VSS para restaurar o banco de dados, permitindo uma restauração sem interromper a aplicação SQL Server ou desconectar quaisquer conexões ativas.

Para instruções detalhadas sobre como usar o runbook de banco de dados Microsoft SQL Server, consulte Restaurar a partir de snapshots com base no VSS, no Guia do usuário do Microsoft SQL Server no Amazon EC2.

Personalizar um script para restaurar volumes do EBS a partir de snapshots da solução AWS VSS

É possível usar o script `RestoreVssSnapshotSampleScript.ps1` como modelo para criar seu próprio script personalizado, que restaura volumes do EBS a partir de snapshots da solução AWS VSS. O script de amostra executa as seguintes tarefas:

- Interrompe uma instância
- Remove todos os discos existentes da instância (exceto o volume de inicialização, se ele tiver sido excluído)
- Cria novos volumes por meio dos snapshots
- Anexa os volumes à instância usando a tag do ID do dispositivo no snapshot
- Reinicia a instância

> **Important**
>
> O script a seguir separa todos os volumes anexados a uma instância e, em seguida, cria novos volumes por meio de um snapshot. É essencial fazer um backup correto da instância. Os volumes antigos não são excluídos. Se desejar, é possível editar o script para excluir os volumes antigos.

Para restaurar volumes por meio de snapshots do EBS baseados no VSS

1. Faça download do arquivo RestoreVssSnapshotSampleScript.zip e extraia o conteúdo dele.
2. Abra `RestoreVssSnapshotSampleScript.ps1` em um editor de texto e edite a chamada de amostra na parte inferior do script com um ID válido de instância do EC2 e o ID do snapshot do EBS. Depois, execute o script pelo PowerShell.

Histórico de versões da solução AWS VSS

Analise as notas de lançamento do pacote de componentes do VSS da AWS, além dos requisitos de versão de componentes e scripts para cada versão compatível do Windows Server.

Tópicos

- Versões do pacote AwsVssComponents

- Suporte para a versão do SO Windows

Versões do pacote AwsVssComponents

A tabela a seguir descreve as versões lançadas do pacote de componentes do AWS VSS.

Versão	Detalhes	Data de lançamento	Disponíveis para download
2.5.1	Foi corrigido um caso em que a restauração do banco de dados SQL poderia falhar quando o parâmetro do banco de dados de destino fosse especificado.	13 de março de 2025	Sim
2.5.0	• Adição da capacidade de ler arquivos de metadados do VSS e de restaurar um banco de dados Microsoft SQL Server na instância. Para obter mais informações, consulte Restaurar a partir de snapshots com base no VSS, no Guia do usuário do Microsoft SQL Server no Amazon EC2. • Foi adicionado suporte para a opção de atualização no próprio local ao instalar ou atualizar o pacote `AwsVssComponents` .	17 de janeiro de 2025	Sim
2.4.0	Adicionada a capacidade de salvar arquivos de metadados do VSS na criação de snapshots. Para habilitar esse recurso, consulte SaveVssMetadata em Parâmetros para documentos de snapshot de VSS do Systems Manager.	7 de outubro de 2024	Sim
2.3.3	O agente do VSS foi atualizado para garantir que o `Ec2VssProvider` seja usado durante a criação do snapshot.	25 de junho de 2024	Sim

Versão	Detalhes	Data de lançamento	Disponíveis para download
2.3.2	Corrigido um caso em que o registro do provedor do VSS não era removido na desinstalação.	9 de maio de 2024	Sim
2.3.1	Adição de uma nova tag padrão `AwsVssConfig` para identificar snapshots e AMIs criados pelo AWS VSS.	7 de março de 2024	Sim
2.2.1	• Adição de compatibilidade com o uso da API `DescribeInstanceAttribute` . • Correções de bugs e aprimoramentos em confiabilidade. • Suporte obsoleto para Windows Server 2012 e 2012 R2. AWS A instalação dos componentes do VSS versão 2.2.1 no Windows Server 2012 e 2012 R2 falhará. AWS A versão 2.1.0 dos componentes do VSS é a última versão compatível com o Windows Server 2012 e 2012 R2.	18 de janeiro de 2024	Sim
2.1.0	Adição de compatibilidade com o uso da API `CreateSnapshots` .	6 de novembro de 2023	Sim
2.0.1	Adicionada compatibilidade com o uso das configurações do proxy WinHTTP.	26 de outubro de 2023	Não

Versão	Detalhes	Data de lançamento	Disponíveis para download
2.0.0	Capacidade adicionada ao componente AWS VSS para criar snapshots e AMIs, o que permite a compatibilidade com os recursos de registro em log do módulo PowerShell, registro em log de blocos de scripts e transcrição.	28 de abril de 2023	Não
1.3.2.0	Corrigido um caso em que a falha de instalação não é relatada corretamente.	10 de maio de 2022	Não
1.3.1.0	• Correção de snapshots com falha em controladores de domínio em relação a um erro de registro de gravador NTDS VSS. • Correção do erro do agente VSS ao desinstalar o provedor VSS versão 1.0.	6 de fevereiro de 2020	Sim
1.3.00	• Registro aprimorado reduzindo a verbosidade indesejada. • Correção de problemas de regionalização durante a instalação. • Correção de códigos de retorno para algumas condições de erro de registro do provedor. • Correção de vários problemas de instalação.	19 de março de 2019	Não

Versão	Detalhes	Data de lançamento	Disponíveis para download
1.2.00	• Adição de parâmetros de linha de comando `-nw` (sem gravadores) e `-copy` (somente cópia) ao agente. • Correção de erros de log de eventos causados por chamadas inadequadas de alocação de memória.	15 de novembro de 2018	Não
1.1	Correção de componentes do AWS VSS que estavam sendo usados incorretamente como o provedor padrão de Backup e Restauração do Windows.	12 de dezembro de 2017	Não
1,0	Versão inicial.	20 de novembro de 2017	Não

Suporte para a versão do SO Windows

A tabela a seguir mostra as versões da solução AWS VSS que devem ser executadas em cada versão do Windows Server no Amazon EC2.

Versão Windows Server	Versão do AwsVssComponents	Nome da versão do AWSEC2-VssInstallAndSnapshot	Nome da versão do AWSEC2-CreateVssSnapshot
Windows Server 2025	padrão	padrão	padrão

Versão Windows Server	Versão do AwsVssComponents	Nome da versão do AWSEC2-VssInstallAndSnapshot	Nome da versão do AWSEC2-CreateVssSnapshot
Windows Server 2022	padrão	padrão	padrão
Windows Server 2019	padrão	padrão	padrão
Windows Server 2016	padrão	padrão	padrão
Windows Server 2012 R2	2.1.0	não compatível	2012R2
Windows Server 2012	2.1.0	não compatível	2012R2
Windows Server 2008 R2	1.3.1.0	não compatível	2008R2

Armazenamento de objetos, armazenamento de arquivos e armazenamento em cache de arquivos no Amazon EC2

O armazenamento de arquivos na nuvem é um método de armazenamento de dados na nuvem que permite que servidores e aplicações acessem os dados por meio de sistemas de arquivos compartilhados. Essa compatibilidade faz do armazenamento de arquivos na nuvem uma opção

ideal para workloads que dependem de sistemas de arquivos compartilhados e oferece simplicidade de integração, sem alterações de código.

Há muitas soluções de armazenamento de arquivos, desde um servidor de arquivos de nó único em uma instância de computação que usa armazenamento em blocos como base sem escalabilidade ou poucas redundâncias para proteger os dados a uma solução clusterizada do tipo "faça você mesmo" ou a uma solução totalmente gerenciada. O conteúdo apresentado a seguir introduz alguns dos serviços de armazenamento fornecidos pela AWS para o uso com instâncias do Amazon EC2.

Conteúdo

- Usar o Amazon S3 com instâncias do Amazon EC2
- Usar o Amazon EFS com instâncias do Linux do Amazon EC2
- Usar o Amazon FSx com instâncias do Amazon EC2
- Usar o Amazon File Cache com instâncias do Amazon EC2

Usar o Amazon S3 com instâncias do Amazon EC2

O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos que oferece escalabilidade líder do setor, disponibilidade de dados, segurança e performance. É possível usar o Amazon S3 para armazenar e recuperar qualquer volume de dados para uma variedade de casos de uso, como data lakes, sites, backups e big data analytics, diretamente de uma instância do Amazon EC2 ou de qualquer lugar na Internet. Para obter mais informações, consulte O que é a Amazon S3?

Os objetos são as entidades fundamentais armazenadas no Amazon S3. Cada objeto armazenado no Amazon S3 é contido em um bucket. Os buckets organizam o namespace do Amazon S3 no nível mais alto e identificam a conta responsável por esse armazenamento. Os buckets do Amazon S3 são semelhantes aos nomes de domínio da Internet. Os objetos armazenados em buckets têm um valor de chave exclusiva e são recuperados usando um URL. Por exemplo, se um objeto com um valor de chave `/photos/mygarden.jpg` estiver armazenado no bucket `amzn-s3-demo-bucket1`, ele será endereçável usando a URL `https://amzn-s3-demo-bucket1.s3.amazonaws.com/photos/mygarden.jpg`. Para obter mais informações, consulte Como o Amazon S3 funciona.

Exemplos de uso

Considerando os benefícios do Amazon S3 para armazenamento, é possívelria usar esse serviço para armazenar arquivos e conjuntos de dados para uso com instâncias do EC2. Há várias maneiras

de mover dados do Amazon S3 para suas instâncias e vice-versa. Além dos exemplos discutidos a seguir, há várias ferramentas escritas por pessoas que é possível usar para acessar seus dados no Amazon S3, no computador ou na instância.

Se você tiver permissão, poderá copiar um arquivo entre o Amazon S3 e sua instância usando um dos seguintes métodos.

wget

> **Note**
>
> Esse método funciona apenas para objetos públicos. Se o objeto não for público, você receberá uma mensagem `ERROR 403: Forbidden`. Se receber esse erro, será necessário usar o console do Amazon S3, a AWS CLI, a API da AWS, o AWS SDK ou AWS Tools for Windows PowerShell e é necessário ter as permissões necessárias. Para obter mais informações, consulte Gerenciamento de identidade e acesso no Amazon S3 e Download de um objeto no Guia do usuário do Amazon S3.

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://amzn-s3-demo-bucket.s3.amazonaws.com/path-to-file
```

PowerShell

É possível usar AWS Tools for Windows PowerShell para mover objetos do e para o Amazon S3.

Use o cmdlet Copy-S3Object para copiar um objeto do Amazon S3 para sua instância Windows, da seguinte maneira.

```
Copy-S3Object `
    -BucketName amzn-s3-demo-bucket `
    -Key path-to-file `
    -LocalFile my_copied_file.ext
```

Como alternativa, você pode abrir o console do Amazon S3 usando um navegador da Web na instância Windows.

AWS CLI

É possível a AWS Command Line Interface (AWS CLI) para baixar itens restritos do Amazon S3 e também para fazer 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. É possível copiar arquivos do Amazon S3 para sua instância, copiar arquivos de sua instância para o Amazon S3, e copiar arquivos de um local do Amazon S3 para outro.

Use o comando a seguir para copiar um objeto do Amazon S3 em sua instância.

```
aws s3 cp s3://amzn-s3-demo-bucket/my_folder/my_file.ext my_copied_file.ext
```

Use o comando a seguir para copiar um objeto de sua instância de volta para o Amazon S3.

```
aws s3 cp my_copied_file.ext s3://amzn-s3-demo-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, será possível enviar o backup do diretório local por push para a nuvem quando concluir invertendo os locais de origem e de destino no comando.

Use o seguinte comando para fazer download de todo o bucket do Amazon S3 para um diretório local em sua instância.

```
aws s3 sync s3://amzn-s3-demo-source-bucket local_directory
```

Amazon S3 API

Se você for um desenvolvedor, poderá usar uma API para acessar dados no Amazon S3. É possível usar essa API para ajudar a desenvolver sua aplicação e integrá-la com outras APIs e SDKs. Para obter mais informações, consulte Exemplos de código para o Amazon S3 usando AWS SDKs na Referência da API do Amazon Simple Storage Service.

Usar o Amazon EFS com instâncias do Linux do Amazon EC2

> **Note**
>
> O Amazon EFS não é compatível com instâncias do Windows.

O Amazon EFS fornece armazenamento de arquivos escalável para uso com o Amazon EC2. É possível usar um sistema de arquivos de EFS como uma fonte de dados comum para workloads e aplicações em execução em várias instâncias. Para obter mais informações, consulte a página do produto Amazon Elastic File System.

Este tutorial demonstra como criar e anexar um sistema de arquivos do Amazon EFS ao usar o assistente de criação rápida do Amazon EFS durante a inicialização da instância. Para obter um tutorial sobre como criar um sistema de arquivos usando o console do Amazon EFS, consulte Getting started with Amazon Elastic File System (Conceitos básicos do Amazon Elastic File System) no Guia do usuário do Amazon Elastic File System.

> **Note**
>
> Quando você cria um sistema de arquivos do EFS usando a Criação rápida do EFS, o sistema de arquivos é criado com as seguintes configurações recomendadas de serviço:
>
> - Backups automáticos habilitados.
> - Gerencie os destinos de montagem na VPC selecionada.
> - Modo de performance de uso geral.
> - Modo de throughput intermitente.
> - Criptografia de dados em repouso habilitada usando a chave padrão para o Amazon EFS (`aws/elasticfilesystem`).
> - Gerenciamento do ciclo de vida do Amazon EFS habilitado com uma política de 30 dias.

Tarefas

- Criar um sistema de arquivos do EFS usando a Criação rápida do Amazon EFS
- Testar o sistema de arquivos do EFS
- Excluir o sistema de arquivos do EFS

Criar um sistema de arquivos do EFS usando a Criação rápida do Amazon EFS

É possível criar um sistema de arquivos do EFS e montá-lo na instância ao iniciar a instância usando o recurso de criação rápida do Amazon EFS do assistente de execução de instâncias do Amazon EC2.

Para criar um sistema de arquivos do EFS usando a Criação Rápida do Amazon EFS

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Escolha Iniciar instância.
3. (Opcional) Em Name and tags (Nome e etiquetas), para Name (Nome), insira um nome para identificar a instância.
4. Em Application and OS Images (Amazon Machine Image) (Imagens de aplicações e sistemas operacionais [imagem de máquina da Amazon]), escolha um sistema operacional Linux e, em Amazon Machine Image (AMI) (Imagem de máquina da Amazon [AMI]), selecione uma AMI do Linux.
5. Em Instance type (Tipo de instância), para Instance type (Tipo de instância), selecione um tipo de instância ou mantenha o padrão.
6. Em Key pair (login) (Par de chaves, login), Key pair name (Nome do par de chaves), escolha um par de chaves existente ou crie um novo.
7. Em Network settings (Configurações de rede), escolha Edit (Editar) à direita e, para Subnet (Sub-rede), selecione uma sub-rede.

   > **Note**
   >
   > É necessário selecionar uma sub-rede antes de adicionar um sistema de arquivos do EFS.

8. Em Configure storage (Configurar armazenamento), escolha Edit (Editar) no canto inferior direito e realize estas etapas:

   a. Em Sistemas de arquivos, certifique-se de que EFS esteja selecionado e, em seguida, escolha Criar sistema de arquivos compartilhado.

   b. Em Nome do sistema de arquivos, insira um nome para o sistema de arquivos do Amazon EFS e, em seguida, escolha Criar sistema de arquivos.

   c. Em Ponto de montagem, especifique um ponto de montagem personalizado ou mantenha o padrão.

d. Para habilitar o acesso ao sistema de arquivos, selecione Automatically create and attach security groups (Criar e anexar grupos de segurança automaticamente). Ao marcar essa caixa de seleção, os seguintes grupos de segurança serão automaticamente criados e anexados à instância e aos destinos de montagem do sistema de arquivos:

   - Grupo de segurança da instância: inclui uma regra de saída que permite o tráfego pela porta NFS 2049, mas não inclui regras de entrada.
   - Grupo de segurança de destinos de montagem do sistema de arquivos: contém uma regra de entrada que permite o tráfego pela porta NFS 2049 proveniente do grupo de segurança da instância (descrito acima) e uma regra de saída que permite o tráfego pela porta NFS 2049.

   > **Note**
   >
   > Como alternativa, é possível criar e anexar os grupos de segurança de forma manual. Para criar e anexar manualmente os grupos de segurança, desmarque Automatically create and attach the required security groups (Criar e anexar automaticamente os grupos de segurança necessários).

e. Para montar automaticamente o sistema de arquivos compartilhado quando a instância for iniciada, selecione Automatically mount shared file system by attaching required user data script (Montar automaticamente o sistema de arquivos compartilhado anexando o script de dados do usuário necessário). Para visualizar os dados do usuário gerados automaticamente, expanda Advanced details (Detalhes avançados) e role para baixo até User data (Dados do usuário).

   > **Note**
   >
   > Se você adicionou dados do usuário antes de marcar essa caixa de seleção, os dados do usuário originais serão substituídos pelos dados do usuário gerados automaticamente.

9. Defina outras configurações da instância, conforme necessário.
10. No painel Resumo, analise a configuração da instância e selecione Iniciar instância. Para ter mais informações, consulte Executar uma instância do EC2 usando o assistente de inicialização de instâncias no console.

Testar o sistema de arquivos do EFS

É possível se conectar à instância 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 à sua instância. Para ter mais informações, consulte Conectar-se à instância do Linux usando SSH.
2. Na janela do terminal da instância, execute o comando df -T para verificar se o sistema de arquivos do 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 na instância e verifique se é possível visualizar o arquivo por outra instância.

   a. Na instância, execute o seguinte comando para criar o arquivo.

   ```
   $ sudo touch /mnt/efs/test-file.txt
   ```

   b. Na outra instância, execute o comando a seguir para visualizar o arquivo.

   ```
   $ ls /mnt/efs
   test-file.txt
   ```

Excluir o sistema de arquivos do EFS

Se não precisar mais do arquivo de sistemas, será possível excluí-lo.

Para excluir o sistema de arquivos

1. Abra o console do Amazon Elastic File System em https://console.aws.amazon.com/efs/.
2. Selecione o sistema de arquivos a ser excluído.
3. Escolha Actions (Ações), Delete file system (Excluir sistema de arquivos).
4. Quando a confirmação for solicitada, insira o ID do sistema de arquivos e escolha Delete file system (Excluir sistema de arquivos).

Usar o Amazon FSx com instâncias do Amazon EC2

A família de serviços Amazon FSx facilita a inicialização, a execução e a escala do armazenamento compartilhado alimentado por sistemas de arquivos comerciais e de código aberto populares. É possível usar o novo assistente de inicialização de instância para anexar automaticamente os seguintes tipos de sistemas de arquivos Amazon FSx às suas instâncias do Amazon EC2 na inicialização:

- O Amazon FSx for NetApp ONTAP fornece armazenamento compartilhado totalmente gerenciado na Nuvem AWS com os recursos populares de acesso e gerenciamento de dados do NetApp ONTAP.
- O Amazon FSx for OpenZFS fornece armazenamento compartilhado econômico e totalmente gerenciado, alimentado pelo popular sistema de arquivos OpenZFS.

> **Note**
>
> - Essa funcionalidade está disponível somente no novo assistente de inicialização de instância. Para obter mais informações, consulte Executar uma instância do EC2 usando o assistente de inicialização de instâncias no console
> - Os sistemas de arquivos do Amazon FSx para Windows File Server e Amazon FSx para Lustre não podem ser montados na inicialização. É necessário montar esses sistemas de arquivos manualmente após a inicialização.

É possível escolher montar um sistema de arquivos existente criado anteriormente ou criar um novo sistema de arquivos para montar em uma instância na inicialização.

Tópicos

- Script de dados do usuário e de grupos de segurança
- Montar um sistema de arquivos Amazon FSx na inicialização

Script de dados do usuário e de grupos de segurança

Quando você monta um sistema de arquivos Amazon FSx em uma instância usando o assistente de inicialização de instância, é possível escolher se deseja criar e anexar automaticamente os grupos de segurança necessários para habilitar o acesso ao sistema de arquivos e se deseja incluir automaticamente os scripts de dados do usuário necessários para montar o sistema de arquivos e torná-lo disponível para uso.

Tópicos

- Grupos de segurança
- Script de dados do usuário

Grupos de segurança

Se você optar por criar automaticamente os grupos de segurança necessários para habilitar o acesso ao sistema de arquivos, o assistente de inicialização de instância criará e anexará dois grupos de segurança: um é anexado à instância e o outro é anexado ao sistema de arquivos. Para obter mais informações sobre os requisitos do grupo de segurança, consulte Controle de acesso do sistema de arquivos FSx for ONTAP com Amazon VPC e Controle de acesso do sistema de arquivos FSx for OpenZFS com Amazon VPC.

Adicionamos a etiqueta `Name=instance-sg-1` ao grupo de segurança que é criado e anexado à instância. O valor na etiqueta é incrementado automaticamente toda vez que o assistente de execução de instância cria um grupo de segurança para sistemas de arquivos do Amazon FSx.

O grupo de segurança inclui as regras de saída a seguir, mas nenhuma regra de entrada.

Regras de saída

Tipo de protocolo	Número da porta	Destino
UDP	111	*grupo de segurança do sistema de arquivos*
UDP	20001 - 20003	*grupo de segurança do sistema de arquivos*
UDP	4049	*grupo de segurança do sistema de arquivos*
UDP	2049	*grupo de segurança do sistema de arquivos*
UDP	635	*grupo de segurança do sistema de arquivos*
UDP	4045 - 4046	*grupo de segurança do sistema de arquivos*
TCP	4049	*grupo de segurança do sistema de arquivos*
TCP	635	*grupo de segurança do sistema de arquivos*
TCP	2049	*grupo de segurança do sistema de arquivos*
TCP	111	*grupo de segurança do sistema de arquivos*
TCP	4045 - 4046	*grupo de segurança do sistema de arquivos*
TCP	20001 - 20003	*grupo de segurança do sistema de arquivos*

Tipo de protocolo	Número da porta	Destino
Todos	Todos	*grupo de segurança do sistema de arquivos*

O grupo de segurança criado e anexado ao sistema de arquivos é marcado com `Name=fsx-sg-`*1*. O valor na etiqueta é incrementado automaticamente toda vez que o assistente de execução de instância cria um grupo de segurança para sistemas de arquivos do Amazon FSx.

O grupo de segurança inclui as regras a seguir.

Regras de entrada

Tipo de protocolo	Número da porta	Origem
UDP	2049	*security group da instância*
UDP	20001 - 20003	*security group da instância*
UDP	4049	*security group da instância*
UDP	111	*security group da instância*
UDP	635	*security group da instância*
UDP	4045 - 4046	*security group da instância*
TCP	4045 - 4046	*security group da instância*
TCP	635	*security group da instância*
TCP	2049	*security group da instância*
TCP	4049	*security group da instância*
TCP	20001 - 20003	*security group da instância*
TCP	111	*security group da instância*

Regras de saída

Tipo de protocolo	Número da porta	Destino
Todos	Tudo	0.0.0.0/0

Script de dados do usuário

Se você optar por anexar automaticamente scripts de dados do usuário, o assistente de inicialização de instância adicionará os seguintes dados do usuário à instância. Este script instala os pacotes necessários, monta o sistema de arquivos e atualiza as configurações da instância para que o sistema de arquivos seja remontado automaticamente sempre que a instância for reiniciada.

```
#cloud-config
package_update: true
package_upgrade: true
runcmd:
- yum install -y nfs-utils
- apt-get -y install nfs-common
- svm_id_1=svm_id
- file_system_id_1=file_system_id
- vol_path_1=/vol1
- fsx_mount_point_1=/mnt/fsx/fs1
- mkdir -p "${fsx_mount_point_1}"
- if [ -z "$svm_id_1" ]; then printf "\n${file_system_id_1}.fsx.eu-
north-1.amazonaws.com:/${vol_path_1} ${fsx_mount_point_1} nfs4
 nfsvers=4.1,rsize=1048576,wsize=1048576,hard,timeo=600,retrans=2,noresvport,_netdev
 0 0\n" >> /etc/fstab; else printf "\n${svm_id_1}.${file_system_id_1}.fsx.eu-
north-1.amazonaws.com:/${vol_path_1} ${fsx_mount_point_1} nfs4
 nfsvers=4.1,rsize=1048576,wsize=1048576,hard,timeo=600,retrans=2,noresvport,_netdev 0
 0\n" >> /etc/fstab; fi
- retryCnt=15; waitTime=30; while true; do mount -a -t nfs4 defaults; if [ $? = 0 ] ||
 [ $retryCnt -lt 1 ]; then echo File system mounted successfully; break; fi; echo File
 system not available, retrying to mount.; ((retryCnt--)); sleep $waitTime; done;
```

Montar um sistema de arquivos Amazon FSx na inicialização

Para montar um sistema de arquivos Amazon FSx novo ou existente na inicialização

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

2. No painel de navegação, selecione Instances (Instâncias) e, depois, escolha Launch instance (Iniciar instância) para abrir o assistente de inicialização de instância.
3. Na seção Application and OS Images (Imagens de aplicações e SO), selecione a AMI a ser usada.
4. Na seção Instance type (Tipo de instância), selecione o tipo de instância.
5. Na seção Key pair (Par de chaves), selecione um par de chaves existente ou crie um novo.
6. Na seção Network settings (Configurações da rede), faça o seguinte:

    a. Escolha Editar.

    b. Se você deseja montar um sistema de arquivos existente, para Subnet (Sub-rede), escolha a sub-rede preferida do sistema de arquivos. Recomendamos que você execute a instância na mesma zona de disponibilidade da sub-rede preferencial do sistema de arquivos para otimizar a performance.

    Se você deseja criar um novo sistema de arquivos para montar em uma instância, para Subnet (Sub-rede), escolha a sub-rede na qual deseja iniciar a instância.

    > **Important**
    >
    > É necessário selecionar uma sub-rede para habilitar a funcionalidade do Amazon FSx no novo assistente de inicialização de instância. Se você não selecionar uma sub-rede, não poderá montar um sistema de arquivos existente ou criar um novo.

7. Na seção Storage (Armazenamento), faça o seguinte:

    a. Configure os volumes conforme necessário.

    b. Expanda a seção File systems (Sistemas de arquivos) e selecione FSx.

    c. Selecione Add shared file system (Adicionar sistema de arquivos compartilhado).

    d. Para File system (Sistema de arquivos), selecione o sistema de arquivos a ser montado.

    > **Note**
    >
    > A lista exibe todos os sistemas de arquivos do Amazon FSx para NetApp ONTAP e Amazon FSx para OpenZFS na sua conta na região selecionada.

    e. Para criar e anexar automaticamente os grupos de segurança necessários para habilitar o acesso ao sistema de arquivos, selecione Automatically create and attach security groups

(Criar e anexar grupos de segurança automaticamente). Se você preferir criar os grupos de segurança manualmente, desmarque a caixa de seleção. Para ter mais informações, consulte Grupos de segurança.

f. Para anexar automaticamente os scripts de dados do usuário necessários para montar o sistema de arquivos, selecione Automatically mount shared file system by attaching required user data script (Montar automaticamente o sistema de arquivos compartilhados anexando o script de dados do usuário necessário). Se você preferir fornecer os scripts de dados do usuário manualmente, desmarque a caixa de seleção. Para ter mais informações, consulte Script de dados do usuário.

8. Na seção Advanced (Avançado), defina as configurações de instância adicionais conforme necessário.
9. Escolha Executar.

Usar o Amazon File Cache com instâncias do Amazon EC2

O Amazon File Cache é um cache de alta velocidade totalmente gerenciado na AWS que facilita processar dados de arquivos, independentemente de onde os dados estejam armazenados. O Amazon File Cache serve como um local temporário e de alto desempenho para armazenamento de dados que ficam em sistemas de arquivos on-premises, sistemas de arquivos da AWS e buckets do Amazon Simple Storage Service (Amazon S3). Você pode usar esse recurso a fim de disponibilizar conjuntos de dados dispersos para aplicações baseadas em arquivos na AWS com uma visão unificada e altas velocidades (latências inferiores a um milissegundo e alto throughput). Para obter mais informações, consulte o Guia do usuário do Amazon File Cache.

O Amazon File Cache funciona com as AMIs mais populares do Linux e é compatível com os tipos de instâncias baseadas em x86 e os tipos de instâncias Graviton. Você pode acessar seu cache por meio de suas instâncias do Amazon EC2 usando o cliente de código aberto Lustre. Você pode montar seu cache e depois trabalhar com os arquivos e diretórios em seu cache usando comandos padrão do Linux. As instâncias do Amazon EC2 podem acessar seu cache por meio de outras zonas de disponibilidade na mesma nuvem privada virtual (VPC), desde que sua configuração de rede permita o acesso entre sub-redes na VPC. Você também pode criar um cache em uma VPC compartilhada.

Para começar, consulte Getting started with Amazon File Cache no Guia do usuário do Amazon File Cache.

Gerenciar recursos do Amazon EC2

Um recurso é uma entidade com a qual você pode trabalhar. O Amazon EC2 cria recursos à medida que você usa os recursos do serviço. Por exemplo, os recursos do Amazon EC2 incluem imagens, instâncias, frotas, pares de chaves e grupos de segurança. Todos os tipos de recursos do Amazon EC2 incluem atributos que descrevem os recursos. Por exemplo, nomes, descrições, identificadores de recursos e nomes do recurso da Amazon (ARN).

Os recursos do Amazon EC2 são específicos para a região ou zona de disponibilidade da AWS em que eles residem. Por exemplo, uma imagem de máquina da Amazon (AMI) é específica para uma região da AWS, mas a instância que você executa em uma AMI é específica para a zona em que você a executa. É possível especificar um recurso do Amazon EC2 em uma política de permissões usando o ARN do recurso.

Sua Conta da AWS tem cotas padrão para o Amazon EC2. Essas cotas definem o número máximo de recursos que você pode criar. Por exemplo, há cotas para o número máximo de vCPUs nas instâncias em execução. Se ao executar uma instância ou iniciar uma instância interrompida fizer com que você exceda sua cota, a operação falhará.

É possível pesquisar recursos específicos em sua Conta da AWS por região usando IDs ou tags de recursos. Para pesquisar recursos específicos ou tipos de recursos específicos em várias regiões, use o Amazon EC2 Global View.

Conteúdo

- Selecionar uma região para os recursos do Amazon EC2
- Encontrar seus recursos do Amazon EC2
- Visualizar recursos entre regiões usando a Visualização Global da AWS
- Marcar com tag os recursos do Amazon EC2
- Service Quotas do Amazon EC2

Selecionar uma região para os recursos do Amazon EC2

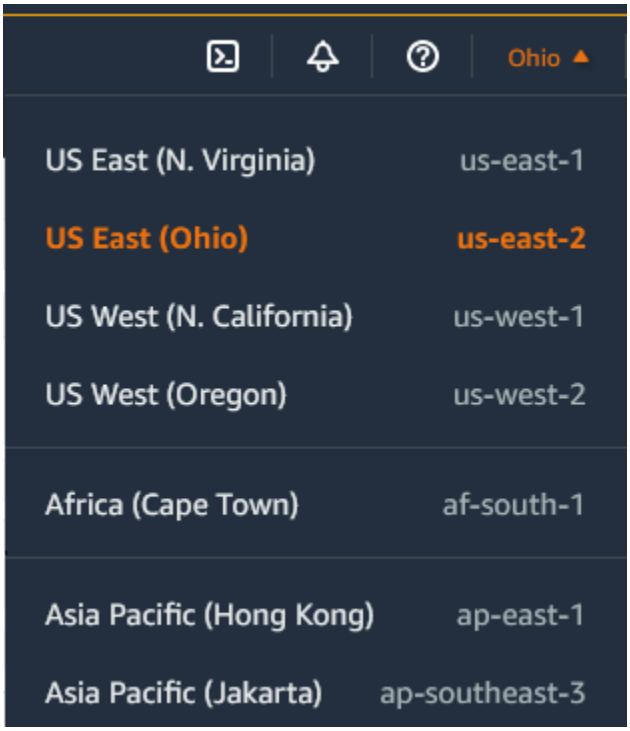
Os recursos do Amazon EC2 são específicos para a região ou zona de disponibilidade da AWS em que eles residem. Ao criar um recurso do Amazon EC2, você seleciona a região para ele.

Considerações

- Alguns recursos da AWS podem não estar disponíveis em todas as regiões. Certifique-se de que você possa criar todos os recursos da AWS necessários em uma região antes de começar a criar recursos nela.
- Algumas regiões estão desabilitadas por padrão. É necessário habilitar essas regiões para que você possa usá-las. Para obter mais informações, consulte Regiões da AWS.

Para selecionar uma região para um recurso usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Na barra de navegação, escolha o seletor Regions (Regiões) e, depois, escolha a região.



3. O seletor Regiões inclui todos os recursos que estão disponíveis para uso em sua Conta da AWS. Escolha o texto sublinhado na parte inferior da lista para exibir as regiões que não estão habilitadas para sua conta.

Para selecionar uma região para um recurso usando a AWS CLI

É possível configurar o AWS CLI para usar uma região padrão. Se você não especificar a região no comando, a região padrão será usada. Para usar uma região diferente para um comando específico, adicione a opção a seguir.

```
--region us-east-1
```

Para selecionar uma região para um recurso usando as Ferramentas para PowerShell

É possível configurar as Ferramentas para Windows PowerShell para usar uma região padrão. Se você não especificar uma região em um comando, a região padrão será usada. Para usar uma região diferente para um comando específico, adicione o parâmetro a seguir.

```
-Region us-east-1
```

Encontrar seus recursos do Amazon EC2

É possível obter uma lista de alguns tipos de recursos usando o console do Amazon EC2. É possível obter uma lista de cada tipo de recurso usando seu comando ou ação de API correspondente. Se você tiver muitos recursos, é possível filtrar os resultados para incluir ou excluir somente aqueles que correspondem a determinados critérios.

Tópicos

- Listar e filtrar recursos usando o console
- Listar e filtrar usando a linha de comando
- Visualizar recursos entre regiões usando a Visualização Global do Amazon EC2

Listar e filtrar recursos usando o console

Sumário

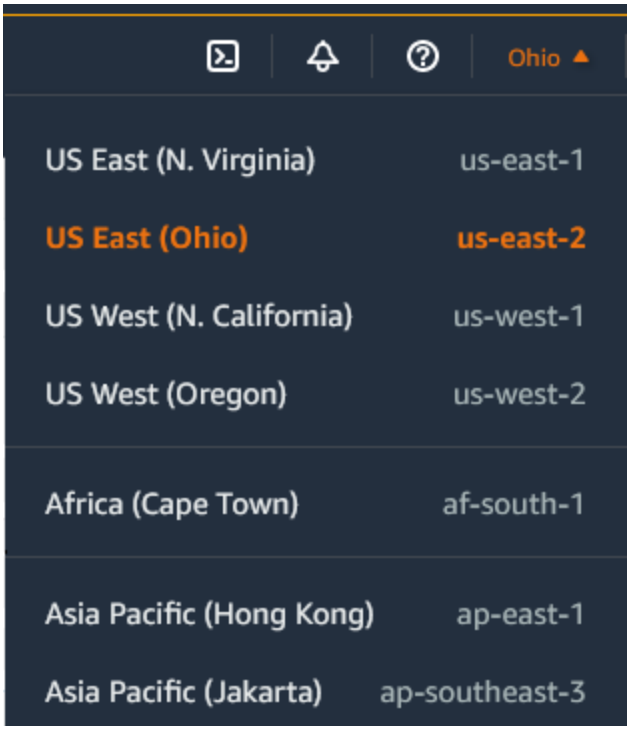
- Listar recursos usando o console
- Filtrar recursos usando o console
  - Filtros compatíveis
- Salvar conjuntos de filtros usando o console
  - Atributos principais
  - Criar um conjunto de filtros
  - Modificar um conjunto de filtros
  - Excluir um conjunto de filtros

Listar recursos usando o console

É possível 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. Os recursos do Amazon EC2 são específicos para uma Região da AWS. Na barra de navegação, escolha a região no seletor Regiões.



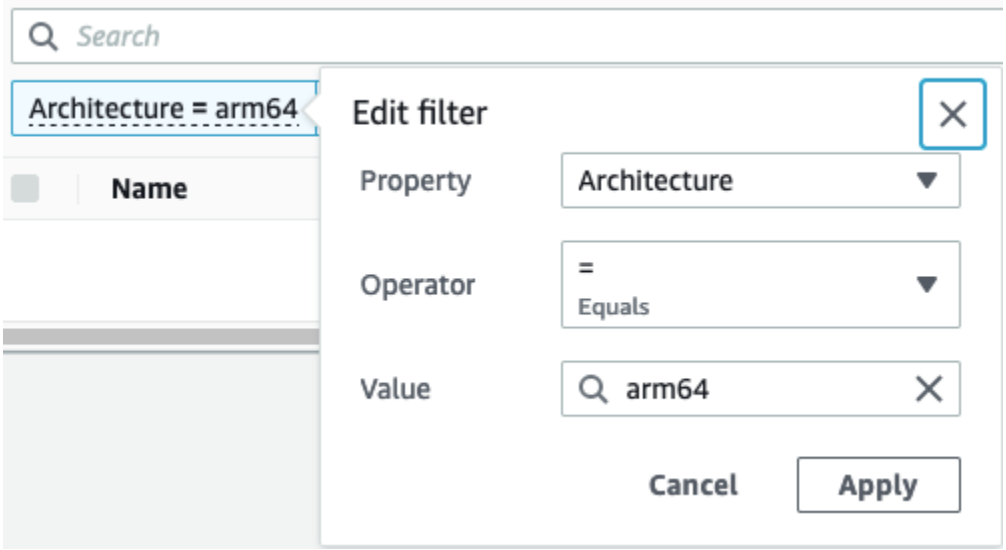
3. No painel de navegação, escolha a opção que corresponde ao tipo de recurso. Por exemplo, para listar todas as instâncias, escolha Instâncias.

Filtrar recursos usando o console

Para filtrar uma lista de recursos

1. No painel de navegação, selecione um tipo de recurso (por exemplo, Instâncias).
2. Escolha o campo de pesquisa.
3. Escolha o filtro na lista.

4. Selecione um operador, por exemplo, = (Igual a). Alguns atributos têm mais operadores disponíveis para selecionar. Observe que nem todas as telas suportam a seleção de um operador.
5. Selecione um valor de filtro.
6. Para editar um filtro selecionado, escolha o token de filtro (caixa azul), faça as edições necessárias e escolha Apply (Aplicar). Observe que nem todas as telas suportam a edição do filtro selecionado.



7. Quando terminar, remova o filtro.

Filtros compatíveis

O console do Amazon EC2 é compatível com dois tipos de filtragem.

- A filtragem de API acontece no lado do servidor. A filtragem é aplicada na chamada de API, o que reduz o número de recursos retornados pelo servidor. Isso permite a filtragem rápida em grandes conjuntos de recursos e pode reduzir o tempo e o custo de transferência de dados entre o servidor e o navegador. A filtragem de API oferece suporte a operadores = (igual a) e : (contém), e sempre diferencia maiúsculas de minúsculas.
- A filtragem do cliente acontece no lado do cliente. Isso permite filtrar dados que já estão disponíveis no navegador (em outras palavras, dados que já foram retornados pela API). A filtragem do cliente funciona bem em conjunto com um filtro de API para filtrar para conjuntos de dados menores no navegador. Além dos operadores = (igual a) e : (contém), a filtragem de clientes também pode incluir suporte a operadores de intervalo, como >= (maior ou igual a) e operadores de negação (inverso), como != (não igual a).

O console do Amazon EC2 é compatível com os seguintes tipos de pesquisa:

Pesquisa por palavra-chave

A pesquisa por palavra-chave é uma pesquisa de texto livre que permite pesquisar um valor em todos os atributos ou tags de seus recursos, sem especificar um atributo a ser pesquisado.

> **Note**
>
> Todas as pesquisas por palavras-chave usam filtragem do cliente.

Para pesquisar por palavra-chave, insira ou cole o que você procura na caixa de pesquisa e selecione Enter. Por exemplo, procurar por `123` corresponde a todas as instâncias que tenham 123 em qualquer um de seus atributos, como um endereço IP, ID de instância, ID de VPC ou ID de AMI, ou em qualquer uma de suas tags, como em Name (Nome). Se sua pesquisa de texto livre retornar correspondências inesperadas, aplique filtros adicionais.

Pesquisar por atributo

A pesquisa por um atributo permite que você pesquise um atributo específico em todos os recursos.

> **Note**
>
> As pesquisas de atributos usam filtragem de API ou filtragem de cliente, dependendo do atributo selecionado. Ao realizar uma pesquisa de atributo, os atributos são agrupados conforme necessário.

Por exemplo, é possível pesquisar o atributo Instance state (Estado da instância) para todas as instâncias para retornar apenas instâncias que estão no estado `stopped`. Para fazer isso:

1. No campo de pesquisa na tela Instances (Instâncias), comece inserindo `Instance state`. À medida que você insere os caracteres, os dois tipos de filtros aparecem para Instance state (Estado da instância): API filters (Filtros de API) e Client filters (Filtros de cliente).
2. Para pesquisar no lado do servidor, escolha Instance state (Estado da instância) em API filters (Filtros de API). Para pesquisar no lado do cliente, escolha Instance state (client) (Estado da instância (cliente)) em Client filters (Filtros de cliente).

   Uma lista de operadores possíveis para o atributo selecionado é exibida.

3. Selecione o operador = (igual a).

   Uma lista de valores possíveis para o atributo e operador selecionado é exibida.

4. Selecione stopped (interrompido) na lista.

Pesquisar por etiqueta

A pesquisa por uma tag permite filtrar os recursos na tabela exibida atualmente por uma chave de tag ou um valor de tag.

Pesquisas de tags usam filtragem de APIs ou filtragem de clientes, dependendo das configurações na janela Preferences (Preferências).

Para garantir a filtragem de APIs para tags

1. Abra a janela Preferences (Preferências).
2. Limpe a caixa de seleção Usar correspondência de expressões regulares. Se essa caixa de seleção estiver marcada, a filtragem do cliente será executada.
3. Marque a caixa de seleção Usar correspondência com distinção de maiúsculas e minúsculas. Se essa caixa de seleção estiver desmarcada, a filtragem do cliente será executada.
4. Escolha Confirmar.

Ao pesquisar por tag, é possível usar os seguintes valores:

- (empty) (vazio): encontra todos os recursos com a chave de tag especificada, mas não deve haver valor de tag.
- All values (Todos os valores): encontra todos os recursos com a chave de tag especificada e qualquer valor de tag.
- Not tagged (Sem tag aplicada): pesquisa por todos os recursos que não tenham uma determinada chave de tag.
- O valor exibido: encontra todos os recursos com a chave de tag especificada e o valor da tag especificado.

É possível usar as seguintes técnicas para aprimorar ou refinar suas pesquisas:

Pesquisa inversa

Pesquisas inversas permitem pesquisar recursos que não correspondem a um valor especificado. Nas telas Instâncias e AMIs, as pesquisas inversas são realizadas selecionando o operador !=

(não igual a) ou !: (não contém) e depois selecionando um valor. Nas outras telas, as pesquisas inversas são realizadas colocando o caractere de ponto de exclamação (!) como prefixo da palavra-chave de pesquisa.

> **Note**
>
> A pesquisa inversa é compatível com pesquisas de palavras-chave e pesquisas de atributos somente em filtros de cliente. Ela não é compatível com pesquisas de atributos em filtros de API.

Por exemplo, é possível pesquisar o atributo Instance state (Estado da instância) para todas as instâncias a fim de excluir todas as instâncias que estão no estado `terminated`. Para fazer isso:

1. No campo de pesquisa na tela Instances (Instâncias), comece inserindo `Instance state`. À medida que você insere os caracteres, os dois tipos de filtros aparecem para Instance state (Estado da instância): API filters (Filtros de API) e Client filters (Filtros de cliente).
2. Em Client filters (Filtros de cliente), escolha Instance state (client) (Estado da instância, cliente). A pesquisa inversa é aceita somente em filtros de cliente.

   Uma lista de operadores possíveis para o atributo selecionado é exibida.
3. Selecione != (Não igual a) e, em seguida, escolha terminated (terminado).

Para filtrar instâncias com base em um atributo de estado de instância, também é possível usar os ícones de pesquisa
( )
na coluna Instance state (Estado da instância). O ícone de pesquisa com um sinal de mais (+) exibe todas as instâncias que correspondem a esse atributo. O ícone de pesquisa com um sinal de menos (-) exclui todas as instâncias que correspondem a esse atributo.

Aqui está outro exemplo de uso da pesquisa inversa: listar todas as instâncias que não são atribuídas ao grupo de segurança chamado `launch-wizard-1`. Em Client filters (Filtros do cliente), pesquise pelo atributo Security group name (Nome do grupo de segurança), escolha != e, na barra de pesquisa, insira `launch-wizard-1`.

Pesquisa parcial

Com pesquisas parciais, é possível procurar valores de string parciais. Para realizar uma pesquisa parcial, insira apenas uma parte da palavra-chave que você deseja pesquisar. Nas

telas Instances (Instâncias) e AMIs, as pesquisas parciais só podem ser realizadas com o operador : (Contém). Em outras telas, é possível selecionar o atributo de filtro do cliente e inserir imediatamente apenas uma parte da palavra-chave que deseja pesquisar. Por exemplo, na tela Instance type (Tipo de instância), para pesquisar todas as instâncias `t2.micro`, `t2.small` e `t2.medium`, pesquise pelo atributo Instance Type (Tipo de instância) e, para a palavra-chave, insira `t2`.

Pesquisa de expressão regular

Para usar pesquisas de expressão regular, é necessário marcar a caixa de seleção Usar correspondência de expressão regular na janela Preferências.

As expressões regulares são úteis quando você precisa corresponder os valores de um campo com um padrão específico. Por exemplo, para procurar um valor que comece com `s`, procure `^s`. Para procurar um valor que termine com `xyz`, procure `xyz$`. Ou para procurar um valor que começa com um número seguido por um ou mais caracteres, procure `[0-9]+.*`.

> **Note**
>
> A pesquisa de expressão regular é compatível com pesquisas de palavras-chave e pesquisas de atributos somente em filtros de cliente. Ela não é compatível com pesquisas de atributos em filtros de API.

Pesquisa com diferenciação de maiúsculas e minúsculas

Para fazer pesquisas que diferenciem maiúsculas de minúsculas, é necessário marcar a caixa de seleção Usar correspondência com distinção de maiúsculas e minúsculas na janela Preferências. A preferência com diferenciação de maiúsculas e minúsculas se aplica somente aos filtros de cliente e tag.

> **Note**
>
> Os filtros de API sempre diferenciam maiúsculas de minúsculas.

Pesquisa por curinga

Use o curinga `*` para corresponder a zero ou mais caracteres. Use o curinga `?` para corresponder a zero ou um caractere. Por exemplo, se você tiver um conjunto de dados com os valores `prod`,

`prods`, e `production`, uma pesquisa por `prod*` corresponde a todos os valores, enquanto `prod?` corresponde somente a `prod` e `prods`. Para usar os valores literais, coloque uma barra invertida (\) antes. Por exemplo, "`prod\*`" corresponderia a `prod*`.

> **Note**
>
> A pesquisa por curingas é compatível apenas com pesquisas de atributos e tags em filtros de API. Não é compatível com pesquisas de palavras-chave e pesquisas de atributos e tags em filtros de cliente.

Combinar pesquisas

Em geral, vários filtros com o mesmo atributo são unidos automaticamente com `OR`. Por exemplo, pesquisar `Instance State : Running` e `Instance State : Stopped` retorna todas as instâncias que estão em execução OU interrompidas. Para unir a pesquisa com `AND`, pesquise em diferentes atributos. Por exemplo, pesquisar `Instance State : Running` e `Instance Type : c4.large` retorna apenas instâncias que são do tipo `c4.large` E que estão no estado de execução.

Salvar conjuntos de filtros usando o console

Um conjunto de filtros salvo é um grupo personalizado de filtros que você pode criar e reutilizar para visualizar com eficiência os recursos do Amazon EC2. Esse recurso ajuda a otimizar o fluxo de trabalho, permitindo acesso rápido a visualizações de recursos específicos.

Os conjuntos de filtros salvos têm suporte apenas no console do Amazon EC2 e, no momento, estão disponíveis somente na página Volumes.

Atributos principais

- Personalização: crie conjuntos de filtros adaptados às suas necessidades. Por exemplo, você pode criar um conjunto de filtros para exibir somente os volumes `gp3` que foram criados após uma data especificada.
- Filtro padrão: defina um conjunto de filtros padrão para uma página, e os filtros padrão serão aplicados automaticamente quando você navegar até a página. Se nenhum padrão for definido, nenhum filtro será aplicado.

- Aplicação fácil: selecione um conjunto de filtros salvo para aplicá-lo instantaneamente. Em seguida, o Amazon EC2 exibe os recursos relevantes, com os filtros ativos indicados por tokens azuis.
- Flexibilidade: crie, modifique e exclua conjuntos de filtros conforme necessário.

Criar um conjunto de filtros

Para criar um conjunto de filtros

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Volumes.

> **Note**
>
> No momento, os conjuntos de filtros salvos estão disponíveis somente para Volumes.

3. No campo de pesquisa, selecione filtros para o conjunto de filtros.
4. Escolha a seta ao lado do botão Limpar filtros e selecione Salvar novo conjunto de filtros.
5. Na janela Salvar conjunto de filtros, faça o seguinte:
   a. Em Nome do conjunto de filtros, insira um nome para o conjunto de filtros.
   b. (Opcional) Em Filtrar descrição do conjunto, insira uma descrição para o conjunto de filtros.
   c. (Opcional) Para definir o conjunto de filtros como padrão, marque a caixa de seleção Definir como padrão.

   > **Note**
   >
   > O filtro padrão é aplicado automaticamente sempre que você abrir a página do console.

   d. Escolha Salvar.

Modificar um conjunto de filtros

Para modificar um conjunto de filtros

1. Na lista Conjuntos de filtros salvos, selecione o filtro a ser modificado.

2. Para adicionar um filtro, no campo de pesquisa, selecione um e adicione-o ao conjunto de filtros. Para excluir um filtro no conjunto, escolha o X no token do filtro.
3. Escolha a seta ao lado do botão Limpar filtros e selecione Modificar conjunto de filtros.
4. Na janela Modificar conjunto de filtros, faça o seguinte:

   a. (Opcional) Para definir o conjunto de filtros como padrão, marque a caixa de seleção Definir como padrão.

   > **Note**
   >
   > O filtro padrão é aplicado automaticamente sempre que você abrir a página do console.

   b. Escolha Modificar.

Excluir um conjunto de filtros

Para excluir um conjunto de filtros

1. Na lista Conjuntos de filtros salvos, selecione o filtro a ser excluído.
2. Escolha a seta ao lado do botão Limpar filtros e selecione Excluir conjunto de filtros.
3. Na janela Excluir conjunto de filtros, revise o filtro para confirmar se é ele que deseja excluir e escolha Excluir.

Listar e filtrar usando a linha de comando

Cada tipo de recurso tem ações de API correspondentes que você usa para descrever, listar ou obter os recursos desse tipo. As listas de recursos resultantes podem ser longas, portanto, pode ser mais rápido e mais útil filtrar os resultados para incluir apenas os recursos que correspondem a critérios específicos.

Considerações sobre filtragem

- É possível especificar até 50 filtros e até 200 valores por filtro em uma única solicitação.
- As strings do filtro podem ter até 255 caracteres.
- Também é possível usar caracteres curinga com os valores de filtro. Um asterisco (*) corresponde a zero ou mais caracteres, e um ponto de interrogação (?) corresponde a zero ou um caractere.

- Os valores do filtro diferenciam maiúsculas de minúsculas.
- Sua pesquisa pode incluir os valores literais dos caracteres curinga; apenas só precisa recuá-los uma barra invertida antes do caractere. Por exemplo, um valor `\*amazon\?\\` pesquisa pela string literal, `*amazon?\`.
- Você não pode especificar um valor de filtro de null. Em vez disso, use a filtragem do lado do cliente. Por exemplo, o comando a seguir usa a opção --query e retorna os IDs das instâncias que foram iniciadas sem um par de chaves.

```
aws ec2 describe-instances \
    --query 'Reservations[*].Instances[?!not_null(KeyName)].InstanceId' \
    --output text
```

AWS CLI

Example Exemplo: Especificar um único filtro

É possível listar suas instâncias do Amazon EC2 usando describe-instances. Sem filtros, a resposta contém informações de todos os recursos. É possível usar a seguinte opção para incluir apenas as instâncias em execução na saída.

```
--filters Name=instance-state-name,Values=running
```

Para listar apenas os IDs de instância das suas instâncias em execução, adicione a opção `--query` como segue.

```
--query "Reservations[*].Instances[*].InstanceId"
```

Example Exemplo: Especificar vários filtros ou valores de filtro

Se você especificar vários filtros ou vários valores de filtro, o recurso deverá corresponder a todos os filtros a serem incluídos na saída.

É possível usar a seguinte opção para listar todas as instâncias cujo tipo seja `m5.large` ou `m5d.large`.

```
--filters Name=instance-type,Values=m5.large,m5d.large
```

É possível usar a seguinte opção para listar todas as instâncias interrompidas cujo tipo seja `t2.micro` ou .

```
--filters Name=instance-state-name,Values=stopped Name=instance-type,Values=t2.micro
```

Example Exemplo: Usar curingas em um valor de filtro

É possível usar a seguinte opção com describe-snapshots para retornar apenas os snapshots cuja descrição seja “banco de dados”.

```
--filters Name=description,Values=database
```

O curinga * corresponde a zero ou mais caracteres. É possível usar a seguinte opção para retornar apenas os snapshots cuja descrição inclua a palavra database.

```
--filters Name=description,Values=*database*
```

O curinga ? corresponde exatamente a 1 caractere. É possível usar a seguinte opção para retornar apenas os snapshots cuja descrição seja “database” ou “database” seguida por um caractere.

```
--filters Name=description,Values=database?
```

É possível usar a seguinte opção para retornar apenas os snapshots cuja descrição seja “banco de dados” seguida por até caractere. Isso exclui descrições com “banco de dados” seguida por cinco ou mais caracteres.

```
--filters Name=description,Values=database????
```

Example Exemplo: filtro baseado em data

Com a AWS CLI, é possível usar JMESPath para filtrar resultados usando expressões. Por exemplo, o seguinte comando describe-snapshots exibe os IDs de todos os snapshots criados pela Conta da AWS especificada antes da data especificada. Se você não especificar o proprietário, os resultados incluirão todos os snapshots públicos.

```
aws ec2 describe-snapshots \
    --filters Name=owner-id,Values=123456789012 \
```

```
    --query "Snapshots[?(StartTime<='2024-03-31')].[SnapshotId]" \
    --output text
```

O exemplo a seguir exibe os IDs de todos os snapshots criados no intervalo de datas especificado.

```
aws ec2 describe-snapshots \
    --filters Name=owner-id,Values=123456789012 \
    --query "Snapshots[?(StartTime>='2024-01-01') && (StartTime<='2024-12-31')].
[SnapshotId]" \
    --output text
```

Exemplo: filtro baseado em tags

Para obter exemplos de como filtrar uma lista de recursos de acordo com suas tags, consulte Filtrar recursos do Amazon EC2 por tag.

PowerShell

Example Exemplo: Especificar um único filtro

É possível listar suas instâncias do Amazon EC2 usando Get-EC2Instance. Sem filtros, a resposta contém informações de todos os recursos. É possível usar o seguinte parâmetro para incluir apenas as instâncias em execução na saída.

```
-Filter @{Name="instance-state-name"; Values="running"}
```

O seguinte exemplo lista apenas os IDs de instância das suas instâncias em execução.

```
(Get-EC2Instance -Filter @{Name="instance-state-name"; Values="stopped"}).Instances
 | Select InstanceId
```

Example Exemplo: Especificar vários filtros ou valores de filtro

Se você especificar vários filtros ou vários valores de filtro, o recurso deverá corresponder a todos os filtros a serem incluídos nos resultados.

É possível usar a seguinte opção para listar todas as instâncias cujo tipo seja `m5.large` ou `m5d.large`.

```
-Filter @{Name="instance-type"; Values="m5.large", "m5d.large"}
```

É possível usar a seguinte opção para listar todas as instâncias interrompidas cujo tipo seja `t2.micro` ou .

```
-Filter @{Name="instance-state-name"; Values="stopped"}, @{Name="instance-type";
 Values="t2.micro"}
```

Visualizar recursos entre regiões usando a Visualização Global do Amazon EC2

A Visualização Global do Amazon EC2 permite que você veja e pesquise recursos do Amazon EC2 e da Amazon VPC em uma única região da AWS ou em várias regiões simultaneamente em um único console. Para obter mais informações, consulte Visualizar recursos entre regiões usando a Visualização Global da AWS.

Visualizar recursos entre regiões usando a Visualização Global da AWS

A Visualização Global da AWS permite que você visualize alguns de seus recursos do Amazon EC2 e da Amazon VPC em uma única região da AWS ou em várias regiões em um único console. A Visualização Global da AWS também fornece a funcionalidade pesquisa global, que permite pesquisar recursos específicos ou tipos de recursos específicos em várias regiões simultaneamente.

A Visualização Global da AWS não permite que você modifique recursos de forma alguma.

Recursos compatíveis

Usando a Visualização Global da AWS, é possível visualizar um resumo global dos recursos a seguir em todas as regiões nas quais a sua Conta da AWS está habilitada.

- Grupos do Auto Scaling
- Reservas de capacidade e blocos de capacidade
- Conjunto de opção de DHCP
- Gateways da Internet apenas de saída
- IPs elásticos
- Serviços de endpoint
- Instâncias

- Gateways da Internet
- Listas de prefixos gerenciados
- Gateways NAT
- Network ACLs
- Interfaces de rede
- Tabelas de rotas
- Grupos de segurança
- Sub-redes
- Volumes
- VPCs
- Endpoints da VPC
- Conexões de emparelhamento de VPC

Permissões obrigatórias

Um usuário deve ter as permissões a seguir para usar a Visualização Global da AWS.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
  {
    "Effect": "Allow",
    "Action": [
    "autoscaling:DescribeAutoScalingGroups",
    "ec2:DescribeRegions",
    "ec2:DescribeCapacityReservations",
    "ec2:DescribeDhcpOptions",
    "ec2:DescribeEgressOnlyInternetGateways",
    "ec2:DescribeAddresses",
    "ec2:DescribeVpcEndpointServices",
    "ec2:DescribeInstances",
    "ec2:DescribeInternetGateways",
    "ec2:DescribePrefixLists",
    "ec2:DescribeNatGateways",
    "ec2:DescribeNetworkAcls",
```

```
    "ec2:DescribeNetworkInterfaces",
    "ec2:DescribeRouteTables",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeVolumes",
    "ec2:DescribeVpcs",
    "ec2:DescribeVpcEndpoints",
    "ec2:DescribeVpcPeeringConnections"
  ],
  "Resource": "*"
  }]
}
```

Para usar a Visualização Global da AWS

Faça login no console da Visualização Global da AWS.

> **Important**
>
> Não é possível usar uma janela privada no Firefox para acessar a Visualização Global da AWS.

O console consiste no seguinte:

- Explorador de região: esta página inclui as seções a seguir:
  - Resumo: fornece uma visão geral de alto nível dos recursos em todas as regiões.

    Expandir Mostrar o resumo de todos os recursos indica o número de regiões para as quais sua Conta da AWS está habilitada. Os campos restantes indicam o número de recursos que você tem atualmente nessas regiões. Escolha qualquer um dos links para visualizar os recursos desse tipo em todas as regiões. Por exemplo, se o link abaixo do rótulo Instâncias for 29 em 10 regiões, ele indica que você tem 29 instâncias em 10 regiões. Escolha o link para visualizar uma lista de todas as 29 instâncias.
  - Explorador de região: lista todas as Regiões da AWS (incluindo aquelas em que a conta não está habilitada) e fornece o número total de cada tipo de recurso em cada região.

    Escolha um nome de região para visualizar todos os recursos de todos os tipos para essa região específica. Por exemplo, escolha Africa (Cape Town) af-south-1 (África [Cidade do Cabo] af-

south-1) para visualizar todas as VPCs, sub-redes, instâncias, grupos de segurança, volumes e grupos do Auto Scaling nessa região. Como alternativa, selecione uma região e escolha Exibir recursos para a região selecionada.

Escolha o valor para um tipo de recurso específico em uma região específica para visualizar somente os recursos desse tipo nessa região. Por exemplo, escolha o valor para Instâncias para África (Cidade do Cabo) af-south-1 para visualizar somente as instâncias nessa região.

- Pesquisa global: esta página permite que você pesquise recursos específicos ou tipos de recursos específicos em uma única região ou em várias regiões. Ela também permite que você veja detalhes de um recurso específico.

  Para pesquisar recursos, insira os critérios de pesquisa no campo anterior à grade. É possível pesquisar por região, por tipo de recurso e pelas etiquetas atribuídas aos recursos.

  Para visualizar os detalhes de um recurso específico, selecione-o na grade. Também é possível escolher o ID de recurso para abrir o recurso no respectivo console. Por exemplo, escolha um ID de instância para abrir a instância no console do Amazon EC2 ou escolha um ID de sub-rede para abrir a sub-rede no console da Amazon VPC.
- Regiões e zonas: esta página permite que você visualize e gerencie todas as regiões, zonas de disponibilidade, zonas locais e zonas do Wavelength disponíveis.

  Na guia Regiões, você pode ver todas as regiões da AWS. A coluna Status mostra as regiões que estão habilitadas para a sua Conta da AWS. Nesta página, você pode selecionar uma região para:

  - Visualizar os detalhes da região, como o código da região, a geografia e o número de cada tipo de zona.

    Você também pode visualizar a lista de zonas de disponibilidade, zonas locais e zonas do Wavelength, e a lista dos seus recursos na região.
  - Habilitar ou desabilitar a região.

  Em cada guia de zona, você pode visualizar a lista desse tipo de zona. Na guia Zonas locais, você pode optar por uma zona local.

> **Tip**
>
> Se você usar apenas regiões ou tipos de recursos específicos, é possível personalizar a Visualização Global da AWS para exibir somente essas regiões e tipos de recursos. Para

personalizar as regiões e os tipos de recursos exibidos, no painel de navegação, escolha Configurações depois, nas guias Recursos e Regiões, selecione as regiões e os tipos de recursos que você não deseja que sejam exibidos na Visão global da AWS.

Marcar com tag os recursos do Amazon EC2

Para ajudá-lo a gerenciar instâncias, imagens e outros recursos do Amazon EC2, é possível atribuir seus próprios metadados a cada recurso na forma de tags. As tags permitem categorizar seus recursos da AWS de diferentes formas (como por finalidade, por proprietário ou por ambiente). Isso é útil quando você tem muitos recursos do mesmo tipo. É possível identificar rapidamente um recurso específico baseado nas tags que você atribuiu a ele. Este tópico descreve tags e mostra a você como criá-los.

Warning

As chaves de tag e seus valores são apresentados por várias chamadas de API diferentes. Negar acesso ao `DescribeTags` não nega automaticamente acesso às tags apresentadas por outras APIs. Como uma prática recomendada, sugerimos que você não inclua dados confidenciais nas suas tags.

Tópicos

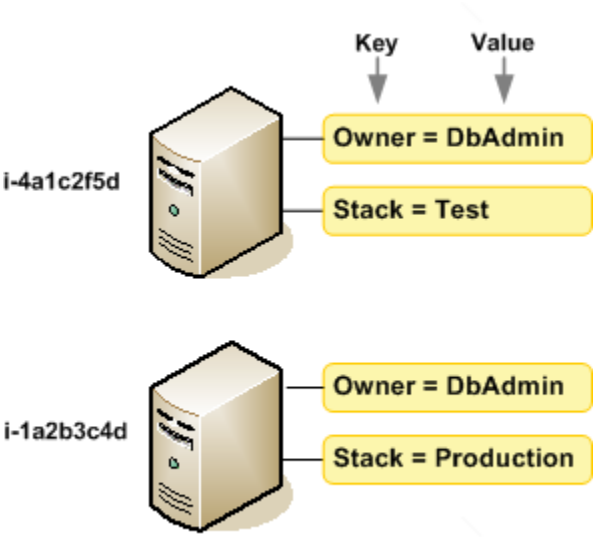
- Conceitos Básicos de Tags
- Marcar seus recursos com tag
- Restrições de tags
- Gerenciamento de tags e acesso
- Marcar com tag recursos para faturamento
- Conceder permissão para marcar recursos do Amazon EC2 durante a criação
- Adicionar e remover tags para recursos do Amazon EC2
- Filtrar recursos do Amazon EC2 por tag
- Visualizar tags para as instâncias do EC2 usando os metadados de instância

Conceitos Básicos de Tags

Uma tag um rótulo atribuído a um recurso da AWS. Cada tag consiste em uma chave e um valor opcional, ambos definidos por você.

As tags permitem categorizar seus recursos da AWS de diferentes formas (como por finalidade, por proprietário ou por ambiente). Por exemplo, é possível 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. É possível pesquisar e filtrar os recursos de acordo com as tags que adicionar. Para obter mais informações sobre como implementar uma estratégia eficaz de marcação de recursos, consulte o whitepaper da AWS Tagging Best Practices (Práticas recomendadas de marcação).

As tags não têm significado semântico no Amazon EC2 e são interpretadas estritamente como uma sequência dos caracteres. Além disso, as tags não são automaticamente atribuídas aos seus recursos. É possível editar chaves de tags e valores, e é possível remover as tags de um recurso a qualquer momento. É possível definir o valor de uma tag a uma string vazia, mas não pode

configurar o valor de um tag como nula. Se você adicionar uma tag que tenha a mesma chave de uma tag existente nesse recurso, o novo valor substituirá o antigo. Se você excluir um recurso, todas as tags do recurso também serão excluídas.

> **Note**
>
> Depois de excluir um recurso, suas etiquetas podem permanecer visíveis nas saídas do console, API e CLI por um curto período. Essas etiquetas serão gradualmente desassociadas do recurso e serão excluídas permanentemente.

Marcar seus recursos com tag

Ao usar o console do Amazon EC2, você pode aplicar tags aos recursos usando a guia Tags na tela de recursos relevante, ou você pode usar o Editor de tags no console do AWS Resource Groups. 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 `Name`, mas ela não tem nenhum significado semântico para serviço do Amazon EC2.

Se você estiver usando a API do Amazon EC2, a AWS CLI ou o AWS SDK, poderá usar a ação `CreateTags` da API do EC2 para aplicar tags aos recursos existentes. Além disso, algumas ações de criação de recursos permitem que você especifique tags para um recurso quando ele é criado. Se as tags não puderem ser aplicadas durante a criação dos recursos, nós reverteremos o processo de criação de recursos. Isso garante que os recursos sejam criados com tags ou, então, não criados, e que nenhum recurso seja deixado sem tags. Ao marcar com tags os recursos no momento da criação, você elimina a necessidade de executar scripts personalizados de uso de tags após a criação do recurso. Para obter mais informações sobre como permitir que os usuários marquem os recursos durante a criação, consulte Conceder permissão para marcar recursos do Amazon EC2 durante a criação.

É possível aplicar permissões no nível do recurso com base em tags nas suas políticas do IAM para ações de API do Amazon EC2 que oferecem suporte à marcação durante a criação para implementar controle granular sobre os usuários e grupos que podem marcar recursos na criação. Seus recursos estão devidamente protegidos contra criação — as tags aplicadas imediatamente aos recursos; portanto, todas as permissões em nível de recurso baseadas em tags que controlam o uso de recursos entram imediatamente em vigor. Seus recursos podem ser rastreados e relatados com

mais precisão. É possível obrigar o uso de marcação com tags nos novos recursos e controlar quais chaves e valores de tag são definidos nos seus recursos.

Também é possível aplicar permissões em nível de recurso às ações `CreateTags` e `DeleteTags` da API do Amazon EC2 nas suas políticas do IAM, de forma a controlar quais chaves e valores de tags são definidos nos recursos existentes. Para obter mais informações, consulte Exemplo: marcar recursos.

Para obter mais informações sobre a aplicação de tags nos seus recursos para faturamento, consulte Uso de tags de alocação de custos no Guia do usuário do AWS Billing.

Restrições de tags

As restrições básicas a seguir se aplicam a tags:

- Número máximo de tags por recurso:- 50
- Em todos os recursos, cada chave de tag deve ser exclusiva e possuir apenas um valor.
- Comprimento máximo da chave:- 128 caracteres Unicode em UTF-8
- Comprimento máximo do valor: 256 caracteres Unicode em UTF-8
- Caracteres permitidos
  - Embora o EC2 permita qualquer caractere em suas tags, outros AWS serviços podem ser mais restritivos. Os caracteres permitidos em todos os serviços AWS são: letras (`a-z`, `A-Z`), números (`0-9`) e espaços representáveis em UTF-8, e os seguintes caracteres: `+ - = . _ : / @`.
  - Se você habilitar etiquetas de instância em metadados de instância, as chaves de etiquetas de instância só poderão usar letras (`a-z`, `A-Z`), números (`0-9`) e os seguintes caracteres:`+ - = . , _ : @`. As chaves de etiqueta de instância não podem conter espaços ou `/`, e não podem formar apenas `.` (um ponto), `..` (dois pontos) ou `_index`. Para obter mais informações, consulte Visualizar tags para as instâncias do EC2 usando os metadados de instância.
- As chaves e os valores de tags diferenciam maiúsculas de minúsculas.
- O prefixo `aws:` é reservado para uso da AWS. Não é possível editar nem excluir a chave ou o valor de uma tag quando ela tem uma chave de tag com esse prefixo. As tags com o prefixo `aws:` não contam para as tags por limite de recurso.

Você não pode encerrar, parar ou excluir um recurso baseado unicamente em suas tags; será preciso especificar o identificador de recursos. Por exemplo, para excluir snapshots marcados com

uma chave de tag chamada `DeleteMe`, use a ação `DeleteSnapshots` com os identificadores de recursos dos snapshots, como `snap-1234567890abcdef0`.

Quando você marca recursos públicos ou compartilhados, as tags atribuídas ficam disponíveis somente para sua conta da AWS. Nenhuma outra conta da AWS terá acesso a essas tags. Para controle de acesso baseado em tags a recursos compartilhados, cada conta da AWS deve atribuir seu próprio conjunto de tags para controlar o acesso ao recurso.

Gerenciamento de tags e acesso

Se você estiver usando o AWS Identity and Access Management (IAM), pode controlar quais usuários na sua conta da AWS têm permissão para criar, editar ou excluir tags. Para obter mais informações, consulte Conceder permissão para marcar recursos do Amazon EC2 durante a criação.

Também é possível usar tags de recurso para implementar o controle baseado em atributo (ABAC). É possível criar políticas do IAM que permitem operações com base nas tags do recurso. Para obter mais informações, consulte Controlar o acesso usando acesso baseado em atributos.

Marcar com tag recursos para faturamento

Também é possível usar tags para organizar sua conta da AWS para refletir sua própria estrutura de custo. Para isso, inscreva-se para obter sua conta da AWS com os valores de chave de tag incluídos. Para obter mais informações sobre como configurar um relatório de alocação de custos com tags, consulte Relatório mensal de alocação de custos no Manual do usuário do AWS Billing. Para ver o custo dos recursos combinados, é possível organizar as informações de faturamento com base nos recursos com os mesmos valores da chave da tag. Por exemplo, é possível 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.

> **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 Manual do usuário do AWS Billing.

> **Note**
>
> Os endereços IP elásticos marcados não são exibidos no seu relatório de alocação de custos.

Conceder permissão para marcar recursos do Amazon EC2 durante a criação

Algumas ações de resource-creating da API do Amazon EC2 permitem especificar tags quando você cria o recurso. É possível usar tags de recursos para implementar o controle baseado em atributo (ABAC). Para obter mais informações, consulte Marcar seus recursos com tag e Controlar o acesso usando acesso baseado em atributos.

Para permitir que os usuários marquem recursos na criação, eles devem ter permissões para usar a ação que cria o recurso, como `ec2:RunInstances` ou `ec2:CreateVolume`. Se as tags forem especificadas na ação resource-creating, a Amazon executará autorização adicional na ação `ec2:CreateTags` para verificar se os usuários têm permissões para criar tags. Portanto, os usuários também precisam ter permissões para usar a ação `ec2:CreateTags`.

Na definição de política do IAM para a ação `ec2:CreateTags`, use o elemento `Condition` com a chave de condição `ec2:CreateAction` para conceder permissões de marcação à ação que cria o recurso.

O exemplo a seguir demonstra uma política que permite que os usuários executem instâncias e apliquem tags a instâncias e volumes durante a execução. Os usuários não têm permissão para marcar recursos existentes (não podem chamar a ação `ec2:CreateTags` diretamente).

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
         "ec2:RunInstances"
      ],
```

```
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
         "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:us-east-1:111122223333:*/*",
      "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:us-east-1:111122223333:*/*",
      "Condition": {
         "StringEquals": {
             "ec2:CreateAction" : "CreateVolume"
          }
       }
    }
  ]
```

```
}
```

A ação `ec2:CreateTags` será avaliada somente se as tags forem aplicadas durante a ação resource-creating. Portanto, um usuário que tiver permissões para criar um recurso (pressupondo-se que não existam condições de marcação) não precisa de permissão para usar a ação `ec2:CreateTags` se nenhuma tag for especificada na solicitação. Contudo, se o usuário tentar criar um recurso com tags, haverá falha na solicitação se o usuário não tiver permissão para usar a ação `ec2:CreateTags`.

A ação `ec2:CreateTags` também é avaliada se as tags forem fornecidas em um modelo de execução. Para ver um exemplo de política, consulte Tags em um modelo de execução.

Controlar o acesso a tags específicas

É possível usar condições adicionais no elemento `Condition` de suas políticas do IAM para controlar as chaves de tag e os valores que podem ser aplicados aos recursos.

As chaves de condição a seguir podem ser usadas com os exemplos na seção anterior:

- `aws:RequestTag`: para indicar que uma chave de tag ou uma chave e um valor de tag específicos devem estar presentes em uma solicitação. Outras tags também podem ser especificadas na solicitação.
  - Use com o operador de condição `StringEquals` para impor uma combinação de chave e valor de tag específica, por exemplo, para impor a tag `cost-center=cc123`:

    ```
    "StringEquals": { "aws:RequestTag/cost-center": "cc123" }
    ```

  - Use com o operador de condição `StringLike` para impor uma chave de tag específica, por exemplo, para impor a chave de tag `purpose`:

    ```
    "StringLike": { "aws:RequestTag/purpose": "*" }
    ```

- `aws:TagKeys`: para aplicar as chaves de tags usadas na solicitação.
  - Use com o modificador `ForAllValues` para impor chaves de tags específicas se forem fornecidas na solicitação (se as tags forem especificadas na solicitação, somente chaves de tags específicas são permitidas; nenhuma outra tag é permitida). Por exemplo, as chaves de tags `environment` ou `cost-center` são permitidas:

    ```
    "ForAllValues:StringEquals": { "aws:TagKeys": ["environment","cost-center"] }
    ```

- Use com o modificador `ForAnyValue` para impor a presença de pelo menos uma das chaves de tags especificadas na solicitação. Por exemplo, pelo menos uma das chaves de tags `environment` ou `webserver` deve estar presente na solicitação:

```
"ForAnyValue:StringEquals": { "aws:TagKeys": ["environment","webserver"] }
```

Essas chaves de condição podem ser aplicadas às ações resource-creating que são compatíveis com a marcação bem como as ações `ec2:CreateTags` e `ec2:DeleteTags`. Para saber se uma ação de API do Amazon EC2 é compatível com marcação, consulte Ações, recursos e chaves de condição para Amazon EC2.

Para forçar os usuários a especificarem tags quando criam um recurso, use a chave de condição `aws:RequestTag` ou a chave de condição `aws:TagKeys` com o modificador `ForAnyValue` na ação resource-creating. A ação `ec2:CreateTags` não será avaliada se um usuário não especificar tags para a ação resource-creating.

Para condições, a chave de condição não diferencia maiúsculas de minúsculas, e o valor da condição diferencia maiúsculas de minúsculas. Portanto, para aplicar a diferenciação de maiúsculas de minúsculas de uma tag, use a chave de condição `aws:TagKeys`, onde a chave da tag é especificada como um valor na condição.

Para obter exemplos de políticas do IAM, consulte Exemplo de políticas para controlar o acesso à API do Amazon EC2. Para obter mais informações, consulte Condições com múltiplas chaves de contexto ou valores no Guia do usuário do IAM.

Adicionar e remover tags para recursos do Amazon EC2

Ao criar um recurso do Amazon EC2, como uma instância do Amazon EC2, você pode especificar as tags a serem adicionadas ao recurso. Você também pode usar o console do Amazon EC2 para exibir as tags de um recurso específico do Amazon EC2. Você também pode adicionar ou remover tags de um recurso existente do Amazon EC2.

É possível usar o Editor de tags no console do AWS Resource Groups para visualizar, adicionar ou remover tags em todos os seus recursos da AWS em todas as regiões. É possível aplicar ou remover tags de vários tipos de recursos ao mesmo tempo. Para obter mais informações, consulte o Guia do usuário de recursos da AWS para marcação.

Tarefas

- Adicionar tags usando o console
- Adicionar tags usando a AWS CLI
- Adicionar tags usando PowerShell
- Adicionar tags usando o CloudFormation

Adicionar tags usando o console

É possível adicionar tags a um recurso existente diretamente na página de um recurso.

Para adicionar tags a um recurso existente

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Na barra de navegação, selecione a região na qual o recurso está localizado.
3. No painel de navegação, selecione um tipo de recurso (por exemplo, Instâncias).
4. Selecione o recurso na lista.
5. Na guia Tags, selecione Gerenciar tags.
6. Escolha Adicionar nova tag e insira uma chave e um valor para a tag.
7. Escolha Salvar.

Adicionar tags usando a AWS CLI

É possível adicionar tags ao criar um recurso ou a um recurso existente.

Para adicionar uma tag durante a criação de recurso

Use a opção `-tag-specifications` para marcar um recurso com tag na criação. A especificação de tag requer o tipo de recurso a ser marcado, a chave e o valor da tag. O exemplo a seguir cria uma tag e a adiciona a uma especificação de tag.

```
--tag-specifications 'ResourceType=instance,Tags=[{Key=stack,Value=production}]'
```

Para adicionar uma tag a um recurso existente

Os exemplos a seguir demonstram como adicionar tags a recursos existentes usando o comando create-tags.

Example Exemplo: adicionar uma tag a um recurso

O seguinte comando adiciona a tag **Stack=production** à imagem especificada ou substitui uma tag existente para a AMI na qual a chave de tag é stack. Se o comando for bem-sucedido, nenhuma saída será retornada.

```
aws ec2 create-tags \
    --resources ami-0abcdef1234567890 \
    --tags Key=stack,Value=production
```

Example Exemplo: adicionar tags a vários recursos

Este exemplo adiciona (ou substitui) duas tags para uma AMI e uma instância. Uma das tags contém apenas uma chave (webserver), sem valor (definimos o valor como uma string vazia). A outra tag consiste em uma chave (stack) e um valor (**Production**). Se o comando for bem-sucedido, nenhuma saída será retornada.

```
aws ec2 create-tags \
    --resources ami-0abcdef1234567890 i-1234567890abcdef0 \
    --tags Key=webserver,Value=  Key=stack,Value=Production
```

Example Exemplo: adicionar tags com caracteres especiais

Este exemplo adiciona a tag [Group]=test a uma instância. Os colchetes ([e]) são caracteres especiais, que devem ser recuados.

Se você estiver usando o Linux ou o OS X, para recuar os caracteres especiais, coloque o elemento com o caractere especial entre aspas duplas (") e coloque toda a estrutura de chave e valor entre aspas simples (').

```
aws ec2 create-tags \
    --resources i-1234567890abcdef0 \
    --tags 'Key="[Group]",Value=test'
```

Se você estiver usando o Windows, para recuar os caracteres especiais, coloque o elemento que tem caracteres especiais entre aspas duplas (") e preceda cada caractere de aspas duplas com uma barra invertida (****) da seguinte maneira:

```
aws ec2 create-tags ^
```

```
    --resources i-1234567890abcdef0 ^
    --tags Key=\"[Group]\",Value=test
```

Se você estiver usando o Windows PowerShell, para recuar os caracteres especiais, coloque o valor que tem caracteres especiais entre aspas duplas (**"**), preceda cada caractere de aspas duplas com uma barra invertida (****) e coloque toda a estrutura de chave e valor entre aspas simples (**'**) da seguinte maneira:

```
aws ec2 create-tags `
    --resources i-1234567890abcdef0 `
    --tags 'Key=\"[Group]\",Value=test'
```

Adicionar tags usando PowerShell

É possível adicionar tags ao criar um recurso ou a um recurso existente.

Para adicionar uma tag durante a criação de recurso

Use o parâmetro `-TagSpecification` para marcar um recurso com tag na criação. A especificação de tag requer o tipo de recurso a ser marcado, a chave e o valor da tag. O exemplo a seguir cria uma tag e a adiciona a uma especificação de tag.

```
$tag = @{Key="stack"; Value="production"}
$tagspec = new-object Amazon.EC2.Model.TagSpecification
$tagspec.ResourceType = "instance"
$tagspec.Tags.Add($tag)
```

O exemplo a seguir especifica essa tag no parâmetro `-TagSpecification`.

```
-TagSpecification $tagspec
```

Para adicionar uma tag a um recurso existente

Use o cmdlet New-EC2Tag. Você precisa especificar o recurso, a chave e o valor da tag.

```
New-EC2Tag `
    -Resource i-1234567890abcdef0 `
    -Tag @{Key="purpose"; Value="production"}
```

Adicionar tags usando o CloudFormation

Com tipos de recursos do Amazon EC2, você especifica tags usando uma propriedade `Tags` ou `TagSpecifications`.

Os exemplos a seguir adicionam a tag **`Stack=Production`** ao AWS::EC2::Instance usando a propriedade `Tags`.

Example Exemplo: tags em YAML

```
Tags:
  - Key: "Stack"
    Value: "Production"
```

Example Exemplo: tags em JSON

```
"Tags": [
    {
        "Key": "Stack",
        "Value": "Production"
    }
]
```

Os exemplos a seguir adicionam a tag **`Stack=Production`** ao AWS::EC2::LaunchTemplate LaunchTemplateData usando a propriedade `TagSpecifications`.

Example Exemplo: TagSpecifications em YAML

```
TagSpecifications:
  - ResourceType: "instance"
    Tags:
    - Key: "Stack"
      Value: "Production"
```

Example Exemplo: TagSpecifications em JSON

```
"TagSpecifications": [
    {
        "ResourceType": "instance",
        "Tags": [
            {
```

```
                "Key": "Stack",
                "Value": "Production"
            }
        ]
    }
]
```

Filtrar recursos do Amazon EC2 por tag

Depois de adicionar tags, você pode filtrar os recursos do Amazon EC2 com base em chaves e valores de tags.

Console

Para filtrar recursos por tag

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione um tipo de recurso (por exemplo, Instâncias).
3. Escolha o campo de pesquisa.
4. Na lista, em Tags, escolha a chave da tag.
5. Escolha o valor de tag correspondente na lista.
6. Quando terminar, remova o filtro.

Para obter mais informações sobre o uso de filtros no console do Amazon EC2, consulte Encontrar seus recursos do Amazon EC2.

AWS CLI

Para descrever recursos de um único tipo com a chave de tag especificada

Adicione o seguinte filtro a um comando `describe` para descrever os recursos desse tipo com uma tag Stack, independentemente do valor da tag.

```
--filters Name=tag-key,Values=Stack
```

Para descrever recursos de um único tipo com a tag especificada

Adicione o seguinte filtro a um comando `describe` para descrever os recursos desse tipo com a tag Stack=production.

```
--filters Name=tag:Stack,Values=production
```

Para descrever recursos de um único tipo com o valor de tag especificado

Adicione o seguinte filtro a um comando `describe` para descrever os recursos desse tipo com uma tag com o valor production, independentemente da chave da tag.

```
--filters Name=tag-value,Values=production
```

Para descrever todos os recursos do EC2 com a tag especificada

Adicione o seguinte filtro ao comando describe-tags para descrever todos os recursos do EC2 com a tag Stack=test.

```
--filters Name=key,Values=Stack Name=value,Values=test
```

PowerShell

Para filtrar recursos de um único tipo por chave de tag

Adicione o seguinte filtro a um cmdlet `Get` para descrever os recursos desse tipo com uma tag Stack, independentemente do valor da tag.

```
-Filter @{Name="tag-key"; Values="Stack"}
```

Para filtrar recursos de um único tipo por tag

Adicione o seguinte filtro a um cmdlet `Get` para descrever os recursos desse tipo com a tag Stack=production.

```
-Filter @{Name="tag:Stack"; Values="production"}
```

Para filtrar recursos de um único tipo por valor de tag

Adicione o seguinte filtro a um cmdlet `Get` para descrever os recursos desse tipo com uma tag com o valor production, independentemente do valor da tag.

```
-Filter @{Name="tag-value"; Values="production"}
```

Para filtrar todos os recursos do EC2 por tag

Adicione o seguinte filtro ao cmdlet Get-EC2Tag para descrever todos os recursos do EC2 com a tag Stack=test.

```
-Filter @{Name="tag:Stack"; Values="test"}
```

Visualizar tags para as instâncias do EC2 usando os metadados de instância

É possível acessar as tags de uma instância a partir dos metadados da instância. Ao acessar tags dos metadados da instância, não é mais necessário usar chamadas de API `DescribeInstances` ou `DescribeTags` para recuperar informações de tags, o que reduz suas transações de API por segundo e permite que as recuperações de tags sejam escaladas com o número de instâncias que você controla. Além disso, os processos locais que estão sendo executados em uma instância podem visualizar as informações de tag da instância diretamente dos metadados da instância.

Por padrão, as tags não estão disponíveis a partir dos metadados da instância; permita explicitamente o acesso. É possível permitir o acesso no início da instância ou após o início em uma instância em execução ou parada. Também é possível permitir o acesso a tags especificando isso em um modelo de execução. As instâncias iniciadas usando o modelo permitem acesso a tags nos metadados da instância.

Se você adicionar ou remover uma tag de instância, os metadados da instância serão atualizados enquanto a instância estiver em execução, sem precisar interromper e iniciar a instância.

Tarefas

- Habilitar o acesso a tags em metadados da instância
- Recuperar tags dos metadados da instância
- Desabilitar o acesso a tags em metadados da instância

Habilitar o acesso a tags em metadados da instância

Por padrão, não há acesso a tags de instância nos metadados da instância. Para cada instância, é necessário habilitar o acesso explicitamente.

> **Note**
>
> Se você permitir o acesso a tags nos metadados da instância, as chaves da tag da instância estarão sujeitas a restrições específicas. A falta de conformidade resultará em falha na execução de novas instâncias ou em um erro para as instâncias existentes. As restrições são:
>
> - Só pode incluir letras (`a-z`, `A-Z`), números (`0-9`) e os seguintes caracteres:`+ - = . , _ : @`.
> - Não pode conter espaços ou `/`.
> - Não pode consistir apenas em `.` (um ponto), `..` (dois pontos) ou `_index`.
>
> Para obter mais informações, consulte Restrições de tags.

Console

Para habilitar o acesso a tags nos metadados da instância durante a inicialização de instância

1. Siga o procedimento para iniciar uma instância.
2. Expanda Detalhes avançados e, em Permitir tags nos metadados, selecione Habilitar.
3. No painel Resumo, analise a configuração da instância e selecione Iniciar instância. Para obter mais informações, consulte Executar uma instância do EC2 usando o assistente de inicialização de instâncias no console.

Para habilitar o acesso a tags nos metadados da instância após a inicialização de 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 e selecione Ações, Configurações da instância, Permitir tags em metadados de instância.
4. Para permitir o acesso a tags nos metadados da instância, marque a caixa de seleção Permitir.
5. Escolha Salvar.

AWS CLI

Para habilitar o acesso a tags nos metadados da instância durante a inicialização de instância

Use o comando run-instances e inclua a seguinte opção `--metadata-options`.

```
--metadata-options "InstanceMetadataTags=enabled"
```

Para habilitar o acesso a tags nos metadados da instância após a inicialização de instância

Use o seguinte comando modify-instance-metadata-options.

```
aws ec2 modify-instance-metadata-options \
    --instance-id i-1234567890abcdef0 \
    --instance-metadata-tags enabled
```

Para verificar se o acesso a tags em metadados de instância está habilitado

Utilize o comando describe-instances e verifique o valor de `InstanceMetadataTags`.

```
aws ec2 describe-instances \
    --instance-ids i-1234567890abcdef0 \
    --query "Reservations[*].Instances[].MetadataOptions[].InstanceMetadataTags"
```

O seguinte é um exemplo de saída. O valor é `enabled` ou `disabled`.

```
[
    "enabled"
]
```

PowerShell

Para habilitar o acesso a tags nos metadados da instância durante a inicialização de instância

Use o cmdlet New-EC2Instance e inclua o seguinte parâmetro `-MetadataOptions_InstanceMetadataTags`.

```
-MetadataOptions_InstanceMetadataTags enabled
```

Para habilitar o acesso a tags nos metadados da instância após a inicialização de instância

Use o cmdlet Edit-EC2InstanceMetadataOption.

```
Edit-EC2InstanceMetadataOption `
    -InstanceId i-1234567890abcdef0 `
    -InstanceMetadataTags enabled
```

Para verificar se o acesso a tags em metadados de instância está habilitado

Use o cmdlet Get-EC2Instance e verifique o valor de `InstanceMetadataTags`.

```
(Get-EC2Instance `
    -
InstanceId i-1234567890abcdef0).Instances.MetadataOptions.InstanceMetadataTags.Value
```

O seguinte é um exemplo de saída. O valor é `enabled` ou `disabled`.

```
enabled
```

Recuperar tags dos metadados da instância

Depois de permitir acesso às tags da instância nos metadados da instância, será possível acessar a categoria `tags/instance` com base nos metadados da instância. Para obter mais informações, consulte Acessar metadados de instância para uma instância do EC2.

IMDSv2

Linux

Execute o comando a seguir na sua instância Linux para listar todas as chaves de tag da instância.

```
TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-
token-ttl-seconds: 21600"` \
    && curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
meta-data/tags/instance
```

O exemplo a seguir obtém o valor de uma chave obtida no exemplo anterior. A solicitação de IMDSv2 usa o token armazenado que foi criado com o comando no exemplo anterior. O token não pode estar expirado.

```
curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/
tags/instance/tag-key
```

Windows

Execute o cmdlet a seguir na sua instância Windows para listar todas as chaves de tag da instância.

```
$token = Invoke-RestMethod `
    -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} `
    -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
Invoke-RestMethod `
    -Headers @{"X-aws-ec2-metadata-token" = $token} `
    -Method GET -Uri http://169.254.169.254/latest/meta-data/tags/instance
```

O exemplo a seguir obtém o valor de uma chave obtida no exemplo anterior. A solicitação de IMDSv2 usa o token armazenado que foi criado com o comando no exemplo anterior. O token não pode estar expirado.

```
Invoke-RestMethod `
    -Headers @{"X-aws-ec2-metadata-token" = $token} `
    -Method GET -Uri http://169.254.169.254/latest/meta-data/tags/instance/tag-key
```

IMDSv1

Linux

Execute o comando a seguir na sua instância Linux para listar todas as chaves de tag da instância.

```
curl http://169.254.169.254/latest/meta-data/tags/instance
```

O exemplo a seguir obtém o valor de uma chave obtida no exemplo anterior.

```
curl http://169.254.169.254/latest/meta-data/tags/instance/tag-key
```

Windows

Execute o cmdlet a seguir na sua instância Windows para listar todas as chaves de tag da instância.

```
Invoke-RestMethod -Uri http://169.254.169.254/latest/meta-data/tags/instance
```

O exemplo a seguir obtém o valor de uma chave obtida no exemplo anterior.

```
Invoke-RestMethod -Uri http://169.254.169.254/latest/meta-data/tags/instance/tag-key
```

Desabilitar o acesso a tags em metadados da instância

É possível desabilitar o acesso a tags de instância nos metadados da instância. Você não precisa desabilitar o acesso a tags de instância nos metadados da instância no início, pois ele está desativado por padrão.

Console

Para desabilitar o acesso a tags em metadados 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 uma instância e escolha Actions (Ações), Instance settings (Configurações da instância), Allow tags in instance metadata (Permitir tags em metadados de instância).
4. Para desativar o acesso a tags nos metadados da instância, limpe a caixa de seleção Permitir.
5. Escolha Salvar.

AWS CLI

Para desabilitar o acesso a tags em metadados da instância

Use o seguinte comando modify-instance-metadata-options.

```
aws ec2 modify-instance-metadata-options \
    --instance-id i-1234567890abcdef0 \
    --instance-metadata-tags disabled
```

PowerShell

Para desabilitar o acesso a tags em metadados da instância

Use o cmdlet Edit-EC2InstanceMetadataOption.

```
Edit-EC2InstanceMetadataOption `
    -InstanceId i-1234567890abcdef0 `
    -InstanceMetadataTag disabled
```

Service Quotas do Amazon EC2

Quando você cria sua Conta da AWS, definimos cotas padrão (também denominadas limites) nesses recursos da AWS de acordo com a região. Se você tentar exceder a cota de um recurso, a solicitação falhará. Por exemplo, há um número máximo de vCPUs do Amazon EC2 que você pode provisionar para instâncias sob demanda em uma região. Se você tentar inicializar uma instância em uma região e essa solicitação fizer com que seu uso exceda essa cota, a solicitação falhará. Se isso acontecer, reduza o uso de recursos ou solicite um aumento de cota.

O console de Service Quotas é um local central onde é possível visualizar e gerenciar suas cotas de serviços da AWS e solicitar um aumento de cota para muitos dos recursos que você usa. Use as informações de cota que fornecemos para gerenciar sua infraestrutura da AWS. Planeje a solicitação de aumentos das cotas com antecedência antes que sejam necessários.

Documentação de cota relacionada

- Amazon EC2 endpoints and quotas
- Amazon EC2 instance type quotas
- Quotas for Amazon EBS
- Cotas da Amazon VPC

Visualizar as cotas atuais

É possível visualizar suas cotas de cada região usando o console do Service Quotas do .

Para visualizar as cotas atuais usando o console do Service Quotas

1. Abra o console Service Quotas em https://console.aws.amazon.com/servicequotas/home/services/ec2/quotas/.
2. Na barra de navegação (na parte superior da tela), selecione uma região.
3. No painel Gerenciar cotas, selecione um serviço; por exemplo, Amazon Elastic Compute Cloud (Amazon EC2). Escolha Visualizar cotas.
4. Use o campo de filtro para filtrar a lista por nome de recurso. Por exemplo, insira **`On-Demand`** para localizar as cotas para instâncias sob demanda.
5. Para ver mais informações, escolha o nome da cota para abrir a página de detalhes sobre a cota.

Solicitar um aumento

É possível solicitar um aumento de cota para cada região.

Para solicitar um aumento, visite o Console do Service Quotas

1. Abra o console Service Quotas em https://console.aws.amazon.com/servicequotas/home/services/ec2/quotas/.
2. Na barra de navegação (na parte superior da tela), selecione uma região.
3. Use o campo de filtro para filtrar a lista por nome de recurso. Por exemplo, insira **`On-Demand`** para localizar as cotas para instâncias sob demanda.
4. Se a cota for ajustável, escolha a cota e, em seguida, escolha Solicitar aumento de cota.
5. Em Alterar valor da cota, insira o novo valor da cota.
6. Escolha Solicitar.
7. Para visualizar quaisquer solicitações pendentes ou resolvidas recentemente no console, escolha Painel no painel de navegação. Para solicitações pendentes, escolha o status da solicitação para abrir o recibo da solicitação. O status inicial de uma solicitação é Pending (Pendente). Depois que o status for alterado para Cota solicitada, você verá o número do caso com o Suporte. Escolha o número do caso para abrir o tíquete de sua solicitação.

Para obter mais informações, incluindo como usar a AWS CLI ou os SDKs para solicitar um aumento de cota, consulte Solicitação de aumento de cota no Guia do usuário do Service Quotas.

Restrição para e-mails enviados usando a porta 25

Por padrão, o Amazon EC2 permite tráfego de saída pela porta 25 somente para endereços IPv4 privados. O tráfego pela porta 25 está bloqueado para endereços IPv4 públicos e endereços IPv6.

É possível solicitar que essa restrição seja removida. Para obter mais informações, consulte Como removo a restrição à porta 25 de uma instância do Amazon EC2 ou de uma função do Lambda?

Essa restrição não se aplica ao tráfego de saída enviado pela porta 25 para:

- Endereços IP no bloco CIDR primário da VPC na qual a interface de rede de origem exista.
- Endereços IP nos CIDRs definidos em RFC 1918, RFC 6598, e RFC 4193.

Monitorar recursos do Amazon EC2

O monitoramento é uma parte importante para manter a confiabilidade, a disponibilidade e a performance das instâncias do Amazon EC2 e das soluções da AWS. É necessário coletar dados de monitoramento de todas as partes de suas soluções da AWS para facilitar a depuração de uma falha de vários pontos (caso ocorra).

AWSA fornece várias ferramentas que é possível usar para monitorar o Amazon EC2. Os painéis do console do Amazon EC2 e do CloudWatch fornecem uma visão rápida do estado do ambiente do Amazon EC2. Além disso, fornecemos o seguinte:

- Verificações do status do sistema: monitore os sistemas da AWS necessários para usar a instância e garantir que eles estejam funcionando corretamente. Essas verificações detectam problemas com sua instância que exigem a participação da AWS para corrigi-los. Quando ocorre uma falha em uma verificação de status do sistema, é possível 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 do status das instâncias do Amazon EC2.
- Verificações do status da instância: monitore o software e a configuração de rede da instância individual. Essas verificações detectam problemas que exigem seu envolvimento para correção. Quando ocorre uma falha em uma verificação de status da instância, normalmente, você precisará resolver o problema por conta própria (por exemplo, reinicializando a instância ou fazendo modificações no sistema operacional). Exemplos de problemas que podem causar falha nas verificações de status da instância incluem:
  - Verificações de status de sistema com falha
  - Configuração incorreta do startup ou da rede
  - Memória exaurida
  - Sistema de arquivos corrompido
  - Kernel incompatível

Para obter mais informações, consulte Verificações do status das instâncias do Amazon EC2.

- 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 alertas invocam ações apenas para alterações de estado mantidas. Os alarmes do CloudWatch não invocarão ações simplesmente porque estão em um estado específico. O estado deve ter sido alterado e mantido por um número específico de períodos. Para obter mais informações, consulte Monitorar instâncias usando o CloudWatch.
- Eventos do Amazon EventBridge: automatize os serviços da AWS e responda automaticamente a eventos do sistema. Os eventos dos produtos da AWS são entregues ao EventBridge em tempo quase real, e é possível especificar ações automáticas a serem executadas quando um evento corresponde a uma regra elaborada por você. Para obter mais informações, consulte the section called “Automatizar usando o EventBridge”.
- Logs do AWS CloudTrail: capture informações detalhadas sobre as chamadas feitas para a API do Amazon EC2 e armazene-as como arquivos de log no Amazon S3. É possível usar esses logs do CloudTrail para determinar quais chamadas foram feitas, o endereço IP de origem da chamada, quem fez a chamada e quando a chamada foi feita etc. Para obter mais informações, consulte the section called “Log chamadas de API usando o CloudTrail”.
- Agente do CloudWatch: colete logs e métricas no nível do sistema de hosts e convidados nas instâncias do EC2 e nos servidores on-premises. Para obter mais informações, consulte Coletar métricas e logs de instâncias do Amazon EC2 e de servidores on-premises com o agente do CloudWatch no Guia do usuário do Amazon CloudWatch.

Monitorar o status das instâncias do Amazon EC2

É possível monitorar o status de suas instâncias visualizando as verificações de status e os eventos programados para elas.

A verificação de status fornece as informações resultantes de verificações automáticas executadas pelo Amazon EC2. Essas verificações automáticas detectam se problemas específicos estão afetando as instâncias. As informações de verificação de status, em conjunto com os dados fornecidos pelo Amazon CloudWatch, oferecem visibilidade operacional detalhada sobre cada uma das instâncias.

Também é possível ver o status de eventos específicos programados para suas instâncias. O status de eventos fornece informações sobre as próximas atividades que estão programadas para suas instâncias, como reinicialização ou desativação. Ele também fornece os horários de início e término programados para cada evento.

Conteúdo

- Verificações do status das instâncias do Amazon EC2
- Eventos de alteração de estado para instâncias do Amazon EC2
- Eventos programados para instâncias do Amazon EC2

Verificações do status das instâncias do Amazon EC2

Com o monitoramento de status de instâncias, por exemplo, é possível determinar rapidamente se o Amazon EC2 detectou problemas que possam impedir que as instâncias executem aplicações. O Amazon EC2 executa verificações automáticas em cada instância do EC2 em execução para identificar problemas de hardware e software. É possível visualizar os resultados dessas verificações de status para identificar problemas específicos e detectáveis. O status do evento expande as informações que o Amazon EC2 já fornece sobre o estado de cada instância (como `pending`, `running`, `stopping`) e as métricas de utilização que o Amazon CloudWatch monitora (utilização de CPU, tráfego de rede e atividade de disco).

As verificações de status são realizadas a cada minuto e elas retornam o status de aprovação e reprovação. Se todas as verificações forem aprovadas, o status geral da instância será OK. Se uma ou mais verificações falharem, o status geral será impaired. As verificações de status são integradas ao Amazon EC2, portanto elas não podem ser desabilitadas ou excluídas.

Quando uma verificação de status falha, a métrica do CloudWatch correspondente para as verificações de status é incrementada. Para obter mais informações, consulte Métricas de verificação de status. É possível usar essas métricas para criar alarmes do CloudWatch que são acionados com base no resultado das verificações de status. Por exemplo, é possível criar um alarme para avisá-lo se as verificações de status falharem em uma instância específica. Para obter mais informações, consulte Criar alarmes do CloudWatch para instâncias do Amazon EC2 que apresentam falha nas verificações de status.

Também é possível 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 Recuperação automática de instâncias.

Tópicos

- Tipos de verificações de status
- Visualizar verificações do status para instâncias do Amazon EC2
- Criar alarmes do CloudWatch para instâncias do Amazon EC2 que apresentam falha nas verificações de status

Tipos de verificações de status

Existem três tipos de verificação de status.

- Verificações de status de sistema
- Verificações de status de instâncias
- Verificações de status do EBS anexado

Verificações de status de sistema

As verificações de status do sistema monitoram os sistemas da AWS nos quais a instância é executada. Essas verificações detectam problemas subjacentes na instância que exigem o envolvimento da AWS para a correção. Quando uma verificação de status do sistema falha, é possível esperar que a AWS corrija o problema ou pode corrigi-lo por conta própria. Para instâncias baseadas no Amazon EBS, é possível interrompê-las e iniciá-las por conta própria, o que, na maioria dos casos, faz com que a instância seja migrada para um novo host. Para instâncias baseadas em armazenamento de instância (com suporte apenas para instâncias Linux), é possível encerrar e substituir a instância. Observe que os volumes de armazenamento de instâncias são efêmeros e todos os dados são perdidos quando a instância é interrompida.

A seguir, temos exemplos de problemas que podem causar falha nas verificações de status do sistema:

- Perda de conectividade de rede
- Perda de energia do sistema
- Problemas de software no host físico
- Problemas de hardware de host físico que afetam a acessibilidade de rede

Se uma verificação de status do sistema falhar, incrementamos a métrica StatusCheckFailed_System.

Instâncias bare metal

Se você executar uma reinicialização do sistema operacional em uma instância bare metal, a verificação de status do sistema poderá retornar temporariamente um status de falha. Quando a instância ficar disponível, a verificação de status do sistema deve retornar um status de aprovação.

Verificações de status de instâncias

As verificações de status da instância monitoram o software e a conectividade de rede da sua instância individual. O Amazon EC2 verifica a integridade da instância enviando uma solicitação de protocolo de resolução de endereço (ARP) para a interface de rede (NIC). Essas verificações detectam problemas que exigem seu envolvimento para correção. Quando uma verificação de status de instância falha, geralmente você precisa lidar com o problema por conta própria (por exemplo, reinicializando a instância ou fazendo alterações de configuração da instância).

> **Note**
>
> As distribuições recentes do Linux que usam `systemd-networkd` para a configuração de rede podem relatar verificações de integridade de maneira diferente das distribuições anteriores. Durante o processo de inicialização, esse tipo de rede pode começar mais cedo e possivelmente terminar antes de outras tarefas de inicialização que também podem afetar a integridade da instância. As verificações de status que dependem da disponibilidade da rede podem relatar um status íntegro antes da conclusão de outras tarefas.

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
- Durante uma reinicialização, uma verificação de status da instância relatará uma falha até que a instância fique disponível novamente.

Se uma verificação de status da instância falhar, incrementamos a métrica StatusCheckFailed_Instance.

Instâncias bare metal

Se você executar uma reinicialização do sistema operacional em uma instância bare metal, a verificação de status da instância poderá retornar temporariamente um status de falha. Quando a instância ficar disponível, a verificação de status dela deve retornar um status de aprovação.

Verificações de status do EBS anexado

As verificações de status do EBS anexado monitoram se os volumes do Amazon EBS anexados a uma instância estão acessíveis e são capazes de concluir operações de E/S. A métrica `StatusCheckFailed_AttachedEBS` é um valor binário que indica deficiência caso um ou mais dos volumes do EBS anexados à instância não sejam capazes de concluir operações de E/S. Essas verificações de status detectam problemas subjacentes com a computação ou a infraestrutura do Amazon EBS. Se ocorrer uma falha na métrica de verificação de status do EBS anexado, você pode esperar a AWS resolver o problema ou tomar medidas, como substituir os volumes afetados ou interromper e reiniciar a instância.

Veja abaixo alguns exemplos de problemas que podem causar falha nas verificações de status do EBS anexado:

- Problemas de hardware ou software nos subsistemas de armazenamento subjacentes aos volumes do EBS
- Problemas de hardware no host físico que afetam a acessibilidade dos volumes do EBS
- Problemas de conectividade entre a instância e os volumes do EBS

É possível usar a métrica `StatusCheckFailed_AttachedEBS` para ajudar a melhorar a resiliência da sua workload. É possível usar essa métrica para criar alarmes do Amazon CloudWatch que são acionados com base no resultado das verificações de status. Por exemplo, você pode fazer o failover para uma instância secundária ou zona de disponibilidade ao detectar um impacto prolongado. Também é possível monitorar a performance de E/S de cada volume anexado usando as métricas do EBS CloudWatch para detectar e substituir o volume danificado. Se a sua workload não estiver conduzindo E/S para nenhum volume do EBS anexado à sua instância, e a verificação de status do EBS indicar uma deficiência, você poderá interromper e iniciar a instância para movê-la para um novo host. Isso pode solucionar problemas subjacentes do host que estejam afetando

a acessibilidade dos volumes do EBS. Para obter mais informações, consulte Métricas de uso do Amazon CloudWatch para o Amazon EBS.

Você também pode configurar seus grupos do Amazon EC2 Auto Scaling para detectar falhas de verificação de status do EBS anexado e, em seguida, substituir a instância afetada por uma nova. Para obter mais informações, consulte Monitor and replace Auto Scaling instances with impaired Amazon EBS volumes no Guia do usuário do Amazon EC2 Auto Scaling.

> **Note**
>
> A métrica de verificação de status do EBS anexado está disponível somente para instâncias do Nitro.

Visualizar verificações do status para instâncias do Amazon EC2

Se a verificação de status da instância falhar, você normalmente precisará lidar com o problema por conta própria (por exemplo, reinicializando a instância ou fazendo alterações de configuração da instância). Para resolver falhas de verificação de status de instância ou sistema, consulte Solucionar problemas de instâncias do Linux do Amazon EC2 com falhas nas verificações de status.

Console

Para visualizar verificações de status

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Na página Instances (Instâncias), a coluna Status check (Verificações de status) lista o status operacional de cada instância.
4. Para visualizar o status de uma instância específica, selecione a instância e escolha a guia Status e alarmes.
5. Para revisar as métricas do CloudWatch para verificações de status, na guia Status e alarmes, expanda Métricas e veja os gráficos das seguintes métricas:
   - Falha na verificação de status do sistema
   - Falha na verificação de status da instância
   - Falha na verificação de status do EBS anexado

Para obter mais informações, consulte the section called “Métricas de verificação de status”.

AWS CLI

Para visualizar verificações de status

Use o comando describe-instance-status.

Exemplo: obter o status de todas as instâncias em execução

```
aws ec2 describe-instance-status
```

Exemplo: obter o status de todas as instâncias

```
aws ec2 describe-instance-status --include-all-instances
```

Exemplo: obter o status de uma única instância em execução

```
aws ec2 describe-instance-status --instance-ids i-1234567890abcdef0
```

Exemplo: obter todas as instâncias com um status de `impaired`

```
aws ec2 describe-instance-status \
--filters Name=instance-status.status,Values=impaired
```

PowerShell

Para visualizar verificações de status

Use o comando Get-EC2InstanceStatus.

Exemplo: obter o status de todas as instâncias em execução

```
Get-EC2InstanceStatus
```

Exemplo: obter o status de todas as instâncias

```
Get-EC2InstanceStatus -IncludeAllInstance $true
```

Exemplo: obter o status de uma única instância em execução

```
Get-EC2InstanceStatus -InstanceId i-1234567890abcdef0
```

Exemplo: obter todas as instâncias com um status de `impaired`

```
Get-EC2InstanceStatus \
-Filter @{Name="instance-status.status"; Values="impaired"}
```

Criar alarmes do CloudWatch para instâncias do Amazon EC2 que apresentam falha nas verificações de status

É possível usar as métricas de verificação de status para criar alarmes do CloudWatch a fim de notificar você quando uma instância apresentou falha na verificação de status.

As verificações de status e os alarmes de verificação de status podem entrar temporariamente em um estado de dados insuficiente se faltarem pontos de dados métricos. Embora raro, isso pode acontecer quando há uma interrupção nos sistemas de relatórios de métricas, mesmo quando uma instância está íntegra. Recomendamos que esse estado seja tratado como dados ausentes em vez de uma falha na verificação de status ou violação de alarme. Isso é especialmente importante ao executar ações de interrupção, encerramento, reinicialização ou recuperação na instância como resposta.

Console

Este exemplo configura um alarme que envia uma notificação quando uma instância falha em uma verificação de status. Opcionalmente, você pode parar, encerrar ou recuperar a instância.

Para criar um alarme de verificação de status (console)

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância, escolha a guia Status Checks (Verificações de status) e selecione Actions (Ações), Create status check alarm (Criar alarme de verificação de status).
4. Na página Manage CloudWatch alarms (Gerenciar alarmes do CloudWatch), em Add or edit alarm (Adicionar ou editar alarme), selecione Create an alarm (Criar um alarme).

5. Em Alarm notification (Notificação de alarme), ative a opção para configurar notificações do Amazon Simple Notification Service (Amazon SNS). Selecione um tópico existente do Amazon SNS ou insira um nome para criar um tópico.

   Se você adicionar um endereço de e-mail à lista de destinatários ou criar um novo tópico, o Amazon SNS enviará um e-mail de confirmação para cada novo endereço. Cada destinatário deve escolher o link de confirmação no e-mail. Somente endereços confirmados recebem notificações de alerta.
6. Em Alarm action (Ação de alarme), ative a opção para especificar uma ação a ser executada quando o alarme for acionado. Selecione a ação.
7. Em Alarm thresholds (Limites de alarme), especifique a métrica e os critérios do alarme.

   Você pode optar por manter os valores padrão para Agrupar exemplos por (Média) e Tipo de dados a serem amostrados (Falha na verificação de status: qualquer), ou modificá-los conforme necessário.

   Para Consecutive Period (Período consecutivo), defina o número de períodos que deseja avaliar e, em Period (Período), insira a duração do período de avaliação antes de acionar o alarme e enviar um e-mail.
8. (Opcional) Em Sample metric data (Dados de métrica de exemplo), escolha Add to dashboard (Adicionar ao painel).
9. Escolha Criar.

Se precisar alterar um alarme de status de instância, você poderá editá-lo.

Para editar um alarme de verificação de status

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância e escolha Actions (Ações), Monitoring (Monitoramento), Manage CloudWatch alarms (Gerenciar alarmes do CloudWatch).
4. Na página Manage CloudWatch alarms (Gerenciar alarmes do CloudWatch), em Add or edit alarm (Adicionar ou editar alarme), escolha Edit an alarm (Editar um alarme).
5. Em Search for alarm (Procurar alarme), escolha o alarme.
6. Quando terminar de fazer alterações, escolha Update (Atualizar).

AWS CLI

No exemplo a seguir, o alarme publica uma notificação para um tópico de SN, quando há falha da instância na verificação de instância ou na verificação de status de sistema por, pelo menos, dois períodos consecutivos. A métrica do CloudWatch usada é `StatusCheckFailed`.

Para criar um alarme de verificação de status (console)

1. Selecione um tópico de SNS existente ou crie um novo. Para obter mais informações, consulte Acesso ao Amazon SNS na AWS CLI 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 seguinte comando put-metric-alarm para criar o alarme.

```
aws cloudwatch put-metric-alarm \
    --alarm-name StatusCheckFailed-Alarm-for-i-1234567890abcdef0 \
    --metric-name StatusCheckFailed \
    --namespace AWS/EC2 \
    --statistic Maximum \
    --dimensions Name=InstanceId,Value=i-1234567890abcdef0 \
    --unit Count \
    --period 300 \
    --evaluation-periods 2 \
    --threshold 1 \
    --comparison-operator GreaterThanOrEqualToThreshold \
    --alarm-actions arn:aws:sns:us-west-2:111122223333:my-sns-topic
```

O período é o intervalo de tempo, em segundos, no qual as métricas do Amazon CloudWatch são coletadas. Este exemplo usa 300, que são 60 segundos multiplicados por 5 minutos. O período de avaliação é o número de períodos consecutivos pelos quais o valor da métrica deve ser comparado ao limite. Este exemplo usa 2. As ações do alarme são as ações a serem executadas quando esse alarme é acionado.

PowerShell

Para criar um alarme de verificação de status (console)

Use o cmdlet Write-CWMetricAlarm conforme mostrado a seguir para publicar notificações em um tópico do SNS quando a instância falhar nas verificações de status por pelo menos dois períodos consecutivos.

```
Write-CWMetricAlarm `
    -AlarmName "StatusCheckFailed-Alarm-for-i-1234567890abcdef0" `
    -MetricName "StatusCheckFailed" `
    -Namespace "AWS/EC2" `
    -Statistic "Maximum" `
    -Dimension @{Name="InstanceId"; Values="i-1234567890abcdef0"} `
    -Unit "Count" `
    -Period 300 `
    -EvaluationPeriod 2 `
    -Threshold 1 `
    -ComparisonOperator "GreaterThanOrEqualToThreshold" `
    -AlarmAction "arn:aws:sns:us-west-2:111122223333:my-sns-topic"
```

O período é o intervalo de tempo, em segundos, no qual as métricas do Amazon CloudWatch são coletadas. Este exemplo usa 300, que são 60 segundos multiplicados por 5 minutos. O período de avaliação é o número de períodos consecutivos pelos quais o valor da métrica deve ser comparado ao limite. Este exemplo usa 2. As ações do alarme são as ações a serem executadas quando esse alarme é acionado.

Eventos de alteração de estado para instâncias do Amazon EC2

O Amazon EC2 envia um evento `EC2 Instance State-change Notification` ao Amazon EventBridge quando o estado de uma instância é alterado.

A seguir estão dados de exemplo para esse evento. Neste exemplo, a instância inseriu o estado `pending`.

```
{
   "id":"7bf73129-1428-4cd3-a780-95db273d1602",
   "detail-type":"EC2 Instance State-change Notification",
   "source":"aws.ec2",
   "account":"123456789012",
   "time":"2021-11-11T21:29:54Z",
   "region":"us-east-1",
   "resources":[
      "arn:aws:ec2:us-east-1:123456789012:instance/i-1234567890abcdef0"
```

```
    ],
    "detail":{
       "instance-id":"i-1234567890abcdef0",
       "state":"pending"
    }
}
```

Os possíveis valores para `state` são:

- `pending`
- `running`
- `stopping`
- `stopped`
- `shutting-down`
- `terminated`

Quando você executa ou inicia uma instância, ela entra no estado `pending` e depois no estado `running`. Quando você interrompe uma instância, ela entra no estado `stopping` e depois no estado `stopped`. Quando você termina uma instância, ela entra no estado `shutting-down` e depois no estado `terminated`. Para obter mais informações, consulte Alterações do estado de instâncias do Amazon EC2.

Criar um alarme que envie um e-mail quando uma instância do Amazon EC2 muda de estado

Para receber notificações por e-mail quando o estado de sua instância for alterado, crie um tópico do Amazon SNS e crie uma regra do EventBridge para o evento `EC2 Instance State-change Notification`.

Para criar um tópico do SNS

1. Abra o console do Amazon SNS em https://console.aws.amazon.com/sns/v3/home.
2. No painel de navegação, escolha Tópicos.
3. Escolha Criar tópico.
4. Em Tipo, escolha Padrão.
5. Em Name (Nome), digite um nome para o tópico.

6. Escolha Criar tópico.
7. Selecione Criar assinatura.
8. Em Protocolo, escolha E-mail.
9. Em Endpoint, insira o endereço de e-mail que receberá as notificações.
10. Selecione Criar assinatura.
11. Você receberá uma mensagem de e-mail com esta linha de assunto: AWS Notification - Subscription Confirmation. Siga as instruções para confirmar sua assinatura.

Para criar uma regra de EventBridge

1. Abra o console do Amazon EventBridge em https://console.aws.amazon.com/events/.
2. Selecione Criar regra.
3. Em Name (Nome), insira um nome para a regra.
4. Em Rule type, escolha Rule with an event pattern.
5. Escolha Próximo.
6. Em Event pattern (Padrão de evento), faça o seguinte:
    a. Para Origem do evento, escolha Serviços da AWS.
    b. Em AWS service (Serviço da AWS), escolha EC2.
    c. Para Event Type (Tipo de evento), escolha EC2 Instance State-change Notification (Notificação de alteração de estado da instância do EC2).
    d. Por padrão, enviamos notificações para qualquer alteração de estado de qualquer instância. Se você preferir, é possível selecionar estados específicos ou instâncias específicas.
7. Escolha Próximo.
8. Especifique um destino desta forma:
    a. Em Target types (Tipos de destino), escolha AWS service (Serviço da AWS).
    b. Em Select a target (Selecionar um destino), escolha SNS topic (Tópico do SNS).
    c. Em Topic (Tópico), selecione o tópico do SNS que você criou no procedimento anterior.
9. Escolha Próximo.
10. (Opcional) Adicione etiquetas à regra.
11. Escolha Próximo.

12. Selecione Criar regra.
13. Para testar a regra, inicie uma alteração de estado. Por exemplo, inicie uma instância interrompida, interrompa uma instância em execução ou inicie uma instância. Você receberá mensagens de e-mail com esta linha de assunto: AWS Notification Message. O corpo do e-mail contém os dados do evento.

Eventos programados para instâncias do Amazon EC2

Para garantir a confiabilidade e o desempenho da infraestrutura, o AWS pode programar eventos para reinicializar, interromper e retirar suas instâncias. Esses eventos não ocorrem com frequência.

Se uma de suas instâncias for afetada por um evento programado, o AWS notificará você com antecedência por e-mail usando o endereço de e-mail associado à sua conta AWS. O e-mail fornece detalhes sobre o evento, como as datas de início e término. Dependendo do tipo de evento, é possível tomar providências para controlar sua duração. A AWS também envia um evento do AWS Health, que é possível monitorar e gerenciar usando o Amazon EventBridge. Para obter mais informações, consulte Monitoramento de eventos no AWS Health com o Amazon EventBridge.

Eventos programados são gerenciados por AWS. Não é possível agendar eventos para suas instâncias. No entanto, você pode:

- Visualizar eventos programados para suas instâncias.
- Personalize as notificações de eventos programados para incluir ou remover etiquetas da notificação por e-mail.
- Reagendar determinados eventos programados.
- Criar janelas de eventos personalizadas para eventos programados.
- Tomar medidas quando uma instância estiver programada para reinicializar, interromper ou ser retirada.

Para garantir que você receba notificações de eventos programados, verifique suas informações de contato na página Conta.

> **Note**
>
> Quando uma instância for afetada por um evento agendado e fizer parte de um grupo do Auto Scaling, o Amazon EC2 Auto Scaling futuramente a substituirá como parte de suas

verificações de integridade, e você não precisará realizar nenhuma outra ação. Para obter mais informações sobre as verificações de integridade realizadas pelo Amazon EC2 Auto Scaling, consulte Health checks for instances in an Auto Scaling group no Guia do usuário do Amazon EC2 Auto Scaling.

Tipos de eventos programados

O Amazon EC2 pode criar os seguintes tipos de eventos programados para suas instâncias, onde o evento ocorre em um horário programado:

Tipo de evento	Código do evento	Ação de evento
Interrupção da instância	`instance-stop`	Na hora programada, a instância é interrompida. Quando você iniciá-la novamente, ela será migrada para um novo host. Aplicável somente a instâncias com um volume raiz do Amazon EBS.
Desativação da instância	`instance-retirement`	Na hora programada, a instância é interrompida se tiver um volume raiz do Amazon EBS ou encerrada se tiver um volume raiz do armazenamento de instância.
Reinicialização da instância	`instance-reboot`	Na hora programada, a instância é reinicializada. A instância permanece no host e, durante a reinicial ização, o host passa por uma manutenção. Isso é conhecido como reinicialização no local.
Reinicialização do sistema	`system-reboot`	Na hora programada, a instância é reinicializada

Tipo de evento	Código do evento	Ação de evento
		e migrada para um novo host. Isso é conhecido como migração com reinicialização.
Manutenção do sistema	`system-maintenance`	Na hora programada, a instância pode ser temporari amente afetada pela manutenção de rede ou pela manutenção de energia.

Determinar o tipo de evento

É possível verificar que tipo de evento está programado para a sua instância.

Console

Para determinar o tipo de evento

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Events.
3. Na tabela, o código de evento aparece na coluna Tipo de evento.
4. Para filtrar a tabela de forma a mostrar somente os eventos de instâncias, no campo de pesquisa, escolha Tipo de recurso: instância na lista de filtros.

AWS CLI

Para determinar o tipo de evento para uma instância

Use o comando describe-instance-status. Se a instância tiver um evento programado associado, a saída fornecerá informações sobre ele.

```
aws ec2 describe-instance-status \
    --instance-id i-1234567890abcdef0 \
    --query InstanceStatuses[].Events
```

O seguinte é um exemplo de saída. O código do evento programado é `system-reboot`.

```
[
    "Events": [
        {
            "InstanceEventId": "instance-event-0d59937288b749b32",
            "Code": "system-reboot",
            "Description": "The instance is scheduled for a reboot",
            "NotAfter": "2020-03-14T22:00:00.000Z",
            "NotBefore": "2020-03-14T20:00:00.000Z",
            "NotBeforeDeadline": "2020-04-05T11:00:00.000Z"
        }
    ]
]
```

PowerShell

Para determinar o tipo de evento para uma instância

Use o cmdlet Get-EC2InstanceStatus. Se a instância tiver um evento programado associado, a saída fornecerá informações sobre ele.

```
(Get-EC2InstanceStatus `
    -InstanceId i-1234567890abcdef0).Events
```

O seguinte é um exemplo de saída. O código do evento programado é `system-reboot`.

```
Code              : system-reboot
Description       : The instance is scheduled for a reboot
InstanceEventId   : instance-event-0d59937288b749b32
NotAfter          : 2020-03-14T22:00:00.000Z
NotBefore         : 2020-03-14T20:00:00.000Z
NotBeforeDeadline : 2020-04-05T11:00:00.000Z
```

Conteúdo

- Gerenciamento das instâncias do Amazon EC2 agendadas para interrupção ou desativação
- Gerenciamento das instâncias do Amazon EC2 agendadas para reinicialização
- Gerenciamento das instâncias do Amazon EC2 agendadas para manutenção
- Visualizar eventos programados que afetam as instâncias do Amazon EC2
- Personalizar notificações de eventos programados para suas instâncias do EC2
- Reagendar um evento programado para uma instância do EC2

- Criar janelas de eventos personalizadas para eventos programados que afetam as instâncias do Amazon EC2

Gerenciamento das instâncias do Amazon EC2 agendadas para interrupção ou desativação

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 a instância tiver um volume raiz do Amazon EBS, a instância será programada para parar.
- Se a instância tiver um volume raiz de armazenamento de instância, ela será programada para ser encerrada.

Para obter mais informações, consulte Desativação da instância.

> **Important**
>
> Todos os dados armazenados nos volumes de armazenamento de instâncias serão perdidos quando a instância for interrompida, hibernada ou encerrada. Isso inclui volumes de armazenamento de instância que estão anexados a uma instância com volume raiz do EBS. Lembre-se de salvar os dados dos volumes do armazenamento de instâncias que poderão ser necessários mais tarde antes que a instância seja interrompida, hibernada ou encerrada.

Ações que você pode realizar

Ações que podem ser realizadas em instâncias com um volume raiz do EBS

Ao receber uma notificação de evento `instance-stop` programada, você pode realizar uma destas seguintes:

- Aguardar a interrupção programada: você pode esperar que a instância seja interrompida dentro da janela de manutenção programada.
- Executar a interrupção e inicialização manuais: você pode interromper e iniciar a instância por conta própria no momento que mais lhe convier, o que a migrará para um novo host. Isso não equivale a reiniciar a instância. Para obter mais informações, consulte Início e interrupção de instâncias do Amazon EC2.

- Automatizar a interrupção e o início: você pode automatizar uma interrupção e um início imediatos em resposta a um evento `instance-stop` programado. Para obter mais informações, consulte Como executar automaticamente operações em instâncias do EC2 em resposta a eventos no AWS Health no Guia do usuário do AWS Health.

Ações que você pode realizar para instâncias com um volume raiz do armazenamento de instâncias

Quando você recebe uma notificação de evento `system-retirement` programado e deseja manter seus dados, pode executar as seguintes ações:

1. Lance uma instância de substituição a partir da sua AMI mais recente.
2. Migrar todos os dados necessários para a instância de substituição antes que a instância seja programada para encerramento.
3. Encerrar a instância original ou esperar que ela seja encerrada conforme programado.

Para obter mais informações sobre as ações que você pode realizar, consulte Desativação da instância.

Gerenciamento das instâncias do Amazon EC2 agendadas para reinicialização

Quando a AWS precisar executar tarefas, como a instalação de atualizações ou a manutenção do host subjacente, ela pode programar uma reinicialização da instância. Durante essa reinicialização programada, a instância permanece no mesmo host ou migra para um diferente, dependendo do evento, da seguinte maneira:

- `instance-reboot`Evento
  - Durante a reinicialização, a instância permanece no host. Isso é conhecido como reinicialização no local.
  - O host atual está passando por manutenção.
  - Normalmente, isso é concluído em segundos.
- `system-reboot`Evento
  - Durante a reinicialização, a instância é migrada para um novo host. Isso é conhecido como migração com reinicialização.
  - Normalmente, isso é concluído em minutos.

Para verificar que tipo de evento está programado para a sua instância, consulte Determinar o tipo de evento.

Ações que você pode realizar

Ao receber uma notificação de evento `instance-reboot` ou `system-reboot` programado, você pode realizar uma destas ações:

- Aguardar a reinicialização programada: você pode esperar que a reinicialização da instância ocorra dentro da janela de manutenção programada.
- Reprogramar a reinicialização: você pode reprogramar a reinicialização da instância para uma data e um horário que forem mais convenientes para você.
- Executar uma reinicialização iniciada pelo usuário: é possível reinicializar manualmente a instância em um momento conveniente para você. No entanto, o resultado depende do evento:
  - Evento `instance-reboot`: sua instância permanece no hardware atual (reinicialização no local), nenhuma manutenção do host ocorre e o evento permanece aberto.
  - `system-reboot`Evento
    - Se a migração com reinicialização estiver habilitada em sua instância, uma reinicialização iniciada pelo usuário tentará migrar sua instância para um novo hardware. Em caso de êxito, o evento será removido. Caso contrário, uma reinicialização local ocorrerá e o evento permanecerá na programação.
    - Se a migração com reinicialização estiver desabilitada em sua instância, uma reinicialização iniciada pelo usuário manterá a instância no mesmo hardware (reinicialização local), nenhuma manutenção do host ocorrerá e o evento permanecerá na programação. Quando o evento programado finalmente ocorrer, a AWS moverá sua instância para um novo hardware (migração com reinicialização).

Depois que a AWS reinicializar sua instância

O seguinte é aplicável depois que a AWS reinicializa sua instância:

- O evento programado é removido.
- A descrição do evento é atualizada.
- Para um evento `instance-reboot`:
  - A manutenção do host subjacente está concluída.
- Para um evento `system-reboot`:

  - A instância é movida para um novo host.
  - A instância mantém seu endereço IP e nome DNS.
  - Todos os dados em volumes de armazenamento de instância local são preservados.
- Você pode usar sua instância depois que ela é totalmente inicializada.

Opções alternativas

Se não conseguir reprogramar o evento de reinicialização ou habilitar a migração com reinicialização para uma reinicialização iniciada pelo usuário, mas quiser manter a operação normal durante a janela de manutenção programada, você poderá fazer o seguinte:

- Para uma instância com um volume raiz do EBS
  - Você pode interromper e iniciar a instância, o que a migra para um novo host. Isso não é o mesmo que reinicializar manualmente a instância, caso em que ela permanece no mesmo host.
  - Opcionalmente, automatize a parada e o início imediatos da instância em resposta ao evento de reinicialização programado. Para obter mais informações, consulte Como executar automaticamente operações em instâncias do EC2 em resposta a eventos no AWS Health no Guia do usuário do AWS Health.

> **Important**
>
> Os dados nos volumes de armazenamento da instância são perdidos quando uma instância é interrompida. Para obter mais informações, consulte Início e interrupção de instâncias do Amazon EC2.

- Para uma instância com um volume raiz de armazenamento de instância
  1. Lance uma instância de substituição a partir da sua AMI mais recente.
  2. Migre todos os dados necessários para a instância substituta antes da janela de manutenção programada.
  3. Encerre a instância original.

Habilitar ou desabilitar a migração com reinicialização

Quando uma instância está programada para um evento `system-reboot`, é possível reiniciá-la antes do evento. O resultado de uma reinicialização iniciada pelo usuário depende da configuração da migração com reinicialização da instância:

- Habilitada: uma reinicialização iniciada pelo usuário tenta migrar sua instância para um novo hardware (migração com reinicialização). Em caso de êxito, o evento será removido. Caso contrário, uma reinicialização local ocorrerá e o evento permanecerá na programação. Observe que, mesmo quando ativada, a migração com reinicialização só poderá ocorrer se sua instância atender aos requisitos de migração com reinicialização.
- Desabilitada: uma reinicialização iniciada pelo usuário mantém a instância no mesmo hardware (reinicialização local), nenhuma manutenção do host ocorre e o evento permanece na programação. Quando o evento programado finalmente ocorrer, a AWS moverá sua instância para um novo hardware (migração com reinicialização).

A reinicialização com migração demora mais do que uma reinicialização local:

- Reinicialização local: aproximadamente 30 segundos
- Reinicialização com migração: vários minutos

> **Note**
>
> Por padrão, as instâncias que recebem uma notificação de evento `system-reboot` são habilitadas para migração com reinicialização iniciada pelo usuário.

Requisitos para habilitar a migração com reinicialização

A migração com reinicialização pode ser habilitada em instâncias que atendem aos seguintes critérios:

Tipos de instância

Nem todos os tipos de instância oferecem suporte à habilitação da migração com reinicialização. É possível visualizar os tipos de instância que oferecem suporte à habilitação da migração com reinicialização.

Console

Para visualizar os tipos de instância que oferecem suporte à habilitação da migração com reinicialização

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. Na barra de filtros, insira Suporte à migração com reinicialização: com suporte. À medida que você insere os caracteres e o nome do filtro aparece, é possível selecioná-lo.

   A tabela Tipos de instâncias exibe todos os tipos de instância que oferecem suporte à habilitação da migração com reinicialização.

AWS CLI

Para visualizar os tipos de instância que oferecem suporte à habilitação da migração com reinicialização

Use o comando describe-instance-types com o filtro `reboot-migration-support`.

```
aws ec2 describe-instance-types \
    --filters Name=reboot-migration-support,Values=supported \
    --query "InstanceTypes[*].[InstanceType]" \
    --output text | sort
```

PowerShell

Para visualizar os tipos de instância que oferecem suporte à habilitação da migração com reinicialização

Use o cmdlet Get-EC2InstanceType com o filtro `reboot-migration-support`.

```
Get-EC2InstanceType `
    -Filter @{Name="reboot-migration-support";Values="true"} | `
    Select InstanceType | Sort-Object InstanceType
```

Locação

- Compartilhada
- Instância Dedicada

Para obter mais informações, consulte Instâncias dedicadas do Amazon EC2.

Limitações

Não há suporte à migração com reinicialização em instâncias com as seguintes características:

- Plataforma: instâncias em execução nativa no hipervisor Xen
- Tamanho da instância: `metal` instâncias
- Locação: host dedicado. Para hosts dedicados, use a recuperação automática de host dedicado em vez disso.
- Armazenamento: instâncias com volumes de armazenamento de instância
- Rede: instâncias usando um adaptador de malha elástica
- Ajuste de escala automático: instâncias que fazem parte de um grupo do Auto Scaling

Etapas para habilitar ou desabilitar a migração com reinicialização

Quando uma instância recebe um evento `system-reboot`, ela é habilitada para a migração com reinicialização por padrão. É possível desabilitar a migração com reinicialização para que, durante uma reinicialização iniciada pelo usuário, a instância permaneça no mesmo hardware (reinicialização no local).

A configuração `default` não habilita a migração com reinicialização para uma instância sem suporte. Para obter mais informações, consulte Requisitos para habilitar a migração com reinicialização.

É possível desabilitar ou habilitar a migração com reinicialização em uma instância em execução ou parada.

AWS CLI

Para desabilitar a migração com reinicialização

Use o comando modify-instance-maintenance-options e defina o parâmetro `--reboot-migration` como `disabled`.

```
aws ec2 modify-instance-maintenance-options \

    --instance-id i-0abcdef1234567890 \

    --reboot-migration disabled
```

Para habilitar a migração com reinicialização

Use o comando modify-instance-maintenance-options e defina o parâmetro `--reboot-migration` como `default`.

```
aws ec2 modify-instance-maintenance-options \

    --instance-id i-0abcdef1234567890 \

    --reboot-migration default
```

PowerShell

Para desabilitar a migração com reinicialização

Use o cmdlet Edit-EC2InstanceMaintenanceOption.

```
Edit-EC2InstanceMaintenanceOption `
    -InstanceId  `
    -RebootMigration Disabled
```

Para habilitar a migração com reinicialização

Use o cmdlet Edit-EC2InstanceMaintenanceOption.

```
Edit-EC2InstanceMaintenanceOption `
    -InstanceId i-1234567890abcdef0 `
    -RebootMigration Enabled
```

Gerenciamento das instâncias do Amazon EC2 agendadas para manutenção

Quando a AWS precisa manter o host subjacente de uma instância, ela programa a instância para manutenção. Há dois tipos de eventos de manutenção: manutenção de rede e manutenção de energia.

- Durante a manutenção de rede, instâncias programadas perdem a conectividade de rede durante um breve período. A conectividade de rede normal com a instância é restaurada depois que a manutenção for concluída.
- Durante a manutenção de energia, as instâncias programadas ficam offline durante um breve período e depois são reinicializadas. Quando uma reinicialização é realizada, todas as definições de configuração da instância são mantidas.

Depois que sua instância tiver sido reinicializada (isso geralmente leva alguns minutos), verifique se a aplicação está funcionando conforme o esperado. Nesse ponto, a instância não deve mais ter um

evento associado a ela ou, se tiver, a descrição do evento programado começará com [Completed]. Às vezes, leva até 1 hora para que a descrição do status da instância seja atualizada. Eventos de manutenção concluídos são exibidos no painel do console do Amazon EC2 por até uma semana.

Ações que você pode realizar

Ações que podem ser realizadas em instâncias com um volume raiz do EBS

Ao receber uma notificação de evento `system-maintenance`, você pode realizar uma destas ações:

- Aguardar a manutenção programada: você pode esperar que a manutenção ocorra conforme programado.
- Executar a interrupção e o início manuais: você pode parar e iniciar a instância, o que a migra para um novo host. Isso não equivale a reiniciar a instância. Para obter mais informações, consulte Início e interrupção de instâncias do Amazon EC2.
- Automatizar a interrupção e o início: você pode automatizar uma interrupção e um início imediatos em resposta a um evento de manutenção programado. Para obter mais informações, consulte Como executar automaticamente operações em instâncias do EC2 em resposta a eventos no AWS Health no Guia do usuário do AWS Health.

Ações que você pode realizar para instâncias com um volume raiz do armazenamento de instâncias

Ao receber uma notificação de evento `system-maintenance`, você pode realizar uma destas ações:

- Aguardar a manutenção programada: você pode esperar que a manutenção ocorra conforme programado.
- Lançar uma instância de substituição: se quiser manter a operação normal durante a janela de manutenção programada:
  1. Lance uma instância de substituição a partir da sua AMI mais recente.
  2. Migre todos os dados necessários para a instância substituta antes da janela de manutenção programada.
  3. Encerre a instância original.

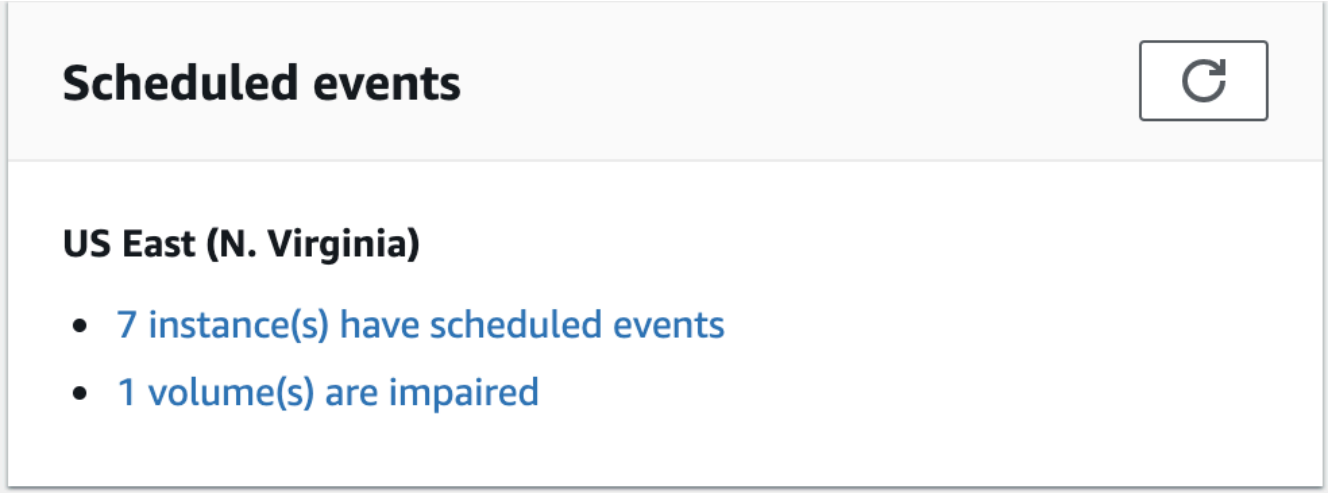
Visualizar eventos programados que afetam as instâncias do Amazon EC2

Além de receber a notificação de eventos programados por e-mail, você pode verificar se há eventos programados.

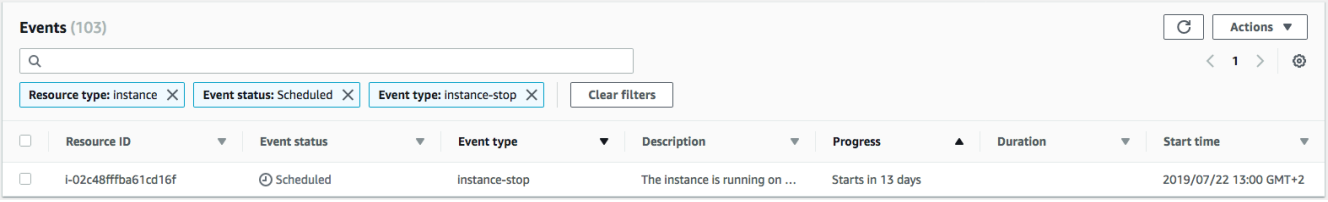
Console

Para visualizar eventos programados para suas instâncias

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. O painel exibe quaisquer recursos com um evento associado em Eventos agendados.



3. Para obter mais detalhes, escolha Eventos no painel de navegação. Todos os recursos com um evento associado serão exibidos. É possível filtrar por características como tipo de evento, tipo de recurso e zona de disponibilidade.



AWS CLI

Para visualizar eventos programados para suas instâncias

Use o comando describe-instance-status.

```
aws ec2 describe-instance-status \
    --instance-id i-1234567890abcdef0 \
```

```
    --query "InstanceStatuses[].Events"
```

O exemplo de saída a seguir mostra um evento de reinicialização.

```
[
    "Events": [
        {
            "InstanceEventId": "instance-event-0d59937288b749b32",
            "Code": "system-reboot",
            "Description": "The instance is scheduled for a reboot",
            "NotAfter": "2019-03-15T22:00:00.000Z",
            "NotBefore": "2019-03-14T20:00:00.000Z",
            "NotBeforeDeadline": "2019-04-05T11:00:00.000Z"
         }

    ]
]
```

O exemplo de saída a seguir mostra um evento de desativação de instância:

```
[
    "Events": [
        {
            "InstanceEventId": "instance-event-0e439355b779n26",

            "Code": "instance-stop",
            "Description": "The instance is running on degraded hardware",
            "NotBefore": "2015-05-23T00:00:00.000Z"
        }
    ]
]
```

PowerShell

Para visualizar eventos programados para suas instâncias

Use o seguinte comando Get-EC2InstanceStatus.

```
(Get-EC2InstanceStatus -InstanceId i-1234567890abcdef0).Events
```

O exemplo de saída a seguir mostra um evento de desativação de instância:

```
Code         : instance-stop
Description  : The instance is running on degraded hardware
NotBefore    : 5/23/2015 12:00:00 AM
```

Instance metadata

Para visualizar os eventos programados para suas instâncias usando metadados de instância

É possível recuperar informações sobre eventos de manutenção ativos para suas instâncias dos metadados de instância usando o Serviço de metadados da instância versão 2 ou o Serviço de metadados da instância versão 1.

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/events/maintenance/scheduled
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/events/maintenance/scheduled
```

A seguir, temos um exemplo de saída com informações sobre um evento de reinicialização do sistema programado, no formato JSON.

```
[
  {
    "NotBefore" : "21 Jan 2019 09:00:43 GMT",
    "Code" : "system-reboot",
    "Description" : "scheduled reboot",
    "EventId" : "instance-event-0d59937288b749b32",
    "NotAfter" : "21 Jan 2019 09:17:23 GMT",
    "State" : "active"
  }
]
```

Para visualizar o histórico de eventos sobre eventos concluídos ou cancelados das suas instâncias usando metadados de instância

É possível recuperar informações sobre eventos concluídos ou cancelados para suas instâncias dos metadados de instância usando o Serviço de metadados da instância versão 2 ou o Serviço de metadados da instância versão 1.

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/events/maintenance/history
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/events/maintenance/history
```

A seguir, temos um exemplo de saída com informações sobre um evento de reinicialização do sistema que foi cancelado e um que foi concluído, no formato JSON.

```
[
  {
    "NotBefore" : "21 Jan 2019 09:00:43 GMT",
    "Code" : "system-reboot",
    "Description" : "[Canceled] scheduled reboot",
    "EventId" : "instance-event-0d59937288b749b32",
    "NotAfter" : "21 Jan 2019 09:17:23 GMT",
    "State" : "canceled"
  },
  {
    "NotBefore" : "29 Jan 2019 09:00:43 GMT",
    "Code" : "system-reboot",
    "Description" : "[Completed] scheduled reboot",
    "EventId" : "instance-event-0d59937288b749b32",
    "NotAfter" : "29 Jan 2019 09:17:23 GMT",
    "State" : "completed"
  }
]
```

AWS Health

É possível usar o AWS Health Dashboard para saber mais sobre eventos que podem afetar a instância. O Health Dashboard organiza problemas em três grupos: ocorrências abertas,

alterações programadas e outras notificações. O grupo de alterações programadas contém itens presentes e futuros.

Para obter mais informações, consulte Como iniciar o AWS Health Dashboard no Guia do usuário do AWS Health.

Personalizar notificações de eventos programados para suas instâncias do EC2

É possível personalizar notificações de eventos programados para incluir tags na notificação por e-mail. Isso facilita a identificação do recurso afetado (instâncias ou Hosts dedicados) e priorizar ações para o próximo evento.

Ao personalizar notificações de eventos para incluir tags, é possível optar por incluir:

- Todas as tags associadas ao recurso afetado
- Somente tags específicas que estão associadas ao recurso afetado

Por exemplo, suponha que você atribua as tags `application`, `costcenter`, `project` e `owner` a todas as suas instâncias. É possível optar por incluir todas as tags nas notificações de eventos. Como alternativa, se você quiser ver apenas as tags `owner` e `project` nas notificações de eventos, poderá optar por incluir apenas essas tags.

Depois de selecionar as tags a serem incluídas, as notificações de evento incluirão o ID do recurso (ID da instância ou ID do Host dedicado) e os pares de chave de tag e valor associados ao recurso afetado.

Tarefas

- Incluir tags em notificações de eventos
- Remover tags de notificações de eventos
- Visualizar as tags a serem incluídas nas notificações de eventos

Incluir tags em notificações de eventos

As tags que você escolher incluir se aplicarão a todos os recursos (instâncias e Hosts dedicados) na região selecionada. Para personalizar notificações de eventos em outras regiões, primeiro selecione a região necessária e execute as etapas a seguir.

Console

Como incluir tags em notificações de eventos

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Events.
3. Escolha Actions (Ações), Manage event notifications (Gerenciar notificações de eventos).
4. Ative a opção Incluir tags em notificações de eventos.
5. Siga um destes procedimentos, dependendo das tags que você deseja incluir nas notificações de eventos:
   - Para incluir todas as tags associadas à instância afetada ou ao Host dedicado, selecione Incluir todas as tags.
   - Para selecionar as tags a serem incluídas, selecione Escolher as tags a serem incluídas e, em seguida, selecione ou insira as chaves de tag.
6. Escolha Salvar.

AWS CLI

Como incluir todas as tags em notificações de eventos

Use o comando register-instance-event-notification-attributes e defina o parâmetro `IncludeAllTagsOfInstance` como `true`.

```
aws ec2 register-instance-event-notification-attributes \
    --instance-tag-attribute "IncludeAllTagsOfInstance=true"
```

Como incluir tags específicas em notificações de eventos

Use o comando register-instance-event-notification-attributes e especifique as tags a serem incluídas usando o parâmetro `InstanceTagKeys`.

```
aws ec2 register-instance-event-notification-attributes \
    --instance-tag-attribute 'InstanceTagKeys=["tag_key_1", "tag_key_2",
 "tag_key_3"]'
```

PowerShell

Como incluir todas as tags em notificações de eventos

Use o cmdlet Register-EC2InstanceEventNotificationAttribute.

```
Register-EC2InstanceEventNotificationAttribute `
    -InstanceTagAttribute_IncludeAllTagsOfInstance $true
```

Como incluir tags específicas em notificações de eventos

Use o cmdlet Register-EC2InstanceEventNotificationAttribute.

```
Register-EC2InstanceEventNotificationAttribute `
    -InstanceTagAttribute_InstanceTagKey tag_key_1, tag_key_2, tag_key_3
```

Remover tags de notificações de eventos

É possível remover tags das notificações de eventos.

Console

Como remover tags de notificações de eventos

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Events.
3. Escolha Actions (Ações), Manage event notifications (Gerenciar notificações de eventos).
4. Para remover todas as tags das notificações de eventos, desmarque Incluir tags nas notificações de eventos.
5. Para remover tags específicas das notificações de eventos, escolha o X para as chaves de tag correspondentes.
6. Escolha Salvar.

AWS CLI

Como remover todas as tags das notificações de eventos

Use o comando deregister-instance-event-notification-attributes e defina o parâmetro `IncludeAllTagsOfInstance` como `false`.

```
aws ec2 deregister-instance-event-notification-attributes \
    --instance-tag-attribute "IncludeAllTagsOfInstance=false"
```

Para remover uma tag de notificações de eventos

Use o comando deregister-instance-event-notification-attributes e especifique as tags a serem removidas usando o parâmetro `InstanceTagKeys`.

```
aws ec2 deregister-instance-event-notification-attributes \
    --instance-tag-attribute 'InstanceTagKeys=["tag_key_3"]'
```

PowerShell

Como remover todas as tags das notificações de eventos

Use o cmdlet Unregister-EC2InstanceEventNotificationAttribute.

```
Unregister-EC2InstanceEventNotificationAttribute `
    -InstanceTagAttribute_IncludeAllTagsOfInstance $false
```

Para remover uma tag de notificações de eventos

Use o cmdlet Unregister-EC2InstanceEventNotificationAttribute.

```
Unregister-EC2InstanceEventNotificationAttribute `
    -InstanceTagAttribute_InstanceTagKey tag_key_3
```

Visualizar as tags a serem incluídas nas notificações de eventos

É possível visualizar as tags que serão incluídas nas notificações de eventos.

Console

Como visualizar as tags a serem incluídas nas notificações de eventos

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Events.
3. Escolha Actions (Ações), Manage event notifications (Gerenciar notificações de eventos).

AWS CLI

Para visualizar as tags que serão incluídas nas notificações de eventos

Use o comando describe-instance-event-notification-attributes.

```
aws ec2 describe-instance-event-notification-attributes
```

PowerShell

Para visualizar as tags que serão incluídas nas notificações de eventos

Use o cmdlet Get-EC2InstanceEventNotificationAttribute.

```
Get-EC2InstanceEventNotificationAttribute
```

Reagendar um evento programado para uma instância do EC2

É possível reagendar um evento para que ele ocorra em uma data e hora específicas que forem convenientes. Após um evento programado ser reagendado, até um ou dois minutos podem ser necessários para que a data atualizada seja exibida.

Limitações

- Somente eventos com uma data de prazo podem ser reprogramados. O evento pode ser reprogramado até a data de prazo do evento. A data limite do evento é indicada na coluna Data limite (console) e o campo `NotBeforeDeadline` (AWS CLI).
- Somente eventos ainda não iniciados podem ser reprogramados. A hora de início é indicada na coluna Hora de início (console) e no campo `NotBefore` (AWS CLI). Eventos programados para início nos próximos cinco minutos não podem ser reprogramados.
- A nova hora de início do evento deve ser pelo menos 60 minutos a partir da hora atual.
- Se você reprogramar vários eventos usando o console, a data de prazo do evento será determinada pelo evento com a data de prazo do evento mais recente.

Console

Para reprogramar um evento

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Events.
3. Escolha Resource type: instance (Tipo de recurso: instância) na lista de filtros.
4. Escolha uma ou mais instâncias e selecione Actions (Ações), Schedule event (Programar evento).

Somente eventos que têm uma data de prazo de evento, indicados por um valor para Deadline (Prazo), podem ser reprogramados. Se um dos eventos selecionados não tiver uma data de prazo, a opção Actions (Ações), Schedule event (Programar evento) será desativada.

5. Em New start time (Nova hora de início), insira uma nova data e hora para o evento. A nova data e hora devem ocorrer antes de Event deadline (Prazo do evento).
6. Escolha Salvar.

   Pode levar um ou dois minutos para a hora de início do evento atualizado ser refletida no console.

AWS CLI

Para reprogramar um evento

Use o comando modify-instance-event-start-time.

```
aws ec2 modify-instance-event-start-time \
    --instance-id i-1234567890abcdef0 \
    --instance-event-id instance-event-0d59937288b749b32 \
    --not-before 2020-03-25T10:00:00.000
```

PowerShell

Para reprogramar um evento

Use o cmdlet Edit-EC2InstanceEventStartTime.

```
Edit-EC2InstanceEventStartTime `
    -InstanceId i-1234567890abcdef0 `
    -InstanceEventId instance-event-0d59937288b749b32 `
    -NotBefore 2020-03-25T10:00:00.000
```

Criar janelas de eventos personalizadas para eventos programados que afetam as instâncias do Amazon EC2

É possível definir janelas de eventos personalizadas recorrentes semanalmente para eventos agendados que reinicializam, interrompem ou terminam suas instâncias do Amazon EC2. É possível

associar uma ou mais instâncias a uma janela de eventos. Se um evento agendado para essas instâncias estiver planejado, a AWS irá programar os eventos na janela de eventos associada.

É possível usar janelas de eventos para maximizar a disponibilidade da workload especificando janelas de eventos que ocorrem durante períodos fora do pico para sua workload. Também é possível alinhar as janelas de eventos com suas programações de manutenção internas.

Você define uma janela de evento especificando um conjunto de intervalos de tempo. O intervalo de tempo mínimo é de duas horas. Os intervalos de tempo combinados devem totalizar pelo menos 4 horas.

É possível associar uma ou mais instâncias a uma janela de evento usando IDs de instância ou tags de instância. Também é possível associar hosts dedicados a uma janela de evento usando o ID do host.

> **Warning**
>
> As janelas de eventos são aplicáveis apenas para eventos agendados que param, reinicializam ou encerram instâncias.
> Janelas de eventos sãonãoaplicável para:
>
> - Eventos agendados e eventos de manutenção de rede acelerados.
> - Manutenção não programada, como recuperação automática de instâncias e reinicializações não planejadas.

Trabalhar com janelas de eventos

- Considerações
- Criar uma janela de eventos
- Associar um alvo a uma janela de evento
- Desassociar uma tag de uma janela de eventos
- Modificar uma janela de eventos
- Excluir uma janela de eventos

Considerações

- Todos os horários da janela de eventos são mostrados em UTC.

- Uma janela de eventos pode conter vários intervalos de tempo. Embora cada intervalo individual deva ter pelo menos duas horas, a duração total em todos os intervalos deve ser de pelo menos quatro horas.
- Apenas um tipo de destino (ID de instância, ID de host dedicado ou tag de instância) pode ser associado a uma janela de evento.
- Um destino (ID de instância, ID de host dedicado ou tag de instância) só pode ser associado a uma janela de evento.
- Um máximo de 100 IDs de instância, ou 50 IDs de host dedicados ou 50 tags de instância podem ser associados a uma janela de evento. As tags de instância podem ser associadas a qualquer número de instâncias.
- Um máximo de 200 janelas de eventos podem ser criadas por AWS região:
- Várias instâncias associadas a janelas de eventos podem potencialmente ter eventos agendados ocorrem ao mesmo tempo.
- Se a AWS já agendou um evento, modificar uma janela de evento não alterará a hora do evento agendado. Se o evento tiver uma data limite, é possívelreprogramar o evento.
- Você pode interromper e iniciar uma instância antes do evento programado. Isso migra essa instância para um novo host e limpa o evento.

Criar uma janela de eventos

É possível criar uma ou mais janelas de eventos. Para cada janela de evento, você especifica um ou mais blocos de tempo. Por exemplo, é possível criar uma janela de evento com blocos de tempo que ocorrem todos os dias às 4h por duas horas. Ou é possível criar uma janela de evento com blocos de tempo que ocorrem aos domingos, das 2h às 4h, e às quartas-feiras, das 3h às 5h.

Janelas de eventos repetem semanalmente até que você as exclua.

Console

Para criar uma janela de eventos

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Events.
3. Selecione Ações, Gerenciar janelas de eventos.
4. Selecione Janela Criar evento de instância.
5. para o Nome da janela de eventos, insira um nome descritivo para a janela de eventos.

6. para o Agendamento de janelas, escolha especificar os blocos de tempo na janela de eventos usando o construtor de cron ou especificando intervalos de tempo.

   - Se escolher o Construtor de cron, especifique o seguinte:
     1. para o Dias (UTC), especifique os dias da semana em que a janela de eventos ocorre.
     2. para o Hora de início (UTC), especifique a hora em que a janela de evento começa.
     3. para a Duração, especifique a duração dos blocos de tempo na janela do evento. A duração mínima por bloco de tempo é de 2 horas. A duração mínima da janela do evento deve ser igual ou superior a 4 horas no total. Todos os horários são em UTC.
   - Se escolher Intervalos de tempo, escolha Adicione um novo intervalo de tempo e especifique o dia e a hora de início e o dia e a hora de término. Repita para cada intervalo de tempo. A duração mínima por intervalo de tempo é de 2 horas. A duração mínima para todos os intervalos de tempo combinados deve ser igual ou superior a 4 horas no total.
7. (Opcional) Em Detalhes do destino, associe uma ou mais instâncias à janela de eventos. Use IDs de instância ou etiquetas de instância para associar instâncias. Use IDs de host para associar Hosts dedicados. Quando esses destinos estiverem programados para manutenção, o evento ocorrerá durante essa janela de eventos.

   É possível criar a janela de evento sem associar um destino à janela. Posteriormente, é possível modificar a janela para associar um ou mais alvos.
8. (Opcional) Para Tags da janela de evento, escolha Adicionar tag e insira a chave e o valor da tag. Repita esse procedimento para cada tag.
9. Selecione Janela Criar eventos.

AWS CLI

Para criar uma janela de eventos com um intervalo de tempo

Use o comando create-instance-event-window.

```
aws ec2 create-instance-event-window \
    --time-range StartWeekDay=monday,StartHour=2,EndWeekDay=wednesday,EndHour=8 \
    --tag-specifications "ResourceType=instance-event-
window,Tags=[{Key=K1,Value=V1}]" \
    --name myEventWindowName
```

O seguinte é um exemplo de saída.

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "TimeRanges": [
            {
                "StartWeekDay": "monday",
                "StartHour": 2,
                "EndWeekDay": "wednesday",
                "EndHour": 8
            }
        ],
        "Name": "myEventWindowName",
        "State": "creating",
        "Tags": [
            {
                "Key": "K1",
                "Value": "V1"
            }
        ]
    }
}
```

Para criar uma janela de eventos com uma expressão cron

Use o comando create-instance-event-window.

```
aws ec2 create-instance-event-window \
    --cron-expression "* 21-23 * * 2,3" \
    --tag-specifications "ResourceType=instance-event-
window,Tags=[{Key=K1,Value=V1}]" \
    --name myEventWindowName
```

O seguinte é um exemplo de saída.

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "Name": "myEventWindowName",
        "CronExpression": "* 21-23 * * 2,3",
        "State": "creating",
        "Tags": [
            {
```

```
                "Key": "K1",
                "Value": "V1"
            }
        ]
    }
}
```

PowerShell

Para criar uma janela de eventos com um intervalo de tempo

Use o cmdlet New-EC2InstanceEventWindow.

```
$timeRange = New-Object Amazon.EC2.Model.InstanceEventWindowTimeRangeRequest
$timeRange.StartWeekDay = "monday"
$timeRange.EndWeekDay = "wednesday"
$timeRange.StartHour = 2
$timeRange.EndHour = 8
$tag = @{Key="key1"; Value="value1"}
$tagspec = New-Object Amazon.EC2.Model.TagSpecification
$tagspec.ResourceType = "instance-event-window"
$tagspec.Tags.Add($tag)
New-EC2InstanceEventWindow `
    -Name my-event-window `
    -TagSpecification $tagspec `
    -TimeRange @($timeRange)
```

O seguinte é um exemplo de saída.

```
AssociationTarget     :
CronExpression        :
InstanceEventWindowId : iew-0abcdef1234567890
Name                  : my-event-window
State                 : creating
Tags                  : {key1}
TimeRanges            : {Amazon.EC2.Model.InstanceEventWindowTimeRange}
```

Para criar uma janela de eventos com uma expressão cron

Use o cmdlet New-EC2InstanceEventWindow.

```
$tag = @{Key="key1"; Value="value1"}
```

```
$tagspec = New-Object Amazon.EC2.Model.TagSpecification
$tagspec.ResourceType = "instance-event-window"
$tagspec.Tags.Add($tag)
New-EC2InstanceEventWindow `
    -Name my-event-window `
    -TagSpecification $tagspec`
    -CronExpression "* 21-23 * * 2,3"
```

O seguinte é um exemplo de saída.

```
AssociationTarget     :
CronExpression        : * 21-23 * * 2,3
InstanceEventWindowId : iew-0abcdef1234567890
Name                  : my-event-window
State                 : creating
Tags                  : {key1}
TimeRanges            : {}
```

Associar um alvo a uma janela de evento

Após criar uma janela de evento, você poderá associar destinos à janela de eventos. É possível associar apenas um tipo de destino a uma janela de eventos. É possível especificar IDs de instância, IDs de host dedicado ou tags de instância.

Console

Para associar destinos adicionais a uma janela de eventos

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Events.
3. Selecione a janela de eventos a ser modificada.
4. Escolha Ações, Modificar janela de eventos da instância.

AWS CLI

Para associar tags de instância a uma janela de eventos

Use o comando associate-instance-event-window.

```
aws ec2 associate-instance-event-window \
```

```
    --instance-event-window-id iew-0abcdef1234567890 \
    --association-target "InstanceTags=[{Key=k2,Value=v2},{Key=k1,Value=v1}]"
```

O seguinte é um exemplo de saída.

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "Name": "myEventWindowName",
        "CronExpression": "* 21-23 * * 2,3",
        "AssociationTarget": {
            "InstanceIds": [],
            "Tags": [
                {
                    "Key": "k2",
                    "Value": "v2"
                },
                {
                    "Key": "k1",
                    "Value": "v1"
                }
            ],
            "DedicatedHostIds": []
        },
        "State": "creating"
    }
}
```

Para associar IDs de instâncias a uma janela de eventos

Use o comando associate-instance-event-window.

```
aws ec2 associate-instance-event-window \
    --instance-event-window-id iew-0abcdef1234567890 \
    --association-target "InstanceIds=i-1234567890abcdef0,i-0598c7d356eba48d7"
```

O seguinte é um exemplo de saída.

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "Name": "myEventWindowName",
```

```
        "CronExpression": "* 21-23 * * 2,3",
        "AssociationTarget": {
            "InstanceIds": [
                "i-1234567890abcdef0",
                "i-0598c7d356eba48d7"
            ],
            "Tags": [],
            "DedicatedHostIds": []
        },
        "State": "creating"
    }
}
```

Para associar um host dedicado a uma janela de eventos

Use o comando associate-instance-event-window.

```
aws ec2 associate-instance-event-window \
    --instance-event-window-id iew-0abcdef1234567890 \
    --association-target "DedicatedHostIds=h-029fa35a02b99801d"
```

O seguinte é um exemplo de saída.

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "Name": "myEventWindowName",
        "CronExpression": "* 21-23 * * 2,3",
        "AssociationTarget": {
            "InstanceIds": [],
            "Tags": [],
            "DedicatedHostIds": [
                "h-029fa35a02b99801d"
            ]
        },
        "State": "creating"
    }
}
```

PowerShell

Para associar tags de instância a uma janela de eventos

Use o cmdlet Register-EC2InstanceEventWindow.

```
$tag1 = @{Key="key1"; Value="value1"}
$tag2 = @{Key="key2"; Value="value2"}
Register-EC2InstanceEventWindow `
    -InstanceEventWindowId iew-0abcdef1234567890 `
    -AssociationTarget_InstanceTag @($tag1,$tag2)
```

Para associar IDs de instâncias a uma janela de eventos

Use o cmdlet Register-EC2InstanceEventWindow.

```
Register-EC2InstanceEventWindow `
    -InstanceEventWindowId iew-0abcdef1234567890 `
    -AssociationTarget_InstanceId i-1234567890abcdef0, i-0598c7d356eba48d7
```

Para associar um host dedicado a uma janela de eventos

Use o cmdlet Register-EC2InstanceEventWindow.

```
Register-EC2InstanceEventWindow `
    -InstanceEventWindowId iew-0abcdef1234567890 `
    -AssociationTarget_DedicatedHostId h-029fa35a02b99801d
```

Desassociar uma tag de uma janela de eventos

Console

Para desassociar destinos com uma janela de eventos

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Events.
3. Selecione a janela de eventos a ser modificada.
4. Escolha Ações, Modificar janela de eventos da instância.

AWS CLI

Para desassociar tags de instância de uma janela de eventos

Use o comando disassociate-instance-event-window.

```
aws ec2 disassociate-instance-event-window \
    --instance-event-window-id iew-0abcdef1234567890 \
    --association-target "InstanceTags=[{Key=k2,Value=v2},{Key=k1,Value=v1}]"
```

O seguinte é um exemplo de saída.

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "Name": "myEventWindowName",
        "CronExpression": "* 21-23 * * 2,3",
        "AssociationTarget": {
            "InstanceIds": [],
            "Tags": [],
            "DedicatedHostIds": []
        },
        "State": "creating"
    }
}
```

Para desassociar IDs de instâncias de uma janela de eventos

Use o comando disassociate-instance-event-window.

```
aws ec2 disassociate-instance-event-window \
    --instance-event-window-id iew-0abcdef1234567890 \
    --association-target "InstanceIds=i-1234567890abcdef0,i-0598c7d356eba48d7"
```

O seguinte é um exemplo de saída.

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "Name": "myEventWindowName",
        "CronExpression": "* 21-23 * * 2,3",
        "AssociationTarget": {
            "InstanceIds": [],
            "Tags": [],
            "DedicatedHostIds": []
        },
```

```
        "State": "creating"
    }
}
```

Para desassociar um host dedicado de uma janela de eventos

Use o comando disassociate-instance-event-window.

```
aws ec2 disassociate-instance-event-window \
    --instance-event-window-id iew-0abcdef1234567890 \
    --association-target DedicatedHostIds=h-029fa35a02b99801d
```

O seguinte é um exemplo de saída.

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "Name": "myEventWindowName",
        "CronExpression": "* 21-23 * * 2,3",
        "AssociationTarget": {
            "InstanceIds": [],
            "Tags": [],
            "DedicatedHostIds": []
        },
        "State": "creating"
    }
}
```

PowerShell

Para desassociar tags de instância de uma janela de eventos

Use o cmdlet Unregister-EC2InstanceEventWindow.

```
$tag1 = @{Key="key1"; Value="value1"}
$tag2 = @{Key="key2"; Value="value2"}
Unregister-EC2InstanceEventWindow `
    -InstanceEventWindowId iew-0abcdef1234567890 `
    -AssociationTarget_InstanceTag @($tag1, $tag2)
```

Para desassociar IDs de instâncias de uma janela de eventos

Use o cmdlet Unregister-EC2InstanceEventWindow.

```
Unregister-EC2InstanceEventWindow `
    -InstanceEventWindowId iew-0abcdef1234567890 `
    -AssociationTarget_InstanceId i-1234567890abcdef0, i-0598c7d356eba48d7
```

Para desassociar um host dedicado de uma janela de eventos

Use o cmdlet Unregister-EC2InstanceEventWindow.

```
Unregister-EC2InstanceEventWindow `
    -InstanceEventWindowId iew-0abcdef1234567890 `
    -AssociationTarget_DedicatedHostId h-029fa35a02b99801d
```

Modificar uma janela de eventos

É possível modificar todos os campos de uma janela de evento, exceto seu ID. Por exemplo, quando o horário de verão começar, convém modificar o agendamento da janela de eventos. Para janelas de eventos existentes, talvez você queira adicionar ou remover destinos.

É possível modificar um intervalo de tempo ou uma expressão cron ao modificar a janela de evento, mas não ambos.

Console

Para modificar uma janela de eventos

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Events.
3. Selecione Ações, Gerenciar janelas de eventos.
4. Selecione a janela de eventos a ser modificada e escolha Ações, Janela Modificar evento da instância.
5. Modifique os campos na janela de eventos e escolha Modificar janela de evento.

AWS CLI

Para modificar o intervalo de tempo de uma janela de eventos

Use o comando modify-instance-event-window.

```
aws ec2 modify-instance-event-window
    --instance-event-window-id iew-0abcdef1234567890 \
    --time-range StartWeekDay=monday,StartHour=2,EndWeekDay=wednesday,EndHour=8
```

O seguinte é um exemplo de saída.

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "TimeRanges": [
            {
                "StartWeekDay": "monday",
                "StartHour": 2,
                "EndWeekDay": "wednesday",
                "EndHour": 8
            }
        ],
        "Name": "myEventWindowName",
        "AssociationTarget": {
            "InstanceIds": [
                "i-0abcdef1234567890",
                "i-0be35f9acb8ba01f0"
            ],
            "Tags": [],
            "DedicatedHostIds": []
        },
        "State": "creating",
        "Tags": [
            {
                "Key": "K1",
                "Value": "V1"
            }
        ]
    }
}
```

Modificar um conjunto de intervalos de tempo para uma janela de eventos

Use o comando modify-instance-event-window.

```
aws ec2 modify-instance-event-window
```

```
    --instance-event-window-id iew-0abcdef1234567890 \
    --time-range '[{"StartWeekDay": "monday", "StartHour": 2, "EndWeekDay":
 "wednesday", "EndHour": 8},
   {"StartWeekDay": "thursday", "StartHour": 2, "EndWeekDay": "friday",
 "EndHour": 8}]'
```

O seguinte é um exemplo de saída.

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "TimeRanges": [
            {
                "StartWeekDay": "monday",
                "StartHour": 2,
                "EndWeekDay": "wednesday",
                "EndHour": 8
            },
            {
                "StartWeekDay": "thursday",
                "StartHour": 2,
                "EndWeekDay": "friday",
                "EndHour": 8
            }
        ],
        "Name": "myEventWindowName",
        "AssociationTarget": {
            "InstanceIds": [
                "i-0abcdef1234567890",
                "i-0be35f9acb8ba01f0"
            ],
            "Tags": [],
            "DedicatedHostIds": []
        },
        "State": "creating",
        "Tags": [
            {
                "Key": "K1",
                "Value": "V1"
            }
        ]
    }
}
```

Para modificar a expressão cron de uma janela de eventos

Use o comando modify-instance-event-window.

```
aws ec2 modify-instance-event-window
    --instance-event-window-id iew-0abcdef1234567890 \
    --cron-expression "* 21-23 * * 2,3"
```

O seguinte é um exemplo de saída.

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "Name": "myEventWindowName",
        "CronExpression": "* 21-23 * * 2,3",
        "AssociationTarget": {
            "InstanceIds": [
                "i-0abcdef1234567890",
                "i-0be35f9acb8ba01f0"
            ],
            "Tags": [],
            "DedicatedHostIds": []
        },
        "State": "creating",
        "Tags": [
            {
                "Key": "K1",
                "Value": "V1"
            }
        ]
    }
}
```

PowerShell

Para modificar o intervalo de tempo de uma janela de eventos

Use o cmdlet Edit-EC2InstanceEventWindow.

```
$timeRange1 = New-Object Amazon.EC2.Model.InstanceEventWindowTimeRangeRequest
$timeRange1.StartWeekDay = "monday"
$timeRange1.EndWeekDay = "wednesday"
```

```
$timeRange1.StartHour = 2
$timeRange1.EndHour = 8
$timeRange2 = New-Object Amazon.EC2.Model.InstanceEventWindowTimeRangeRequest
$timeRange2.StartWeekDay = "thursday"
$timeRange2.EndWeekDay = "friday"
$timeRange2.StartHour = 1
$timeRange2.EndHour = 6
Edit-EC2InstanceEventWindow `
    -InstanceEventWindowId iew-0abcdef1234567890 `
    -TimeRange @($timeRange1, $timeRange2)
```

Para modificar a expressão cron de uma janela de eventos

Use o cmdlet Edit-EC2InstanceEventWindow.

```
Edit-EC2InstanceEventWindow `
    -InstanceEventWindowId iew-0abcdef1234567890 `
    -CronExpression "* 21-23 * * 2,3"
```

Excluir uma janela de eventos

É possível excluir uma janela de eventos de cada vez.

Console

Para excluir uma janela de eventos

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Events.
3. Selecione Ações, Gerenciar janelas de eventos.
4. Selecione a janela de eventos a ser excluída e escolha Ações, Janela de evento Excluir instância.
5. Quando solicitado, digite **`delete`** e escolha Delete (Excluir).

AWS CLI

Para excluir uma janela de eventos

Usar adelete-instance-event-windowe especifique a janela de evento a ser excluída.

```
aws ec2 delete-instance-event-window \
    --instance-event-window-id iew-0abcdef1234567890
```

Para forçar a exclusão de uma janela de eventos

Usar a`--force-delete`se a janela de evento estiver atualmente associada a destinos.

```
aws ec2 delete-instance-event-window \
    --instance-event-window-id iew-0abcdef1234567890 \
    --force-delete
```

PowerShell

Para excluir uma janela de eventos

Use o cmdlet Remove-EC2InstanceEventWindow.

```
Remove-EC2InstanceEventWindow `
    -InstanceEventWindowId iew-0abcdef1234567890
```

Para forçar a exclusão de uma janela de eventos

Use o cmdlet Remove-EC2InstanceEventWindow.

```
Remove-EC2InstanceEventWindow `
    -InstanceEventWindowId iew-0abcdef1234567890 `
    -ForceDelete $true
```

Monitorar instâncias usando o CloudWatch

É possível monitorar suas instâncias usando o Amazon CloudWatch, que coleta e processa os dados brutos do Amazon EC2 em métricas legíveis, quase em tempo real. Essas estatísticas são registradas para um período de 15 meses, de forma que você possa acessar informações históricas e ganhar uma perspectiva melhor sobre como seu serviço ou aplicação Web está se saindo.

Por padrão, o Amazon EC2 envia dados de métrica ao CloudWatch em períodos de 5 minutos. Para enviar dados de métrica para sua instância ao CloudWatch em períodos de 1 minuto, é possível habilitar o monitoramento detalhado na instância. Para obter mais informações, consulte Gerenciar o monitoramento detalhado das instâncias do Amazon EC2.

O console do Amazon EC2 exibe uma série de gráficos com base nos dados brutos do Amazon CloudWatch. Dependendo de suas necessidades, é possível preferir obter dados para suas instâncias do Amazon CloudWatch em vez de gráficos no console.

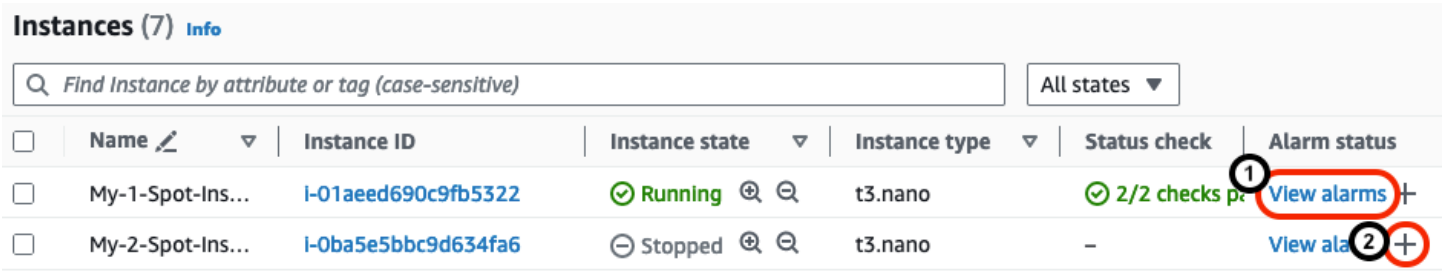
Para saber mais sobre faturamento e custos do Amazon CloudWatch, consulte Faturamento e custos do CloudWatch no Guia do usuário do Amazon CloudWatch.

Conteúdo

- Gerenciar os alarmes do CloudWatch para as instâncias do EC2 no console do Amazon EC2
- Gerenciar o monitoramento detalhado das instâncias do Amazon EC2
- As métricas do CloudWatch que estão disponíveis para as instâncias
- Instale e configure o agente do CloudWatch usando o console do Amazon EC2 para adicionar métricas adicionais
- Estatísticas para as métricas do CloudWatch para as instâncias
- Exibir os grafos de monitoramento para as instâncias
- Criar um alarme do CloudWatch para uma instância
- Criar alarmes para interromper, encerrar, reinicializar ou recuperar uma instância

Gerenciar os alarmes do CloudWatch para as instâncias do EC2 no console do Amazon EC2

Na tela Instâncias do console do Amazon EC2, você pode gerenciar os alarmes do Amazon CloudWatch para as suas instâncias. Na tabela Instâncias, a coluna Status do alarme fornece dois controles do console: um controle para visualizar os alarmes e outro para criá-los ou editá-los. A captura de tela a seguir indica esses controles do console, numerados com 1 (Visualizar alarmes) e 2 (um sinal de + para criar ou editar um alarme).



Visualizar alarmes na tela Instâncias

É possível visualizar os alarmes de cada instância na tela Instâncias.

Para visualizar o alarme de uma instância na tela Instâncias

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Na tabela Instâncias, para a instância escolhida, escolha Visualizar alarmes (numerados com 1 na captura de tela anterior).
4. Na janela Detalhes do alarme para ***i-1234567890abcdef0***, escolha o nome do alarme para visualizar no console do CloudWatch.

Criar alarmes na tela Instâncias

É possível criar um alarme para cada instância na tela Instâncias.

Para criar um alarme para uma instância na tela Instâncias

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Na tabela Instâncias, para a instância escolhida, escolha o sinal de adição (numerado com 2 na captura de tela anterior).
4. Na tela Gerenciar alarmes do CloudWatch, crie seu alarme. Para obter mais informações, consulte Criar um alarme do CloudWatch para uma instância.

Editar alarmes na tela Instâncias

É possível editar um alarme para uma instância na tela Instâncias.

Para editar um alarme para uma instância na tela Instâncias

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Na tabela Instâncias, para a instância escolhida, escolha o sinal de adição (numerado com 2 na captura de tela anterior).
4. Na tela Gerenciar alarmes do CloudWatch, edite o alarme. Para obter mais informações, consulte Editar ou excluir um alarme do CloudWatch no Guia do usuário do Amazon CloudWatch.

Gerenciar o monitoramento detalhado das instâncias do Amazon EC2

O Amazon CloudWatch fornece duas categorias de monitoramento: monitoramento básico e monitoramento detalhado. Por padrão, a instância está configurada para monitoramento básico. Como opção, é possível habilitar o monitoramento detalhado para ajudar você a identificar e atuar mais rapidamente em problemas operacionais. É possível habilitar ou desativar o monitoramento detalhado em uma instância quando executá-la ou depois de a instância estar sendo executada ou ter sido interrompida.

Habilitar o monitoramento detalhado em uma instância não afeta o monitoramento dos volumes do EBS anexados. Para obter mais informações, consulte Métricas de uso do Amazon CloudWatch para o Amazon EBS.

A tabela a seguir destaca as diferenças entre o monitoramento básico e o monitoramento detalhado de instâncias.

Tipo de monitoramento	Descrição	Cobranças
Monitoramento básico	As métricas de verificação de status estão disponíveis em períodos de um minuto. Todas as outras métricas estão disponíveis em períodos de cinco minutos.	Sem cobrança.
Monitoramento detalhado	É possível obter métricas em intervalos de 1 minuto, desde que você habilite o monitoramento detalhado para a instância. Depois de ativar o monitoramento detalhado, será possível agregar os dados em grupos de instâncias semelhantes.	A cobrança é feita pela métrica que o Amazon EC2 envia para o CloudWatch. Você não é cobrado pelo armazenamento de dados. Para obter mais informações, consulte Nível pago na página de preços do Amazon CloudWatch.

Conteúdo

- Permissões obrigatórias

- Habilitar o monitoramento detalhado no momento da execução
- Gerenciar o monitoramento detalhado

Permissões obrigatórias

Para habilitar o monitoramento detalhado de uma instância, o usuário deve ter permissão para usar a ação de API MonitorInstances. Para desativar o monitoramento detalhado de uma instância, o usuário deve ter permissão para usar a ação de API UnmonitorInstances.

Habilitar o monitoramento detalhado no momento da execução

Use os procedimentos a seguir para habilitar o monitoramento detalhado no momento da execução. Por padrão, a instância usa o monitoramento básico.

Console

Para habilitar o monitoramento detalhado ao executar uma instância

Ao executar uma instância usando o console do Amazon EC2, em Detalhes avançados, marque a caixa de seleção Monitoramento detalhado do CloudWatch.

AWS CLI

Para habilitar o monitoramento detalhado ao executar uma instância

Use o comando run-instances com a opção `--monitoring`.

```
--monitoring Enabled=true
```

PowerShell

Para habilitar o monitoramento detalhado ao executar uma instância

Use o cmdlet New-EC2Instance com o parâmetro `-Monitoring`.

```
-Monitoring $true
```

Gerenciar o monitoramento detalhado

Use os procedimentos a seguir para gerenciar o monitoramento detalhado para uma instância em execução ou interrompida.

Console

Para gerenciar o monitoramento detalhado

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância.
4. Escolha Ações, Monitorar e solucionar problemas, Gerenciar monitoramento detalhado.
5. Na página Monitoramento detalhado, para Monitoramento detalhado, faça o seguinte:
   - Monitoramento detalhado: selecione Habilitar.
   - Monitoramento básico: desmarque Habilitar.
6. Escolha Confirmar.

AWS CLI

Para habilitar o monitoramento detalhado

Use o seguinte comando monitor-instances.

```
aws ec2 monitor-instances --instance-ids i-1234567890abcdef0
```

Para desabilitar o monitoramento detalhado

Use o seguinte comando unmonitor-instances.

```
aws ec2 unmonitor-instances --instance-ids i-1234567890abcdef0
```

PowerShell

Para habilitar o monitoramento detalhado

Use o cmdlet Start-EC2InstanceMonitoring.

```
Start-EC2InstanceMonitoring -InstanceId i-1234567890abcdef0
```

Para desabilitar o monitoramento detalhado

Use o cmdlet Stop-EC2InstanceMonitoring.

```
Stop-EC2InstanceMonitoring -InstanceId i-1234567890abcdef0
```

As métricas do CloudWatch que estão disponíveis para as instâncias

O Amazon EC2 envia métricas para o Amazon CloudWatch. É possível 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. Observe que, para as estatísticas Mínimo, Máximo e Média, a granularidade mínima para as métricas que o EC2 fornece é de 1 minuto.

Para obter informações sobre como visualizar as métricas disponíveis usando o Console de gerenciamento da AWS ou a AWS CLI, consulte Visualizar métricas disponíveis no Guia do usuário do Amazon CloudWatch.

Para obter informações sobre a obtenção de estatísticas para essas métricas, consulte Estatísticas para as métricas do CloudWatch para as instâncias.

Tópicos

- Métricas de instância
- Métricas do acelerador
- Métricas de crédito de CPU
- Métricas de host dedicado
- Métricas do Amazon EBS para instâncias baseadas em Nitro
- Métricas de verificação de status
- Métricas de espelhamento de tráfego
- Métricas do grupo do Auto Scaling
- Dimensões de métrica do Amazon EC2
- Métricas de uso do Amazon EC2

Métricas de instância

O namespace `AWS/EC2` inclui as métricas de instância a seguir.

Métrica	Descrição	Unidade	Estatísticas significativas
`CPUUtilization`	A porcentagem de tempo físico de CPU que o Amazon EC2 usa para executar a instância do EC2, que inclui o tempo gasto para executar o código do usuário e o código do Amazon EC2. Em um nível muito alto, `CPUUtilization` é a soma da `CPUUtilization` do guest e da `CPUUtilization` do hypervisor. As ferramentas em seu sistema operacional podem mostrar uma porcentagem diferente da do CloudWatch devido a fatores como simulação de dispositivos legados, configuração de dispositivos não legados, workloads com interrupções pesadas, migração ao vivo e atualização ao vivo.	Percent	• Average • Minimum • Maximum
`DiskReadOps`	Operações de leitura concluídas de todos os volumes de armazenamento de instâncias disponíveis para a instância em um período de tempo especificado. 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. Se não houver nenhum volume de armazenamento de instâncias, o valor será 0 ou a métrica não será relatada.	Count	• Sum • Average • Minimum • Maximum
`DiskWriteOps`	Operações de gravação concluídas em todos os volumes de armazenamento de instâncias disponíveis para a instância em um período de tempo especificado.	Count	• Sum • Average • Minimum

Métrica	Descrição	Unidade	Estatísticas significativas
	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. Se não houver nenhum volume de armazenamento de instâncias, o valor será 0 ou a métrica não será relatada.		• Maximum

Métrica	Descrição	Unidade	Estatísticas significativas
`DiskReadBytes`	Bytes lidos de todos os volumes de armazenamento de instâncias disponíveis para a instância. Essa métrica é utilizada para determinar o volume de dados que a aplicação lê do disco rígido da instância. Isso pode ser usado para determinar a velocidade da aplicação. O número relatado é o número de bytes recebidos durante o período. Se você estiver usando o monitoramento básico (5 minutos), divida esse número por 300 para encontrar o número de bytes/segundo. Se você estiver usando o monitoramento detalhado (1 minuto), divida o número por 60. Você também pode usar a função métrica matemática `DIFF_TIME` do CloudWatch para encontrar os bytes por segundo. Por exemplo, se você tiver representado graficamente `DiskReadBytes` no CloudWatch como `m1`, a fórmula métrica matemática `m1/(DIFF_TIME(m1))` retornará a métrica em bytes/segundo. Para obter mais informações sobre `DIFF_TIME` e outras funções métricas matemáticas, consulte Usar métrica matemática no Guia do usuário do Amazon CloudWatch. Se não houver nenhum volume de armazenamento de instâncias, o valor será 0 ou a métrica não será relatada.	Bytes	• Sum • Average • Minimum • Maximum

Métrica	Descrição	Unidade	Estatísticas significativas
`DiskWriteBytes`	Bytes gravados em todos os volumes de armazenamento de instâncias disponíveis para a instância. Essa métrica é utilizada para determinar o volume de dados que a aplicação grava no disco rígido da instância. Isso pode ser usado para determinar a velocidade da aplicação. O número relatado é o número de bytes recebidos durante o período. Se você estiver usando o monitoramento básico (5 minutos), divida esse número por 300 para encontrar o número de bytes/segundo. Se você estiver usando o monitoramento detalhado (1 minuto), divida o número por 60. Você também pode usar a função métrica matemática `DIFF_TIME` do CloudWatch para encontrar os bytes por segundo. Por exemplo, se você tiver representado graficamente `DiskWriteBytes` no CloudWatch como `m1`, a fórmula métrica matemática `m1/(DIFF_TIME(m1))` retornará a métrica em bytes/segundo. Para obter mais informações sobre `DIFF_TIME` e outras funções métricas matemáticas, consulte Usar métrica matemática no Guia do usuário do Amazon CloudWatch. Se não houver nenhum volume de armazenamento de instâncias, o valor será 0 ou a métrica não será relatada.	Bytes	• Sum • Average • Minimum • Maximum

Métrica	Descrição	Unidade	Estatísticas significativas
`MetadataNoToken`	O número de vezes que o serviço de metadados de instância (IMDS) foi acessado com êxito por meio de um método que não usa um token. Essa métrica é usada para determinar se existem processos que acessam metadados de instância que usam o serviço de metadados de instância versão 1 (IMDSv1), que não usa um token. Se todas as solicitações usarem sessões baseadas em tokens, por exemplo, o serviço de metadados de instância versão 2 (IMDSv2), o valor será 0. Para obter mais informações, consulte Transição para usar o Serviço de metadados da instância versão 2.	Instâncias Nitro: nenhuma Instâncias Xen: Count	• Sum • Percentiles
`MetadataNoTokenRejected`	O número de vezes que uma chamada ao IMDSv1 foi tentada após a desabilitação do IMDSv1. Se essa métrica aparecer, ela indica que uma chamada ao IMDSv1 foi tentada e rejeitada. É possível reabilitar o IMDSv1 ou garantir que todas as suas chamadas usem o IMDSv2. Para obter mais informações, consulte Transição para usar o Serviço de metadados da instância versão 2.	Instâncias Nitro: nenhuma Instâncias Xen: Count	• Sum • Percentiles

Métrica	Descrição	Unidade	Estatísticas significativas
`NetworkIn`	A quantidade de bytes recebidos em todas as interfaces de rede pela instância. Essa métrica identifica o volume de tráfego de rede de entrada para uma única instância. O número relatado é o número de bytes recebidos durante o período. Se você estiver usando o monitoramento básico (5 minutos) e a estatística for Sum (Soma), divida esse número por 300 para encontrar o número de bytes/segundo. Se você tiver o monitoramento detalhado (1 minuto) e a estatística for Sum (soma), divida o número por 60.	Bytes	• Sum • Average • Minimum • Maximum
`NetworkOut`	A quantidade de bytes enviados em todas as interfaces de rede pela instância. Essa métrica identifica o volume de tráfego de rede de saída de uma única instância. O número relatado é o número de bytes enviados durante o período. Se você estiver usando o monitoramento básico (5 minutos) e a estatística for Sum (Soma), divida esse número por 300 para encontrar o número de bytes/segundo. Se você tiver o monitoramento detalhado (1 minuto) e a estatística for Sum (soma), divida o número por 60.	Bytes	• Sum • Average • Minimum • Maximum

Métrica	Descrição	Unidade	Estatísticas significativas
`NetworkPackets In`	A quantidade de pacotes recebidos em todas as interfaces de rede pela instância. Essa métrica identifica o volume de tráfego de entrada em termos do número de pacotes em uma única instância. Essa métrica está disponível apenas para monitoramento básico (períodos de 5 minutos). Para calcular a quantidade de pacotes por segundo (PPS) que sua instância recebeu nos 5 minutos, divida o valor da estatística Sum por 300.	Count	• Sum • Average • Minimum • Maximum
`NetworkPackets Out`	A quantidade de pacotes enviados em todas as interfaces de rede pela instância. Essa métrica identifica o volume de tráfego de saída em termos do número de pacotes em uma única instância. Essa métrica está disponível apenas para monitoramento básico (períodos de 5 minutos). Para calcular a quantidade de pacotes por segundo (PPS) que sua instância enviou nos cinco minutos, divida o valor da estatística Sum (soma) por 300.	Count	• Sum • Average • Minimum • Maximum

Métricas do acelerador

O namespace `AWS/EC2` inclui a métrica aceleradora a seguir para suas instâncias de computação acelerada. Com suporte somente em um subconjunto dos tipos de instância com computação acelerada.

Métrica	Descrição	Unidade	Estatísticas significativas
`GPUPowerUtilization`	Uso de energia ativa como percentual da potência ativa máxima.	Percentual	• Average • Minimum • Maximum

Métricas de crédito de CPU

O namespace `AWS/EC2` inclui as seguintes métricas de crédito de CPU para suas instâncias expansíveis.

Métrica	Descrição	Unidade	Estatísticas significativas
`CPUCreditUsage`	O número de créditos de CPU gastos pela instância por utilização de CPU. Um crédito de CPU equivale a um vCPU em execução em 100% de utilização por um minuto ou a uma combinação equivalente de vCPUs, utilização e tempo (por exemplo, um vCPU em execução a 50% de utilização por dois minutos ou dois vCPUs em execução a 25% de utilização por dois minutos). As métricas de crédito de CPU estão disponíveis apenas a uma frequência de 5 minutos. Se você especificar um período de mais cinco minutos, use a estatística `Sum` em vez da estatística `Average`.	Créditos (minutos de vCPU)	• Sum • Average • Minimum • Maximum
`CPUCreditBalance`	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.	Créditos (minutos de vCPU)	• Sum • Average • Minimum • Maximum

Métrica	Descrição	Unidade	Estatísticas significativas
	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. Os créditos do `CPUCreditBalance` são disponibilizados para que a instância gaste e apresente expansão com uma utilização de CPU acima da linha de base. Quando uma instância está em execução, os créditos do `CPUCreditBalance` não expiram. Quando uma instância T3 ou T3a é interrompida, o valor `CPUCreditBalance` persiste por sete dias. Consequentemente, todos os créditos acumulados são perdidos. Quando uma instância T2 é interrompida, o valor `CPUCreditBalance` não persiste, e todos os créditos acumulados são perdidos. As métricas de crédito de CPU estão disponíve is apenas a uma frequência de 5 minutos.		

Métrica	Descrição	Unidade	Estatísticas significativas
`CPUSurplusCreditBalance`	O número de créditos excedentes gastos por uma instância `unlimited` quando seu valor `CPUCreditBalance` é zero. 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. As métricas de crédito de CPU estão disponíveis apenas a uma frequência de 5 minutos.	Créditos (minutos de vCPU)	• Sum • Average • Minimum • Maximum
`CPUSurplusCreditsCharged`	O número de créditos excedentes gastos que não são pagos pelos créditos de CPU ganhos e que, portanto, incorrem em uma cobrança adicional. Os créditos excedentes gastos são cobrados quando uma das seguintes situações ocorre: • 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 `unlimited` para `standard`. As métricas de crédito de CPU estão disponíveis apenas a uma frequência de 5 minutos.	Créditos (minutos de vCPU)	• Sum • Average • Minimum • Maximum

Métricas de host dedicado

O namespace AWS/EC2 inclui as métricas a seguir para hosts dedicados T3.

Métrica	Descrição	Unidade	Estatísticas significativas
DedicatedHostCPUUtilization	A porcentagem de capacidade computacional alocada que está atualmente em uso pelas instâncias em execução no host dedicado.	Percent	• Sum • Average • Minimum • Maximum

Métricas do Amazon EBS para instâncias baseadas em Nitro

O namespace AWS/EC2 inclui métricas adicionais do Amazon EBS para os volumes anexados a instâncias baseadas no Nitro que não são instâncias bare metal.

Métrica	Descrição	Unidade	Estatísticas significativas
InstanceEBSIOPSExceededCheck	Indica se uma aplicação tentou realizar operações de IOPS que excederam os limites máximos de IOPS do EBS para a instância durante o último minuto. Essa métrica pode assumir o valor 0 (IOPS não excedido) ou 1 (IOPS excedido).	Nenhum	• Soma • Média • Mínimo • Máximo
InstanceEBSThroughputExceededCheck	Indica se uma aplicação tentou realizar operações de throughput que excederam os limites máximos de throughput do EBS para a instância durante o último minuto. Essa métrica pode assumir o valor 0 (throughput não excedido) ou 1 (throughput excedido).	Nenhum	• Soma • Média • Mínimo • Máximo
EBSReadOps	Operações de leitura concluídas de todos os volumes do Amazon EBS anexados à instância em um período especificado.	Contagem	• Soma • Média

Métrica	Descrição	Unidade	Estatísticas significativas
	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 (5 minutos), divida esse número por 300 para calcular o IOPS de leitura. Se você estiver usando o monitoramento detalhado (1 minuto), divida o número por 60. Você também pode usar a função métrica matemática `DIFF_TIME` do CloudWatch para encontrar as operações por segundo. Por exemplo, se você tiver representado graficamente `EBSReadOps` no CloudWatch como `m1`, a função métrica matemática `m1/(DIFF_TIME(m1))` retornará a métrica em operações/segundo. Para obter mais informações sobre `DIFF_TIME` e outras funções métricas matemáticas, consulte Usar métrica matemática no Guia do usuário do Amazon CloudWatch.		• Mínimo • Máximo

Métrica	Descrição	Unidade	Estatísticas significativas
`EBSWriteOps`	Operações de gravação concluídas para todos os volumes do EBS anexados à instância em um período especificado. Para calcular a média de operações de E/S de gravação por segundo (IOPS de gravação) para o período, divida o total das operações pelo número de segundos no período em questão. Se você estiver usando o monitoramento básico (5 minutos), divida esse número por 300 para calcular o IOPS de gravação. Se você estiver usando o monitoramento detalhado (1 minuto), divida o número por 60. Você também pode usar a função métrica matemática `DIFF_TIME` do CloudWatch para encontrar as operações por segundo. Por exemplo, se você tiver representado graficamente `EBSWriteOps` no CloudWatch como `m1`, a função métrica matemática `m1/(DIFF_TIME(m1))` retornará a métrica em operações/segundo. Para obter mais informações sobre `DIFF_TIME` e outras funções métricas matemáticas, consulte Usar métrica matemática no Guia do usuário do Amazon CloudWatch.	Contagem	• Soma • Média • Mínimo • Máximo

Métrica	Descrição	Unidade	Estatísticas significativas
`EBSReadBytes`	Bytes lidos de todos os volumes do EBS anexados à instância em um período especificado. O número relatado é o número de bytes lidos durante o período. Se você estiver usando o monitoramento básico (5 minutos), divida esse número por 300 para encontrar o número de bytes lidos/segundo. Se você estiver usando o monitoramento detalhado (1 minuto), divida o número por 60. Você também pode usar a função métrica matemática `DIFF_TIME` do CloudWatch para encontrar os bytes por segundo. Por exemplo, se você tiver representado graficamente `EBSReadBytes` no CloudWatch como `m1`, a fórmula métrica matemática `m1/(DIFF_TIME(m1))` retornará a métrica em bytes/segundo. Para obter mais informações sobre `DIFF_TIME` e outras funções métricas matemáticas, consulte Usar métrica matemática no Guia do usuário do Amazon CloudWatch.	Bytes	• Soma • Média • Mínimo • Máximo

Métrica	Descrição	Unidade	Estatísticas significativas
`EBSWriteBytes`	Bytes gravados em todos os volumes do EBS anexados à instância em um período especificado. O número relatado é o número de bytes gravados durante o período. Se você estiver usando o monitoramento básico (5 minutos), divida esse número por 300 para encontrar o número de bytes gravados/segundo. Se você estiver usando o monitoramento detalhado (1 minuto), divida o número por 60. Você também pode usar a função métrica matemática `DIFF_TIME` do CloudWatch para encontrar os bytes por segundo. Por exemplo, se você tiver representado graficamente `EBSWriteBytes` no CloudWatch como `m1`, a fórmula métrica matemática `m1/(DIFF_TIME(m1))` retornará a métrica em bytes/segundo. Para obter mais informações sobre `DIFF_TIME` e outras funções métricas matemáticas, consulte Usar métrica matemática no Guia do usuário do Amazon CloudWatch.	Bytes	• Soma • Média • Mínimo • Máximo

Métrica	Descrição	Unidade	Estatísticas significativas
`EBSIOBalance%`	Fornece informações sobre a porcentagem de créditos de E/S restantes no bucket de expansão. Essa métrica está disponível somente para monitoramento básico. Essa métrica está disponível apenas para alguns tamanhos de instância `*.4xlarge` e tamanhos menores que se expandam à performance máxima por apenas 30 minutos pelo menos uma vez a cada 24 horas. A estatística `Sum` não é aplicável a essa métrica.	Percentual	• Mínimo • Máximo
`EBSByteBalance%`	Fornece informações sobre a porcentagem de créditos de throughput restantes no bucket de expansão. Essa métrica está disponível somente para monitoramento básico. Essa métrica está disponível apenas para alguns tamanhos de instância `*.4xlarge` e tamanhos menores que se expandam à performance máxima por apenas 30 minutos pelo menos uma vez a cada 24 horas. A estatística `Sum` não é aplicável a essa métrica.	Percentual	• Mínimo • Máximo

Para obter informações sobre as métricas fornecidas para seus volumes do EBS, consulte Métricas para volumes do Amazon EBS no Guia do usuário do Amazon EBS. Para obter informações sobre as métricas fornecidas para frotas do EC2 e para frotas spot, consulte Monitorar a frota do EC2 ou frota spot usando o CloudWatch.

Métricas de verificação de status

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 depois que a instância concluir o estado de inicialização (alguns minutos após a instância entrar no estado de `running`). Para obter mais informações sobre verificações de status do EC2, consulte Verificações do status das instâncias do Amazon EC2.

O namespace `AWS/EC2` inclui as métricas de verificação de status a seguir.

Métrica	Descrição	Unidade	Estatísticas significativas
`StatusCheckFailed`	Informam se a instância foi aprovada nas verificação de status no último minuto. Essa métrica pode ser `0` (aprovada) ou 1 (reprovada). Por padrão, esta métrica está disponível a uma frequência de um minuto gratuitamente.	Count	• Average • Minimum • Maximum
`StatusCheckFailed_Instance`	Informa se a instância foi aprovada na verificação de status de instância no último minuto. Essa métrica pode ser `0` (aprovada) ou 1 (reprovada). Por padrão, esta métrica está disponível a uma frequência de um minuto gratuitamente.	Count	• Average • Minimum • Maximum
`StatusCheckFailed_System`	Informa se a instância foi aprovada na verificação de status de sistema do &; no último minuto. Essa métrica pode ser `0` (aprovada) ou 1 (reprovada). Por padrão, esta métrica está disponível a uma frequência de um minuto gratuitamente.	Count	• Average • Minimum • Maximum

Métrica	Descrição	Unidade	Estatísticas significativas
`StatusCheckFailed_AttachedEBS`	Informa se a instância foi aprovada na verificação de status do EBS anexado no último minuto. Essa métrica pode ser `0` (aprovada) ou 1 (reprovada). Por padrão, esta métrica está disponível a uma frequência de um minuto gratuitamente.	Count	• Average • Minimum • Maximum

O namespace `AWS/EBS` inclui a métrica de verificação de status apresentada a seguir.

Métrica	Descrição	Unidade	Estatísticas significativas
`VolumeStalledIOCheck`	Observação: somente para instâncias do Nitro. Não publicado para volumes anexados ao Amazon ECS e tarefas do AWS Fargate. Informa se um volume foi aprovado ou reprovado em uma verificação de E/S paralisada no último minuto. Essa métrica pode ser `0` (aprovada) ou 1 (reprovada).	Nenhum	• Average • Minimum • Maximum

Métricas de espelhamento de tráfego

O namespace `AWS/EC2` inclui métricas para tráfego espelhado. Para obter mais informações, consulte Monitorar o tráfego espelhado usando o Amazon CloudWatch no Guia do Amazon VPC Traffic Mirroring.

Métricas do grupo do Auto Scaling

O namespace `AWS/AutoScaling` inclui métricas para grupos do Auto Scaling. Para obter mais informações, consulte Monitorar métricas do CloudWatch para grupos do Auto Scaling e instâncias no Guia do usuário do Amazon EC2 Auto Scaling.

Dimensões de métrica do Amazon EC2

É possível usar as seguintes dimensões para refinar as métricas listadas nas tabelas anteriores.

Dimensão	Descrição
`AutoScalingGroupName`	Essa dimensão filtra os dados solicitados para todas as instâncias em um grupo de capacidade especificado. Um Grupo de Auto Scaling é uma coleção de instâncias que você define se estiver usando o Auto Scaling. Essa dimensão está disponíve l somente para métricas do Amazon EC2 quando as instâncias estão em um grupo de Auto Scaling. Disponível para instâncias com monitoramento básico ou detalhado habilitado.
`ImageId`	Essa dimensão filtra os dados que você solicita para todas as instâncias executando essa Imagem de máquina da Amazon (AMI) do Amazon EC2. Disponível para instâncias com monitoramento detalhado habilitado.
`InstanceId`	Essa dimensão filtra os dados que você solicita somente para a instância identificada. Isso ajuda você a identificar uma instância exata para monitorar os dados.
`InstanceType`	Essa dimensão filtra os dados que você solicita para todas as instâncias executando esse tipo de instância especificado. Isso ajuda você a categorizar seus dados pelo tipo de instância em execução. Por exemplo, é possível comparar dados de uma instância m1.small e uma instância m1.large para determina r qual delas tem o melhor valor comercial para sua aplicação . Disponível para instâncias com monitoramento detalhado habilitado.

Métricas de uso do Amazon EC2

É possível usar métricas de uso do CloudWatch para fornecer visibilidade sobre o uso de recursos de sua conta. Use essas métricas para visualizar o uso do serviço atual nos gráficos e painéis do CloudWatch.

As métricas de uso do Amazon EC2 correspondem às Service Quotas da AWS. Também é possível configurar alarmes que alertem você quando o uso se aproximar de uma cota de serviço. Para obter mais informações sobre a integração do CloudWatch com o Service Quotas, consulte Métricas de uso da AWS no Guia do usuário do Amazon CloudWatch.

O Amazon EC2 publica as seguintes métricas no namespace `AWS/Usage`.

Métrica	Descrição
`ResourceCount`	O número dos recursos especificados em execução em sua conta. Os recursos são definidos pelas dimensões associadas à métrica. A estatística mais útil para essa métrica é `MAXIMUM`, que representa o número máximo de recursos usados durante o período de um minuto.

As dimensões a seguir são usadas para refinar as métricas de uso publicadas pelo Amazon EC2.

Dimensão	Descrição
`Service`	O nome do serviço da AWS que contém o recurso. Para as métricas de uso do Amazon EC2, o valor dessa dimensão é `EC2`.
`Type`	O tipo de entidade que está sendo relatado. Atualmente, o único valor válido para métricas de uso do Amazon EC2 é `Resource`.
`Resource`	O tipo de recurso que está em execução. Atualmente, o único valor válido para métricas de uso do Amazon EC2 é `vCPU`, que retorna informações sobre as instâncias em execução.
`Class`	A classe do recurso que está sendo acompanhado. Para as métricas de uso do Amazon EC2 com `vCPU` como o valor da dimensão `Resource`, os valores válidos são `Standard/OnDemand` , `F/OnDemand` , `G/OnDemand` , `Inf/OnDemand` , `P/OnDemand` e `X/OnDemand` .

Dimensão	Descrição
	Os valores dessa dimensão definem a primeira letra dos tipos de instância relatados pela métrica. Por exemplo, `Standard/OnDemand` retorna informações sobre todas as instâncias em execução com tipos que começam com A, C, D, H, I, M, R, T e Z, e `G/OnDemand` retorna informações sobre todas as instâncias em execução com tipos que começam com G.

Instale e configure o agente do CloudWatch usando o console do Amazon EC2 para adicionar métricas adicionais

A instalação e configuração do agente do CloudWatch usando o console do Amazon EC2 está em versão beta para o Amazon EC2 e está sujeita a alterações.

Por padrão, o Amazon CloudWatch fornece métricas básicas, como `CPUUtilization` e `NetworkIn`, para monitorar suas instâncias do Amazon EC2. Para coletar métricas adicionais, você pode instalar o agente do CloudWatch nas suas instâncias do EC2 e, em seguida, configurar o agente para emitir métricas selecionadas. Em vez de instalar e configurar manualmente o agente do CloudWatch em cada instância do EC2, você pode usar o console do Amazon EC2 para fazer isso por você.

É possível usar o console do Amazon EC2 para instalar o agente do CloudWatch nas instâncias e configurar esse agente para emitir métricas selecionadas.

Como alternativa, para concluir esse processo manualmente, consulte Instalação do atendente do CloudWatch no Guia do usuário do Amazon CloudWatch. Para obter mais informações sobre o agente do CloudWatch, consulte Coleta de métricas, logs e rastreamentos usando o agente do CloudWatch.

Conteúdos

- Pré-requisitos
- Como funciona
- Custos
- Baixar e configurar o atendente do CloudWatch

Pré-requisitos

Para usar o Amazon EC2 para instalar e configurar o agente do CloudWatch, é necessário atender aos pré-requisitos de usuário e instância descritos nesta seção.

> **Tip**
>
> Este recurso ainda não está disponível em todos os Regiões da AWS. Se o item de menu descrito no procedimento de instalação desta página não existir no console do Amazon EC2 e você tiver flexibilidade em relação a onde suas instâncias são executadas, tente outra região. Do contrário, você pode usar as instruções manuais do Guia do usuário do Amazon CloudWatch para instalar e configurar o agente.

Pré-requisitos da conta

Para usar esse recurso, o usuário ou perfil do console do IAM deve ter as permissões necessárias para usar o Amazon EC2 e as seguintes permissões do IAM:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ssm:GetParameter",
                "ssm:PutParameter"
            ],
            "Resource": "arn:aws:ssm:*:*:parameter/EC2-Custom-Metrics-*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ssm:SendCommand",
                "ssm:ListCommandInvocations",
                "ssm:DescribeInstanceInformation"
            ],
            "Resource": [
```

```
                "*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:GetInstanceProfile",
                "iam:SimulatePrincipalPolicy"
            ],
            "Resource": "*"
        }
    ]
}
```

Pré-requisitos da instância

- Estado da instância: `running`
- Sistema operacional com suporte: Linux
- AWS Systems Manager Agent (SSM Agent): Instalado. Duas notas sobre o SSM Agent:
  - O SSM Agent está pré-instalado em algumas imagens de máquina da Amazon (AMIs) fornecidas por terceiros confiáveis AWS. Para obter informações sobre as AMIs com suporte e as instruções para instalar o SSM Agent, consulte Imagens de máquina da Amazon (AMIs) com o SSM Agent pré-instalado, no Guia do usuário do AWS Systems Manager.
  - Se tiver problemas com o SSM Agent, consulte Solução de problemas com o SSM Agent, no Guia do usuário do AWS Systems Manager.
- Permissões do IAM para a instância: as seguintes políticas AWS gerenciadas devem ser adicionadas ao perfil do IAM anexado à instância:
  - AmazonSSMManagedInstanceCore: permite que uma instância use o Systems Manager para instalar e configurar o agente do CloudWatch.
  - CloudWatchAgentServerPolicy: permite que uma instância use o agente do CloudWatch para gravar dados no CloudWatch.

  Para obter informações sobre como adicionar permissões do IAM à sua instância, consulte Usar perfis de instância no Guia do usuário do IAM.

Como funciona

Antes de usar o console do Amazon EC2 para instalar e configurar o agente do CloudWatch, você deve se certificar de que seu usuário ou perfil do IAM e as instâncias nas quais você deseja adicionar métricas atendam a determinados pré-requisitos. Em seguida, você pode usar o console do Amazon EC2 para instalar e configurar o agente do CloudWatch nas instâncias selecionadas.

Primeiro, atenda aos pré-requisitos

- Você precisa das permissões do IAM necessárias: antes de começar, certifique-se de que seu usuário ou perfil do console tenha as permissões do IAM necessárias para usar esse recurso.
- Instâncias: para usar o recurso, suas instâncias do EC2 devem ser instâncias Linux, ter o SSM Agent instalado, ter as permissões do IAM necessárias e estar em execução.

Em seguida, será possível usar o recurso

1. Selecione suas instâncias: no console do Amazon EC2, você seleciona as instâncias nas quais instalar e configurar o agente do CloudWatch. Em seguida, inicia o processo escolhendo Configurar agente do CloudWatch.
2. Validar o SSM Agent: o Amazon EC2 verifica se o SSM Agent está instalado e iniciado em cada instância. Todas as instâncias que falharem nessa verificação serão excluídas do processo. O SSM Agent é usado para realizar ações na instância durante esse processo.
3. Valide as permissões do IAM: o Amazon EC2 verifica se cada instância tem as permissões do IAM necessárias para esse processo. Todas as instâncias que falharem nessa verificação serão excluídas do processo. As permissões do IAM permitem que o agente do CloudWatch colete métricas da instância e se integre ao AWS Systems Manager para usar o SSM Agent.
4. Validar o agente do CloudWatch: o Amazon EC2 verifica se o agente do CloudWatch está instalado e em execução em cada instância. Se alguma instância falhar nessa verificação, o Amazon EC2 oferecerá a instalação e a inicialização do agente do CloudWatch para você. O agente do CloudWatch coletará as métricas selecionadas em cada instância quando esse processo for concluído.
5. Selecionar a configuração de métricas: você seleciona as métricas que o agente do CloudWatch emitirá de suas instâncias. Depois de selecionado, o Amazon EC2 armazena um arquivo de configuração no Parameter Store, onde permanece até que o processo seja concluído. O Amazon EC2 excluirá o arquivo de configuração do Parameter Store, a menos que o processo seja interrompido. Observe que, se você não selecionar uma métrica, mas a tiver adicionado

anteriormente à sua instância, ela será removida da sua instância quando esse processo for concluído.

6. Atualizar a configuração do agente do CloudWatch: o Amazon EC2 envia a configuração da métrica para o agente do CloudWatch. Essa é a última etapa do processo. Se for bem-sucedida, suas instâncias poderão emitir dados para as métricas selecionadas, e o Amazon EC2 excluirá o arquivo de configuração do Parameter Store.

Custos

As métricas adicionais acrescentadas durante esse processo são cobradas como métricas personalizadas. Para obter mais informações sobre o preço de métricas do CloudWatch, consulte Preço do Amazon CloudWatch.

Baixar e configurar o atendente do CloudWatch

É possível usar o console do Amazon EC2 para instalar e configurar o agente do CloudWatch para adicionar métricas adicionais.

> **Note**
>
> Todas as vezes que você executa esse procedimento, você substitui a configuração existente do agente do CloudWatch. Se você não selecionar uma métrica que tenha sido selecionada anteriormente, ela será removida da instância.

Para instalar e configurar o agente do CloudWatch 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 as instâncias nas quais instalar e configurar o agente do CloudWatch.
4. Escolha Ações, Monitorar e solucionar problemas, Configurar agente do CloudWatch.
5. Para cada etapa do processo, leia o texto do console e escolha Avançar.
6. Para concluir o processo, na etapa final, escolha Concluir.

Para atualizar a configuração do agente criada pelo console do Amazon EC2

É possível personalizar manualmente a configuração criada pelo console do EC2. Para obter mais informações, consulte Criar ou editar manualmente o arquivo de configuração do atendente do CloudWatch no Guia do usuário do Amazon CloudWatch.

Estatísticas para as métricas do CloudWatch para as instâncias

É possível obter estatísticas para as métricas do CloudWatch para suas instâncias. 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. É possível usar esse valor para determinar baixos volumes de atividade para a sua aplicação
`Maximum`	O valor mais alto observado durante o período especificado. É possível usar esse valor para determinar altos volumes de atividade para a sua aplicação.
`Sum`	Todos os valores enviados para a métrica correspondente, somados. Essa estatística pode ser útil para determinar o volume total de uma métrica.
`Average`	O valor de `Sum` / `SampleCount` durante o período especificado. Ao comparar essa estatística com o `Minimum` e o `Maximum`, é possível 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. É possível especificar qualquer percentil usando até duas casas decimais (por exemplo, p95.45).

Conteúdo

- Obter estatísticas para uma instância específica

- Agregar estatísticas entre instâncias
- Agregar estatísticas por grupo de Auto Scaling
- Agregar estatísticas por AMI

Obter estatísticas para uma instância específica

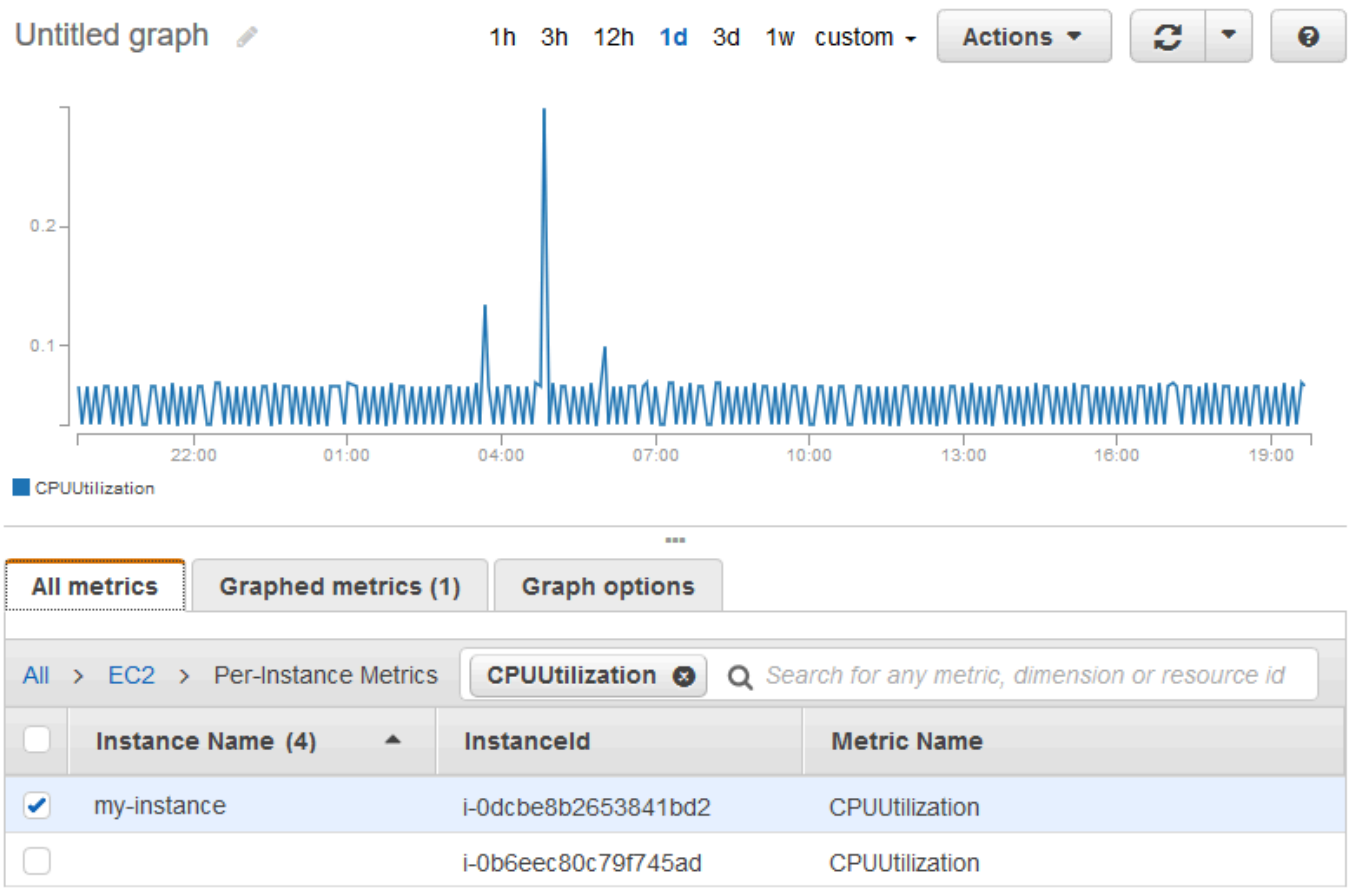
É possível usar o Console de gerenciamento da AWS ou a AWS CLI para obter estatísticas para uma instância específica. Os exemplos a seguir mostram como usar o Console de gerenciamento da AWS ou a AWS CLI para determinar a utilização horária de CPU de uma instância do EC2 específica.

Requisitos

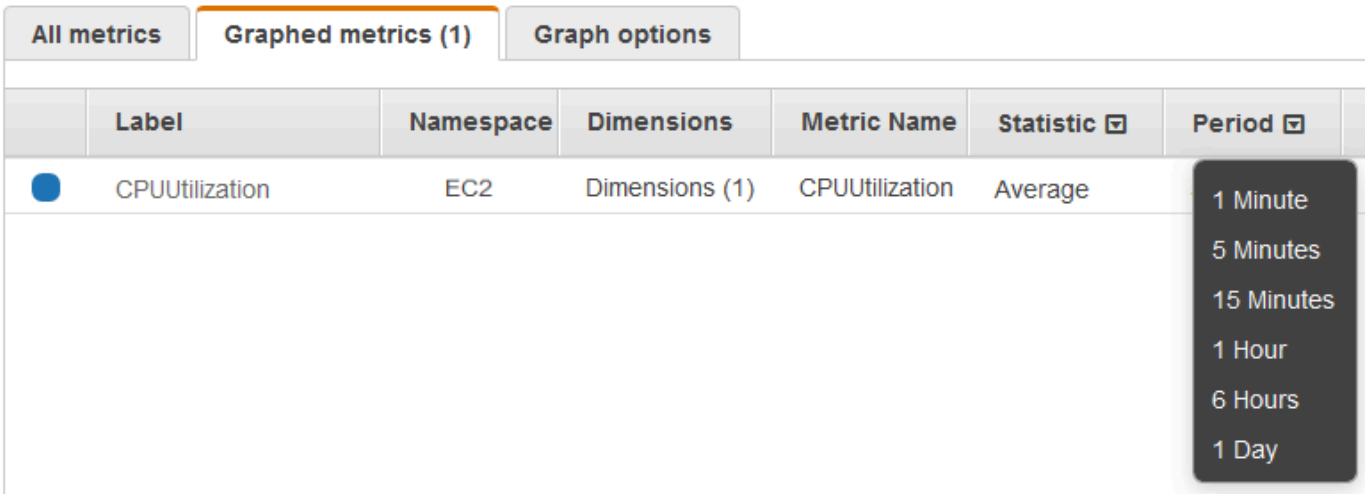
- É necessário ter o ID da instância. É possível obter o ID da instância usando o Console de gerenciamento da AWS ou o comando describe-instances.
- Por padrão, o monitoramento básico é ativado, mas é possível habilitar o monitoramento detalhado. Para obter mais informações, consulte Gerenciar o monitoramento detalhado das instâncias do Amazon EC2.

Para exibir a utilização de CPU para uma instância específica (console)

1. Abra o console do CloudWatch em https://console.aws.amazon.com/cloudwatch/.
2. No painel de navegação, selecione Metrics (Métricas).
3. Escolha o namespace de métricas do EC2.
4. Escolha a dimensão Per-Instance Metrics (Métricas por instância).
5. No campo de pesquisa, digite **`CPUUtilization`** e pressione Enter. Escolha a linha da instância específica, que exibe um gráfico da métrica CPUUtilization para a instância. Para dar nome a um gráfico, selecione o ícone do lápis. Para alterar o período, selecione um dos valores predefinidos ou escolha custom (personalizado).



6. Para alterar a estatística ou o período da métrica, selecione a guia Graphed metrics (Métricas em gráfico). Escolha o cabeçalho de coluna ou um valor individual e, em seguida, escolha um valor diferente.



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 2022-10-18T23:18:00 --end-time 2022-10-19T23:18:00
```

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": "2022-10-19T00:18:00Z",
            "Maximum": 0.33000000000000002,
            "Unit": "Percent"
        },
        {
            "Timestamp": "2022-10-19T03:18:00Z",
            "Maximum": 99.670000000000002,
            "Unit": "Percent"
        },
        {
            "Timestamp": "2022-10-19T07:18:00Z",
            "Maximum": 0.34000000000000002,
            "Unit": "Percent"
        },
        {
            "Timestamp": "2022-10-19T12:18:00Z",
            "Maximum": 0.34000000000000002,
            "Unit": "Percent"
        }
    ],
    "Label": "CPUUtilization"
}
```

Agregar estatísticas entre instâncias

Estatísticas agregadas estão disponíveis para as instâncias que têm o monitoramento detalhado habilitado. As instâncias que usam o monitoramento básico não estão incluídas nos agregados.

Antes que seja possível obter estatísticas agregadas em todas as instâncias, é necessário habilitar o monitoramento detalhado (a uma cobrança adicional), que fornece dados em períodos de um minuto.

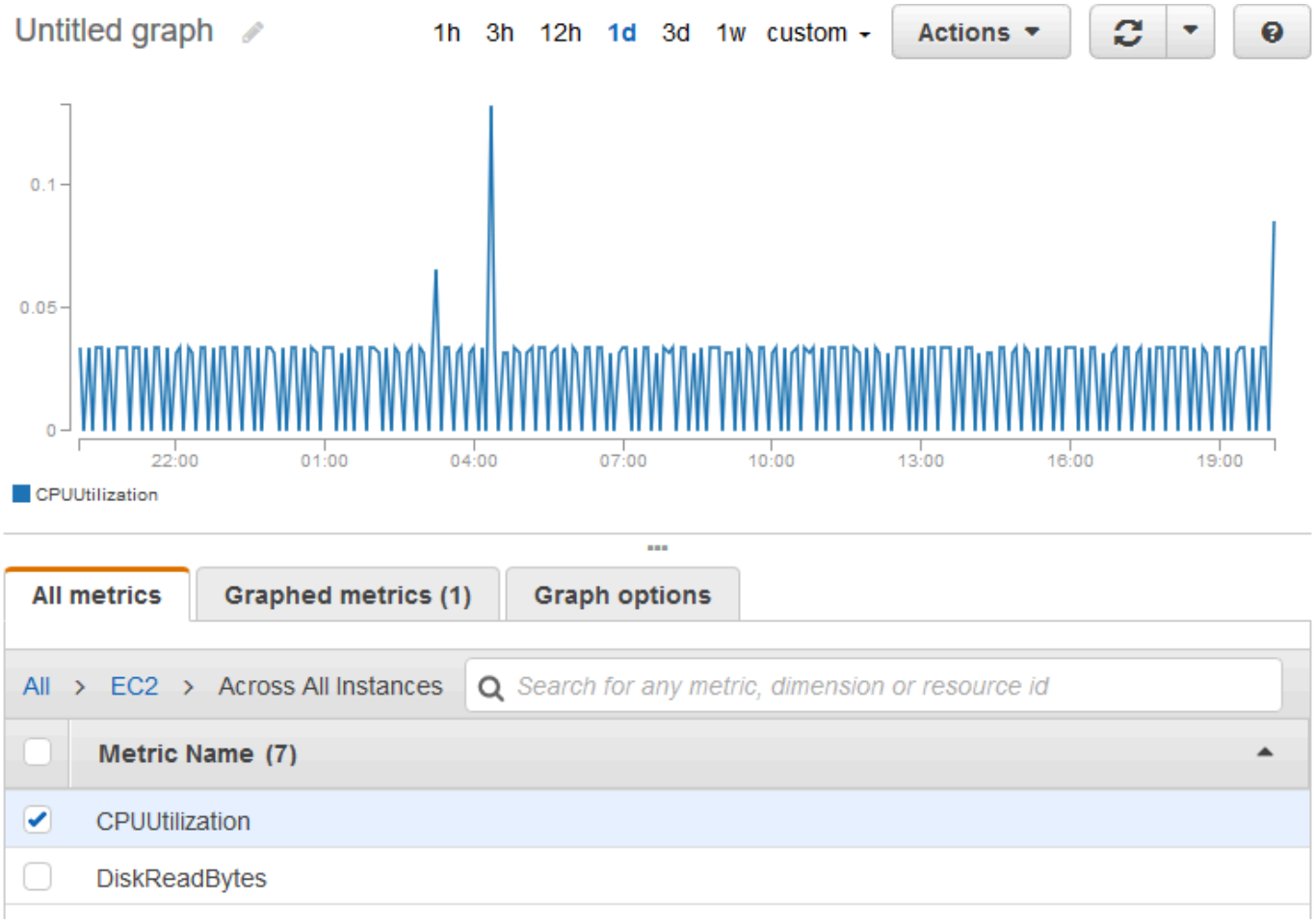
O Amazon CloudWatch não pode agregar dados entre regiões da AWS. As métricas são completamente separadas entre regiões.

Este exemplo mostra a você como usar o monitoramento detalhado para obter uso médio de CPU para suas instâncias do EC2. Como nenhuma dimensão é especificada, o CloudWatch retorna estatísticas para todas as dimensões no namespace `AWS/EC2`.

> **Important**
>
> Essa técnica para recuperar todas as dimensões em um namespace da AWS não funciona para namespaces personalizados que você publicar no Amazon CloudWatch. Com namespaces personalizados, especifique o conjunto completo de dimensões associadas a um determinado ponto de dados para recuperar estatísticas que incluam o ponto de dados.

Para exibir a utilização média de CPU em suas instâncias (console)

1. Abra o console do CloudWatch em https://console.aws.amazon.com/cloudwatch/.
2. No painel de navegação, selecione Metrics (Métricas).
3. Escolha o namespace EC2 e escolha Across All Instances (Em todas as instâncias).
4. Escolha a linha que contém CPUUtilization, que exibe um gráfico da métrica para todas as instâncias do EC2. Para dar nome a um gráfico, selecione o ícone do lápis. Para alterar o período, selecione um dos valores predefinidos ou escolha custom (personalizado).



5. Para alterar a estatística ou o período da métrica, selecione a guia Graphed metrics (Métricas em gráfico). Escolha o cabeçalho de coluna ou um valor individual e, em seguida, escolha um valor diferente.

Para obter a utilização média de CPU em suas instâncias (AWS CLI)

Use o comando get-metric-statistics da seguinte forma para obter a média da métrica CPUUtilization em todas as suas instâncias.

```
aws cloudwatch get-metric-statistics \
    --namespace AWS/EC2 \
    --metric-name CPUUtilization \
    --period 3600  --statistics "Average" "SampleCount" \
    --start-time 2022-10-11T23:18:00 \
    --end-time 2022-10-12T23:18:00
```

A seguir está um exemplo de saída:

```
{
    "Datapoints": [
        {
            "SampleCount": 238.0,
            "Timestamp": "2022-10-12T07:18:00Z",
            "Average": 0.038235294117647062,
            "Unit": "Percent"
        },
        {
            "SampleCount": 240.0,
            "Timestamp": "2022-10-12T09:18:00Z",
            "Average": 0.16670833333333332,
            "Unit": "Percent"
        },
        {
            "SampleCount": 238.0,
            "Timestamp": "2022-10-11T23:18:00Z",
            "Average": 0.041596638655462197,
            "Unit": "Percent"
        }
    ],
    "Label": "CPUUtilization"
}
```


Agregar estatísticas por grupo de Auto Scaling

É possível agregar estatísticas para as instâncias do EC2 em um grupo do Auto Scaling. O Amazon CloudWatch não pode agregar dados entre regiões da AWS. As métricas são completamente separadas entre regiões.

Este exemplo mostra como recuperar o total de bytes gravados em disco para um grupo do Auto Scaling. O total é calculado para períodos de 1 minuto para um intervalo de 24 horas em todas as instâncias do EC2 no grupo do Auto Scaling especificado.

Para exibir DiskWriteBytes para as instâncias em um grupo do Auto Scaling (console)

1. Abra o console do CloudWatch em https://console.aws.amazon.com/cloudwatch/.
2. No painel de navegação, selecione Metrics (Métricas).
3. Escolha o namespace EC2 e escolha By Auto Scaling Group (Por grupo de Auto Scaling).
4. Escolha a linha da métrica DiskWriteBytes e o grupo do Auto Scaling específico, que exibe um gráfico da métrica para as instâncias no grupo do Auto Scaling. Para dar nome a um gráfico,

selecione o ícone do lápis. Para alterar o período, selecione um dos valores predefinidos ou escolha custom (personalizado).

5. Para alterar a estatística ou o período da métrica, selecione a guia Graphed metrics (Métricas em gráfico). Escolha o cabeçalho de coluna ou um valor individual e, em seguida, escolha um valor diferente.

Para exibir DiskWriteBytes para as instâncias em um grupo do Auto Scaling (AWS CLI)

Use o comando get-metric-statistics da seguinte forma.

```
aws cloudwatch get-metric-statistics --namespace AWS/EC2 --metric-name DiskWriteBytes
 --period 360 \
--statistics "Sum" "SampleCount" --dimensions Name=AutoScalingGroupName,Value=my-asg --
start-time 2022-10-16T23:18:00 --end-time 2022-10-18T23:18:00
```

A seguir está um exemplo de saída:

```
{
    "Datapoints": [
        {
            "SampleCount": 18.0,
            "Timestamp": "2022-10-19T21:36:00Z",
            "Sum": 0.0,
            "Unit": "Bytes"
        },
        {
            "SampleCount": 5.0,
            "Timestamp": "2022-10-19T21:42:00Z",
            "Sum": 0.0,
            "Unit": "Bytes"
        }
    ],
    "Label": "DiskWriteBytes"
}
```

Agregar estatísticas por AMI

É possível agregar estatísticas pela AMI para as instâncias com monitoramento detalhado habilitado. As instâncias que usam o monitoramento básico não estão incluídas nos agregados. Antes que seja

possível obter estatísticas agregadas em todas as instâncias, é necessário habilitar o monitoramento detalhado (a uma cobrança adicional), que fornece dados em períodos de um minuto.

O Amazon CloudWatch não pode agregar dados entre regiões da AWS. As métricas são completamente separadas entre regiões.

Este exemplo mostra como determinar a utilização média da CPU para todas as instâncias que usam uma imagem de máquina da Amazon (AMI) específica. A média é intervalos de mais de 60 segundos para um período de um dia.

Para exibir a utilização média de CPU por AMI (console)

1. Abra o console do CloudWatch em https://console.aws.amazon.com/cloudwatch/.
2. No painel de navegação, selecione Metrics (Métricas).
3. Escolha o namespace EC2 e escolha By Image (AMI) Id (Por ID de imagem (AMI)).
4. Escolha a linha da métrica CPUUtilization e a AMI específica, que exibe um gráfico da métrica para a AMI especificada. Para dar nome a um gráfico, selecione o ícone do lápis. Para alterar o período, selecione um dos valores predefinidos ou escolha custom (personalizado).
5. Para alterar a estatística ou o período da métrica, selecione a guia Graphed metrics (Métricas em gráfico). Escolha o cabeçalho de coluna ou um valor individual e, em seguida, escolha um valor diferente.

Para obter utilização média de CPU para um ID de imagem (AWS CLI)

Use o comando get-metric-statistics da seguinte forma.

```
aws cloudwatch get-metric-statistics --namespace AWS/EC2 --metric-name CPUUtilization
 --period 3600 \
--statistics Average --dimensions Name=ImageId,Value=ami-3c47a355 --start-
time 2022-10-10T00:00:00 --end-time 2022-10-11T00:00:00
```

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": "2022-10-10T07:00:00Z",
```

```
            "Average": 0.041000000000000009,
            "Unit": "Percent"
        },
        {
            "Timestamp": "2022-10-10T14:00:00Z",
            "Average": 0.079579831932773085,
            "Unit": "Percent"
        },
        {
            "Timestamp": "2022-10-10T06:00:00Z",
            "Average": 0.036000000000000011,
            "Unit": "Percent"
        }
    ],
    "Label": "CPUUtilization"
}
```

Exibir os grafos de monitoramento para as instâncias

Depois que executar uma instância, é possível abrir o console do Amazon EC2 e ver os gráficos de monitoramento para a instância na guia Monitoring (Monitoramento). Cada gráfico se baseia em uma das métricas disponíveis do Amazon EC2.

Os gráficos a seguir estão disponíveis:

- Utilização média da CPU (porcentagem)
- Leituras médias do disco (bytes)
- Gravações médias em disco (bytes)
- Rede máxima dentro (bytes)
- Rede máxima fora (bytes)
- Operações de leitura de disco de resumo (contagem)
- Operações de gravação de disco de resumo (contagem)
- Status de resumo (qualquer)
- Instância do status de resumo (contagem)
- Sistema de status de resumo (contagem)

Para mais informações sobre as métricas e os dados que elas fornecem aos gráficos, consulte As métricas do CloudWatch que estão disponíveis para as instâncias.

Represente graficamente métricas usando o console CloudWatch

Também é possível usar o console do CloudWatch para representar graficamente os dados gerados pelo Amazon EC2 e outros serviços da AWS. Para obter mais informações, consulte Representação gráfica de métricas no Guia do usuário do Amazon CloudWatch.

Criar um alarme do CloudWatch para uma instância

É possível criar um alarme do CloudWatch que monitore métricas do CloudWatch de uma de suas instâncias. O CloudWatch enviará automaticamente para você uma notificação quando a métrica atingir um limite especificado. É possível 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 e escolha Actions (Ações), Monitor and troubleshoot (Monitorar e solucionar problemas), Manage CloudWatch alarms (Gerenciar alarmes do CloudWatch).
4. Na página de detalhes Manage CloudWatch alarms (Gerenciar alarmes do CloudWatch), em Add or edit alarm (Adicionar ou editar alarme), selecione Create an alarm (Criar alarme).
5. Em Notificação de alarme, escolha se deseja configurar as notificações do Amazon Simple Notification Service (Amazon SNS). Insira um tópico de Amazon SNS existente ou insira um nome para criar um tópico.
6. Em Ação do alarme, selecione se deseja especificar uma ação a ser feita quando o alarme for acionado. Escolha uma ação na lista.
7. Em Alarm thresholds (Limites de alarme), selecione a métrica e os critérios do alarme. Por exemplo, para criar um alarme que é acionado quando a utilização da CPU atinge 80% por um período de 5 minutos, faça o seguinte:

    a. Mantenha as configurações padrão para Agrupar amostras por (Média) e Tipo de dados a amostrar (Utilização da CPU).

    b. Escolha >= para Alarme quando e insira **`0.80`** em Por cento.

c. Insira **1** em Período consecutivo e selecione 5 minutos em Período.

8. (Opcional) Em Sample metric data (Dados de métrica de exemplo), escolha Add to dashboard (Adicionar ao painel).
9. Escolha Criar.

É possível editar suas configurações de alarme do CloudWatch no console do Amazon EC2 ou no console do CloudWatch. Se você quiser excluir seu alarme, poderá fazê-lo a partir no console do CloudWatch. Para obter mais informações, consulte Editar ou excluir um alarme do CloudWatch no Guia do usuário do Amazon CloudWatch.

Criar alarmes para interromper, encerrar, reinicializar ou recuperar uma instância

Usando as ações de alarme do Amazon CloudWatch, você cria alarmes que automaticamente param, encerram, reinicializam ou recuperam suas instâncias. É possível usar as ações de parada ou encerramento para ajudar a economizar dinheiro quando não precisar mais que uma instância seja executada. É possível usar as ações de reinicialização e recuperação para reinicializar automaticamente essas instâncias ou recuperá-las para um novo hardware caso ocorra um problema no sistema.

> **Note**
>
> Para saber mais sobre alarmes de faturamento e custos do Amazon CloudWatch, consulte Faturamento e custos do CloudWatch no Guia do usuário do Amazon CloudWatch.

A função `AWSServiceRoleForCloudWatchEvents` ligado ao serviço permite que a AWS execute ações de alarme em seu nome. A primeira vez que você criar um alarme no Console de gerenciamento da AWS, na AWS CLI ou na API do IAM, o CloudWatch cria o perfil vinculado ao serviço para você.

Há várias situações nas quais é possível querer interromper ou encerrar sua instância automaticamente. Por exemplo, é possível 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), é possível interrompê-las ou encerrá-las, o que pode ajudá-lo a fazer uma economia. A principal diferença entre usar as ações de alarme de interrupção e encerramento é que

é possível facilmente iniciar uma instância interrompida se precisar executá-la novamente mais tarde e manter o mesmo ID de instância e volume do dispositivo raiz. No entanto, não é possível iniciar uma instância encerrada. Em vez disso, é necessário executar uma nova instância. Quando uma instância é interrompida ou encerrada, os dados nos volumes de armazenamento da instância são perdidos.

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.

> **Important**
>
> Os alarmes de verificação de status podem entrar temporariamente no estado `INSUFFICIENT_DATA` se faltarem pontos de dados de métricas. Embora raro, isso pode acontecer quando há uma interrupção nos sistemas de relatórios de métricas, mesmo quando uma instância está íntegra. Recomendamos que você trate o estado `INSUFFICIENT_DATA` como dados ausentes em vez de uma violação de alarme, especialmente ao configurar o alarme para parar, encerrar, reinicializar ou recuperar uma instância.

Suporte a consoles

É possível 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

Você deve ter a permissão `iam:CreateServiceLinkedRole` para criar ou modificar um alarme que executa as ações de alarme do EC2. O perfil de serviço é um perfil do IAM que um serviço assume para executar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para saber mais, consulte Criar um perfil para delegar permissões a um AWS service (Serviço da AWS) no Guia do Usuário do IAM.

Conteúdo

- Adicionar ações de interrupção a alarmes do Amazon CloudWatch
- Adicionar ações de encerramento a alarmes do Amazon CloudWatch
- Adicionar ações de reinicialização a alarmes do Amazon CloudWatch
- Adicionar ações de recuperação a alarmes do Amazon CloudWatch
- Cenários de ação do alarme do Amazon CloudWatch

Adicionar ações de interrupção a alarmes do Amazon CloudWatch

É possível criar um alarme que pare uma instância do Amazon EC2 quando o limite for atingido. Por exemplo, é possível executar instâncias de desenvolvimento ou teste e ocasionalmente se esquecer de desativá-las. É possível 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. É possível 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 volume raiz podem ser interrompidas ou encerradas, enquanto instâncias que usam o armazenamento de instância como volume raiz só podem ser encerradas. Os dados nos volumes de armazenamento de instância são perdidos quando a instância é interrompida ou encerrada.

Para criar um alarme para parar uma instância em repouso (console do Amazon EC2)

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância e escolha Actions (Ações), Monitor and troubleshoot (Monitorar e solucionar problemas), Manage CloudWatch alarms (Gerenciar alarmes do CloudWatch).

   Como alternativa, é possível escolher o sinal de mais (

) na coluna Alarm status (Status do alarme) .
4. Na página Manage CloudWatch alarms (Gerenciar alarmes do CloudWatch), faça o seguinte:

   a. Escolha Create an alarm (Criar um alarme).

   b. Para receber um e-mail quando o alarme for acionado, para Alarm notification (Notificação de alarme), escolha um Amazon SNS tópico existente. Para fazer isso, você precisa

criar um tópico do Amazon SNS usando o console do Amazon SNS. Para obter mais informações, consulte Usar o Amazon SNS para mensagens de aplicação para pessoa (A2P) no Guia do desenvolvedor do Amazon Simple Notification Service.

c. Alterne em Ação alarme e escolha Parar.

d. Para Group samples by (Agrupar amostras por) e Type of data to sample (Tipo de dados a serem amostrados), escolha uma estatística e uma métrica. Neste exemplo, escolha Average (Média) e CPU utilization (Utilização da CPU).

e. Para Alarm When (Alarme quando) e Percent (Percentual), especifique o limite da métrica. Neste exemplo, especifique <= e 10%.

f. Para Consecutive period (Período consecutivo) e Period (Período), especifique o período de avaliação do alarme. Neste exemplo, especifique 1 período consecutivo de 5 minutos.

g. Amazon CloudWatch cria automaticamente um nome de alarme para você. Para alterar o nome, em Alarm name (Nome do alarme), insira um novo nome. Os nomes de alarme devem conter somente caracteres ASCII.

> **Note**
>
> É possível ajustar a configuração do alarme com base em suas próprias necessidades antes de criá-lo, ou pode editá-las mais tarde. Aí incluem-se as configurações de métrica, limiar, duração, ação e notificação. No entanto, depois de criar um alarme, você não pode mais editar seu nome.

h. Escolha Criar.

Adicionar ações de encerramento a alarmes do Amazon CloudWatch

É possível 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, é possível 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. Os dados nos volumes de armazenamento de instância são perdidos quando a instância é encerrada. Para obter informações sobre a habilitação e a desabilitação da proteção contra encerramento de uma instância, consulte Alterar proteção contra encerramento de instância.

Para criar um alarme para encerrar uma instância em repouso (console do Amazon EC2)

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

2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância e escolha Actions (Ações), Monitor and troubleshoot (Monitorar e solucionar problemas), Manage CloudWatch alarms (Gerenciar alarmes do CloudWatch).

   Como alternativa, é possível escolher o sinal de mais (

) na coluna Alarm status (Status do alarme) .
4. Na página Manage CloudWatch alarms (Gerenciar alarmes do CloudWatch), faça o seguinte:

   a. Escolha Create an alarm (Criar um alarme).

   b. Para receber um e-mail quando o alarme for acionado, para Alarm notification (Notificação de alarme), escolha um Amazon SNS tópico existente. Para fazer isso, você precisa criar um tópico do Amazon SNS usando o console do Amazon SNS. Para obter mais informações, consulte Usar o Amazon SNS para mensagens de aplicação para pessoa (A2P) no Guia do desenvolvedor do Amazon Simple Notification Service.

   c. Alterne em Ação alarme e escolha Encerrar.

   d. Para Group samples by (Agrupar amostras por) e Type of data to sample (Tipo de dados a serem amostrados), escolha uma estatística e uma métrica. Neste exemplo, escolha Average (Média) e CPU utilization (Utilização da CPU).

   e. Para Alarm When (Alarme quando) e Percent (Percentual), especifique o limite da métrica. Neste exemplo, especifique => e 10 por cento.

   f. Para Consecutive period (Período consecutivo) e Period (Período), especifique o período de avaliação do alarme. Neste exemplo, especifique 24 períodos consecutivos de 1 hora.

   g. Amazon CloudWatch cria automaticamente um nome de alarme para você. Para alterar o nome, em Alarm name (Nome do alarme), insira um novo nome. Os nomes de alarme devem conter somente caracteres ASCII.

      > **Note**
      >
      > É possível ajustar a configuração do alarme com base em suas próprias necessidades antes de criá-lo, ou pode editá-las mais tarde. Aí incluem-se as configurações de métrica, limiar, duração, ação e notificação. No entanto, depois de criar um alarme, você não pode mais editar seu nome.

   h. Escolha Criar.

Adicionar ações de reinicialização a alarmes do Amazon CloudWatch

É possível criar um alarme do Amazon CloudWatch que monitore uma instância do Amazon EC2 e reinicialize 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). Reinicializar a instância equivale a reinicializar o sistema operacional. Na maioria dos casos, leva apenas alguns minutos para reinicializar sua instância. Quando você reinicializa uma instância, ela permanece no mesmo host físico, para que sua instância mantenha seu nome DNS público, o endereço IP privado e os dados em seus volumes de armazenamento de instância.

A reinicialização de uma instância não inicia uma nova hora de faturamento de instância (com uma cobrança mínima de um minuto), diferente do que acontece na interrupção e na reinicialização da instância. Os dados nos volumes de armazenamento de instância são retidos quando a instância é reinicializada. Os volumes de armazenamento de instâncias devem ser remontados no sistema de arquivos após uma reinicialização. Para obter mais informações, consulte Reinicializar uma instância do Amazon EC2.

> **Important**
>
> Para evitar um comportamento de disputa entre as ações de reinicialização e recuperação, evite configurar o mesmo número de períodos de avaliação para um alarme de reinicialização e um alarme de recuperação. Recomendamos que você defina alarmes de reinicialização para três períodos de avaliação de um minuto cada. Para obter mais informações, consulte Avaliar um alarme no Guia do usuário do Amazon CloudWatch.

Para criar um alarme para reinicializar uma instância (console do Amazon EC2)

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância e escolha Actions (Ações), Monitor and troubleshoot (Monitorar e solucionar problemas), Manage CloudWatch alarms (Gerenciar alarmes do CloudWatch).

   Como alternativa, é possível escolher o sinal de mais (

) na coluna Alarm status (Status do alarme) .

4. Na página Manage CloudWatch alarms (Gerenciar alarmes do CloudWatch), faça o seguinte:

   a. Escolha Create an alarm (Criar um alarme).

   b. Para receber um e-mail quando o alarme for acionado, para Alarm notification (Notificação de alarme), escolha um Amazon SNS tópico existente. Para fazer isso, você precisa criar um tópico do Amazon SNS usando o console do Amazon SNS. Para obter mais informações, consulte Usar o Amazon SNS para mensagens de aplicação para pessoa (A2P) no Guia do desenvolvedor do Amazon Simple Notification Service.

   c. Alterne em Ação alarme e escolha Reinicializar.

   d. Para Group samples by (Agrupar amostras por) e Type of data to sample (Tipo de dados a serem amostrados), escolha uma estatística e uma métrica. Neste exemplo, escolha Average (Média) e Status check failed: instance (Falha na verificação de status: instância).

   e. Para Consecutive period (Período consecutivo) e Period (Período), especifique o período de avaliação do alarme. Nesse exemplo, digite 3 períodos consecutivos de 1 minuto. Se 1 minuto estiver desabilitado, você deverá habilitar o monitoramento detalhado ou escolher 5 minutos.

   f. Amazon CloudWatch cria automaticamente um nome de alarme para você. Para alterar o nome, em Alarm name (Nome do alarme), insira um novo nome. Os nomes de alarme devem conter somente caracteres ASCII.

   g. Escolha Criar.

Adicionar ações de recuperação a alarmes do Amazon CloudWatch

É possível criar um alarme do Amazon CloudWatch que monitore uma instância do Amazon EC2. Se a instância for invalidada devido a uma falha de hardware subjacente ou a um problema que exija o envolvimento da AWS para corrigi-lo, será possível 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.

> **Note**
>
> 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 características a seguir. Para obter mais informações, consulte Recuperação automática de instâncias.

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 Avaliar um alarme no 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 e escolha Actions (Ações), Monitor and troubleshoot (Monitorar e solucionar problemas), Manage CloudWatch alarms (Gerenciar alarmes do CloudWatch).

   Como alternativa, é possível escolher o sinal de mais (

) na coluna Alarm status (Status do alarme) .
4. Na página Manage CloudWatch alarms (Gerenciar alarmes do CloudWatch), faça o seguinte:

   a. Escolha Create an alarm (Criar um alarme).

   b. Para receber um e-mail quando o alarme for acionado, para Alarm notification (Notificação de alarme), escolha um Amazon SNS tópico existente. Para fazer isso, você precisa criar um tópico do Amazon SNS usando o console do Amazon SNS. Para obter mais informações, consulte Usar o Amazon SNS para mensagens de aplicação para pessoa (A2P) no Guia do desenvolvedor do Amazon Simple Notification Service.

      > **Note**
      >
      > Os usuários devem se inscrever no tópico do SNS especificado para receber notificações por email quando o alarme for acionado. O Usuário raiz da conta da AWS sempre recebe notificações por e-mail quando ocorrem ações de recuperação automática de instância, mesmo que um tópico do SNS não esteja especificado ou o usuário raiz não esteja inscrito no tópico de SNS especificado.

   c. Alterne em Ação alarme e escolha Recuperar.

   d. Para Group samples by (Agrupar amostras por) e Type of data to sample (Tipo de dados a serem amostrados), escolha uma estatística e uma métrica. Neste exemplo, escolha Average (Média) e Status check failed: system (Falha na verificação de status: sistema).

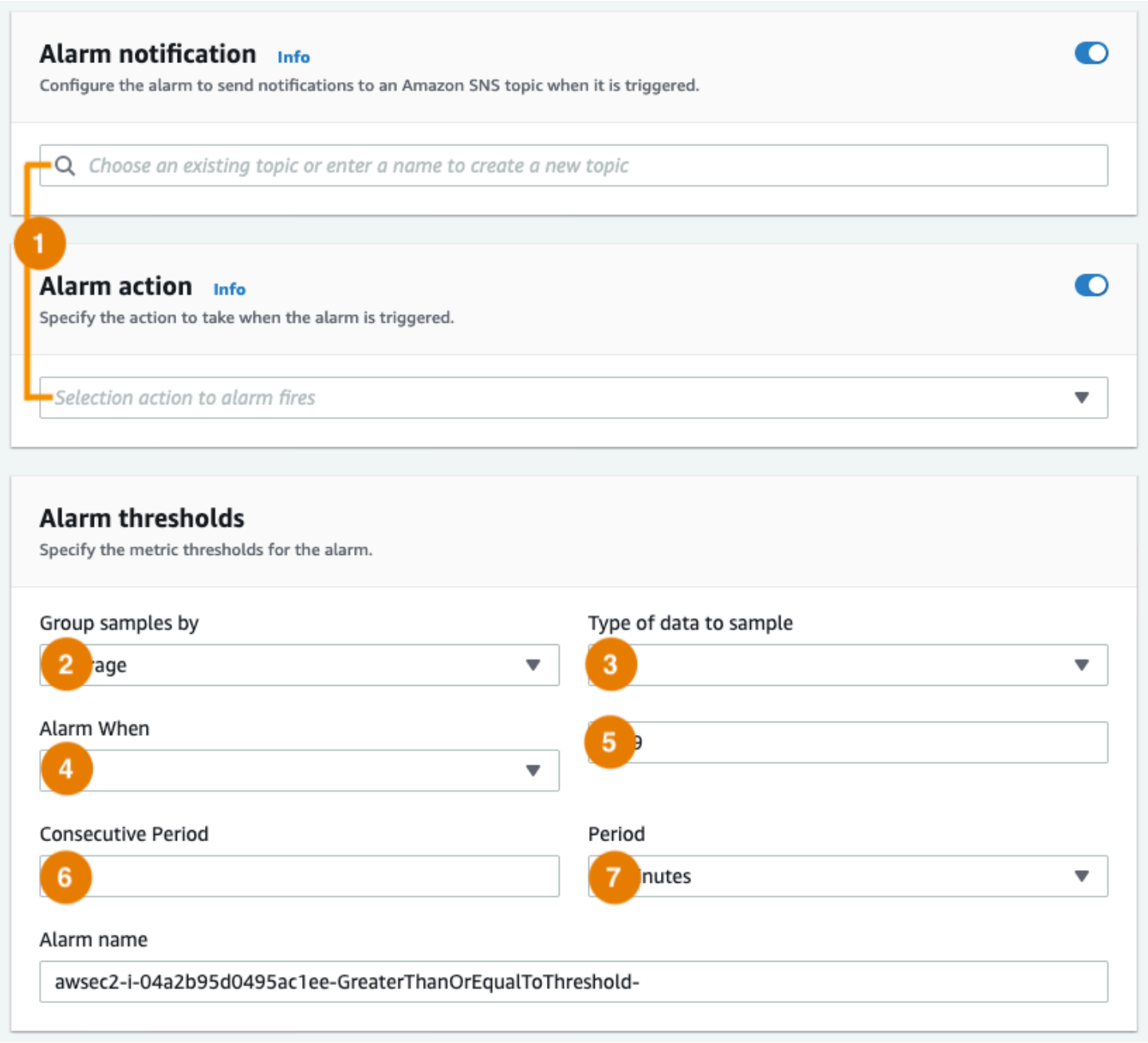
   e. Para Consecutive period (Período consecutivo) e Period (Período), especifique o período de avaliação do alarme. Nesse exemplo, digite 2 períodos consecutivos de 1 minuto. Se 1 minuto estiver desabilitado, você deverá habilitar o monitoramento detalhado ou escolher 5 minutos.

   f. Amazon CloudWatch cria automaticamente um nome de alarme para você. Para alterar o nome, em Alarm name (Nome do alarme), insira um novo nome. Os nomes de alarme devem conter somente caracteres ASCII.

   g. Escolha Criar.

Cenários de ação do alarme do Amazon CloudWatch

É possível 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.



Cenário 1: interromper instâncias de teste e desenvolvimento ociosas

Crie um alarme que interrompa uma instância usada para desenvolvimento ou teste de software quando estiver inativa pelo menos uma hora.

Configuração	Valor
1	Interromper
2	Máximo
3	Utilização da CPU
4	<=
5	10%
6	1
7	1 hora

Cenário 2: interromper instâncias ociosas

Crie um alarme que interrompa uma instância e envie um e-mail quando a instância estiver inativa por 24 horas.

Configuração	Valor
1	Interromper e enviar e-mail
2	Média
3	Utilização da CPU
4	<=
5	5%
6	24

Configuração	Valor
7	1 hora

Cenário 3: enviar e-mail em servidores Web com tráfego incomumente alto

Crie um alarme que envie o e-mail quando uma instância ultrapassar 10 GB de tráfego de rede de saída por dia.

Configuração	Valor
1	E-mail
2	Soma
3	Saída de rede
4	>
5	10 GB
6	24
7	1 hora

Cenário 4: interromper servidores Web com tráfego incomumente alto

Crie um alarme que pare uma instância e envie uma mensagem de texto (SMS) se o tráfego de saída exceder 1 GB por hora.

Configuração	Valor
1	Parar e enviar SMS
2	Soma
3	Saída de rede
4	>

Configuração	Valor
5	1 GB
6	1
7	1 hora

Cenário 5: Interromper uma instância danificada

Crie um alarme que interrompa uma instância em falhe três verificações de status consecutivas (executadas em intervalos de 5 minutos).

Configuração	Valor
1	Interromper
2	Média
3	Falha na verificação de status: sistema
4	-
5	-
6	1
7	15 minutos

Cenário 6: Encerrar instâncias quando os trabalhos de processamento em lote estiverem concluídos

Crie um alarme que encerre uma instância que execute trabalhos em lote quando não estiver mais enviando os dados dos resultados.

Configuração	Valor
1	Encerrar
2	Máximo

Configuração	Valor
3	Saída de rede
4	<=
5	100,000 bytes
6	1
7	5 minutos

Automatizar o Amazon EC2 usando o EventBridge

Você pode usar o Amazon EventBridge para automatizar seus Serviços da AWS e responder automaticamente a eventos do sistema, como problemas de disponibilidade de aplicações ou alterações de recursos. Os eventos dos serviços da AWS são entregues ao EventBridge quase em tempo real. É possível criar regras para indicar os eventos de seu interesse e quais ações deverão ser executadas quando um evento corresponder a uma regra. Ações que podem ser automaticamente acionadas incluem:

- Invocar uma função do AWS Lambda
- Invocar o Run Command do Amazon EC2
- Retransmitir o evento para o Amazon Kinesis Data Streams
- Ativar máquina de estado do AWS Step Functions
- Notificar um tópico do Amazon SNS
- Notificar uma fila do Amazon SQS

Veja a seguir exemplos de como utilizar o EventBridge com o Amazon EC2:

- Ative uma função Lambda sempre que uma instância entrar no estado de execução.
- Notifique um tópico do Amazon SNS quando um volume do Amazon EBS for criado ou modificado.
- Envie um comando para uma ou mais instâncias do Amazon EC2 usando o Run Command do Amazon EC2 sempre que um evento ocorrer em outro produto da AWS.

Para obter mais informações, consulte o Guia do Usuário do Amazon EventBridge.

Tipos de eventos do Amazon EC2

O Amazon EC2 oferece suporte aos seguintes tipos de evento:

- Alteração do estado da AMI do EC2
- Notificação de alteração de estado do EC2 Fast Launch
- Erro de frota do EC2
- Informações de frota do EC2
- Alteração da instância da frota do EC2
- Alteração da solicitação de instância spot da frota do EC2
- Alteração do estado da frota do EC2
- Recomendação de redistribuição de instâncias do EC2
- Notificação de alteração do estado da instância do EC2
- Erro na frota spot do EC2
- Informações sobre a frota spot do EC2
- Alteração da instância da frota spot do EC2
- Alteração da solicitação de instância spot da frota spot do EC2
- Alteração do estado da frota spot do EC2
- Alerta de interrupção da instância spot do EC2
- Atendimento de solicitação de instância spot do EC2
- Notificação de subutilização de ODCR do EC2

Para obter informações sobre os tipos de evento compatíveis com o Amazon EBS, consulte Amazon EventBridge for Amazon EBS.

Registro em log das chamadas de API do Amazon EC2 usando o AWS CloudTrail

A API do Amazon EC2 está integrada ao AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, por um perfil ou por um AWS service (Serviço da AWS). O CloudTrail captura todas as chamadas de API do Amazon EC2 como eventos. As chamadas capturadas incluem as chamadas feitas pelo console. Ao usar as informações coletadas pelo

CloudTrail, você pode determinar a solicitação que foi feita à API do Amazon EC2, o endereço IP do qual a solicitação foi feita e quando ela foi feita.

Cada entrada de log ou evento contém informações sobre quem gerou a solicitação. As informações de identidade ajudam a determinar:

- Se a solicitação foi feita com credenciais de usuário raiz ou credenciais de usuário.
- Se a solicitação foi feita em nome de um usuário do Centro de Identidade 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 AWS service (Serviço da AWS).

O CloudTrail está ativo em sua Conta da AWS e você tem acesso automático ao Histórico de eventos do CloudTrail. O Histórico de eventos do CloudTrail fornece um registro visualizável, pesquisável, baixável e imutável dos últimos 90 dias de eventos de gerenciamento gravados em uma Região da AWS. Para obter mais informações, consulte Trabalhar com histórico de eventos do CloudTrail no Guia do usuário do AWS CloudTrail. Não há cobranças do CloudTrail pela visualização do Histórico de eventos.

Para obter um registro contínuo de eventos em sua Conta da AWS nos últimos 90 dias, crie uma trilha ou um um armazenamento de dados de eventos do CloudTrail Lake.

Trilhas do CloudTrail

Uma trilha permite que o CloudTrail entregue arquivos de log a um bucket do Amazon S3. As trilhas criadas usando o Console de gerenciamento da AWS são de várias regiões. Só é possível criar uma trilha de região única ou de várias regiões usando a AWS CLI. Criar uma trilha de várias regiões é uma prática recomendada, pois você captura atividades em todas as Regiões da AWS da conta. Se você criar uma trilha de região única, poderá visualizar somente os eventos registrados na Região da AWS da trilha. Para obter mais informações sobre trilhas, consulte Criar uma trilha para a Conta da AWS e Criar uma trilha para uma organização no Guia do usuário do AWS CloudTrail.

Uma cópia dos seus eventos de gerenciamento em andamento pode ser entregue no bucket do Amazon S3 sem nenhum custo via CloudTrail com a criação de uma trilha. No entanto, há cobranças de armazenamento do Amazon S3. Para obter mais informações sobre os preços do CloudTrail, consulte Preços do AWS CloudTrail. Para receber informações sobre a definição de preço do Amazon S3, consulte Definição de preço do Amazon S3.

Armazenamentos de dados de eventos do CloudTrail Lake

O CloudTrail Lake permite executar consultas baseadas em SQL em seus eventos. O CloudTrail Lake converte eventos existentes em formato JSON baseado em linhas para o formato Apache ORC. O ORC é um formato colunar de armazenamento otimizado para recuperação rápida de dados. Os eventos são agregados em armazenamentos de dados de eventos, que são coleções imutáveis de eventos baseados nos critérios selecionados com a aplicação de seletores de eventos avançados. Os seletores que você aplica a um armazenamento de dados de eventos controlam quais eventos persistem e estão disponíveis para você consultar. Para obter mais informações sobre o CloudTrail Lake, consulte Trabalhar com o AWS CloudTrail Lake, no Guia do usuário do AWS CloudTrail.

Os armazenamentos de dados de eventos e consultas do CloudTrail Lake incorrem em custos. Ao criar um armazenamento de dados de eventos, você escolhe a opção de preço que deseja usar para ele. A opção de preço determina o custo para a ingestão e para o armazenamento de eventos, e o período de retenção padrão e máximo para o armazenamento de dados de eventos. Para obter mais informações sobre os preços do CloudTrail, consulte Preços do AWS CloudTrail.

Eventos de gerenciamento da API do Amazon EC2 no CloudTrail

Os Eventos de gerenciamento fornecem informações sobre operações de gerenciamento executadas em recursos na sua Conta da AWS. Elas também são conhecidas como operações de plano de controle. Por padrão, o CloudTrail registra eventos de gerenciamento em logs.

Todas as ações da API do Amazon EC2 são registradas como eventos de gerenciamento. Para ver a lista das ações da API que são registradas no CloudTrail, consulte a referência de APIs do Amazon EC2. Por exemplo, chamadas para as ações RunInstances, DescribeInstances e StopInstances são registradas como eventos de gerenciamento.

Exemplos de eventos da API do Amazon EC2

Um evento representa uma única solicitação de qualquer origem e inclui informações sobre a operação solicitada, a data e a hora da operação da API, os parâmetros de solicitação etc. Os arquivos de log do CloudTrail não são um rastreamento de pilha ordenada de chamadas de API pública, portanto não são exibidos em uma ordem específica.

O arquivo de log a seguir mostra que um usuário encerrou uma instância.

```
{
```

```
{
   "Records":[
      {
         "eventVersion":"1.03",
         "userIdentity":{
            "type":"Root",
            "principalId":"123456789012",
            "arn":"arn:aws:iam::123456789012:root",
            "accountId":"123456789012",
            "accessKeyId":"AKIAIOSFODNN7EXAMPLE",
            "userName":"user"
         },
         "eventTime":"2016-05-20T08:27:45Z",
         "eventSource":"ec2.amazonaws.com",
         "eventName":"TerminateInstances",
         "awsRegion":"us-west-2",
         "sourceIPAddress":"198.51.100.1",
         "userAgent":"aws-cli/1.10.10 Python/2.7.9 Windows/7botocore/1.4.1",
         "requestParameters":{
            "instancesSet":{
               "items":[{
                  "instanceId":"i-1a2b3c4d"
               }]
            }
         },
         "responseElements":{
            "instancesSet":{
               "items":[{
                  "instanceId":"i-1a2b3c4d",
                  "currentState":{
                     "code":32,
                     "name":"shutting-down"
                  },
                  "previousState":{
                     "code":16,
                     "name":"running"
                  }
               }]
            }
         },
         "requestID":"be112233-1ba5-4ae0-8e2b-1c302EXAMPLE",
         "eventID":"6e12345-2a4e-417c-aa78-7594fEXAMPLE",
         "eventType":"AwsApiCall",
         "recipientAccountId":"123456789012"
      }
```

```
    ]
}
```

Para obter informações sobre o conteúdo dos registros do CloudTrail, consulte Conteúdo dos registros do CloudTrail no Guia do usuário do AWS CloudTrail.

Auditar conexões realizadas com o EC2 Instance Connect

Você pode usar o AWS CloudTrail para auditar os usuários que se conectam às instâncias por meio do EC2 Instance Connect.

Para auditar a atividade do SSH por meio do EC2 Instance Connect usando o console do AWS CloudTrail

1. Abra o console do CloudTrail em https://console.aws.amazon.com/cloudtrail/.
2. Verifique se você está na região correta.
3. No painel de navegação, selecione Event history (Histórico de eventos).
4. Para Filter (Filtro), selecione Event source (Fonte do evento), ec2-instance-connect.amazonaws.com.
5. (Opcional) Para Time range (Intervalo de tempo), selecione um intervalo de tempo.
6. Selecione o ícone Refresh events (Atualizar eventos).
7. A página exibe os eventos que correspondem às chamadas de API de SendSSHPublicKey. Expanda um evento usando a seta para visualizar detalhes adicionais, como nome de usuário e chave de acesso da AWS usada para fazer a conexão SSH e o endereço IP de origem.
8. Para exibir todas as informações do evento no formato JSON, selecione View event (Exibir evento). O campo requestParameters contém o ID da instância de destino, o nome do usuário do sistema operacional e a chave pública usada para fazer a conexão SSH.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "ABCDEFGONGNOMOOCB6XYTQEXAMPLE",
        "arn": "arn:aws:iam::1234567890120:user/IAM-friendly-name",
        "accountId": "123456789012",
        "accessKeyId": "ABCDEFGUKZHNAW4OSN2AEXAMPLE",
        "userName": "IAM-friendly-name",
```

```
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2018-09-21T21:37:58Z"}
        }
    },
    "eventTime": "2018-09-21T21:38:00Z",
    "eventSource": "ec2-instance-connect.amazonaws.com",
    "eventName": "SendSSHPublicKey ",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "123.456.789.012",
    "userAgent": "aws-cli/1.15.61 Python/2.7.10 Darwin/16.7.0 botocore/1.10.60",
    "requestParameters": {
        "instanceId": "i-0123456789EXAMPLE",
        "osUser": "ec2-user",
        "SSHKey": {
            "publicKey": "ssh-rsa ABCDEFGHIJKLMNO01234567890EXAMPLE"
        }
     },
    "responseElements": null,
    "requestID": "1a2s3d4f-bde6-11e8-a892-f7ec64543add",
    "eventID": "1a2w3d4r5-a88f-4e28-b3bf-30161f75be34",
    "eventType": "AwsApiCall",
    "recipientAccountId": "0987654321"
}
```

Se você tiver configurado a conta da AWS para coletar eventos do CloudTrail em um bucket do S3, poderá fazer download e auditar as informações de forma programática. Para obter mais informações, consulte Obter e visualizar arquivos de log do CloudTrail no Guia do usuário do AWS CloudTrail.

Monitorar as aplicações .NET e SQL Server com o CloudWatch Application Insights

O CloudWatch Application Insights for .NET e SQL Server ajuda você a monitorar as aplicações .NET e SQL Server que usam instâncias do Amazon EC2 juntamente com outros recursos de aplicações da AWS. Ele identifica e configura os principais logs de métricas e alarmes na pilha de tecnologia e nos recursos da aplicação (por exemplo, banco de dados Microsoft SQL Server, servidores Web (IIS) e de aplicações, SO, balanceadores de carga e filas). Ele monitora continuamente os logs e as métricas para detectar e correlacionar anomalias e erros. Quando

erros e anomalias são detectados, o Application Insights gera eventos que podem ser usados para configurar notificações ou executar ações. Para auxiliar na solução de problemas, ele cria painéis automatizados para os problemas detectados, que incluem anomalias de métricas correlacionadas e erros de log com informações adicionais para indicar a potencial causa do problema. Os painéis automatizados ajudam você a tomar medidas corretivas rápidas para manter suas aplicações íntegras e para evitar o impacto nos usuários finais do sua aplicação.

Informações fornecidas sobre os problemas detectados:

- Um breve resumo do problema
- A data e a hora de início do problema
- A gravidade do problema: High/Medium/Low (Alta/média/baixa)
- O status do problema detectado: In-progress/Resolved (Em andamento/resolvido)
- Insights: insights gerados automaticamente sobre o problema detectado e a possível causa
- Feedback sobre os insights: o feedback que você forneceu sobre a utilidade dos insights gerados pelo CloudWatch Application Insights para .NET e SQL Server
- Observações relacionadas: uma visão detalhada das anomalias da métrica e dos trechos do erro de logs relevantes relacionados ao problema em vários componentes da aplicação

Feedback

É possível fornecer feedback em relação aos insights gerados automaticamente sobre problemas detectados designando-os como úteis ou não úteis. Seu feedback sobre os insights com o diagnóstico da aplicação (anomalias da métrica e exceções de log) são usados para melhorar a futura detecção de problemas semelhantes.

Para obter mais informações, consulte a documentação CloudWatch Application Insights (Insights sobre aplicações do CloudWatch) no Guia do usuário do Amazon CloudWatch.

Acompanhamento do uso do nível gratuito para o Amazon EC2

Ao criar uma Conta da AWS, é possível começar a usar o Amazon EC2 gratuitamente usando o nível gratuito da AWS. Os benefícios do nível gratuito são diferentes para contas criadas antes ou depois de 15 de julho de 2025. Para obter mais informações, consulte Explore AWS services with AWS Free Tier no Guia do usuário do AWS Billing.

Benefícios do nível gratuito antes e depois de 15 de julho de 2025

A tabela abaixo compara os benefícios do nível gratuito com base na data de criação da Conta da AWS:

Benefício do nível gratuito	Conta criada antes de 15 de julho de 2025	Conta criada a partir de 15 de julho de 2025
Tipos de instância marcados como elegíveis para o nível gratuito	`t2.micro`, `t3.micro`	`t3.micro`, `t3.small`, `t4g.micro` , `t4g.small` , `c7i-flex.large` , `m7i-flex.large`
Tipos de volume do Amazon EBS marcados com Elegíveis ao nível gratuito	`standard`, `st1`, `sc1`, `gp2`, e `gp3`	`standard`, `st1`, `sc1`, `gp2`, e `gp3`
AMIs marcadas como elegíveis para o nível gratuito	Verifique se há AMIs marcadas como elegíveis para o nível gratuito.	Verifique se há AMIs marcadas como elegíveis para o nível gratuito.
Limite de uso	Restritos aos limites de uso, após os quais são cobradas tarifas de pagamento conforme o uso.	Receba um crédito de USD 100 pela inscrição e ganhe até USD 100 em créditos adicionais.
Duração do nível gratuito	Seu nível gratuito dura 12 meses após a data de criação da conta. Durante esse período, se você exceder os limites de uso do nível gratuito, serão cobradas tarifas de pagamento conforme o uso.	O nível gratuito dura seis meses após a data de criação da conta ou quando os créditos acabarem, o que ocorrer primeiro. Você não pode exceder os limites do nível gratuito.

Para listar os tipos de instância qualificados para o nível gratuito

Use o comando describe-instance-types com o filtro `free-tier-eligible`.

```
aws ec2 describe-instance-types \
    --filters Name=free-tier-eligible,Values=true \
    --query "InstanceTypes[*].[InstanceType]" \
    --output text | sort
```

Para listar as AMIs qualificadas para o nível gratuito

Use o comando describe-images com o filtro `free-tier-eligible`.

```
aws ec2 describe-images \
    --filters Name=free-tier-eligible,Values=true \
    --query "Images[*].[ImageId]" \
    --output text | sort
```

Rastrear o uso do nível gratuito para contas criadas antes de 15 de julho de 2025

> **Note**
>
> Esta seção se aplica somente aos usuários do nível gratuito que criaram Contas da AWS antes de 15 de julho de 2025. Caso tenha criado sua conta em 15 de julho de 2025 ou após essa data, consulte Tracking your AWS Free Tier usage no Guia do usuário do AWS Billing.

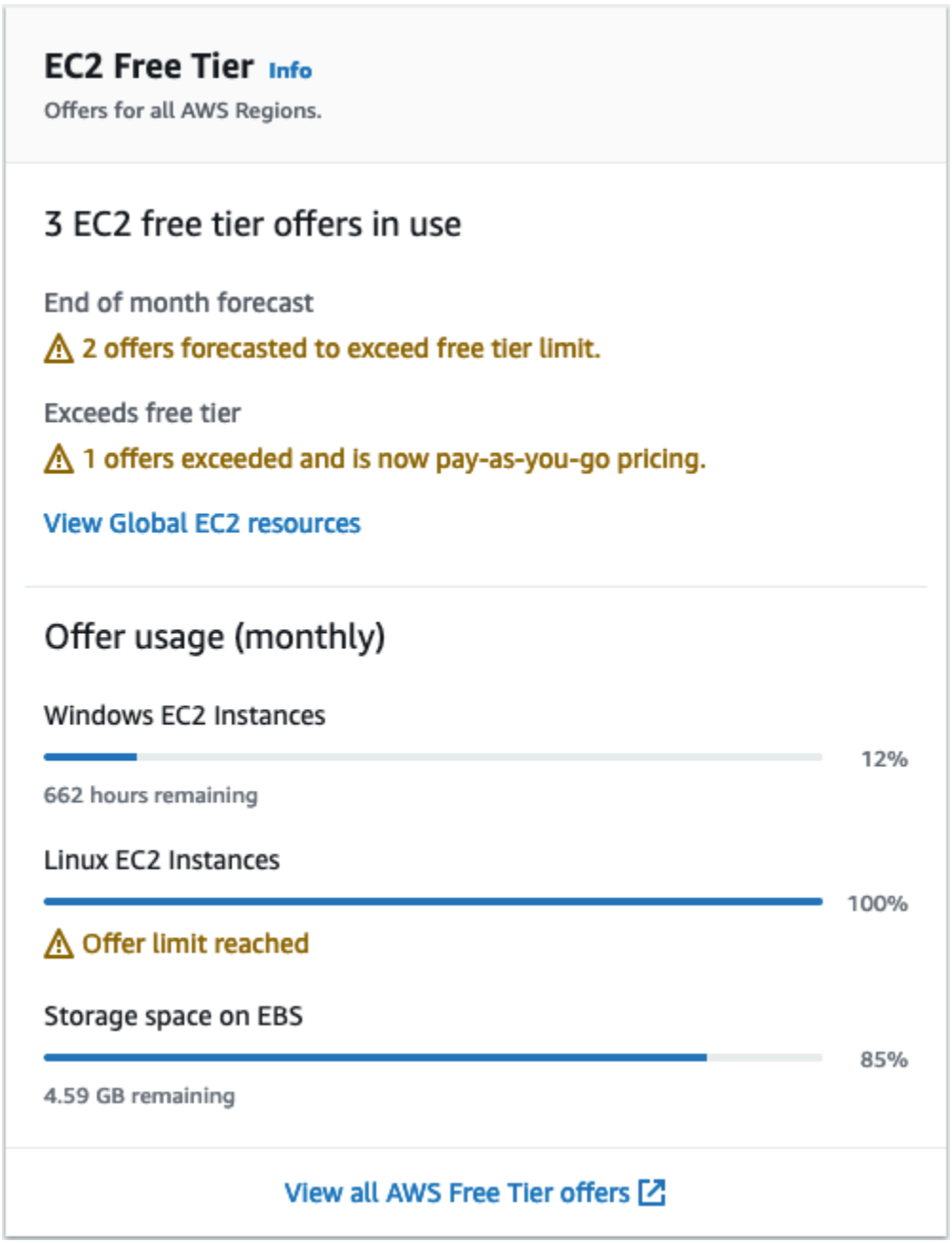
Caso tenha criado sua conta antes de 15 de julho de 2025, é possível usar o Amazon EC2 sem custos se for cliente da AWS há menos de 12 meses e permanecer dentro dos limites de uso do Nível gratuito da AWS. É importante acompanhar seu uso do nível gratuito para evitar surpresas na cobrança. Se você exceder os limites do nível gratuito, incorrerá nas tarifas padrão para pagamento de acordo com o uso. Para obter mais informações, consulte Nível gratuito da AWS.

> **Note**
>
> Se você for cliente da AWS há mais de 12 meses, não estará mais qualificado para usar o nível gratuito e não verá a caixa Nível gratuito do EC2, descrita no procedimento a seguir.

Para acompanhar seu uso do nível gratuito

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

2. No painel de navegação, escolha EC2 Dashboard (Painel do EC2).
3. Localize a caixa Nível gratuito do EC2 (no canto superior direito).



4. Na caixa Nível gratuito do EC2, verifique seu uso do nível gratuito, da seguinte maneira:
   - Em Ofertas do nível gratuito do EC2 em uso, anote os avisos:
     - Previsão de fim do mês: esse é um aviso de que você incorrerá em custos este mês se continuar com seu padrão de uso atual.

- Excede o nível gratuito: esse é um aviso de que você excedeu os limites do nível gratuito e já está incorrendo em custos.
- Em Uso da oferta (mensal), anote seu uso de instâncias do Linux, instâncias do Windows e armazenamento do EBS. A porcentagem indica quanto você usou este mês dos seus limites de nível gratuito. Se estiver em 100%, você incorrerá em custos para continuar a usar.

> **Note**
>
> Essas informações só aparecem depois que você criou uma instância. Porém, as informações de uso não são atualizadas em tempo real; elas são atualizadas três vezes ao dia.

5. Para evitar incorrer em custos adicionais, exclua todos os recursos que estão sendo cobrados agora ou que serão cobrados se você exceder o limite de uso do nível gratuito.
   - Para obter instruções para excluir a instância, consulte Encerramento de instâncias do Amazon EC2.
   - Para verificar se você tem recursos em outras regiões que possam estar gerando custos, na caixa Nível gratuito do EC2, escolha Exibir recursos globais do EC2 para abrir a Visão global do EC2. Para obter mais informações, consulte Visualizar recursos entre regiões usando a Visualização Global da AWS.
6. Para visualizar seu uso dos recursos de todos os Serviços da AWSNível gratuito da AWS, na parte inferior da caixa Nível gratuito do EC2, escolha Exibir todas as ofertas do Nível gratuito da AWS. Para obter mais informações, consulte Trying services using Nível gratuito da AWS no Guia do usuário de faturamento da AWS.

Entender os códigos do Amazon EC2 em relatórios de faturamento e uso

Quando você utiliza o Amazon EC2, incluímos códigos relacionados nos relatórios de faturamento e uso da AWS. A análise desses códigos ajuda você a entender seus custos e padrões de uso do Amazon EC2. Acompanhar e gerenciar suas despesas é essencial para otimizar custos.

As tabelas a seguir descrevem os códigos do Amazon EC2 que aparecem nos relatórios de faturamento e uso. Para obter uma lista dos códigos de região utilizados nos relatórios de uso e faturamento, consulte AWS Region billing codes.

Códigos de faturamento para:

- Instâncias
- Instâncias bare metal
- Hosts dedicados
- Dedicated Instances
- Otimização de EBS
- Reservas de capacidade

Recursos relacionados

- the section called “Opções de faturamento e compra”
- the section called “Noções básicas sobre o faturamento da AMI”
- Definição de preços do Amazon EC2

Instâncias

Código	Descrição	Unidades
region-BoxUsage :*instance-type*	O tempo de execução das instâncias sob demanda.	Horas
region-HostBoxUsage :*instance-type*	O tempo de execução das instâncias em hosts dedicados.	Horas
region-SpotUsage :*instance-type*	O tempo de execução das instâncias spot.	Horas

Instâncias bare metal

Código	Descrição	Unidades
region-BoxUsage :*instance-family* .metal	O tempo de execução das instâncias bare metal sob demanda.	Horas
region-HostBoxUsage :*instance-family* .metal	O tempo de execução das instâncias bare metal em hosts dedicados.	Horas
region-SpotUsage :*instance-family* .metal	O tempo de execução das instâncias spot bare metal.	Horas

Hosts dedicados

Código	Descrição	Unidades
region-HostUsage :*host-type*	O tempo em que os hosts dedicados são provisionados.	Horas
region-ReservedHostUsage :*host-type*	O tempo em que as reservas de host dedicado são aplicadas.	Horas

Dedicated Instances

Código	Descrição	Unidades
region-DedicatedUsage :*instance-type*	O tempo de execução das instâncias dedicadas.	Horas + taxa por região

Otimização de EBS

Código	Descrição	Unidades
region-EBSOptimized :*instance-type*	O tempo em que a otimização do EBS é habilitada.	Horas

Reservas de capacidade

Código	Descrição	Unidades
region-Reservation :*instance-type*	O tempo de instância reservado para reservas de capacidade.	Horas
region-UnusedBox :*instance-type*	O tempo de instância reservado não utilizado para reservas de capacidade.	Horas
region-DedicatedRes :*instance-type*	O tempo de instância reservado para reservas de capacidade dedicadas.	Horas
region-UnusedDed :*instance-type*	O tempo de instância reservado não utilizado para reservas de capacidade dedicadas.	Horas

Criar um inventário das instâncias do EC2

O Amazon EC2 fornece capacidade de computação escalável e sob demanda. Uma instância do EC2 é um servidor virtual executado na rede da AWS.

A tabela a seguir descreve as principais características de uma instância do EC2. Um administrador do sistema pode usar as orientações fornecidas neste guia para obter informações sobre essas

características e usá-las na configuração de servidores com funcionalidades equivalentes executados on-premises ou na rede de outro provedor de nuvem.

Característica	Descrição
Localização geográfica	O Amazon EC2 está hospedado em todas as regiões da AWS ao redor do mundo. Selecione locais para suas instâncias que as coloquem perto de seus clientes. Você pode inicializar instâncias em vários locais.
Especificações de hardware	O Amazon EC2 fornece uma ampla seleção de tipos de instância otimizadas para diferente s casos de uso. Os tipos de instância que você seleciona para as suas determinam os recursos de computação, memória, rede e armazenamento delas.
Imagens	Uma imagem de máquina da Amazon (AMI) inclui o software a ser instalado na instância durante a inicialização. Isso inclui o sistema operacional, os pacotes de software e as configurações personalizadas.
Endereços IP e nomes do host DNS	As instâncias recebem endereços IP privados e um nome do host DNS privado. Se você configurar um endereço IP público para uma instância, ela também receberá um nome do host DNS público.
Regras de grupos de segurança	As regras do grupo de segurança associada s às instâncias determinam qual tráfego de entrada e de saída é permitido.
Dados do usuário	Os dados do usuário são disponibilizados para as instâncias na inicialização. Eles consistem em scripts shell (Linux) ou scripts PowerShell (Windows).

Localização geográfica

O Amazon EC2 está disponível em todas as regiões da AWS no mundo todo. Cada Região é uma área geográfica separada. Você pode diminuir a latência da rede ao selecionar regiões para servidores que estejam próximas à maioria dos usuários.

Você pode usar o Amazon EC2 Global View para listar as instâncias do Amazon EC2 em todas as regiões. Com o Console de gerenciamento da AWS e a API, você deve listar as instâncias de cada região individualmente.

Por que isso é importante

Depois de determinar onde as instâncias estão localizadas, você decide se deseja implantar servidores com funcionalidades equivalentes nos mesmos locais ou em locais diferentes, dependendo de suas necessidades.

Para obter um resumo das instâncias do EC2 em todas as regiões

1. Abra o console do Amazon EC2 Global View em https://console.aws.amazon.com/ec2globalview/home.
2. Na guia Explorador de regiões, em Resumo, verifique a contagem de recursos das Instâncias, o que inclui o número de instâncias e o de regiões. Clique no texto sublinhado para ver como a contagem de instâncias está distribuída entre as regiões.
3. Na guia Pesquisa global, selecione o filtro de cliente Tipo de recurso = Instância. Você pode filtrar ainda mais os resultados especificando uma região ou uma tag.

Para obter o número de instâncias do EC2 em uma região usando a AWS CLI

Use o comando describe-instances a seguir para contar as instâncias na região especificada. Você precisa executar esse comando em cada região na qual tenha instâncias.

```
aws ec2 describe-instances \
    --region us-east-2 \
    --query "length(Reservations[*].Instances[])"
```

O seguinte é um exemplo de saída.

```
27
```

Para obter uma lista dos IDs de instância em vez da contagem de instâncias, use o parâmetro `--query` a seguir.

```
--query "Reservations[*].Instances[].InstanceId"
```

Especificações de hardware

O tipo de instância especificado para uma instância do EC2 determina os recursos de computação, memória, armazenamento e rede que estão disponíveis para ela. Cada família de instâncias oferece um equilíbrio diferente entre recursos de computação, memória, rede e armazenamento. Para obter mais informações, consulte o Guia de tipos de instância do Amazon EC2.

Por que isso é importante

Depois de determinar as especificações de hardware das instâncias, você pode decidir as especificações mínimas necessárias para servidores com funcionalidades equivalentes.

Para obter um resumo dos tipos de instância usados por suas instâncias

Use o seguinte comando describe-instances. O comando sed remove linhas com colchetes e linhas vazias. Você precisa executar esse comando em cada região na qual tenha instâncias.

```
aws ec2 describe-instances \
    --query "Reservations[*].Instances[].InstanceType" | sed 's/[][]//g;/^$/d' | sort |
 uniq -c | sort -nr
```

O seguinte é um exemplo de saída.

```
  20    "c6i.4xlarge",
   5    "t2.micro",
   2    "g6e.2xlarge",
```

Para obter informações sobre tipos de instância específicos

Use o comando describe-instance-types para descrever os tipos de instância. O parâmetro `--query` inclui somente os campos especificados na saída. Essas são as características básicas. É possível exibir os campos adicionais de que você precisa ou consultar Especificações de tipos de instâncias do Amazon EC2 no Guia de tipos de instância do Amazon EC2.

```
aws ec2 describe-instance-types \
```

```
    --instance-types c6i.4xlarge t2.micro g6e.2xlarge \
    --query "InstanceTypes[*].
[InstanceType,VCpuInfo.DefaultVCpus,MemoryInfo.SizeInMiB,NetworkInfo.NetworkPerformance]"
 \
    --output table
```

O seguinte é um exemplo de saída. As colunas são tipo de instância, vCPUs, memória (GiB) e largura de banda da rede (Gbps).

```
-----------------------------------------------------
|               DescribeInstanceTypes               |
+--------------+-----+--------+----------------------+
|  t2.micro    |  1  |  1024  |  Low to Moderate     |
|  c6i.4xlarge |  16 |  32768 |  Up to 12.5 Gigabit  |
|  g6e.2xlarge |  8  |  65536 |  Up to 20 Gigabit    |
+--------------+-----+--------+----------------------+
```

Imagens

Uma imagem de máquina da Amazon (AMI) fornece o software que é instalado em sua instância na inicialização, como sistema operacional, serviços, ferramentas de desenvolvimento e aplicações. Você pode exportar uma AMI para outros formatos e usá-la com outros servidores.

Por que isso é importante

Depois de determinar as AMIs das instâncias, planeje as imagens necessárias para servidores com funcionalidades equivalentes. Talvez seja possível exportar suas AMIs para um formato que possa ser usado em outros lugares. Como alternativa, talvez você precise se conectar a uma instância inicializada em cada AMI, confirmar o que está instalado e como está configurado e garantir que tenha uma cópia de tudo o que precisa.

Para obter as AMIs das suas instâncias

Use o seguinte comando describe-instances. O comando sed remove linhas com colchetes e linhas vazias. Você precisa executar esse comando em cada região na qual tenha instâncias.

```
aws ec2 describe-instances \
    --query "Reservations[*].Instances[].ImageId" | sed 's/[][]//g;/^$/d' | sort | uniq
 -c | sort -nr
```

O seguinte é um exemplo de saída.

```
20     "ami-0a70b9d193ae8a79",
 5     "ami-07d9cf938edb0739b",
 2     "ami-09245d5773578a1d6",
```

Para obter informações sobre AMIs específicas

Use o seguinte comando describe-images. O parâmetro `--query` inclui somente os campos especificados na saída. É possível incluir quaisquer campos adicionais necessários.

```
aws ec2 describe-images \
    --image-id ami-0a70b9d193ae8a79 ami-07d9cf938edb0739b ami-09245d5773578a1d6 \
    --query "Images[*].
{ID:ImageId,CreateDate:CreationDate,Name:Name,Description:Description}"
```

O seguinte é um exemplo de saída.

```
[
    {
        "ID": "ami-0a70b9d193ae8a799",
        "CreateDate": "2025-03-01T02:22:41.000Z",
        "Name": "web-server-3.1",
        "Description": "Image for web servers"
    },
    {
        "ID": "ami-07d9cf938edb0739b",
        "CreateDate": "2025-02-01T23:59:03.000Z",
        "Name": "awesome-application-11.5",
        "Description": "Image for Awesome Application"
    },
    {
        "ID": "ami-09245d5773578a1d6",
        "CreateDate": "2025-01-31T02:22:41.000Z",
        "Name": "monitoring-4.2",
        "Description": "Monitoring software"
    }
]
```

Para criar um arquivo de VM usando uma AMI

Use o comando export-image. Os formatos de imagem compatíveis são VHD (compatível com Citrix Xen e Microsoft Hyper-V), VMDK (compatível com VMware ESX e VMware vSphere) e formato

bruto (compatível com hipervisores KVM e Xen). Para obter informações sobre os requisitos e as limitações do VM Import/Export, consulte VM Import/Export Requirements.

Endereços IP e nomes do host DNS

Seus usuários se conectam às instâncias do EC2 pela internet usando nomes do host DNS públicos. O nome do host DNS público de uma instância do EC2 é resolvido no endereço IP público. As instâncias do EC2 podem se comunicar entre si usando os endereços IP privados.

Por que isso é importante

Os endereços IP permitem que dispositivos se comuniquem entre si por meio de uma rede local ou da internet. Ao observar os endereços IP e os nomes DNS das instâncias, você pode ajudar a garantir que servidores com funcionalidades equivalentes possam se comunicar com os mesmos clientes ou dispositivos que suas instâncias. Por exemplo, você pode atualizar a configuração do balanceador de carga ou os registros de DNS criados para o provedor de DNS.

Para obter os endereços IP e os nomes do host DNS das instâncias

Use o seguinte comando describe-instances. Você precisa executar esse comando em cada região na qual tenha instâncias. O parâmetro `--query` inclui somente os campos especificados na saída. É possível incluir quaisquer campos adicionais necessários.

```
aws ec2 describe-instances \
    --query "Reservations[*].Instances[].[InstanceId,PrivateIpAddress,PublicDnsName]" \
    --output table
```

O seguinte é um exemplo de saída. As colunas são ID da instância, endereço IPv4 privado e nome DNS IPv4 público.

```
----------------------------------------------------------------------------------
|                                DescribeInstances
 |
+---------------------+-----------+-------------------------------------------------
+
| i-0bac57d7472c89bac | 10.0.2.139 | ec2-192-0-2-142.us-east-2.compute.amazonaws.com
 |
| i-0fa8b7678975a3fff | 10.0.14.85 | ec2-198-51-100-56.us-east-2.compute.amazonaws.com
 |
  ...
```

```
  ...
| i-08fd74f3f1595fdbd | 10.0.1.241 | ec2-203.0.113.13.us-east-2.compute.amazonaws.com
 |
+--------------------+-----------+-----------------------------------------------
+
```

Regras de grupos de segurança

Um grupo de segurança funciona como um firewall virtual. Depois de associar um grupo de segurança a uma instância do EC2, as regras permitem tráfego de entrada e saída da instância do EC2 em portas e protocolos específicos.

Por que isso é importante

Depois de determinar o tráfego de entrada permitido para chegar ao servidor e o tráfego de saída permitido para sair dele, você pode planejar as regras de firewall necessárias para servidores com funcionalidades equivalentes.

Para obter os grupos de segurança das instâncias

Use o seguinte comando describe-instances. O comando sed remove linhas com colchetes e linhas vazias. Você precisa executar esse comando em cada região na qual tenha instâncias.

```
aws ec2 describe-instances \
    --query "Reservations[*].Instances[].SecurityGroups[].GroupId" | sed 's/[][]//g;/^
$/d' | sort | uniq -c | sort -nr
```

O seguinte é um exemplo de saída.

```
27     "sg-01dd3383691d02f42",
10     "sg-08c77cc910c0b3b2c",
 2     "sg-00f4e409629f1a42d",
```

Para obter as regras de entrada de um grupo de segurança

Use o comando describe-security-group-rules a seguir para exibir as regras do grupo de segurança especificado em que `IsEgress` é `false`.

```
aws ec2 describe-security-group-rules \
```

```
    --filters Name=group-id,Values=sg-01dd3383691d02f42 \
    --query 'SecurityGroupRules[?IsEgress==`false`]'
```

O seguinte é um exemplo de saída. A primeira regra é a de entrada padrão, que permite tráfego de entrada proveniente de todos os recursos atribuídos a esse grupo de segurança. A outra regra permite tráfego SSH proveniente dos endereços IP na lista de prefixos especificada. Para descrever os blocos CIDR em uma lista de prefixos, use o comando describe-prefix-lists.

```
[
    {
        "SecurityGroupRuleId": "sgr-06c8b42574a91db1b",
        "GroupId": "sg-01dd3383691d02f42",
        "GroupOwnerId": "123456789012",
        "IsEgress": false,
        "IpProtocol": "-1",
        "FromPort": -1,
        "ToPort": -1,
        "ReferencedGroupInfo": {
            "GroupId": "sg-01dd3383691d02f42",
            "UserId": "123456789012"
        },
        "Tags": [],
        "SecurityGroupRuleArn": "arn:aws:ec2:us-west-2:123456789012:security-group-
rule/sgr-06c8b42574a91db1b"
    },
    {
        "SecurityGroupRuleId": "sgr-0886a5d46afcd1758",
        "GroupId": "sg-01dd3383691d02f42",
        "GroupOwnerId": "123456789012",
        "IsEgress": false,
        "IpProtocol": "tcp",
        "FromPort": 22,
        "ToPort": 22,
        "PrefixListId": "pl-f8a6439125e7bf465",
        "Tags": [],
        "SecurityGroupRuleArn": "arn:aws:ec2:us-east-2:123456789012:security-group-
rule/sgr-0886a5d46afcd1758"
    }
]
```

Para obter as regras de saída de um grupo de segurança

Use o comando describe-security-group-rules a seguir para exibir as regras do grupo de segurança especificado em que `IsEgress` é `true`.

```
aws ec2 describe-security-group-rules \
    --filters Name=group-id,Values=sg-01dd3383691d02f42 \
    --query 'SecurityGroupRules[?IsEgress==`true`]'
```

O seguinte é um exemplo de saída. Ele contém somente a regra de saída padrão, que permite todo o tráfego IPv4 de saída.

```
[
    {
        "SecurityGroupRuleId": "sgr-048f09a719247dce7",
        "GroupId": "sg-01dd3383691d02f42",
        "GroupOwnerId": "123456789012",
        "IsEgress": true,
        "IpProtocol": "-1",
        "FromPort": -1,
        "ToPort": -1,
        "CidrIpv4": "0.0.0.0/0",
        "Tags": [],
        "SecurityGroupRuleArn": "arn:aws:ec2:us-east-2:123456789012:security-group-
rule/sgr-048f09a719247dce7"
    }
]
```

Dados do usuário

Ao inicializar uma instância do EC2, é possível transmitir um script shell para a instância usando dados do usuário. Observe que os dados do usuário são codificados em base64, portanto, é necessário decodificá-los para ler o script.

Por que isso é importante

Se você estiver executando comandos na inicialização como parte da configuração das instâncias, talvez seja necessário realizar as mesmas tarefas ao configurar servidores com funcionalidades equivalentes.

Para visualizar os dados decodificados do usuário de uma instância

Use o comando describe-instance-attribute a seguir. O comando base64 decodifica os dados do usuário.

```
aws ec2 describe-instance-attribute \
    --instance-id i-1234567890abcdef0 \
    --attribute userData \
    --output text \
    --query "UserData.Value" | base64 --decode
```

O seguinte é um exemplo de saída.

```
#!/bin/bash
yum update -y
service httpd start
chkconfig httpd on
```

Recursos relacionados

Estas são as características adicionais das instâncias do EC2:

- Pares de chaves
- Armazenamento
- Tags

Você pode verificar se está usando os seguintes recursos para inicializar instâncias do EC2 ou distribuir o tráfego entre as instâncias do EC2:

- Grupos do Auto Scaling
- EC2 Fleet
- Elastic Load Balancing

Solucionar problemas com instâncias do Amazon EC2

Os procedimentos e dicas apresentados a seguir podem ajudar você a solucionar problemas com instâncias do Amazon EC2.

Problemas

- Solucionar problemas de inicialização de instâncias do Amazon EC2
- Solucionar problemas de interrupção de instâncias do Amazon EC2
- Solucionar problemas de encerramento de instâncias do Amazon EC2
- Solucionar problemas de uma instância inacessível do Amazon EC2
- Solucionar problemas de conexão com a instância do Linux do Amazon EC2
- Solucionar problemas de instâncias do Linux do Amazon EC2 com falhas nas verificações de status
- Solução de problemas de inicialização da instância do Linux do Amazon EC2 devido a volume errado
- Solucionar problemas de conexão à instância do Windows do Amazon EC2
- Solucionar problemas de inicialização de instâncias do Windows do Amazon EC2
- Solucionar problemas com instâncias do Windows do Amazon EC2
- Redefinir a senha de administrador do Windows para uma instância do Windows do Amazon EC2
- Solucionar problemas de Sysprep com instâncias do Windows do Amazon EC2
- Solucionar problemas de instâncias danificadas do Amazon EC2 no Linux usando o EC2Rescue
- Solucionar problemas de uma instância Amazon EC2 Windows danificada usando o EC2Rescue
- EC2 Serial Console para instâncias do
- Enviar uma interrupção para diagnóstico para depurar uma instância inacessível do Amazon EC2

Solucionar problemas de inicialização de instâncias do Amazon EC2

Veja a seguir dicas para ajudar na solução de problemas de inicialização de instâncias do Amazon EC2.

Problemas de execução

- Nome de dispositivo inválido
- Limite de instâncias excedido
- Capacidade insuficiente da instância
- A configuração solicitada não é suportada atualmente. Verifique a documentação quanto às configurações compatíveis.
- A instância é encerrada imediatamente
- Permissões insuficientes
- Alto uso da CPU logo após a inicialização do Windows (somente para instâncias do Windows)

Nome de dispositivo inválido

Descrição

Você obtém o erro `Invalid device name` *`device_name`* ao tentar iniciar uma nova instância.

Causa

Se você receber esse erro ao tentar executar uma instância, o nome do dispositivo especificado para um ou mais volumes da solicitação terá um nome de dispositivo inválido. As possíveis causas incluem:

- O nome do dispositivo pode estar em uso pela AMI selecionada.
- O nome do dispositivo pode estar reservado para volumes raiz.
- O nome do dispositivo pode estar sendo usado para outro volume da solicitação.
- O nome do dispositivo pode não ser válido para o sistema operacional.

Solução

Como resolver o problema:

- Verifique se o nome do dispositivo não está sendo usado na AMI que você selecionou. Execute o comando a seguir para visualizar os nomes de dispositivo usados pela AMI.

```
aws ec2 describe-images --image-id ami-0abcdef1234567890 --query
 'Images[*].BlockDeviceMappings[].DeviceName'
```

- Verifique se não está usando um nome de dispositivo reservado para volumes raiz. Para obter mais informações, consulte Nomes de dispositivos disponíveis.
- Verifique se cada volume especificado em sua solicitação tem um nome de dispositivo exclusivo.
- Verifique se os nomes de dispositivo especificados estão no formato correto. Para obter mais informações, consulte Nomes de dispositivos disponíveis.

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 Service Quotas do Amazon EC2.

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 esse erro ao tentar executar uma instância ou reiniciar uma instância interrompida, isso significa que, no momento, a AWS não tem capacidade sob demanda suficiente para atender à sua solicitação.

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 Alterações no tipo de instância do Amazon EC2.
- Se você estiver executando instâncias em um placement group de cluster, é possível obter um erro de capacidade insuficiente.

A configuração solicitada não é suportada atualmente. Verifique a documentação quanto às configurações compatíveis.

Descrição

Você obtém o erro `Unsupported` ao tentar executar uma nova instância porque a configuração da instância não é compatível.

Causa

A mensagem de erro fornece detalhes adicionais. Por exemplo, é possível que um tipo de instância ou opção de compra de instância não seja compatível com a região ou Zona de Disponibilidade especificada.

Solução

Tente uma configuração de instância diferente. Para pesquisar um tipo de instância que atenda aos seus requisitos, consulte Localizar um tipo de instância do Amazon EC2.

A instância é encerrada imediatamente

Descrição

Sua instância passa do estado `pending` para o estado `terminated`.

Causa

A seguir estão alguns motivos pelos quais a instância pode ser imediatamente encerrada:

- Você excedeu os limites de volume do EBS. Para obter mais informações, consulte Limites de volume do Amazon EBS para instâncias do Amazon EC2.
- Um snapshot do EBS está corrompido.
- O volume raiz do EBS está criptografado e você não tem permissões para acessar a Chave do KMS para descriptografia.
- Um snapshot especificado no mapeamento de dispositivo de blocos para a AMI está criptografado e você não tem permissões para acessar a Chave do KMS para descriptografia ou não tem acesso à Chave do KMS para criptografar os volumes restaurados.
- A AMI baseada no Amazon S3 usada para criar a instância está incompleta, faltando uma parte necessária (um arquivo image.part.xx).

Para obter mais informações, saiba o motivo do encerramento usando um dos métodos a seguir.

Para obter o motivo do encerramento usando o console do Amazon EC2

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Instâncias e selecione a instância.
3. Na primeira guia, encontre o motivo ao lado de State transition reason (Motivo de transição de estado).

Para obter o motivo do encerramento usando a AWS CLI

1. Use o comando describe-instances e especifique o ID da instância.

```
aws ec2 describe-instances --instance-id i-1234567890abcdef0
```

2. Revise a resposta JSON retornada pelo comando e observe os valores no elemento de resposta `StateReason`.

O bloco de código a seguir mostra um exemplo de elemento de resposta `StateReason`:

```
"StateReason": {
  "Message": "Client.VolumeLimitExceeded: Volume limit exceeded",
  "Code": "Server.InternalError"
},
```

Como saber o motivo do encerramento usando a AWS CloudTrail

Para obter mais informações, consulte o tópico sobre como Visualizar eventos com o histórico de eventos do CloudTrail, no Guia do usuário do AWS CloudTrail.

Solução

Dependendo do motivo do encerramento, execute uma das seguintes ações:

- **`Client.VolumeLimitExceeded: Volume limit exceeded`** — exclua volumes não utilizados. É possível enviar uma solicitação para aumentar seu limite de volume.
- **`Client.InternalError: Client error on launch`**: verifique se você tem as permissões necessárias para acessar as AWS KMS keys usadas para descriptografar e criptografar volumes. Para obter mais informações, consulte Using key policies in AWS KMS (Como usar políticas de chaves no AWS KMS) no Guia do desenvolvedor do AWS Key Management Service.

Permissões insuficientes

Descrição

Você recebe o erro `"errorMessage": "You are not authorized to perform this operation."` ao tentar iniciar uma nova instância e não é possível iniciá-la.

Causa

Se você receber esse erro ao tentar iniciar uma instância, você não tem as permissões do IAM necessárias para iniciá-la.

As possíveis permissões ausentes incluem:

- `ec2:RunInstances`

- `iam:PassRole`

Outras permissões também podem estar faltando. Para ver a lista de permissões necessárias para iniciar uma instância, consulte o exemplo de políticas do IAM em Exemplo: uso do assistente de início de instância do EC2 e Executar instâncias (RunInstances).

Solução

Como resolver o problema:

- Se você estiver fazendo solicitações como um usuário IAM, verifique se tem as seguintes permissões:
  - `ec2:RunInstances` com um caractere curinga ("*")
  - `iam:PassRole` com o recurso correspondente ao nome de região da Amazon (ARN) da função (por exemplo, `arn:aws:iam::999999999999:role/ExampleRoleName`)
- Se você não tiver as permissões anteriores, edite a política do IAM associada ao perfil ou usuário do IAM para adicionar as permissões necessárias que estão faltando.

Se o problema não for resolvido e um erro de falha na inicialização continuar sendo recebido, você poderá decodificar a mensagem de falha de autorização incluída no erro. A mensagem decodificada inclui as permissões que estão faltando na política do IAM. Para obter mais informações, consulte Como posso decodificar uma mensagem de falha de autorização depois de receber um erro de "UnauthorizedOperation" durante a execução de uma instância do EC2?

Alto uso da CPU logo após a inicialização do Windows (somente para instâncias do Windows)

> **Note**
>
> Esta dica de solução de problemas é dedicada somente para instâncias do Windows.

Se o Windows Update for definido como Verificar se há atualizações, mas permitir que eu escolha fazer download e instalá-las (a configuração de instância padrão), essa verificação poderá consumir entre 50 e 99% da CPU na instância. Se esse consumo de CPU causar problemas para seus aplicativos, você poderá alterar manualmente as configurações do Windows Update no Painel de controle ou usar o seguinte script no campo de dados de usuário do Amazon EC2:

```
reg add "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Auto Update" /v
 AUOptions /t REG_DWORD /d 3 /f net stop wuauserv net start wuauserv
```

Quando você executar esse script, especifique um valor para /d. O valor padrão é 3. Os valores possíveis incluem o seguinte:

1. Nunca verificar se há atualizações
2. Verificar se há atualizações, mas permitir que eu escolha fazer download e instalá-las
3. Fazer download de atualizações, mas permitir que eu escolha fazer download e instalá-las
4. Instalar atualizações automaticamente

Depois de modificar os dados do usuário para sua instância, você poderá executá-la. Para obter mais informações, consulte Run commands on your Windows instance at launch.

Solucionar problemas de interrupção de instâncias do Amazon EC2

Se a instância baseada no Amazon EBS parecer travada no estado `stopping`, o problema pode estar no computador host subjacente.

Para resolver o problema, siga estas etapas:

1. Forçar a interrupção da instância

   Use o console do Amazon EC2 ou a AWS CLI para forçar a interrupção da instância. Para obter as etapas, consulte Forçar a interrupção de uma instância.

   Primeiro, a instância tentará um desligamento normal, o que inclui descarregar os caches e metadados do sistema de arquivos (embora seja possível ignorar o desligamento normal). Se o desligamento normal não for concluído dentro do período de tempo limite, a instância será encerrada à força sem descarregar os caches e os metadados do sistema de arquivos.
2. Após a interrupção forçada

   Execute a verificação do sistema de arquivos e os procedimentos de reparo.

> **Important**
>
> A execução desses procedimentos é crucial porque uma interrupção forçada impede a descarga dos caches e metadados do sistema de arquivos.

3. Se a interrupção forçada falhar

   Se a instância não foi interrompida após dez minutos, faça o seguinte:

   a. Publique uma solicitação de ajuda no AWS re:Post. Para ajudar a agilizar uma resolução, inclua o ID da instância e descreva as etapas que você já realizou.

   b. Alternativamente, se você possui um plano de suporte, crie um caso de suporte técnico no Atendimento ao cliente.

   c. Enquanto espera por assistência, crie uma instância de substituição, se necessário. Para obter as etapas, consulte (Opcional) Criar uma instância de substituição.

Não existe qualquer custo para uso da instância enquanto ela está no estado `stopping` ou em qualquer outro estado, exceto `running`. Você só é cobrado pelo uso da instância quando ela está no estado `running`.

Conteúdo

- Forçar a interrupção de uma instância
- (Opcional) Criar uma instância de substituição

Forçar a interrupção de uma instância

É possível forçar a interrupção de uma instância. Se, após dez minutos, a instância não tiver sido interrompida, publique uma solicitação de ajuda em AWS re:Post. 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.

> **Note**
>
> Usando o console, é possível forçar uma instância a parar apenas enquanto ela está no estado `stopping`. Usando a AWS CLI, é possível forçar uma instância a parar apenas enquanto ela está no estado `pending`, `running` ou `stopping`.

Console

Para forçar uma instância a parar

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 Estado da instância, Forçar parada da instância.

   A opção Force stop instance (Forçar interrupção de instância) estará disponível no console somente se a instância estiver no estado `stopping`. Se a instância estiver em outro estado (exceto `shutting-down` e `terminated`), será possível usar AWS CLI para forçar a interrupção da instância.
4. (Opcional) Para ignorar o desligamento normal do sistema operacional durante a parada forçada, marque a caixa de seleção Ignorar desligamento do sistema operacional.
5. Escolha Forçar parada.

AWS CLI

Para forçar uma instância a parar

Use o comando stop-instances com a opção `--force`.

```
aws ec2 stop-instances \
    --instance-ids i-1234567890abcdef0 \
    --force
```

Para ignorar o desligamento normal do sistema operacional durante a parada forçada, inclua a opção `--skip-os-shutdown`.

```
aws ec2 stop-instances \
    --instance-ids i-1234567890abcdef0 \
```

```
    --force \
    --skip-os-shutdown
```

PowerShell

Para forçar uma instância a parar

Use o cmdlet Stop-EC2Instance e defina `-Enforce` como `true`.

```
Stop-EC2Instance `
    -InstanceId i-1234567890abcdef0 `
    -Enforce $true
```

Para ignorar o desligamento normal do sistema operacional durante a parada forçada, inclua `-SkipOsShutdown $true`.

```
Stop-EC2Instance `
    -InstanceId i-1234567890abcdef0 `
    -Enforce $true `
    -SkipOsShutdown $true
```

(Opcional) Criar uma instância de substituição

Enquanto estiver esperando pela assistência do AWS re:Post ou do Support Center, crie uma instância de substituição, se necessário. Crie uma AMI da instância travada e inicie uma instância usando a nova AMI.

> **Important**
>
> É possívelrá criar uma instância de substituição se a instância travada só produzir as verificações de status do sistema, pois as verificações de status da instância farão com que a AMI copie sobre uma réplica exata do sistema operacional danificado. Depois de confirmar a mensagem de status, crie a AMI e inicie uma instância usando a nova AMI.

Console

Para criar uma instância de substituição

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

2. No painel de navegação, selecione Instances (Instâncias) e selecione a instância travada.
3. Escolha Actions (Ações), Image and templates (Imagem e modelos), Create image (Criar imagem).
4. Na página Create image (Criar imagem), faça o seguinte:

   a. Digite um nome e uma descrição para a AMI.

   b. Desmarque Reinicializar instância.

   c. Escolha Create Image (Criar imagem).

   Para obter mais informações, consulte the section called “Criação de uma AMI usando uma instância”.
5. Execute uma nova instância a partir da AMI e verifique se a instância nova está funcionando.
6. Selecione a instância travada e escolha Ações, Estado da instância e Encerrar (excluir) instância. Se a instância também ficar travada ao ser encerrada, o Amazon EC2 automaticamente forçará o encerramento dela dali a algumas horas.

Caso você não consiga criar uma AMI a partir da instância, conforme descrito no procedimento anterior, configure uma instância de substituição da seguinte forma:

(Alternativa) Para criar uma instância de substituição usando o console

1. Selecione a instância e escolha Description (Descrição), Block devices (Dispositivos de bloco). Selecione cada volume e anote o ID do volume. Note qual é o volume do dispositivo raiz.
2. No painel de navegação, escolha Volumes. Selecione cada volume para a instância e escolha Ações, Criar snapshot.
3. No painel de navegação, selecione Snapshots. Selecione o snapshot que você acabou de criar, e escolha Ações, Criar volume.
4. Execute uma instância com o mesmo sistema operacional da instância travada. Observe o ID do volume e o nome do dispositivo de seu volume do dispositivo raiz.
5. No painel de navegação, escolha Instances (Instâncias), selecione a instância que acabou de executar e escolha Instance state (Estado da instância) e Stop instance (Parar instância).
6. No painel de navegação, selecione Volumes, selecione o volume do dispositivo raiz da instância parada e escolha Ações, Separar volume.

7. Selecione o volume do dispositivo raiz de que você criou usando a instância presa, selecione Actions (Actions), Attach Volume (Associar volume) e associe-o à nova instância como volume raiz (usando o nome do dispositivo que você anotou). Associe todos os volumes adicionais não raiz à instância.
8. No painel de navegação, selecione Instâncias e selecione a instância de substituição. Escolha Instance state (Estado da instância) e Start instance (Iniciar instância). Verifique se a instância está trabalhando.
9. Selecione a instância travada e escolha Estado da instância e Encerrar (excluir) instância. Se a instância também ficar travada ao ser encerrada, o Amazon EC2 automaticamente forçará o encerramento dela dali a algumas horas.

AWS CLI

Para criar uma instância de substituição

1. Crie uma AMI com base na instância travada usando o comando create-image com a opção `--no-reboot`.

```
aws ec2 create-image \
    --instance-id i-1234567890abcdef0 \
    --name "my-replacement-ami" \
    --description "AMI for replacement instance" \
    --no-reboot
```

2. Inicialize uma nova instância com base na AMI recém-criada usando o comando run-instances.
3. Verifique se a nova instância está funcionando.
4. (Opcional) Encerre a instância travada usando o comando terminate-instances.

```
aws ec2 terminate-instances --instance-ids i-1234567890abcdef0
```

PowerShell

Para criar uma instância de substituição

1. Crie uma AMI com base na instância travada usando o cmdlet New-EC2Image e defina `-NoReboot` como `true`.

```
New-EC2Image `
    -InstanceId i-1234567890abcdef0 `
    -Name "my-replacement-ami" `
    -Description "AMI for replacement instance" `
    -NoReboot $true
```

2. Inicialize uma nova instância com base na AMI recém-criada usando o cmdlet New-EC2Instance.
3. Verifique se a nova instância está funcionando.
4. (Opcional) Encerre a instância travada usando o cmdlet Remove-EC2Instance.

```
Remove-EC2Instance -InstanceId i-1234567890abcdef0
```

Solucionar problemas de encerramento de instâncias do Amazon EC2

O ato de desligar ou excluir a instância é conhecido como encerramento da instância. As informações a seguir podem ajudar você a solucionar problemas quando você encerra a instância.

Você não paga por nenhum uso de instância enquanto ela não estiver no estado `running`. Em outras palavras, ao encerrar uma instância, você para de ser cobrado por ela assim que o estado mudar para `shutting-down`.

A instância é encerrada imediatamente

Vários problemas podem fazer com que a sua instância seja encerrada imediatamente na inicialização. Consulte A instância é encerrada imediatamente para obter mais informações.

Encerramento atrasado da instância

Se sua instância permanecer no estado `shutting-down` por mais de alguns minutos, isso pode ser devido a:

- A instância está executando scripts de desligamento.
- Há um problema com o computador host subjacente.

Se ela permanecer no estado `shutting-down` por várias horas, o Amazon EC2 tratará a instância como uma instância travada e a encerrará à força.

Para resolver uma instância bloqueada por conta própria:

1. Encerre a instância à força

   Use o console do Amazon EC2 ou a AWS CLI para forçar o término da instância. Para obter as etapas, consulte Encerrar uma instância à força.

   Primeiro, a instância tentará um desligamento normal, o que inclui descarregar os caches e metadados do sistema de arquivos (embora seja possível ignorar o desligamento normal). Se o desligamento normal não for concluído dentro do período de tempo limite, a instância será encerrada à força sem descarregar os caches e os metadados do sistema de arquivos.
2. Se o término forçado falhar

   Se, após várias horas, a instância não tiver sido encerrada e parecer estar travada no processo de encerramento, faça o seguinte:

   a. Publique uma solicitação de ajuda no AWS re:Post. Para ajudar a agilizar uma resolução, inclua o ID da instância e descreva as etapas que você já realizou.
   b. Alternativamente, se você possui um plano de suporte, crie um caso de suporte técnico no Atendimento ao cliente.

Encerrar uma instância à força

Se parecer que o encerramento da sua instância está travado, você pode forçá-lo. Se, após várias horas, a instância não tiver sido terminada, envie uma solicitação de ajuda para AWS re:Post. 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.

Console

Para terminar uma instância à força

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 Estado da instância e Forçar término da instância.

A opção Forçar término da instância estará disponível no console somente se a instância estiver no estado `stopping`. Se sua instância estiver em outro estado (exceto `shutting-down` e `terminated`), você poderá usar o AWS CLI para forçar o encerramento da instância.

4. (Opcional) Para ignorar o desligamento normal do sistema operacional durante o término forçado, marque a caixa de seleção Ignorar desligamento do sistema operacional.
5. Escolha Forçar término.

AWS CLI

Para terminar uma instância à força

Use o comando terminate-instances com a opção `--force`.

```
aws ec2 terminate-instances \
    --instance-ids i-1234567890abcdef0 \
    --force
```

Para ignorar o desligamento normal do sistema operacional durante o término forçado, inclua a opção `--skip-os-shutdown`.

```
aws ec2 terminate-instances \
    --instance-ids i-1234567890abcdef0 \
    --force \
    --skip-os-shutdown
```

PowerShell

Para terminar uma instância à força

Use o cmdlet Remove-EC2Instance e defina `-Enforce` como `true`.

```
Remove-EC2Instance `
    -InstanceId i-1234567890abcdef0 `
    -Enforce $true
```

Para ignorar o desligamento normal do sistema operacional durante o término forçado, inclua `-SkipOsShutdown $true`.

```
Remove-EC2Instance `
    -InstanceId i-1234567890abcdef0 `
    -Enforce $true `
    -SkipOsShutdown $true
```

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.

Erro: a instância não pode ser encerrada. Modifique seu atributo de instância 'disableApiTermination'

Se você tentar encerrar uma instância e receber a mensagem de erro `The instance i-1234567890abcdef0 may not be terminated. Modify its 'disableApiTermination' instance attribute`, isso indica que a instância foi habilitada para proteção contra encerramento. A proteção contra encerramento impede que a instância seja encerrada acidentalmente.

Você deve desativar a proteção contra encerramento antes de encerrar a instância.

Para obter mais informações, consulte Alterar proteção contra encerramento de instância.

Instâncias executadas ou encerradas automaticamente

De modo geral, os comportamentos a seguir indicam que você usou o Amazon EC2 Auto Scaling, a frota do EC2 ou a frota spot para escalar os recursos de computação automaticamente com base nos critérios que você definiu.

- Você encerra uma instância e uma nova instância é iniciada automaticamente.
- Você inicia uma instância e uma de suas instâncias é encerrada automaticamente.
- Você interrompe uma instância e ela é encerrada e uma nova instância é iniciada automaticamente.

Para interromper a escalabilidade automática, encontre o grupo do Auto Scaling ou a frota que está executando as instâncias e defina sua capacidade como 0 ou exclua-o.

Solucionar problemas de uma instância inacessível do Amazon EC2

As informações a seguir podem ajudar você a solucionar problemas de instâncias inacessíveis do Amazon EC2. É possível obter capturas de tela ou acessar o console para ajudar a diagnosticar problemas e determinar se é necessário reinicializar a instância. Para instâncias inacessíveis do Windows, solucione o problema analisando as capturas de tela retornadas pelo serviço.

Conteúdo

- Reinicialização da instância
- Saída do console da instância
- Fazer uma captura de tela de uma instância inacessível
- Capturas de tela comuns para solucionar problemas de instâncias inacessíveis do Windows
- Recuperação da instância quando um computador host falhar
- A instância apareceu offline e foi reiniciada inesperadamente

Reinicialização da instância

A capacidade de reinicializar instâncias que de outra forma seriam inacessíveis é valiosa para a solução de problemas e o gerenciamento geral de instâncias.

Assim como poderá redefinir um computador pressionando o botão de restauração, você pode também redefinir instâncias do EC2 usando o console, a CLI ou a API do Amazon EC2. Para obter mais informações, consulte Reinicializar uma instância do Amazon EC2.

Saída do console da instância

A saída do console é uma ferramenta valiosa para o diagnóstico de problemas. É especialmente útil para resolver problemas de kernel e problemas de configuração de serviço que possam fazer com que uma instância seja encerrada ou torne-se inalcançável antes de seu daemon SSH ser iniciado.

- Instâncias do Linux: a saída do console da instância exibe exatamente o que seria mostrado em um monitor físico conectado 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, reinicializar e finalizar). A saída publicada não é atualizada continuamente; somente quando for provável que seja do valor principal.

- Instâncias do Windows: a saída do console da instância inclui os três últimos erros do log de eventos do sistema.

Somente o proprietário da instância pode acessar a saída do console.

É possível recuperar a última saída do console serial durante o ciclo de vida da instância. Essa opção só é compatível com instâncias baseadas em Nitro.

Console

Para obter o resultado do console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação à esquerda, escolha Instances (Instâncias).
3. Selecione a instância.
4. Escolha Actions (Ações), Monitor and troubleshoot (Monitorar e solucionar problemas), Get system log Obter log do sistema.

AWS CLI

Para obter o resultado do console

Use o comando get-console-output.

```
aws ec2 get-console-output --instance-id i-1234567890abcdef0
```

PowerShell

Para obter o resultado do console

Use o cmdlet Get-EC2ConsoleOutput.

```
Get-EC2ConsoleOutput -InstanceId i-1234567890abcdef0
```

Fazer uma captura de tela de uma instância inacessível

Caso não seja possível realizar a conexão com a instância, você pode capturar uma captura de tela da instância e visualizá-la como uma imagem. A imagem pode dar visibilidade quanto ao status da instância e permite uma solução de problemas mais rápida.

É possível gerar capturas de tela enquanto a instância estiver em execução ou após haver falha. A imagem é gerada em formato JPG e não é maior que 100 KB. Não há custo de transferência de dados para a captura de tela.

Limitações

Este recurso não é compatível com as seguintes instâncias:

- Instâncias bare metal (instâncias do tipo `*.metal`)
- A instância está usando um driver NVIDIA GRID
- Instâncias com processadores Graviton baseados em ARM
- Instâncias Windows em AWS Outposts
- Instâncias do Windows nas zonas locais da AWS

Suporte da região da

Esse atributo não está disponível nas seguintes regiões:

- Ásia-Pacífico (Tailândia)
- México (Central)
- Regiões do GovCloud

Console

Para obter uma captura de tela de uma instância

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação à esquerda, escolha Instances (Instâncias).
3. Selecione a instância a ser capturada.
4. Escolha Actions (Ações), Monitor and troubleshoot (Monitorar e solucionar problemas), Get instance screenshot (Obter captura de tela da instância).
5. Escolha Download ou clique com o botão direito do mouse na imagem para fazer download e salvá-la.

AWS CLI

Para obter uma captura de tela de uma instância

Use o comando get-console-screenshot. A saída é codificada em base64.

```
aws ec2 get-console-screenshot --instance-id i-1234567890abcdef0
```

PowerShell

Para obter uma captura de tela de uma instância

Use o cmdlet Get-EC2ConsoleScreenshot. A saída é codificada em base64.

```
Get-EC2ConsoleScreenshot -InstanceId i-1234567890abcdef0
```

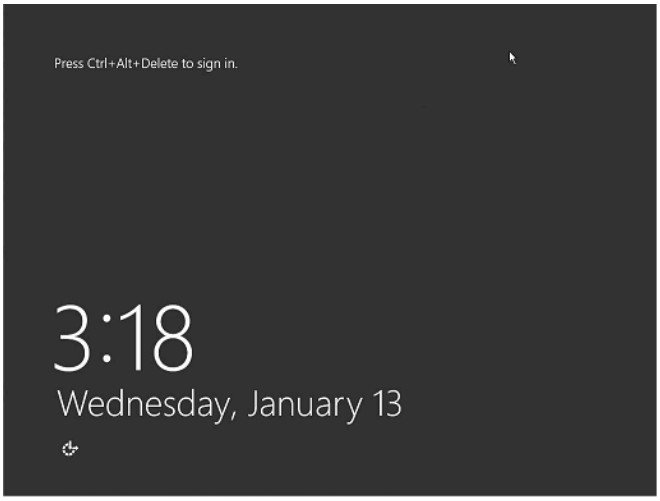
Capturas de tela comuns para solucionar problemas de instâncias inacessíveis do Windows

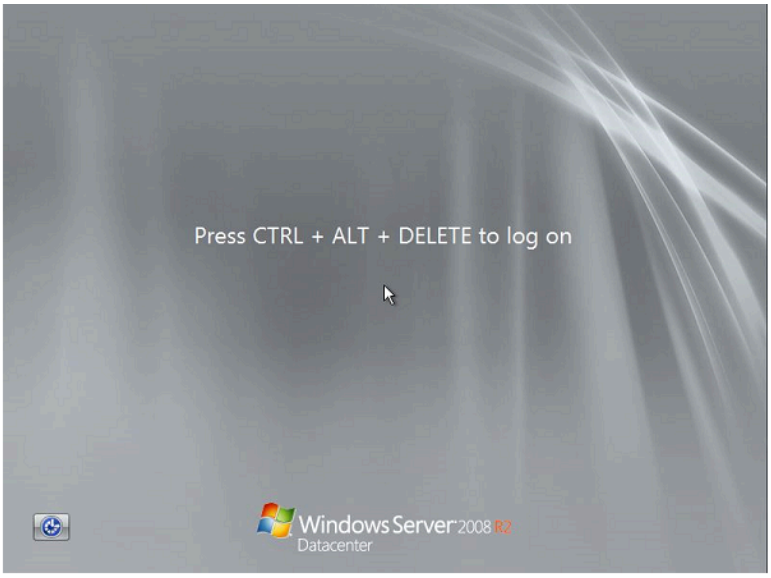
É possível usar as informações a seguir para ajudar a solucionar problemas de uma instância inacessível do Windows com base nas capturas de tela retornadas pelo serviço.

- Tela de login (Ctrl+Alt+Delete)
- Tela de console de recuperação
- Tela do gerenciador de inicialização do Windows
- Tela Sysprep
- Tela de preparação
- Tela do Windows Update
- Chkdsk

Tela de login (Ctrl+Alt+Delete)

O serviço de captura de tela de console retornou o seguinte.





Se uma instância se tornar inacessível durante o login, talvez haja um problema com a configuração de rede ou com os Serviços de Área de Trabalho Remota do Windows. Uma instância também poderá não responder se um processo estiver usando grandes quantidades de CPU.

Configuração de rede

Use as seguintes informações para verificar se as configurações da AWS, do Microsoft Windows e da rede local (ou on-premises) não estão bloqueando o acesso à instância.

AWSConfiguração de rede da

Configuração	Verificar
Configuração do security group	Verifique se a porta 3389 está aberta para o security group. Verifique se você está se conectando ao endereço IP público certo. Se a instância não foi associada a um IP elástico, o IP público será alterado depois que a instância for interrompida/iniciada. Para obter mais informações, consulte O Remote Desktop não pode se conectar ao computador remoto.
Configuração da VPC (Network ACLs)	Verifique se a lista de controle de acesso (ACL) para sua Amazon VPC não está bloqueand o acesso. Para obter informações, consulte

Configuração	Verificar
	Network ACLs no Guia do usuário da Amazon VPC.
Configuração de VPN	Se você estiver se conectando à VPC usando uma rede virtual privada (VPN), verifique a conectividade do túnel VPN. Para obter mais informações, consulte Troubleshooting AWS Client VPN: Tunnel connectivity issues to a VPC.

Configuração de rede do Windows

Configuração	Verificar
Firewall do Windows	Verifique se o firewall do Windows não está bloqueando as conexões com a sua instância . Desabilite o firewall do Windows como descrito no item 7 da seção sobre solução de problemas do Remote Desktop, O Remote Desktop não pode se conectar ao computador remoto.
Configuração avançada de TCP/IP (uso de IP estático)	A instância pode não responder porque você configurou um endereço IP estático. Para uma VPC, crie uma interface de rede e anexe-a à instância.

Configuração de rede local ou on-premises

Verifique se uma configuração de rede local não está bloqueando o acesso. Tente se conectar a uma outra instância na mesma VPC onde se encontra a instância inacessível. Se você não conseguir acessar outra instância, trabalhe com o administrador de rede local para determinar se uma política local está restringindo o acesso.

Problemas com o Remote Desktop Services

Se não for possível acessar a instância durante o login, talvez haja um problema com os Serviços de Área de Trabalho Remota (RDS - Remote Desktop Services) na instância.

> **Tip**
>
> É possível usar o runbook `AWSSupport-TroubleshootRDP` para verificar e modificar várias configurações que podem afetar as conexões do Remote Desktop Protocol (RDP). Para obter mais informações, consulte `AWSSupport-TroubleshootRDP` na Referência do runbook do AWS Systems Manager Automation.

Configuração do Remote Desktop Services

Configuração	Verificar
O RDS está em execução	Verifique se o RDS está em execução na instância. Conecte-se à instância usando o snap-in de serviços do Microsoft Management Console (MMC) (`services.msc`). Na lista de serviços, verifique se o Remote Desktop Services está Running (Em execução). Se não estiver, inicie-o e defina o tipo de inicialização como Automático. Se você não puder se conectar à instância usando o snap-in Services, desanexe o volume raiz da instância, crie um snapshot do volume ou crie uma AMI dele, anexe o volume original a outra instância na mesma zona de disponibilidade como um volume secundário e modifique a chave de Registro Start. Ao terminar, anexe novamente o volume raiz à instância original.
O RDS está habilitado	Mesmo se o serviço tiver sido iniciado, ele pode estar desabilitado. Desanexe o volume raiz da instância, crie um snapshot do volume ou crie uma AMI dele, anexe o volume original a outra instância na mesma zona de disponibilidade como um volume secundário e habilite o serviço modificando a chave do registro Terminal Server (Servidor de terminal) conforme descrito em Habilitar a área de trabalho remota em uma instância do EC2 com o registro remoto.

Configuração	Verificar
	Ao terminar, anexe novamente o volume raiz à instância original.

Alto uso da CPU

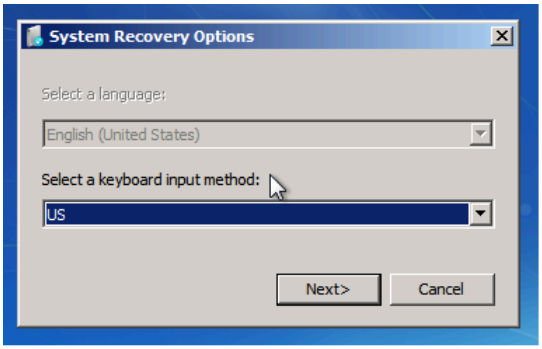
Verifique a métrica CPUUtilization (máximo) em sua instância usando o Amazon CloudWatch. Se CPUUtilization (máximo) for um número alto, aguarde a desativação da CPU e tente se conectar novamente. A utilização elevada da CPU pode ser causada por:

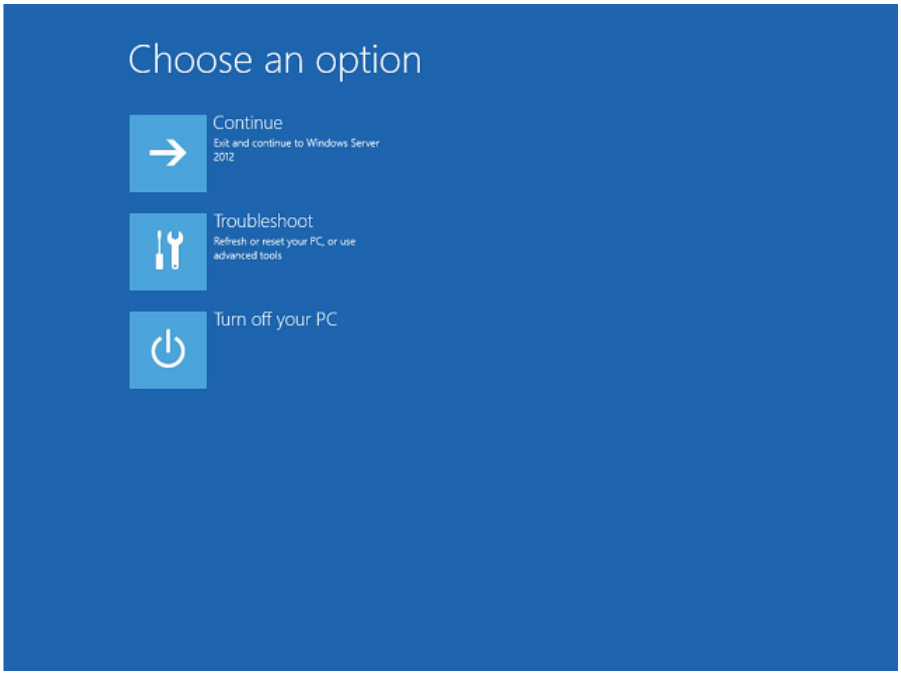
- Atualizações do Windows
- Verificação de software de segurança
- Script de inicialização personalizado
- Programador de tarefas

Para obter mais informações, consulte Obter as estatísticas de um recurso específico no Guia do usuário do Amazon CloudWatch. Para obter mais dicas sobre solução de problemas, consulte Alto uso da CPU logo após a inicialização do Windows (somente para instâncias do Windows).

Tela de console de recuperação

O serviço de captura de tela de console retornou o seguinte.





O sistema operacional pode ser inicializado no console de recuperação e travar nesse estado se `bootstatuspolicy` não estiver definido como `ignoreallfailures`. Use o procedimento a seguir para alterar a configuração de `bootstatuspolicy` para `ignoreallfailures`.

Por padrão, a configuração de políticas para AMIs públicas do Windows fornecidas pela AWS é definida como `ignoreallfailures`.

1. Interrompa a instância inacessível.
2. Crie um snapshot de novo volume raiz. O volume raiz é anexado à instância como `/dev/sda1`.

   Desanexe o volume raiz da instância inacessível, crie um snapshot do volume ou crie uma AMI dele e anexe-a a outra instância na mesma zona de disponibilidade que um volume secundário.

   > **Warning**
   >
   > Se sua instância temporária e instância original tiverem sido iniciadas usando a mesma AMI, será necessário executar etapas adicionais ou você não poderá iniciar a instância original após restaurar o volume raiz, por causa de uma colisão de assinatura de disco. Se você precisar criar uma instância temporária com base na mesma AMI, siga as etapas em Colisão de assinatura em disco para evitar uma colisão de assinatura de disco.

> Como alternativa, selecione uma AMI diferente para a instância temporária. Por exemplo, se a instância original usa uma AMI para Windows Server 2016, inicie a instância temporária usando uma AMI para Windows Server 2019.

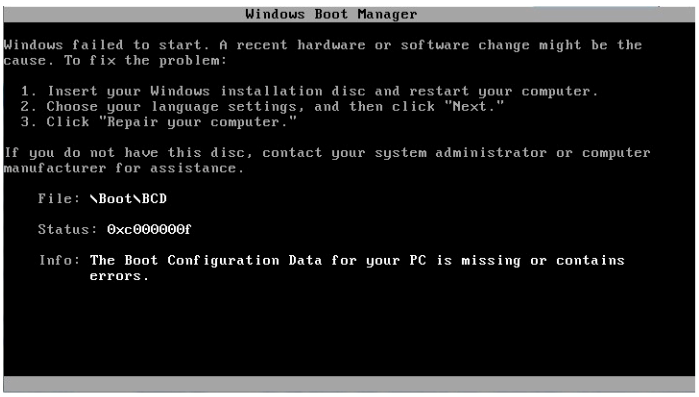
3. Faça login na instância e execute o seguinte comando em um prompt de comando para alterar a configuração de `bootstatuspolicy` para `ignoreallfailures`.

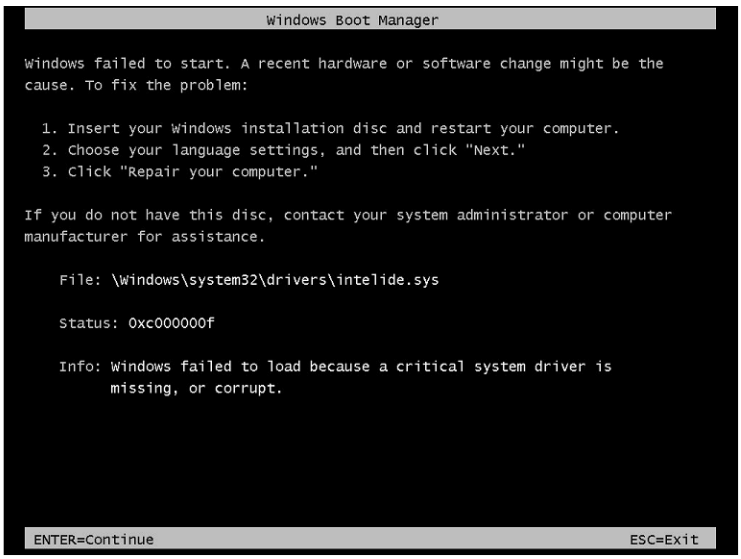
```
bcdedit /store Drive Letter:\boot\bcd /set {default} bootstatuspolicy
 ignoreallfailures
```

4. Reanexe o volume à instância inacessível e inicie a instância novamente.

Tela do gerenciador de inicialização do Windows

O serviço de captura de tela de console retornou o seguinte.

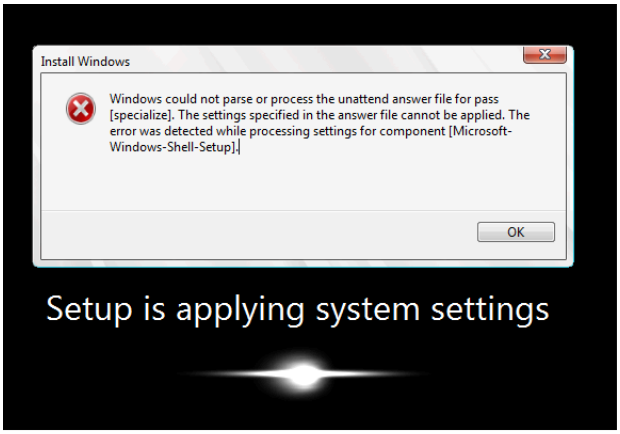


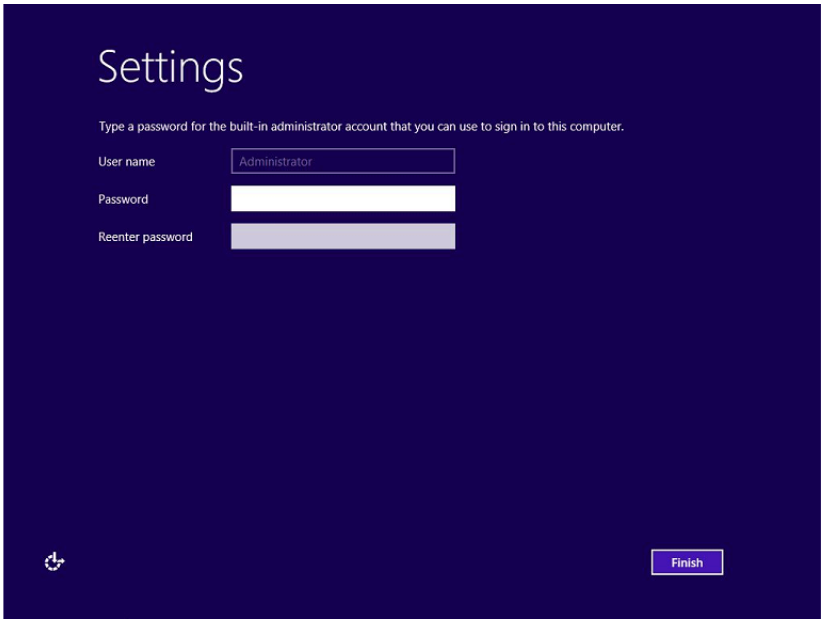


O sistema operacional experimentou um dano fatal no arquivo de sistema e/ou no Registro. Quando a instância trava nesse estado, é necessário recuperá-la de uma AMI de backup recente ou executar uma instância de substituição. Se você precisar acessar dados na instância, desanexe todos os volumes raiz da instância inacessível, crie um snapshot desses volumes ou crie uma AMI deles e anexe-os a outra instância na mesma zona de disponibilidade como um volume secundário.

Tela Sysprep

O serviço de captura de tela de console retornou o seguinte.

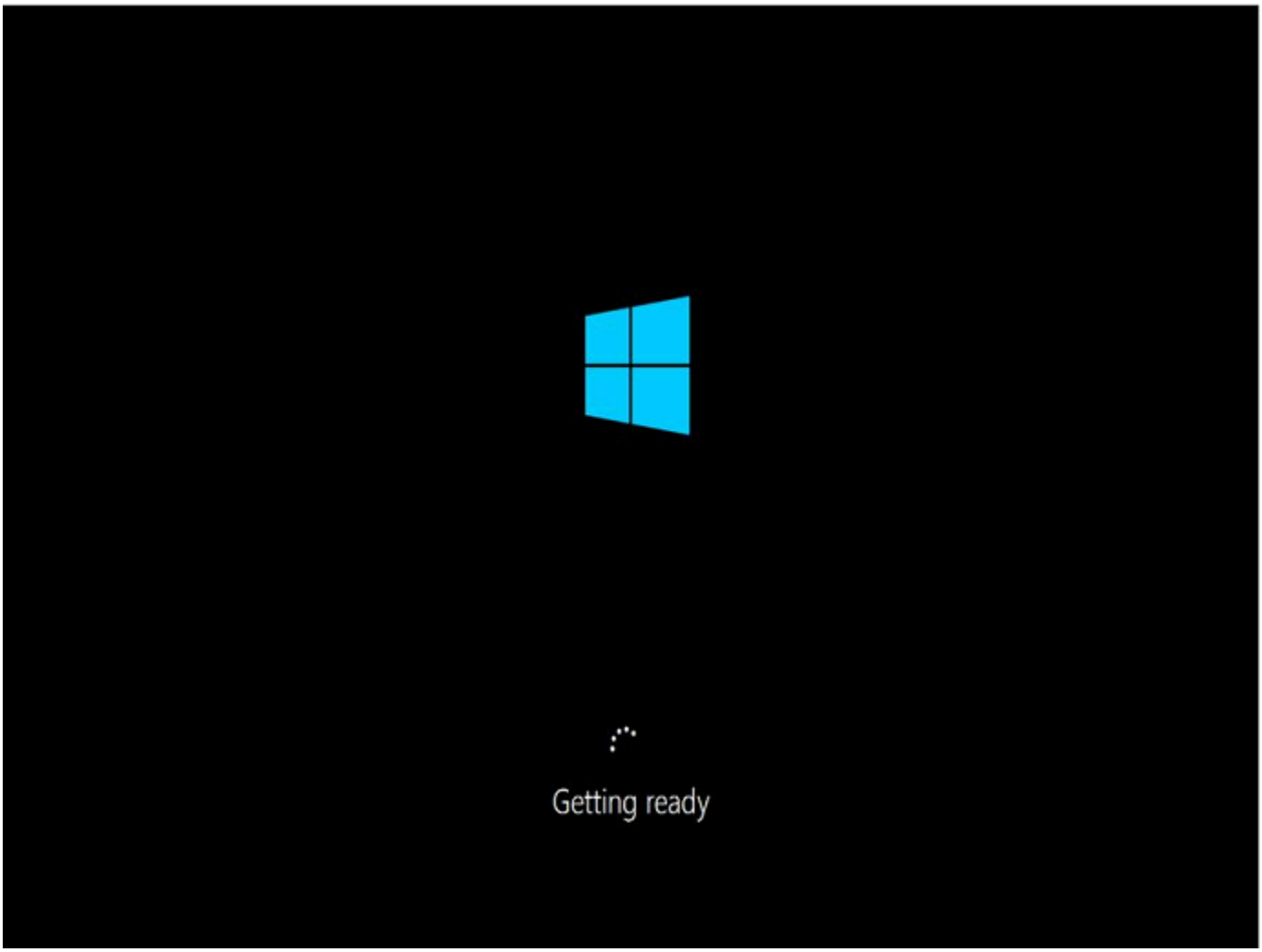




Será possível ver essa tela se você não tiver usado o EC2Config Service para chamar Sysprep ou se o sistema operacional falhar ao executar o Sysprep. É possível redefinir a senha usando o EC2Rescue. Caso contrário, consulte Criar uma AMI do Amazon EC2 usando o Sysprep do Windows.

Tela de preparação

O serviço de captura de tela de console retornou o seguinte.



Atualize o Instance Console Screenshot Service repetidamente para verificar se o anel de andamento está girando. Se o anel estiver girando, aguarde a inicialização do sistema operacional. Também é possível verificar a métrica CPUUtilization (máximo) em sua instância usando o Amazon CloudWatch para ver se o sistema operacional está ativo. Se o anel de andamento não estiver girando, a instância poderá travar no processo de inicialização. Reinicialize a instância. Se a reinicialização não resolver o problema, recupere a instância de uma AMI de backup recente ou execute uma instância de substituição. Se você precisar acessar os dados na instância, desanexe o volume raiz da instância inacessível, crie um snapshot do volume ou crie uma AMI dele. Em seguida, anexe-o a outra instância na mesma zona de disponibilidade que o volume secundário.

Tela do Windows Update

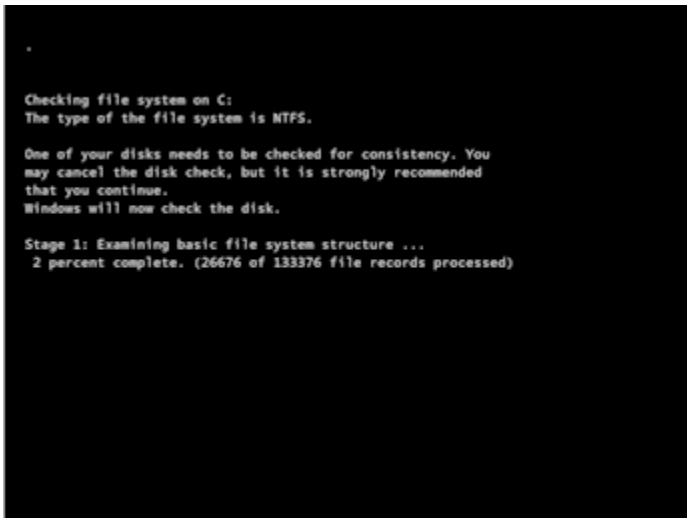
O serviço de captura de tela de console retornou o seguinte.

O processo do Windows Update está atualizando o Registro. Aguarde o término da atualização. Não reinicialize nem interrompa a instância, pois isso pode causar danos aos dados durante a atualização.

> **Note**
>
> O processo do Windows Update pode consumir recursos no servidor durante a atualização. Se você tiver esse problema com frequência, considere usar um tipo de instância e volumes do EBS mais rápidos.

Chkdsk

O serviço de captura de tela de console retornou o seguinte.



O Windows está executando a ferramenta de sistema chkdsk na unidade para verificar a integridade do sistema de arquivos e corrigir os erros lógicos do sistema de arquivos. Aguarde a conclusão do processo.

Recuperação da instância quando um computador host falhar

Se houver um problema irrecuperável com o hardware de um computador host subjacente, a AWS poderá programar um evento de interrupção da instância. Você será notificado desse evento com antecedência, por e-mail.

Para recuperar uma instância baseada no 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 Início e interrupção de instâncias do Amazon EC2.

Para recuperar uma instância com volume raiz do tipo armazenamento de instância que está em um host com falha

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.

A instância apareceu offline e foi reiniciada inesperadamente

Se sua instância parecer ter ficado offline e depois reiniciada inesperadamente, ela pode ter passado por uma recuperação automática de instância. Isso acontece quando a AWS detecta que a instância não está disponível devido a um problema subjacente de hardware ou software, e a recuperação automática simplificada ou a recuperação baseada em ações do CloudWatch está ativada na instância.

Durante o processo de recuperação, a AWS tenta restaurar a disponibilidade da instância migrando-a para um hardware diferente. Para verificar se a recuperação automática da instância ocorreu em sua instância, consulte Verificar se ocorreu a recuperação automática da instância.

> **Note**
>
> Se sua workload ou aplicação não estiver respondendo, verifique se ela está sendo executada na instância. Se não estiver, inicie-a manualmente. Para evitar esse problema no futuro, implemente um plano de recuperação para garantir que sua workload ou aplicação funcione adequadamente após a recuperação da instância.

Solucionar problemas de conexão com a instância do Linux do Amazon EC2

As informações e os erros comuns a seguir podem ajudar você a solucionar problemas de conexão com a instância Linux.

Problemas de conectividade

- Causas comuns de problemas de conexão
- Erro ao se conectar à sua instância: limite de tempo da conexão atingido
- Erro: não foi possível carregar a chave ... Esperando: QUALQUER CHAVE PRIVADA
- Erro: Chave do usuário não reconhecida pelo servidor
- Erro: permissão negada ou conexão fechada pela porta 22 de [instância]
- Erro: arquivo de chave privada desprotegido
- Erro: a chave privada deve começar com "-----BEGIN RSA PRIVATE KEY-----" e terminar com "-----END RSA PRIVATE KEY-----"
- Erro: falha na verificação de chaves do host
- Erro: o servidor recusou nossa chave ou não há métodos de autenticação compatíveis
- Não é possível fazer o ping da instância
- Erro: Server unexpectedly closed network connection (A conexão de rede foi fechada inesperadamente pelo servidor)
- Erro: falha na validação da chave do host para EC2 Instance Connect
- Não é possível conectar a uma instância Ubuntu usando o EC2 Instance Connect

- Perdi minha chave privada. Como posso me conectar à instância?

Causas comuns de problemas de conexão

Recomendamos que você comece a solucionar problemas de conexão de instâncias verificando se realizou com precisão as tarefas a seguir.

Verificar o nome de usuário da instância

É possível se conectar à instância usando o nome de usuário da conta de usuário ou o nome de usuário padrão da AMI que você usou para iniciar a instância.

- Obtenha o nome de usuário da sua conta de usuário.

  Para obter mais informações sobre como criar uma conta de usuário, consulte Gerenciar usuários do sistema na instância do Linux do Amazon EC2.
- Obtenha o nome de usuário padrão da AMI que você usou para iniciar a instância.

A AMI usada para iniciar a instância	Nome de usuário padrão
Amazon Linux	`ec2-user`
CentOS	`centos` ou `ec2-user`
Debian	`admin`
Fedora	`fedora` ou `ec2-user`
FreeBSD	`ec2-user`
RHEL	`ec2-user` ou `root`
SUSE	`ec2-user` ou `root`
Ubuntu	`ubuntu`
Oracle	`ec2-user`
Bitnami	`bitnami`
Rocky Linux	`rocky`

A AMI usada para iniciar a instância	Nome de usuário padrão
Outros	Verificar com o provedor de AMI

Verificar se as regras do grupo de segurança permitem tráfego

Verifique se o grupo de segurança associado à instância permite tráfego SSH de entrada do endereço IP. O grupo de segurança padrão para a VPC não permite o tráfego SSH de entrada por padrão. O grupo de segurança criado pelo assistente de execução de instância permite o tráfego SSH de entrada por padrão. Para ver as etapas para adicionar uma regra para o tráfego SSH de entrada à sua instância do Linux, consulte Regras para se conectar a instâncias pelo computador. Para obter as etapas de verificação, consulte Erro ao se conectar à sua instância: limite de tempo da conexão atingido.

Verificar se a instância está pronta

Depois que você inicia uma instância, pode demorar alguns minutos para que ela fique pronta para aceitar solicitações de conexão. Verifique a instância para se certificar de que ela está sendo executada e passou em suas verificações de status.

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Instâncias e, em seguida, sua instância.
3. Verifique o seguinte:

    a. Na coluna Instance state (Estado da instância), verifique se sua instância está no estado `running`.

    b. Na coluna Verificação de status, verifique se sua instância passou nas duas verificações de status.

Verifique se você atendeu a todos os pré-requisitos para se conectar

Certifique-se de ter todas as informações necessárias para se conectar. Para obter mais informações, consulte Conectar-se à instância do Linux usando SSH.

Conectar-se do Linux ou do macOS

Se o sistema operacional do computador local for Linux ou macOS X, verifique os seguintes pré-requisitos específicos para conexão com uma instância do Linux:

- Cliente SSH

- EC2 Instance Connect
- AWS Systems Manager Session Manager do

Conectar do Windows

Se o sistema operacional do computador local for Windows, verifique os seguintes pré-requisitos específicos para conexão com uma instância do Linux:

- OpenSSH
- PuTTY
- AWS Systems Manager Session Manager do
- Subsistema Windows para Linux

Verificar se a instância é uma instância gerenciada

Não são permitidas conexões iniciadas pelo usuário para instâncias gerenciadas. Para determinar se a instância é gerenciada, encontre o campo Gerenciada da instância. Se o valor for true, essa é uma instância gerenciada. Para obter mais informações, consulte Instâncias gerenciadas do Amazon EC2.

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 de grupo de segurança que permita tráfego de entrada proveniente do endereço IPv4 público do seu computador local na porta adequada.

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Instâncias e, em seguida, sua instância.
3. Na guia Security (Segurança) na parte inferior da página do console, em Inbound rules (Regras de entrada), verifique a lista de regras que estão em vigor para a instância selecionada. Verifique se existe uma regra que permita tráfego do computador local para a porta 22 (SSH).

   Se seu grupo de segurança não tiver uma regra que permita tráfego de entrada proveniente do seu computador local, adicione uma regra para seu grupo de segurança. Para obter mais informações, consulte Regras para se conectar a instâncias pelo computador.

4. Para a regra que permite tráfego de entrada, verifique o campo Source (Origem). Se o valor for um só endereço IP e se o endereço IP não for estático, um novo endereço IP será atribuído sempre que você reiniciar o computador. Isso fará com que a regra não inclua o tráfego de endereço IP do seu computador. Talvez o endereço IP não seja estático se seu computador estiver em uma rede corporativa, se você estiver se conectando por um provedor de serviços de Internet (ISP), ou se seu endereço IP do computador for dinâmico e mudar sempre que você reiniciar o computador. Para garantir que a regra do grupo de segurança permita o tráfego de entrada do computador local, em vez de especificar um único endereço IP para Source (Origem), em vez disso, especifique o intervalo de endereços IP usado por seus computadores cliente.

   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 Networking (Redes), anote os valores para VPC ID (ID da VPC) e Subnet ID (ID de sub-rede).
4. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
5. No painel de navegação, escolha Gateways da Internet. Verifique se há um gateway de internet associado à sua VPC. Caso contrário, escolha Create internet gateway (Criar gateway da Internet), insira um nome para o gateway da Internet e escolha Create internet gateway (Criar gateway da Internet). Em seguida, para o gateway da internet criado, escolha Actions (Ações), Attach to VPC (Anexar à VPC), selecione sua VPC e, em seguida, escolha Attach internet gateway (Anexar gateway da internet)para anexá-lo à sua VPC.
6. No painel de navegação, selecione Sub-redes e selecione sua sub-rede.
7. Na guia Route tabl (Tabela de rotas), verifique se há uma rota com `0.0.0.0/0` como destino e o gateway da Internet para sua VPC como alvo. Se você estiver se conectando à sua instância usando o endereço IPv6, verifique se há uma rota para todo o tráfego IPv6 (`::/0`) que aponta para o gateway de Internet. Caso contrário, faça o seguinte:

a. Escolha o ID da tabela de rotas (rtb-xxxxxxxx) para navegar para a tabela de rotas.
b. Na guia Routes (Rotas), escolha Edit routes (Editar rotas). Escolha Add route (Adicionar rota), use `0.0.0.0/0` como o destino, e o gateway da Internet como o destino. Para IPv6, escolha Add route (Adicionar rota), use `::/0` como o destino, e o gateway da Internet como o destino.
c. Escolha Save routes (Salvar rotas).

Verifique a lista de controle de acesso (ACL) da rede para a sub-rede.

As ACLs da rede devem permitir tráfego SSH de entrada do seu endereço IP local na porta 22. Também deve permitir tráfego de saída para as portas efêmeras (1024-65535).

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Sub-redes.
3. Selecione a sub-rede.
4. Na guia Network ACL (ACL da rede), em Inbound rules,(Regras de entrada), verifique se as regras permitem tráfego de entrada na porta obrigatória de seu computador. Caso contrário, exclua ou modifique a regra que está bloqueando tráfego.
5. Em Outbound rules (Regras de saída), verifique se as regras permitem tráfego nas portas efêmeras para seu computador. Caso contrário, exclua ou modifique a regra que está bloqueando tráfego.

Caso seu computador esteja em uma rede corporativa

Pergunte ao administrador da rede se o firewall interno permite tráfego de entrada e saída do seu computador na porta 22.

Se você tiver um firewall no computador, verifique se ele permite tráfego de entrada e saída do computador na porta 22.

Verifique se sua instância tem um endereço IPv4 público.

Se não tiver, associe um endereço IP elástico à sua instância. Para obter mais informações, consulte Endereços IP elásticos.

Verifique a carga de CPU na sua instância; o servidor pode estar sobrecarregado.

AWSA fornece automaticamente dados, como status de métricas e instâncias de Amazon CloudWatch, que é possível usar para ver quanta carga de CPU está na sua instância e, caso necessário, ajusta como suas cargas são manuseadas. Para obter mais informações, consulte Monitorar instâncias usando o CloudWatch.

- Se sua carga for variável, será possível 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 Alterações no tipo de instância do Amazon EC2.

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 grupo de segurança devem permitir tráfego de entrada do endereço IPv6 local na porta 22.
- As regras de Network ACL devem permitir tráfego de IPv6 de entrada e saída.
- Se você executou a instância de uma AMI mais antiga, ela pode não estar configurada para DHCPv6 (endereços IPv6 não são automaticamente reconhecidos na interface de rede). Para obter mais informações, consulte Configurar o IPv6 em suas instâncias no Guia do usuário da Amazon VPC.
- Seu computador local deve ter um endereço IPv6 e ser configurado para usar IPv6.

Erro: não foi possível carregar a chave ... Esperando: QUALQUER CHAVE PRIVADA

Se você tentar se conectar à sua instância e obter a mensagem de erro `unable to load key ... Expecting: ANY PRIVATE KEY`, o arquivo no qual a chave privada está armazenada foi configurado incorretamente. Se o arquivo da chave privada terminar em `.pem`, ele ainda poderá estar configurado incorretamente. Uma possível causa para um arquivo da chave privada configurado incorretamente é a ausência de um certificado.

Se o arquivo da chave privada estiver configurado incorretamente, siga estas etapas para solucionar o erro:

1. Crie um novo par de chaves. Para obter mais informações, consulte Criar um par de chaves usando o Amazon EC2.

   > **Note**
   >
   > Como alternativa, é possível criar um novo par de chaves usando uma ferramenta de terceiros. Para obter mais informações, consulte Criar um par de chaves usando uma ferramenta de terceiros e importe a chave pública para o Amazon EC2.

2. Adicione o novo par de chaves à sua instância. Para obter mais informações, consulte Perdi minha chave privada. Como posso me conectar à instância?.
3. Conecte-se à instância usando o novo par de chaves.

Erro: Chave do usuário não reconhecida pelo servidor

Se você usar o SSH para conectar à sua instância

- Use `ssh -vvv` para obter o triplo de informações de depuração detalhadas (verbose) ao se conectar:

  ```
  ssh -vvv -i path/key-pair-name.pem instance-user-
  name@ec2-203-0-113-25.compute-1.amazonaws.com
  ```

  O exemplo de saída a seguir demonstra o que é possível 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: boguspem.pem ((nil))
debug1: Authentications that can continue: publickey
debug3: start over, passed a different list publickey
debug3: preferred gssapi-keyex,gssapi-with-mic,publickey,keyboard-
interactive,password
debug3: authmethod_lookup publickey
debug3: remaining preferred: keyboard-interactive,password
debug3: authmethod_is_enabled publickey
debug1: Next authentication method: publickey
debug1: Trying private key: boguspem.pem
debug1: read PEM private key done: type RSA
debug3: sign_and_send_pubkey: RSA 9c:4c:bc:0c:d0:5c:c7:92:6c:8e:9b:16:e4:43:d8:b2
debug2: we sent a publickey packet, wait for reply
debug1: Authentications that can continue: publickey
debug2: we did not send a packet, disable method
debug1: No more authentication methods to try.
Permission denied (publickey).
```

Se você usar o PuTTY para se conectar à instância

- Verifique se o arquivo de chave privada (.pem) foi convertido para o formato reconhecido pelo PuTTY (.ppk). Para obter mais informações sobre a conversão da sua chave privada, consulte Conectar-se à instância do Linux usando PuTTY.

  > **Note**
  >
  > No PuTTYgen, carregue o arquivo de chave privada e selecione Salvar chave privada em vez de Gerar.

- Verifique se você está se conectando com o nome de usuário apropriado para sua AMI. Insira o nome de usuário na caixa Nome do host na janela Configuração do PuTTY.

A AMI usada para iniciar a instância	Nome de usuário padrão
Amazon Linux	`ec2-user`
CentOS	`centos` ou `ec2-user`

A AMI usada para iniciar a instância	Nome de usuário padrão
Debian	`admin`
Fedora	`fedora` ou `ec2-user`
FreeBSD	`ec2-user`
RHEL	`ec2-user` ou `root`
SUSE	`ec2-user` ou `root`
Ubuntu	`ubuntu`
Oracle	`ec2-user`
Bitnami	`bitnami`
Rocky Linux	`rocky`
Outros	Verificar 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 obter mais informações, consulte Regras para se conectar a instâncias pelo computador.

Erro: permissão negada ou conexão fechada pela porta 22 de [instância]

Se você se conectar à instância usando SSH e encontrar qualquer um dos erros `Host key not found in [directory]`, `Permission denied (publickey)`, `Authentication failed, permission denied` ou `Connection closed by [instance] port 22`, verifique se está utilizando o nome de usuário correto para sua AMI e se especificou a chave privada adequada (arquivo `.pem`)) para a instância.

Os nomes de usuários apropriados são os seguintes:

A AMI usada para iniciar a instância	Nome de usuário padrão
Amazon Linux	`ec2-user`

A AMI usada para iniciar a instância	Nome de usuário padrão
CentOS	`centos` ou `ec2-user`
Debian	`admin`
Fedora	`fedora` ou `ec2-user`
FreeBSD	`ec2-user`
RHEL	`ec2-user` ou `root`
SUSE	`ec2-user` ou `root`
Ubuntu	`ubuntu`
Oracle	`ec2-user`
Bitnami	`bitnami`
Rocky Linux	`rocky`
Outros	Verificar 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/key-pair-name.pem instance-user-
name@ec2-203-0-113-25.compute-1.amazonaws.com
```

Confirme se você está usando um arquivo de chave privada que corresponde ao par de chaves que selecionou ao executar a instância.

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Instances (Instâncias) e, em seguida, selecione sua instância.
3. Na guia Details (Detalhes), em Instance details (Detalhes da instância), verifique o valor do Nome do par de chaves.

4. Se você não tiver especificado um par de chaves ao executar a instância, pode encerrar a instância e executar uma nova, especificando um par de chaves. Se essa for uma instância que você está usando mas não tiver mais o arquivo `.pem` para seu par de chaves, pode substituir o par de chaves por um novo. Para obter mais informações, consulte Perdi minha chave privada. Como posso me conectar à instância?.

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/`*`instance-user-name`*`/.ssh/authorized_keys` devem ser limitadas somente ao proprietário.

Para verificar as permissões na sua instância

1. Pare sua instância e separe o volume do dispositivo raiz. Para obter mais informações, consulte Início e interrupção de instâncias do Amazon EC2.
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.
3. Conecte-se à instância temporária, crie um ponto de montagem e monte o volume associado.
4. Na instância temporária, verifique as permissões do diretório `/home/`*`instance-user-name`*`/` do volume associado. Se necessário, ajuste as permissões da seguinte forma:

```
[ec2-user ~]$ chmod 600 mount_point/home/instance-user-name/.ssh/authorized_keys
```

```
[ec2-user ~]$ chmod 700 mount_point/home/instance-user-name/.ssh
```

```
[ec2-user ~]$ chmod 700 mount_point/home/instance-user-name
```

5. Desmonte o volume, separe-o da instância temporária e reassocie-o à instância original. Especifique o nome correto do dispositivo para o volume do dispositivo raiz; por exemplo, `/dev/xvda`.
6. Execute sua instância. Se você não precisar mais da instância temporária, pode encerrá-la.

Erro: arquivo de chave privada desprotegido

Seu arquivo de chave privada deve estar protegido contra operações de leitura e gravação por parte de qualquer outro usuário. Se sua chave privada puder ser lida ou gravada por qualquer pessoa menos você, o SSH ignorará sua chave e você verá a mensagem de advertência abaixo.

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@         WARNING: UNPROTECTED PRIVATE KEY FILE!          @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Permissions 0777 for '.ssh/my_private_key.pem' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
bad permissions: ignore key: .ssh/my_private_key.pem
Permission denied (publickey).
```

Se você vir uma mensagem semelhante ao tentar fazer login na sua instância, examine a primeira linha da mensagem de erro para verificar se está usando a chave pública correta para sua instância. O exemplo acima usa a chave privada `.ssh/my_private_key.pem` com permissões de arquivo `0777`, que permitem que qualquer pessoa leia ou grave nesse arquivo. O nível de permissão é muito inseguro, por isso o SSH ignora essa chave.

Se você está se conectando do macOS ou Linux, execute o comando a seguir para corrigir esse erro, substituindo o caminho para o arquivo de chave privada.

```
[ec2-user ~]$ chmod 0400 .ssh/my_private_key.pem
```

Se você estiver se conectando a uma instância do Linux no Windows, execute as etapas a seguir no computador local.

1. Navegue até o arquivo .pem.
2. Clique com o botão direito do mouse no arquivo .pem e selecione Properties (Propriedades).
3. Escolha a guia Segurança.
4. Selecione Advanced (Avançado).
5. Verifique se você é o proprietário do arquivo. Caso contrário, altere o proprietário para seu nome de usuário.
6. Selecione Disable inheritance (Desabilitar herança) e Remove all inherited permissions from this object (Remover todas as permissões herdadas deste objeto).

7. Selecione Add (Adicionar), Select a principal (Selecionar um principal), insira seu nome de usuário e selecione OK.
8. Na janela Permission Entry (Entrada de permissão), conceda as permissões Read (Leitura) e selecione OK.
9. Clique em Apply (Aplicar) para garantir que todas as configurações sejam salvas.
10. Selecione OK para fechar a janela Advanced Security Settings (Configurações avançadas de segurança).
11. Selecione OK para fechar a janela Properties (Propriedades).
12. Você deve ser capaz de se conectar à instância do Linux no Windows usando SSH.

No prompt de comando do Windows, execute os comandos a seguir.

1. No prompt de comando, navegue até o local do caminho do arquivo .pem.
2. Execute o seguinte comando para redefinir e remover permissões explícitas:

```
icacls.exe $path /reset
```

3. Execute o seguinte comando para conceder permissões de leitura ao usuário atual:

```
icacls.exe $path /GRANT:R "$($env:USERNAME):(R)"
```

4. Execute o seguinte comando para desabilitar a herança e remover permissões herdadas.

```
icacls.exe $path /inheritance:r
```

5. Você deve ser capaz de se conectar à instância do Linux no Windows usando SSH.

Erro: a chave privada deve começar com "-----BEGIN RSA PRIVATE KEY-----" e terminar com "-----END RSA PRIVATE KEY-----"

Se usar uma ferramenta de terceiros, como ssh-keygen, para criar um par de chaves RSA, ela gerará a chave privada no formato de chave OpenSSH. Quando você se conecta à sua instância, se você usar a chave privada no formato OpenSSH para descriptografar a senha, você receberá o erro `Private key must begin with "-----BEGIN RSA PRIVATE KEY-----" and end with "-----END RSA PRIVATE KEY-----"`.

Para resolver o erro, a chave privada deve estar no formato PEM. Use o comando a seguir para criar a chave privada no formato PEM:

```
ssh-keygen -m PEM
```

Erro: falha na verificação de chaves do host

Esse erro ocorre quando há uma incompatibilidade entre a chave do host armazenada na instância no arquivo `known_hosts` e no cliente. Por exemplo, uma incompatibilidade pode ocorrer quando você se conectar a uma instância usando um endereço IP público e, em seguida, tenta se conectar a ela novamente usando um endereço IP público diferente. Isso pode acontecer depois que você adiciona ou remove um endereço IP elástico, pois isso modifica o endereço IP público de uma instância.

Para solucionar esse erro, comece confirmando que houve uma alteração esperada na chave do host ou na configuração da rede da instância. Antes de se conectar à instância, talvez também convém verificar a impressão digital do host. Depois de se conectar à instância, você poderá remover a chave de host antiga do arquivo `known_hosts`. Para obter instruções, consulte a documentação da distribuição Linux em uso na sua instância.

Erro: o servidor recusou nossa chave ou não há métodos de autenticação compatíveis

Se você usar o PuTTY para se conectar à instância e obtiver 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 a AMI. Digite o nome de usuário em Nome do usuário na janela Configuração do PuTTY.

Os nomes de usuários apropriados são os seguintes:

A AMI usada para iniciar a instância	Nome de usuário padrão
Amazon Linux	`ec2-user`
CentOS	`centos` ou `ec2-user`
Debian	`admin`

A AMI usada para iniciar a instância	Nome de usuário padrão
Fedora	`fedora` ou `ec2-user`
FreeBSD	`ec2-user`
RHEL	`ec2-user` ou `root`
SUSE	`ec2-user` ou `root`
Ubuntu	`ubuntu`
Oracle	`ec2-user`
Bitnami	`bitnami`
Rocky Linux	`rocky`
Outros	Verificar com o provedor de AMI

Você também deve verificar:

- Se está usando a versão mais recente do PuTTY. Para obter mais informações, consulte a página do PuTTY.
- Se o arquivo de chave privada (.pem) foi convertido corretamente para o formato reconhecido pelo PuTTY (.ppk). Para obter mais informações sobre a conversão da sua chave privada, consulte Conectar-se à instância do Linux usando PuTTY.

Não é possível fazer o ping da instância

O comando `ping` é um tipo de tráfego de ICMP — se você não conseguir fazer o ping da sua instância, verifique se as regras do grupo de segurança de entrada permitem tráfego de ICMP para a mensagem `Echo Request` de todas as origens, ou do computador ou da instância em que você está emitindo o comando.

Caso você não consiga emitir um comando `ping` por sua instância, assegure-se de que suas regras do security group de saída permitam tráfego de ICMP para a mensagem `Echo Request` a todos os destinos ou para o host no qual você está tentando fazer o ping.

`Ping`Os comandos também podem ser bloqueados por um firewall ou tempo de espera devido a problemas de latência de rede ou hardware. É necessário consultar o administrador de sistema ou de rede local para obter ajuda com mais solução de problemas.

Erro: Server unexpectedly closed network connection (A conexão de rede foi fechada inesperadamente pelo servidor)

Se você estiver se conectando à instância com o PuTTY e receber o erro "A conexão de rede foi fechada inesperadamente pelo servidor", verifique se os keepalives estão habilitados na página Conexão da Configuração do PuTTY para evitar ser desconectado. Alguns servidores desconectam clientes quando eles não recebem nenhum dado em determinado período. Defina os segundos entre os keepalives para 59 segundos.

Se você ainda tiver problemas após habilitar os keepalives, tente desabilitar o algoritmo de Nagle na página Conexão da Configuração do PuTTY.

Erro: falha na validação da chave do host para EC2 Instance Connect

Se você alternar as chaves do host da instância, as novas chaves do host não serão automaticamente carregadas para o banco de dados de chaves de host confiáveis da AWS. Isso faz com que a validação da chave do host apresente falha quando você tenta se conectar à instância usando o cliente EC2 Instance Connect baseado em navegador e você não consegue se conectar à instância.

Para resolver o erro, é necessário executar o script `eic_harvest_hostkeys` na instância, o que carregará sua nova chave de host para EC2 Instance Connect. O script está localizado em `/opt/aws/bin/` nas instâncias do Amazon Linux 2 e em `/usr/share/ec2-instance-connect/` nas instâncias do Ubuntu.

Amazon Linux 2

Para resolver o erro de falha de validação da chave de host em uma instância do Amazon Linux 2.

1. Conecte-se à sua instância usando SSH.

   É possível se conectar usando a CLI do EC2 Instance Connect ou o par de chaves de SSH atribuído à instância quando você a executou e o nome do usuário padrão da AMI usada para executar a instância. Para o Amazon Linux 2, o nome do usuário padrão é `ec2-user`.

Por exemplo, se a instância tiver sido executada usando o Amazon Linux 2, o nome DNS público da instância for `ec2-a-b-c-d.us-west-2.compute.amazonaws.com` e o par de chaves for `my_ec2_private_key.pem`, use o seguinte comando para o SSH na instância:

```
$ ssh -i my_ec2_private_key.pem ec2-user@ec2-a-b-c-d.us-
west-2.compute.amazonaws.com
```

Para obter mais informações sobre como se conectar à sua instância, consulte Conectar-se à instância do Linux usando um cliente SSH.

2. Navegue até a seguinte pasta.

```
[ec2-user ~]$ cd /opt/aws/bin/
```

3. Execute o seguinte comando na sua instância.

```
[ec2-user ~]$ ./eic_harvest_hostkeys
```

Observe que uma chamada bem-sucedida não resulta em saída.

Agora é possível usar o cliente EC2 Instance Connect baseado em navegador para se conectar à instância.

Ubuntu

Para resolver o erro de falha de validação da chave de host em uma instância do Ubuntu

1. Conecte-se à sua instância usando SSH.

   É possível se conectar usando a CLI do EC2 Instance Connect ou o par de chaves de SSH atribuído à instância quando você a executou e o nome do usuário padrão da AMI usada para executar a instância. Para Ubuntu, o nome de usuário padrão é `ubuntu`.

   Por exemplo, se a instância tiver sido executada usando o Ubuntu, o nome DNS público da instância for `ec2-a-b-c-d.us-west-2.compute.amazonaws.com` e o nome do par de chaves for `my_ec2_private_key.pem`, use o seguinte comando para o SSH na instância:

```
$ ssh -i my_ec2_private_key.pem ubuntu@ec2-a-b-c-d.us-
west-2.compute.amazonaws.com
```

Para obter mais informações sobre como se conectar à sua instância, consulte Conectar-se à instância do Linux usando um cliente SSH.

2. Navegue até a seguinte pasta.

```
[ec2-user ~]$ cd /usr/share/ec2-instance-connect/
```

3. Execute o seguinte comando na sua instância.

```
[ec2-user ~]$ ./eic_harvest_hostkeys
```

Observe que uma chamada bem-sucedida não resulta em saída.

Agora é possível usar o cliente EC2 Instance Connect baseado em navegador para se conectar à instância.

Não é possível conectar a uma instância Ubuntu usando o EC2 Instance Connect

Se você usar o EC2 Instance Connect para se conectar à sua instância do Ubuntu e receber um erro ao tentar se conectar, poderá usar as informações a seguir para tentar corrigir o problema.

Possível causa

O pacote `ec2-instance-connect` na instância não é a versão mais recente.

Solução

Atualize o pacote `ec2-instance-connect` na instância para a versão mais recente, desta forma:

1. Conecte-se à sua instância usando um método diferente do EC2 Instance Connect.
2. Execute o comando a seguir em sua instância para atualizar o pacote `ec2-instance-connect` para a versão mais recente.

```
apt update && apt upgrade
```

Perdi minha chave privada. Como posso me conectar à instância?

Se você perder a chave privada de uma instância com EBS, poderá recobrar o acesso à sua instância. É necessário parar a instância, separar seu volume raiz e associá-lo a outra instância como um volume de dados, modificar o arquivo `authorized_keys` com uma nova chave pública, mover o volume de volta para a instância original e reiniciar a instância. Para obter mais informações sobre executar, conectar e parar instâncias, consulte Alterações do estado de instâncias do Amazon EC2.

Este procedimento é compatível apenas com instâncias com volumes raiz do EBS. Se a instância tiver um volume raiz do tipo armazenamento de instância, não é possível recuperar o acesso usando este procedimento. É necessário ter a chave privada para se conectar à instância. Para determinar o tipo de volume raiz da instância, abra o console do Amazon EC2, escolha Instâncias, selecione a instância, clique na guia Armazenamento e, na seção Detalhes do dispositivo raiz, verifique o valor de Tipo de dispositivo raiz.

O valor é `EBS` ou `INSTANCE-STORE`.

Além das etapas a seguir, há outras formas de se conectar à instância do Linux em caso de perda da chave privada. Para obter mais informações, consulte Como posso me conectar à instância do Amazon EC2 se tiver perdido meu par de chaves SSH após o lançamento inicial?

Etapas para se conectar a uma instância com EBS com um par de chaves diferente

- Etapa 1: Criar um novo par de chaves
- Etapa 2: Obter informações sobre a instância original e seu volume raiz
- Etapa 3: Interromper a instância original
- Etapa 4: Executar uma instância temporária
- Etapa 5: Separar o volume raiz da instância original e associá-lo à instância temporária
- Etapa 6: Adicionar a nova chave pública authorized_keys no volume original montado à instância temporária
- Etapa 7: Desmontar e separar o volume original da instância temporária e associá-lo novamente à instância original
- Etapa 8: Conectar-se à instância original usando o novo par de chaves
- Etapa 9: Limpeza

Etapa 1: Criar um novo par de chaves

Crie um novo par de chaves usando o console do Amazon EC2 ou uma ferramenta de terceiros. Se você quiser nomear seu novo par de chaves exatamente igual ao par de chaves privadas perdido, primeiro exclua o par de chaves existente. Para obter mais informações sobre como criar um par de chaves, consulte Criar um par de chaves usando o Amazon EC2 ou Criar um par de chaves usando uma ferramenta de terceiros e importe a chave pública para o Amazon EC2.

Etapa 2: Obter informações sobre a instância original e seu volume raiz

Anote as seguintes informações, porque elas serão necessárias para a conclusão deste procedimento.

Como obter informações sobre a instância original

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Escolha Instâncias no painel de navegação e selecione a instância à qual você deseja se conectar. (Nós a chamamos de instância original.)
3. Na guia Details (Detalhes) , anote o ID da instância e a ID da AMI.
4. Na guia Networking (Redes), anote a zona de disponibilidade.
5. Na guia Storage (Armazenamento), em Root device name (Nome do dispositivo raiz), anote o nome do dispositivo para o volume raiz (por exemplo, `/dev/xvda`). Em seguida, em Block devices (Dispositivos de bloco), encontre este nome do dispositivo e anote o ID do volume (por exemplo, vol-0a1234b5678c910de).

Etapa 3: Interromper a instância original

Escolha Instance state (Estado da instância) e Stop instance (Interromper instância). Se a opção estiver desabilitada, significa que a instância já está interrompida ou que o volume raiz é um armazenamento de instância.

> **Warning**
>
> Quando você interrompe uma instância, os dados em todos os volumes de armazenamento de instâncias são apagados. Para manter dados longe dos volumes de armazenamento de instância, faça backup no armazenamento persistente.

Etapa 4: Executar uma instância temporária

Para executar uma instância temporária

1. No painel de navegação, escolha Instances (Instâncias) e Launch instances (Executar instâncias).
2. Na seção Name and tags (Nome e etiquetas), em Name (Nome), insira Temporary (Temporário).
3. Na seção Application and OS Images (Imagens de aplicações e SO), selecione a mesma AMI usada para iniciar a instância original. Se essa AMI estiver indisponível, será possível criar uma AMI que pode usar a partir da instância interrompida. Para obter mais informações, consulte Criação de uma AMI baseada no Amazon EBS.
4. Na seção Instance type (Tipo de instância), mantenha o tipo de instância padrão.
5. Na seção Key pair (Par de chaves), em Key pair name (Nome do par de chaves), selecione o par de chaves existente para usar ou crie um novo.
6. Na seção Network settings (Configurações de rede), selecione Edit (Editar), e, em seguida, em Subnet (Sub-rede), selecione uma sub-rede na mesma zona de disponibilidade que a instância original.
7. No painel Summary (Resumo) painel, escolha Launch (Iniciar).

Etapa 5: Separar o volume raiz da instância original e associá-lo à instância temporária

1. No painel de navegação, escolha Volumes e selecione o volume raiz da instância original, cujo ID você registrou na etapa anterior. Escolha Actions (Ações), Detach Volume (Desanexar volume) e Yes, Detach (Sim, desanexar). Espere o estado do volume tornar-se `available`. (É possível precisar escolher o ícone Atualizar.)
2. Com o volume ainda selecionado, escolha Actions (Ações) e, em seguida, Attach volume (Anexar volume). Selecione o ID de instância da instância temporária, anote o nome do dispositivo especificado em Device (Dispositivo) (por exemplo, `/dev/sdf`) e selecione Attach (Anexar).

> **Note**
>
> Se você tiver executado a instância original a partir de uma AMI de AWS Marketplace e seu volume contiver códigos de AWS Marketplace, você deverá primeiro parar a instância temporária antes de associar o volume.

Etapa 6: Adicionar a nova chave pública **authorized_keys** no volume original montado à instância temporária

1. Conecte-se à instância temporária.
2. Na instância temporária, monte o volume que você associou à instância de forma que possa acessar seu sistema de arquivos. Por exemplo, se o nome do dispositivo for `/dev/sdf`, use os comandos a seguir para montar o volume como `/mnt/tempvol`.

> **Note**
>
> O nome de dispositivo pode aparecer de forma diferente em sua instância. Por exemplo, dispositivos montados como `/dev/sdf` podem ser exibidos como `/dev/xvdf` na instância. Algumas versões do Red Hat (ou suas variantes, como o CentOS) podem até mesmo incrementar a letra final com 4 caracteres, em que `/dev/sdf` torna-se `/dev/xvdk`.

   a. Use o comando lsblk determinar se o volume é particionado.

```
[ec2-user ~]$ lsblk
NAME    MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
xvda    202:0    0    8G  0 disk
##xvda1 202:1    0    8G  0 part /
xvdf    202:80   0  101G  0 disk
##xvdf1 202:81   0  101G  0 part
xvdg    202:96   0   30G  0 disk
```

   No exemplo acima, `/dev/xvda` e `/dev/xvdf` são volumes particionados, e `/dev/xvdg` não é. Se seu volume estiver particionado, você montará a partição (`/dev/xvdf1`) em vez do dispositivo raw (`/dev/xvdf`) nas próximas etapas.

b. Crie um diretório temporário para montar o volume.

```
[ec2-user ~]$ sudo mkdir /mnt/tempvol
```

c. Monte o volume (ou a partição) no ponto de montagem temporário usando o nome do volume ou do dispositivo identificado anteriormente. O comando necessário depende do sistema de arquivos do sistema operacional. Observe que o nome de dispositivo pode aparecer de forma diferente em sua instância. Consulte note na etapa 6 para obter mais informações.

- Amazon Linux, Ubuntu e Debian

```
[ec2-user ~]$ sudo mount /dev/xvdf1 /mnt/tempvol
```

- Amazon Linux 2, CentOS, SUSE Linux 12 e RHEL 7.x

```
[ec2-user ~]$ sudo mount -o nouuid /dev/xvdf1 /mnt/tempvol
```

> **Note**
>
> Se você receber um erro informando que o sistema de arquivos está corrompido, execute o seguinte comando para usar o utilitário fsck para verificar o sistema de arquivos e reparar quaisquer problemas:
>
> ```
> [ec2-user ~]$ sudo fsck /dev/xvdf1
> ```

3. Pela instância temporária, use o comando a seguir para atualizar `authorized_keys` no volume montado com a nova chave pública nova de `authorized_keys` para a instância temporária.

> **Important**
>
> Os exemplos a seguir usam o nome de usuário `ec2-user` do Amazon Linux. É possível precisar substituir um nome de usuário diferente, como `ubuntu` para instâncias do Ubuntu.

```
[ec2-user ~]$ cp .ssh/authorized_keys /mnt/tempvol/home/ec2-user/.ssh/
authorized_keys
```

Se essa cópia tiver sido bem-sucedida, será possível passar para a próxima etapa.

(Opcional) Caso contrário, se você não tiver permissão para editar arquivos em `/mnt/tempvol`, será necessário atualizar o arquivo usando sudo e conferir as permissões no arquivo para verificar se é possível fazer login na instância original. Use o comando a seguir para verificar as permissões no arquivo:

```
[ec2-user ~]$ sudo ls -l /mnt/tempvol/home/ec2-user/.ssh
total 4
-rw------- 1 222 500 398 Sep 13 22:54 authorized_keys
```

Nesta saída de exemplo, *222* é o ID do usuário e *500* é o ID do grupo. Em seguida, use sudo para executar novamente o comando de cópia que falhou.

```
[ec2-user ~]$ sudo cp .ssh/authorized_keys /mnt/tempvol/home/ec2-user/.ssh/
authorized_keys
```

Execute o comando a seguir novamente para determinar se as permissões foram alteradas.

```
[ec2-user ~]$ sudo ls -l /mnt/tempvol/home/ec2-user/.ssh
```

Se o ID do usuário e do grupo tiverem sido alterados, use o comando a seguir para restaurá-los.

```
[ec2-user ~]$ sudo chown 222:500 /mnt/tempvol/home/ec2-user/.ssh/authorized_keys
```

Etapa 7: Desmontar e separar o volume original da instância temporária e associá-lo novamente à instância original

1. Na instância temporária, desmonte o volume que você associou para que possa reassociá-lo à instância original. Por exemplo, use o comando a seguir para desmontar o volume em `/mnt/tempvol`.

```
[ec2-user ~]$ sudo umount /mnt/tempvol
```

2. Para desanexar o volume da instância temporária (que você desmontou anteriormente): no console do Amazon EC2, escolha Volumes no painel de navegação, selecione o volume raiz da instância original, cujo ID você anotou anteriormente, clique em Ações, escolha Desanexar volume e, em seguida, selecione Desanexar. Espere o estado do volume tornar-se `available`. (É possível precisar escolher o ícone Atualizar.)
3. Associe o volume novamente à instância original: com o volume ainda selecionado, escolha Actions (Ações), Attach Volume (Anexar volume). Selecione o ID da instância original, informe o nome do dispositivo que você anotou na Etapa 2 para a anexação do volume raiz original (`/dev/sda1` ou `/dev/xvda`) e, em seguida, escolha Anexar volume.

> **Important**
>
> Se você não especificar o mesmo nome do dispositivo do anexo original, não poderá iniciar a instância original. O Amazon EC2 espera que o volume raiz esteja em `sda1` ou `/dev/xvda`.

Etapa 8: Conectar-se à instância original usando o novo par de chaves

Selecione a instância original e escolha Instance state (Estado da instância) e Start instance (Iniciar instância). Após a instância entrar no estado `running`, é possível se conectar a ela usando o arquivo de chave privada do seu novo par de chaves.

> **Note**
>
> Se o nome do novo par de chaves e do arquivo de chaves privadas correspondente for diferente do nome do par de chaves original, especifique o nome do novo arquivo de chave privada conectado à sua instância.

Etapa 9: Limpeza

(Opcional) É possível encerrar a instância temporária se não tiver utilização adicional para ela. Selecione a instância temporária e escolha IEstado da instância e Encerrar instância.

Solucionar problemas de instâncias do Linux do Amazon EC2 com falhas nas verificações de status

As informações apresentadas a seguir podem ajudar você a solucionar problemas caso sua instância do Linux apresente falhas em uma verificação de status. Determine primeiro se suas aplicações exibem quaisquer problemas. Se você verificar que a instância não está executando suas aplicações como esperado, analise as informações de verificação de status e os logs do sistema.

Para obter exemplos de problemas que podem causar falha nas verificações de status, consulte Verificações do status das instâncias do Amazon EC2.

Tópicos

- Analisar informações de verificação de status
- Recuperar os logs do sistema
- Solução de problemas relacionados aos erros de log do sistema para instâncias do Linux
- Sem memória: encerrar processo
- ERRO: falha em mmu_update (falha na atualização do gerenciamento de memória)
- Erro de E/S (falha de dispositivo de blocos)
- ERRO DE E/S: nem disco local nem disco remoto (o dispositivo de blocos distribuído está quebrado)
- request_module: modprobe de loop descontrolado (modprobe do kernel legado do looping, em versões mais antigas do Linux)
- "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)
- "FATAL: Não foi possível carregar os módulos /lib/" ou "BusyBox" (módulos do kernel ausentes)
- ERRO Kernel inválido (kernel incompatível com EC2)
- fsck: Nenhum arquivo ou diretório ao tentar abrir… (Sistema de arquivos não encontrado)
- Erro geral ao montar os sistemas de arquivos (falha na montagem)
- VFS: Não foi possível montar o fs raiz em um bloco desconhecido (falta de correspondência no sistema de arquivos-raiz)
- Erro: não foi possível determinar o número principal/secundário do dispositivo raiz... (Incompatibilidade entre sistema de arquivos/dispositivo raiz)
- XENBUS: Dispositivo sem driver…

- …dias sem ser verificada, verificação forçada (verificação necessária para o sistema de arquivos)
- O fsck morreu com status de saída… (Dispositivo ausente)
- Prompt do GRUB (grubdom>)
- Acessando a interface eth0: O dispositivo eth0 tem um endereço MAC diferente do esperado, ignorando. (Endereço MAC hard-coded)
- Não foi possível carregar a Política do SELinux. A máquina está no modo de força. Parando agora. (Erro de configuração do SELinux)
- XENBUS: Excedido o limite de tempo para se conectar a dispositivos (tempo limite do Xenbus)

Analisar 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. Selecione a guia Status e alarmes para ver os resultados individuais de todas as verificações de status do sistema, verificações de status da instância e verificações de status do EBS anexado.

Se uma verificação do status falhar, é possível tentar uma das opções a seguir:

- Crie um alarme para recuperar a instância em resposta à falha na verificação de status. Para obter mais informações, consulte Criar alarmes para interromper, encerrar, reinicializar ou recuperar uma instância.
- (Verificações de status da instância) Se você alterou o tipo de instância para uma instância baseada em Nitro, as verificações de status falharão caso tenha migrado de uma instância que não possui os drivers ENA e NVMe necessários. Para obter mais informações, consulte Compatibilidade para alterar o tipo de instância.
- Para uma instância com volume raiz do EBS, realize a interrupção e o reinício da instância. Para obter mais informações, consulte Início e interrupção de instâncias do Amazon EC2.
- Para uma instância com volume raiz do tipo armazenamento de instância, encerre a instância e inicie uma instância substituta. Para obter mais informações, consulte Encerramento de instâncias do Amazon EC2.
- Espere o Amazon EC2 resolver o problema.
- Entre em contato com Suporte ou publique seu problema no AWS re:Post.

- Se sua instância estiver em um grupo do Auto Scaling:
  - (Verificações do status do sistema e verificações do status da instância) Por padrão, o Amazon EC2 Auto Scaling executará uma instância de substituição automaticamente. Para obter mais informações, consulte Health checks for instances in an Auto Scaling group no Amazon EC2 Auto Scaling User Guide.
  - (Verificações de status do EBS anexado) Você deve configurar o Amazon EC2 Auto Scaling para iniciar automaticamente uma instância substituta. Para obter mais informações, consulte Monitor and replace Auto Scaling instances with impaired Amazon EBS volumes no Guia do usuário do Amazon EC2 Auto Scaling.
- Recupere o log do sistema e procure erros. Para obter mais informações, consulte Recuperar os logs do sistema.

Recuperar os logs do sistema

Se uma verificação de status da instância falhar, será possível reinicializar a instância e recuperar os logs do sistema. Os logs podem revelar um erro que pode ajudar você a resolver o problema. Reinicializar limpa as informações desnecessária dos logs.

Para reinicializar uma instância e recuperar o log do sistema

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Instâncias e selecione sua instância.
3. Escolha Instance state (Estado da instância) e Reboot instance (Reinicializar instância). Pode demorar alguns minutos para a instância reinicializar.
4. Verifique o problema ainda existe; em alguns casos, reinicializar pode resolver o problema.
5. Quando a ação estiver no estado `running`, escolha Actions (Ações), Monitor and troubleshoot (Monitorar e solucionar problemas), Get system log (Obter log do sistema).
6. Revise o log que aparece na tela e use a lista de declarações conhecidas de erro do log do sistema, abaixo, para solucionar seu problema.
7. Se seu problema não for resolvido, você pode publicar seu problema no AWS re:Post.

Solução de problemas relacionados aos erros de log do sistema para instâncias do Linux

Para instâncias do Linux que apresentaram falhas na 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 é possível utilizar para resolver o problema de cada erro.

Erros de memória

- Sem memória: encerrar processo
- ERRO: falha em mmu_update (falha na atualização do gerenciamento de memória)

Erros do dispositivo

- Erro de E/S (falha de dispositivo de blocos)
- ERRO DE E/S: nem disco local nem disco remoto (o dispositivo de blocos distribuído está quebrado)

Erros de kernel

- request_module: modprobe de loop descontrolado (modprobe do kernel legado do looping, em versões mais antigas do Linux)
- "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)
- "FATAL: Não foi possível carregar os módulos /lib/" ou "BusyBox" (módulos do kernel ausentes)
- ERRO Kernel inválido (kernel incompatível com EC2)

Erros do sistema de arquivos

- fsck: Nenhum arquivo ou diretório ao tentar abrir… (Sistema de arquivos não encontrado)
- Erro geral ao montar os sistemas de arquivos (falha na montagem)
- VFS: Não foi possível montar o fs raiz em um bloco desconhecido (falta de correspondência no sistema de arquivos-raiz)

- Erro: não foi possível determinar o número principal/secundário do dispositivo raiz... (Incompatibilidade entre sistema de arquivos/dispositivo raiz)
- XENBUS: Dispositivo sem driver…
- …dias sem ser verificada, verificação forçada (verificação necessária para o sistema de arquivos)
- O fsck morreu com status de saída… (Dispositivo ausente)

Erros do sistema operacional

- Prompt do GRUB (grubdom>)
- Acessando a interface eth0: O dispositivo eth0 tem um endereço MAC diferente do esperado, ignorando. (Endereço MAC hard-coded)
- Não foi possível carregar a Política do SELinux. A máquina está no modo de força. Parando agora. (Erro de configuração do SELinux)
- XENBUS: Excedido o limite de tempo para se conectar a dispositivos (tempo limite do Xenbus)

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
Baseada no Amazon EBS	Execute um destes procedimentos: • Pare a instância, modifique-a para usar um tipo de instância diferente e inicie-

Para este tipo de instância	Faça o seguinte
	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	Execute um destes procedimentos: • 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 logo 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 em AWS re:Post ou entre em contato com Suporte.

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	Use o procedimento a seguir: 1. Pare a instância. 2. Separe o volume. 3. Tentativa de recuperar o volume. **Note** É boa prática tirar um snapshot dos seus volumes do Amazon EBS com frequência. Isso diminui drasticam ente o risco de perda de dados como resultado da falha. 4. Reassocie o volume à instância. 5. Inicie a instância.
Com armazenamento de instâncias	Encerre a instância e execute uma nova instância. **Note** Os dados não podem ser recuperados. Recupere os backups.

Para este tipo de instância	Faça o seguinte
	Note 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.

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 baseada no Amazon EBS, é possível 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 no startup.

```
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	Use um kernel mais novo, baseado em GRUB ou estático, usando uma das seguintes opções:

Para este tipo de instância	Faça o seguinte
	Opção 1: Encerre a instância e execute uma nova, especificando os parâmetros `-kernel` e `-ramdisk`. Opção 2: 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 `-kernel` e `-ramdisk`.

"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:

Para este tipo de instância	Faça o seguinte
	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.

```
[    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	Use o procedimento a seguir: 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.

Para este tipo de instância	Faça o seguinte
	5. Inicie a instância. 6. Modifique a AMI para usar o ramdisk corrigido.
Com armazenamento de instâncias	Use o procedimento a seguir: 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/sda1 ro

initrd /initrd.img

ERROR Invalid kernel: elf_xen_note_check: ERROR: Will only load images
built for the generic loader or Linux images
xc_dom_parse_image returned -1

Error 9: Unknown boot failure

  Booting 'Fallback'

root (hd0)

 Filesystem type is ext2fs, using whole disk

kernel /vmlinuz.old root=/dev/sda1 ro

Error 15: File not found
```

Possíveis causas

Uma ou ambas as condições a seguir podem causar esse problema:

- O kernel fornecido não é compatível com GRUB
- O kernel de fallback não existe

Ações sugeridas

Para este tipo de instância	Faça o seguinte
Baseado em Amazon EBS	Use o procedimento a seguir: 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: 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 Suporte.

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	Use o procedimento a seguir:

Para este tipo de instância	Faça o seguinte
	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. 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 disponíve l atualmente no Amazon EC2. Tenha cuidado com esse recurso e leia a man page do Linux para fstab.
Com armazenamento de instâncias	Use o procedimento a seguir: 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 Suporte.

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	• Volume do Amazon EBS destacado ou com falha. • Sistema de arquivos corrompido.

Tipo de instância	Possível causa
	• Combinação malfeita de ramdisk e AMI (por exemplo, ramdisk Debian com AMI SUSE).
Com armazenamento de instâncias	• 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	Use o procedimento a seguir: 1. Pare a instância. 2. Separe o volume de raiz. 3. Associe o volume do dispositivo raiz a uma instância de trabalho conhecida. 4. Execute uma verificação no sistema de arquivos (fsck -a /dev/...). 5. Corrija todos os erros. 6. Separe o volume de instância de trabalho conhecida. 7. Associe o volume à instância parada. 8. Inicie a instância. 9. Verifique novamente o status da instância.
Com armazenamento de instâncias	Faça uma das coisas a seguir: • Execute uma nova instância. • (Opcional) Procure assistência técnica para recuperação de dados usando o Suporte.

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	• 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
Baseada no Amazon EBS	Execute um destes procedimentos:

Para este tipo de instância	Faça o seguinte
	• 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. • Pare e modifique para usar o kernel moderno. • Consulte a documentação para sua distribui ção 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: 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.
Com armazenamento de instâncias	Use o procedimento a seguir: 1. Crie nova AMI com a correção apropriada (mapeie o dispositivo de blocos corretame nte). 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.
Com armazenamento de instâncias	Use o procedimento a seguir:

Para este tipo de instância	Faça o seguinte
	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	Teste uma ou mais das opções a seguir para resolver o problema: • 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 recomenda dos).
Com armazenamento de instâncias	Teste uma ou mais das opções a seguir para resolver o problema: • Reempacote o ramdisk com as ferramentas corretas. • Modifique os parâmetros de ajuste do sistema de arquivos para remover os

Para este tipo de instância	Faça o seguinte
	requisitos de consistência (não recomendados). • Encerre a instância e execute uma nova instância. • (Opcional) Procure assistência técnica para recuperação de dados usando o Suporte.

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	• 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

Tipo de instância	Possíveis causas
	é compatível com uma versão anterior do GRUB).
Com armazenamento de instâncias	• 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 configura ção 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	Opção 1: Modifique a AMI e reexecute a instância: 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.

Para este tipo de instância	Faça o seguinte
	Opção 2: Corrija a instância existente: 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. 9. Modifique o atributo do kernel para usar a imagem adequada do GRUB (1º disco ou 1ª partição no 1ª disco). 10. Inicie a instância.

Para este tipo de instância	Faça o seguinte
Com armazenamento de instâncias	Opção 1: Modifique a AMI e reexecute a instância: 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. Opção 2: Encerre a instância e execute uma nova, especificando o kernel correto. **Note** Para recuperar dados da instância existente, entre em contato com o Suporte.

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
Baseada no Amazon EBS	Execute um destes procedimentos: • Modifique a AMI para remover o hard code e reexecute a instância. • Modifique a instância para remover o endereço MAC hard-coded. OU Use o procedimento a seguir: 1. Pare a instância. 2. Separe o volume de raiz. 3. Associe o volume a outra instância e modifique o volume para remover o endereço MAC hard-coded. 4. Associe o volume à instância original. 5. Inicie a instância.
Com armazenamento de instâncias	Execute um destes procedimentos: • 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	Use o procedimento a seguir: 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 (posterio rmente chamada de instância de recuperaç ão). 4. Conecte-se à instância de recuperação e monte o volume do dispositivo raiz da instância falha. 5. Desabilite o SELinux no volume do dispositi vo raiz montado. Esse processo varia nas distribuições de Linux; para obter mais

Para este tipo de instância	Faça o seguinte
	informações, consulte a documentação específica do seu SO. **Note** Em alguns sistemas, você desabilita o SELinux configurando `SELINUX=disabled` no arquivo `/mount_point /etc/sysconfig/selinux`, onde *mount_point* é o local onde você montou o volume da sua instância de recuperação. 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	Use o procedimento a seguir: 1. Encerre a instância e execute uma nova instância. 2. (Opcional) Procure assistência técnica para recuperação de dados usando o Suporte.

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
Baseada no Amazon EBS	Execute um destes procedimentos: • Modifique a AMI e a instância para usar um kernel moderno e reexecutar a instância. • Reinicialize a instância.
Com armazenamento de instâncias	Execute um destes procedimentos: • Encerre a instância. • Modifique as AMIs para usar um kernel moderno e execute uma nova instância usando essa AMI.

Solução de problemas de inicialização da instância do Linux do Amazon EC2 devido a volume errado

Em algumas situações, um volume diferente do volume associado a `/dev/xvda` ou a `/dev/sda` torna-se o volume raiz de uma instância do Linux. 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, existe a possibilidade de `/dev/xvdf1` se tornar o volume raiz pelo qual a instância inicializa depois que o ramdisk inicial é executado, substituindo o volume `/dev/xvda1` que você pretendia usar para inicialização. 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, será possível 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 /.

Solucionar problemas de conexão à instância do Windows do Amazon EC2

As informações e os erros comuns apresentados a seguir podem ajudar na solução de problemas de conexão com a instância do Windows.

Problemas de conexão

- O Remote Desktop não pode se conectar ao computador remoto
- Erro ao usar o cliente RDP do macOS
- O RDP exibe uma tela preta em vez da área de trabalho
- Não foi possível fazer login remotamente em uma instância com um usuário que não é administrador
- Resolução de problemas do desktop remoto usando o AWS Systems Manager
- Habilitar a área de trabalho remota em uma instância do EC2 com o registro remoto
- Perdi minha chave privada. Como posso me conectar à minha instância do Windows?

O Remote Desktop não pode se conectar ao computador remoto

Tente o seguinte para resolver problemas relacionados à conexão com sua instância:

- Verifique se você está usando o nome de host DNS público correto. No console do Amazon EC2, selecione a instância e verifique o DNS público (IPv4) no painel de detalhes. Se sua instância estiver em uma VPC e você não vir um nome DNS público, deverá habilitar nomes de host DNS. Para ter mais informações, consulte Atributos de DNS para sua VPC no Guia do usuário da Amazon VPC.
- Verifique se sua instância tem um endereço IPv4 público. Se não tiver, associe um endereço IP elástico à sua instância. Para obter mais informações, consulte Endereços IP elásticos.
- Para conectar-se à sua instância usando um endereço IPv6, verifique se seu computador local tem um endereço IPv6 e está configurado para usar IPv6. Para obter mais informações, consulte Configurar o IPv6 em suas instâncias no Guia do usuário da Amazon VPC.
- Verifique se o grupo de segurança tem uma regra que permita acesso RDP na porta 3389.
- Se você copiou a senha, mas obtiver o erro `Your credentials did not work`, tente digitá-la manualmente quando solicitado. É possível que você tenha omitido um caractere ou inserido um espaço em branco extra ao copiar a senha.
- Verifique se a instância passou nas verificações de status. Para obter mais informações, consulte Verificações do status das instâncias do Amazon EC2 e the section called “Falhas nas verificações de status de instâncias do Linux”.
- Verifique se a tabela de rotas da sub-rede tem uma rota que envie todo o tráfego destinado para fora da VPC para o gateway da Internet da VPC. Para obter mais informações, consulte Criação de uma tabela de rotas personalizada (gateways da Internet) no Guia do usuário da Amazon VPC.
- Verifique se o Firewall do Windows ou outros softwares de firewall não estão bloqueando o tráfego de RDP para a instância. Recomendamos que você desabilite o Firewall do Windows e controle o acesso à sua instância usando regras de grupo de segurança. Experimente uma das seguintes opções:
  - Use AWSSupport-TroubleshootRDP para disable the Windows Firewall profiles using SSM Agent. Essa opção requer que a instância esteja configurada para AWS Systems Manager.
  - Use AWSSupport-ExecuteEC2Rescue.
  - Pare a instância, desanexe o volume raiz e anexe o volume a uma instância temporária como volume de dados. Conecte-se à instância temporária e coloque o volume online. Carregue o hive do registro desde o volume de dados. Em `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters`

`\FirewallPolicyStandardProfile`, defina `EnableFirewall` como 0. Descarregue o hive do registro e, em seguida, coloque o volume offline. Desanexe o volume raiz da instância temporária e anexe-o à instância original como o volume raiz. Inicie a instância original.

- Verifique se a autenticação no nível de rede está desabilitada nas instâncias que não fazem parte de um domínio do Active Directory (use AWSSupport-TroubleshootRDP para disable NLA).
- Verifique se o tipo de startup do serviço da área de trabalho remota (TermService) é automático e se o serviço foi iniciado (use AWSSupport-TroubleshootRDP para enable and start the RDP service).
- Verifique se você está se conectando à porta correta do protocolo RDP, que por padrão é 3389 (use AWSSupport-TroubleshootRDP para read the current RDP port e change it back to 3389).
- Verifique se as conexões da área de trabalho remota são permitidas na sua instância (use AWSSupport-TroubleshootRDP para enable Remote Desktop connections).
- Verifique se a senha não expirou. Se a senha expirou, será possível redefini-la. Para obter mais informações, consulte Redefinir a senha de administrador do Windows para uma instância do Windows do Amazon EC2.
- Se você tentar conectar-se usando um usuário que você criou na instância e receber o erro `The user cannot connect to the server due to insufficient access privileges`, verifique se você concedeu ao usuário o direito de fazer login localmente. Para obter mais informações, consulte Conceder o direito de fazer login localmente a um membro.
- Se você tentar mais sessões simultâneas do RDP do que o máximo permitido, sua sessão será encerrada com a mensagem `Your Remote Desktop Services session has ended. Another user connected to the remote computer, so your connection was lost.` Por padrão, são permitidas duas sessões simultâneas do RDP para sua instância.

Erro ao usar o cliente RDP do macOS

Se estiver se conectando a uma instância do Windows Server usando o cliente de Conexão de Área de Trabalho Remota do site da Microsoft, poderá receber o seguinte erro:

```
Remote Desktop Connection cannot verify the identity of the computer that you want to
 connect to.
```

Faça download do aplicativo Área de Trabalho Remota da App Store do Mac e use o aplicativo para conectar-se à instância.

O RDP exibe uma tela preta em vez da área de trabalho

Tente o seguinte para resolver esse problema:

- Verifique a saída do console para ver se há informações adicionais. Para obter a saída do console da instância usando o console do Amazon EC2, selecione a instância e escolha Actions (Ações), Monitor and troubleshoot (Monitorar e solucionar problemas), Get system log (Obter log do sistema).
- Verifique se você está executando a versão mais recente do cliente do RDP.
- Tente as configurações padrão para o cliente do RDP.
- Se você estiver usando o Remote Desktop Connection, tente iniciá-lo com a opção `/admin` da seguinte forma.

```
mstsc /v:instance /admin
```

- Se o servidor estiver executando um aplicativo de tela total, talvez tenha parado de responder. Use Ctrl+Shift+Esc para iniciar o Windows Task Manager e feche o aplicativo.
- Se o servidor for utilizado em excesso, talvez tenha parado de responder. Para monitorar a instância usando o console do Amazon EC2, selecione a instância e escolha a guia Monitoramento. Se você precisar alterar o tipo de instância para um tamanho maior, consulte Alterações no tipo de instância do Amazon EC2.

Não foi possível fazer login remotamente em uma instância com um usuário que não é administrador

Se você não puder fazer login remotamente em uma instância do Windows com um usuário que não seja uma conta de administrador, conceda ao usuário o direito de fazer login localmente. Veja Dar a um usuário ou grupo o direito de entrar localmente nos controladores de domínio no domínio.

Resolução de problemas do desktop remoto usando o AWS Systems Manager

É possível usar o AWS Systems Manager para resolver problemas conectando-se à sua instância do Windows usando RDP.

AWSSupport-TroubleshootRDP

O documento de automação AWSSupport-TroubleshootRDP permite ao usuário verificar ou modificar configurações comuns na instância de destino que possam afetar as conexões RDP (Remote Desktop Protocol), como os perfis RDP Port, Network Layer Authentication (NLA) e Windows Firewall. Por padrão, o documento lê e exibe os valores dessas configurações.

O documento de automação AWSSupport-TroubleshootRDP pode ser usado com instâncias do EC2, instâncias on-premises e máquinas virtuais (VMs) habilitadas para uso com o AWS Systems Manager (instâncias gerenciadas). Além disso, ele também pode ser usado com instâncias do EC2 para Windows Server não habilitadas para uso com o Systems Manager. Para obter informações sobre a habilitação de instâncias para uso com o AWS Systems Manager, consulte Nós gerenciado do no Guia do usuário do AWS Systems Manager.

Para resolver os problemas usando o documento AWSSupport-TroubleshootRDP

1. Faça login no console do Systems Manager.
2. Verifique se você está na mesma região que a instância prejudicada.
3. Escolha Documents (Documentos) no painel de navegação à esquerda.
4. Na guia Owned by Amazon (Pertencente à Amazon), insira `AWSSupport-TroubleshootRDP` no campo de pesquisa. Quando o documento `AWSSupport-TroubleshootRDP` aparecer, selecione-o.
5. Escolha Execute automation.
6. Em Execution Mode (Modo de execução), escolha Simple execution (Execução simples).
7. Em Input parameters (Parâmetros de entrada), InstanceId, ative Show interactive instance picker (Mostrar seletor interativo de instâncias).
8. Escolha a instância do Amazon EC2.
9. Revise os exemplos e escolha Execute (Executar).
10. Para monitorar o progresso da execução, no Execution status (Status execução), aguarde o status mudar de Pending (Pendente) para Success (Êxito). Expanda Outputs (Saídas) para visualizar os resultados. Para visualizar a saída de etapas individuais, Executed Steps (Etapas executadas), escolha um item da Step ID (ID da etapa).

Exemplos do AWSSupport-TroubleshootRDP

Os exemplos a seguir mostram como conquistar tarefas de resolução de problema comuns usando AWSSupport-TroubleshootRDP. É possível usar o comando de exemplo AWS CLI start-automation-execution ou o link fornecido para o Console de gerenciamento da AWS.

Example Exemplo: verifique o status atual de RDP

AWS CLI:

```
aws ssm start-automation-execution --document-name "AWSSupport-TroubleshootRDP" --
parameters "InstanceId=i-1234567890abcdef0, Action=Custom" --region region_code
```

Console do AWS Systems Manager:

```
https://console.aws.amazon.com/systems-manager/automation/execute/AWSSupport-
TroubleshootRDP?region=region#documentVersion=$LATEST
```

Example Exemplo: desativar o Firewall do Windows

AWS CLI:

```
aws ssm start-automation-execution --document-name "AWSSupport-TroubleshootRDP"
 --parameters "InstanceId=i-1234567890abcdef0, Action=Custom, Firewall=Disable" --
region region_code
```

AWS Systems ManagerConsole do :

```
https://console.aws.amazon.com/systems-manager/automation/execute/AWSSupport-
TroubleshootRDP?region=region_code#documentVersion=$LATEST&Firewall=Disable
```

Example Exemplo: desativar a autenticação no nível da rede

AWS CLI:

```
aws ssm start-automation-execution --document-name "AWSSupport-TroubleshootRDP" --
parameters "InstanceId=i-1234567890abcdef0, Action=Custom, NLASettingAction=Disable" --
region region_code
```

AWS Systems ManagerConsole do :

```
https://console.aws.amazon.com/systems-manager/automation/execute/AWSSupport-
TroubleshootRDP?region=region_code#documentVersion
```

Example Exemplo: definir o tipo de startup do serviço RDP como automático e iniciar o serviço RDP

AWS CLI:

```
aws ssm start-automation-execution --document-name "AWSSupport-TroubleshootRDP" --
parameters "InstanceId=i-1234567890abcdef0, Action=Custom, RDPServiceStartupType=Auto,
 RDPServiceAction=Start" --region region_code
```

AWS Systems ManagerConsole do :

```
https://console.aws.amazon.com/systems-manager/automation/execute/
AWSSupport-TroubleshootRDP?region=region_code#documentVersion=
$LATEST&RDPServiceStartupType=Auto&RDPServiceAction=Start
```

Example Exemplo: restaurar a porta RDP padrão (3389)

AWS CLI:

```
aws ssm start-automation-execution --document-name "AWSSupport-TroubleshootRDP" --
parameters "InstanceId=i-1234567890abcdef0, Action=Custom, RDPPortAction=Modify" --
region region_code
```

AWS Systems ManagerConsole do :

```
https://console.aws.amazon.com/systems-manager/automation/execute/AWSSupport-
TroubleshootRDP?region=region_code#documentVersion=$LATEST&RDPPortAction=Modify
```

Example: permitir conexões remotas

AWS CLI:

```
aws ssm start-automation-execution --document-name "AWSSupport-TroubleshootRDP" --
parameters "InstanceId=i-1234567890abcdef0, Action=Custom, RemoteConnections=Enable" --
region region_code
```

AWS Systems ManagerConsole do :

```
https://console.aws.amazon.com/systems-manager/automation/execute/AWSSupport-
TroubleshootRDP?region=region_code#documentVersion=$LATEST&RemoteConnections=Enable
```

AWSSupport-ExecuteEC2Rescue

O documento de automação AWSSupport-ExecuteEC2Rescue usa o EC2Rescue para Windows Server com a finalidade de solucionar e restaurar automaticamente a conectividade e os problemas relacionados ao protocolo RDP da instância do EC2. Para obter mais informações, consulte Executar a ferramenta EC2Rescue em instâncias inacessíveis.

O documento de automação AWSSupport-ExecuteEC2Rescue exige que a instância seja interrompida e reiniciada. O Systems Manager Automation interrompe a instância e cria uma Imagem de máquina da Amazon (AMI). Dados armazenados nos volumes de armazenamento da instância são perdidos. O endereço IP público será alterado se você não estiver usando um endereço IP elástico. Para obter mais informações, consulte Executar a ferramenta EC2Rescue em instâncias inacessíveis no Guia do usuário do AWS Systems Manager.

Para resolver o problema usando o documento AWSSupport-ExecuteEC2Rescue

1. Abra o console do Systems Manager.
2. Verifique se você está na mesma região que a instância Amazon EC2 prejudicada.
3. No painel de navegação, escolha Documentos.
4. Pesquise e selecione o documento `AWSSupport-ExecuteEC2Rescue` e depois escolha Executar automação.
5. Em Execution Mode (Modo de execução), escolha Simple execution (Execução simples).
6. Na seção Input parameters (Parâmetros de entrada), em UnreachableInstanceId, insira o ID da instância do Amazon EC2 para a instância inacessível.
7. (Opcional) Para LogDestination, insira o nome do bucket do Amazon Simple Storage Service (Amazon S3) se quiser coletar logs do sistema operacional para solucionar problemas da sua instância do Amazon EC2. Os logs são enviados automaticamente para o bucket especificado.
8. Selecione Execute (Executar).
9. Para monitorar o progresso da execução, no status Execution (Execução), aguarde o status mudar de Pending (Pendente) para Success (Concluído com sucesso). Expanda Outputs (Saídas) para visualizar os resultados. Para visualizar a saída de etapas individuais, Executed Steps (Etapas executadas), escolha Step ID (ID da etapa).

Habilitar a área de trabalho remota em uma instância do EC2 com o registro remoto

Se a instância inacessível não for gerenciada pelo Gerenciador de sessões do AWS Systems Manager, será possível usar o registro remoto para habilitar a área de trabalho remota.

1. No console do EC2, interrompa a instância inacessível.
2. Desvincule o volume raiz da instância inacessível e anexe-o a uma instância acessível na mesma zona de disponibilidade como um volume de armazenamento. Se você não tiver uma instância acessível na mesma zona de disponibilidade, inicie uma. Observe o nome do dispositivo do volume raiz na instância inacessível.
3. Na instância acessível, abra Gerenciamento de disco. Você pode fazer isso executando o comando a seguir em uma janela de prompt de comando.

   ```
   diskmgmt.msc
   ```

4. Clique com o botão direito do mouse no volume recém-conectado que veio da instância inacessível e escolha Online.
5. Abrir o Editor do Registro do Windows. Você pode fazer isso executando o comando a seguir em uma janela de prompt de comando.

   ```
   regedit
   ```

6. No Editor do registro, escolha HKEY_LOCAL_MACHINE e selecione Arquivo, Carregar hive.
7. Selecione a unidade do volume conectado, navegue até `\Windows\System32\config\`, `SYSTEM`, selecione e escolha Open (Abrir).
8. Em Key Name (Nome da chave), insira um nome exclusivo para o hive e escolha OK.
9. Faça uma cópia de backup do hive do registro antes de fazer qualquer alteração no registro.

   a. *Na árvore de console do Editor do Registro, selecione o hive que você carregou:* ***HKEY_LOCAL_MACHINE*** *your-key-name*.

   b. Escolha Arquivo, Exportar.

   c. Na caixa de diálogo Export Registry File (Exportar arquivo do registro), escolha o local no qual deseja salvar a cópia de backup e digite um nome para o arquivo de backup no campo File Name (Nome do arquivo).

   d. Escolha Salvar.

10. No Editor do Registro, navegue para `HKEY_LOCAL_MACHINE\your key name\ControlSet001\Control\Terminal Server` e depois no painel de detalhes, clique duas vezes em fDenyTSConnections.
11. Na caixa de valor Edit DWORD (Editar DWORD) insira `0` no campo Value Data (Dados do valor).
12. Escolha OK.

> **Note**
>
> Se o valor no campo Value data (Dados do valor) for 1, a instância negará conexões de área de trabalho remota. Um valor de `0` permitirá conexões de área de trabalho remota.

13. No Editor do Registro, escolha HKEY_LOCAL_MACHINE*your-key-name* e selecione Arquivo, Descarregar hive.
14. Feche o Editor do registro e Gerenciamento de disco.
15. No console do EC2, desanexe o volume raiz da instância acessível à qual você o anexou e anexe-o novamente à instância inacessível. Ao anexar o volume à instância inacessível, insira o nome do dispositivo que você salvou anteriormente no campo dispositivo.
16. Reinicie a instância inacessível.

Perdi minha chave privada. Como posso me conectar à minha instância do Windows?

Quando você se conecta a uma instância do Windows recém-iniciada, você descriptografa a senha da conta do administrador usando a chave privada para o par de chaves que você especificou quando iniciou a instância.

Se você perder a senha do Administrador e não tiver mais a chave privada, é preciso redefinir a senha ou criar uma nova instância. Para obter mais informações, consulte Redefinir a senha de administrador do Windows para uma instância do Windows do Amazon EC2. Para conhecer as etapas e redefinir a senha usando um documento do Systems Manager, consulte Redefinir senhas e chaves SSH nas instâncias do EC2 no Manual do usuário do AWS Systems Manager.

Solucionar problemas de inicialização de instâncias do Windows do Amazon EC2

Veja a seguir dicas de solução de problemas para ajudar na resolução de problemas de senhas e ativação com instâncias do Windows do Amazon EC2.

Problemas

- "A senha não está disponível"
- "A senha ainda não está disponível"
- "Não é possível recuperar a senha do Windows"
- "Esperando o serviço de metadados"
- "Não é possível ativar o Windows"
- "O Windows não é genuíno (0x80070005)"
- "Nenhum servidor de licença do servidor terminal disponível para fornecer uma licença"
- “Algumas configurações são gerenciadas pela sua organização”

"A senha não está disponível"

Para se conectar a uma instância do Windows usando Remote Desktop, você deve especificar uma conta e uma senha. As contas e as senhas são fornecidas com base na AMI usada para executar a instância. É possível recuperar a senha gerada automaticamente para a conta de administrador ou usar a conta e a senha que estavam em uso na instância original na qual a AMI foi criada.

É possível gerar uma senha para a conta do administrador para instâncias iniciadas usando uma AMI personalizada do Windows. Para gerar a senha, você precisará definir algumas configurações no sistema operacional antes da criação da AMI. Para ter mais informações, consulte Criação de uma AMI baseada no Amazon EBS.

Se sua instância do Windows não estiver configurada para gerar uma senha aleatória, você receberá a seguinte mensagem quando recuperar a senha gerada automaticamente usando o console:

```
Password is not available.
The instance was launched from a custom AMI, or the default password has changed. A
password cannot be retrieved for this instance. If you have forgotten your password,
 you can
```

```
reset it using the Amazon EC2 configuration service. For more information, see
 Passwords for a
Windows Server instance.
```

Verifique a saída do console relativa à instância para ver se a AMI usada para executá-la foi criada com a geração de senha desabilitada. Se a geração de senha estiver desabilitada, a saída do console conterá o seguinte:

```
Ec2SetPassword: Disabled
```

Se a geração de senha estiver desabilitada e não se lembrar da senha da instância original, será possível redefinir a senha para essa instância. Para ter mais informações, consulte Redefinir a senha de administrador do Windows para uma instância do Windows do Amazon EC2.

"A senha ainda não está disponível"

Para se conectar a uma instância do Windows usando Remote Desktop, você deve especificar uma conta e uma senha. As contas e as senhas são fornecidas com base na AMI usada para executar a instância. É possível recuperar a senha gerada automaticamente para a conta de administrador ou usar a conta e a senha que estavam em uso na instância original na qual a AMI foi criada.

A senha deve estar disponível em instantes. Se a senha não estiver disponível, você receberá a seguinte mensagem quando recuperar a senha gerada automaticamente usando o console:

```
Password not available yet.
Please wait at least 4 minutes after launching an instance before trying to retrieve
 the
auto-generated password.
```

Se estiver demorando mais do que quatro minutos e você ainda não conseguiu obter a senha, é possível que o agente de execução da sua instância não esteja configurado para gerar uma senha. Verifique se a saída do console está vazia. Para ter mais informações, consulte Não foi possível obter o resultado do console.

Verifique também se a conta do AWS Identity and Access Management (IAM) que está sendo usada para acessar o Portal de Gerenciamento tem a ação `ec2:GetPasswordData` permitida. Para obter mais informações sobre as permissões do IAM, consulte O que é IAM?.

"Não é possível recuperar a senha do Windows"

Para recuperar a senha gerada automaticamente para a conta de administrador, você deve usar a chave privada para o par de chaves que você especificou ao executar a instância. Se você não tiver especificado um par de chaves quando executou a instância, você receberá a seguinte mensagem.

```
Cannot retrieve Windows password
```

É possível encerrar essa instância e executar uma nova instância usando a mesma AMI, certificando-se de especificar um par de chaves.

"Esperando o serviço de metadados"

Uma instância do Windows deve obter informações dos metadados de sua instância para poder se ativar. Por padrão, a configuração `WaitForMetaDataAvailable` assegura que o serviço EC2Config aguardará que os metadados da instância fiquem acessíveis antes de continuar com o processo de inicialização. Para ter mais informações, consulte Usar metadados da instância para gerenciar a instância do EC2.

Se a instância falhar no teste de acessibilidade, experimente o seguinte para resolver o problema.

- Verifique o bloco CIDR de sua VPC. Uma instância do Windows não pode ser inicializada corretamente se for executada em uma VPC com um intervalo de endereços IP de `224.0.0.0` a `255.255.255.255` (intervalos de endereços IP de classe D e classe E). Esses intervalos de endereços IP são reservados e não devem ser atribuídos a dispositivos de host. Recomendamos criar uma VPC com um bloco CIDR dos intervalos de endereços IP (não roteáveis publicamente) privados especificados na RFC 1918.
- É possível que o sistema foi configurado com um endereço IP estático. Tente criar uma interface de rede e anexá-la à instância.
- Para habilitar o DHCP em uma instância do Windows à qual você não pode se conectar

  1. Interrompa a instância afeta e desanexe seu volume raiz.
  2. Execute uma instância temporária na mesma zona de disponibilidade que a instância afetada.

     > **Warning**
     >
     > Se sua instância temporária for baseada na mesma AMI que a instância original, você deverá concluir as etapas adicionais ou não será possível iniciar a instância

original depois de restaurar o volume raiz, por causa de uma colisão de assinatura de disco. Como alternativa, selecione uma AMI diferente para a instância temporária. Por exemplo, se a instância original usa a AMI AWS do Windows para Windows Server 2016, inicie a instância temporária usando a AMI AWS do Windows para Windows Server 2019.

3. Anexe o volume raiz da instância afetada a essa instância temporária. Conecte-se à instância temporária, abra o utilitário Disk Management e ative a unidade.
4. Na instância temporária, abra o Regedit e selecione HKEY_LOCAL_MACHINE. No menu Arquivo, escolha Carregar Hive. Selecione a unidade, abra o arquivo `Windows\System32\config\SYSTEM` e especifique um nome de chave quando solicitado (você pode usar qualquer nome).
5. Selecione a chave que você acabou de carregar e vá até `ControlSet001\Services\Tcpip\Parameters\Interfaces`. Cada interface de rede é listada por um GUID. Selecione a interface de rede correta. Se o DHCP estiver desabilitado e um endereço IP estático for atribuído, `EnableDHCP` será definido como 0. Para habilitar o DHCP, defina `EnableDHCP` como 1 e exclua as seguintes chaves se existirem: `NameServer`, `SubnetMask`, `IPAddress` e `DefaultGateway`. Selecione a chave novamente e, no menu Arquivo, escolha Descarregar Hive.

   > **Note**
   >
   > Se você possuir várias interfaces de rede, precisará identificar a interface correta para habilitar o DHCP. Para identificar a interface de rede correta, reveja os seguintes valores de chave `NameServer`, `SubnetMask`, `IPAddress` e `DefaultGateway`. Esses valores exibem a configuração estática da instância anterior.

6. (Opcional) Se o DHCP já estiver ativado, é possível que você não tenha uma rota para o serviço de metadados. Atualizar o EC2Config pode resolver esse problema.

   a. Faça download e instale a versão mais recente do serviço EC2Config. Para obter mais informações sobre como instalar esse serviço, consulte the section called “Instalar o EC2Config”.

   b. Extraia arquivos do arquivo `.zip` para o diretório `Temp` na unidade que você associou.

c. Abra Regedit e selecione HKEY_LOCAL_MACHINE. No menu Arquivo, escolha Carregar Hive. Selecione a unidade, abra o arquivo `Windows\System32\config\SOFTWARE` e especifique um nome de chave quando solicitado (você pode usar qualquer nome).

d. Selecione a chave que você acabou de carregar e vá até `Microsoft\Windows\CurrentVersion`. Selecione a chave `RunOnce`. (Se essa chave não existir, clique com o botão direito do mouse em `CurrentVersion`, aponte para Novo, selecione Chave e nomeie a chave `RunOnce`.) Clique com o botão direito do mouse, aponte para Novo e selecione Valor de string. Insira `Ec2Install` como o nome e `C:\Temp\Ec2Install.exe -q` como dados.

e. Selecione a chave novamente e, no menu Arquivo, escolha Descarregar Hive.

7. (Opcional) Se sua instância temporária for baseada na mesma AMI que a instância original, você deverá concluir as etapas a seguir ou não será possível iniciar a instância original depois de restaurar o volume raiz, por causa de uma colisão de assinatura de disco.

> **Warning**
>
> O procedimento a seguir descreve como editar o Registro do Windows usando o Editor do Registro. Se você não estiver familiarizado com o Registro do Windows ou como fazer alterações com segurança usando o Editor do Registro, consulteConfigure the Registry (Configurar o Registro).

a. Abra um prompt de comando, digite regedit.exe e pressione Enter.

b. No Editor do Registro, escolha HKEY_LOCAL_MACHINE no menu contextual (clique com o botão direito do mouse), depois escolha Localizar.

c. Digite Windows Boot Manager e escolha Localizar Próxima.

d. Escolha a chave chamada `11000001`. Essa chave é irmã da chave que você localizou na etapa anterior.

e. No painel direito, selecione `Element` e escolha Modificar no menu de contexto (clique com o botão direito do mouse).

f. Localize a assinatura de disco de quatro bytes no deslocamento 0x38 nos dados. Inverta os bytes para criar a assinatura de disco e anote-a. Por exemplo, a assinatura de disco representada pelos seguintes dados é `E9EB3AA5`:

```
...
```

```
0030  00 00 00 00 01 00 00 00
0038  A5 3A EB E9 00 00 00 00
0040  00 00 00 00 00 00 00 00
...
```

g. Em uma janela do prompt de comando, execute o comando a seguir para iniciar o Microsoft DiskPart.

```
diskpart
```

h. Execute o comando DiskPart a seguir para selecionar o volume. (É possível verificar se o número do disco é 1 usando o utilitário Gerenciamento de disco.)

```
DISKPART> select disk 1

Disk 1 is now the selected disk.
```

i. Execute o comando DiskPart a seguir para obter a assinatura do disco.

```
DISKPART>  uniqueid disk

Disk ID: 0C764FA8
```

j. Se a assinatura de disco mostrada na etapa anterior não corresponder à assinatura de disco do BCD que você anotou anteriormente, use o seguinte comando DiskPart para alterar a assinatura de disco para que ela corresponda:

```
DISKPART> uniqueid disk id=E9EB3AA5
```

8. Usando o utilitário Disk Management, desative o volume da unidade.

> **Note**
>
> A unidade ficará offline automaticamente se a instância temporária estiver executando o mesmo sistema operacional que a instância afetada, portanto, você não precisará deixá-la offline manualmente.

9. Desanexe o volume da instância temporária. É possível encerrar a instância temporária se você não tiver utilização adicional para ela.
10. Restaure o volume raiz da instância afetada anexando o volume como `/dev/sda1`.

11. Inicie a instância afetada.

Se você estiver conectado à instância, abra um navegador de Internet na instância e insira a seguinte URL do servidor de metadados:

```
http://169.254.169.254/latest/meta-data/
```

Se você não conseguir entrar em contato com o servidor de metadados, tente o seguinte para resolver o problema:

- Faça download e instale a versão mais recente do serviço EC2Config. Para obter mais informações sobre como instalar esse serviço, consulte the section called “Instalar o EC2Config”.
- Verifique se a instância do Windows está executando drivers PV de Red Hat. Em caso afirmativo, atualize os drivers PV. Para ter mais informações, consulte the section called “Atualizar drivers de PV”.
- Verifique se o firewall, o IPSec e as configurações de servidor não bloquearem o tráfego de saída para o serviço de metadados (`169.254.169.254`) ou os servidores de AWS KMS (os endereços são especificados nos elementos do `TargetKMSServer` em `C:\Program Files\Amazon\Ec2ConfigService\Settings\ActivationSettings.xml`).
- Verifique se você tem uma rota para o serviço de metadados (`169.254.169.254`) usando o seguinte comando.

  ```
  route print
  ```

- Verifique se há problemas de rede que podem afetar a zona de disponibilidade para sua instância. Acesse http://status.aws.amazon.com/.

"Não é possível ativar o Windows"

As instâncias do Windows usam a ativação do AWS KMS no Windows. É possível receber esta mensagem: `A problem occurred when Windows tried to activate. Error Code 0xC004F074`, se sua instância não conseguir acessar o servidor de AWS KMS. O Windows deve ser ativado a cada 180 dias. O EC2Config tenta entrar em contato com o servidor de AWS KMS antes que o período de ativação expire para garantir que o Windows permaneça ativado.

Se você detectar um problema de ativação do Windows, execute o procedimento a seguir para resolver o problema.

Para EC2Config (AMIs do Windows Server 2012 R2 e anteriores)

1. Faça download e instale a versão mais recente do serviço EC2Config. Para obter mais informações sobre como instalar esse serviço, consulte the section called “Instalar o EC2Config”.
2. Faça login na instância e abra o seguinte arquivo: `C:\Program Files\Amazon\Ec2ConfigService\Settings\config.xml`.
3. Localize o plugin Ec2WindowsActivate no arquivo `config.xml`. Altere o estado para Habilitado e salve suas alterações.
4. No snap-in Windows Services, reinicie o serviço EC2Config ou reinicialize a instância.

Se isso não resolver o problema de ativação, siga estas etapas adicionais.

1. Defina o AWS KMS de destino: C:\> slmgr.vbs /skms 169.254.169.250:1688
2. Ative o Windows: C:\> slmgr.vbs /ato

Para EC2Launch (AMIs do Windows Server 2016 e posteriores)

1. De um prompt do PowerShell com direitos administrativos, importe o módulo do EC2Launch:

```
PS C:\> Import-Module "C:\ProgramData\Amazon\EC2-Windows\Launch\Module
\Ec2Launch.psd1"
```

2. Chame a função Add-Routes para ver a lista de novas rotas:

```
PS C:\> Add-Routes
```

3. Chamar a função Set-ActivationSettings:

```
PS C:\> Set-Activationsettings
```

4. Em seguida, execute o seguinte script para ativar o Windows:

```
PS C:\> cscript "${env:SYSTEMROOT}\system32\slmgr.vbs" /ato
```

Tanto para EC2Config como para EC2Launch, se você ainda estiver recebendo um erro de ativação, verifique as informações a seguir.

- Verifique se você tem rotas para os servidores de AWS KMS. Abra `C:\Program Files\Amazon\Ec2ConfigService\Settings\ActivationSettings.xml` e localize os elementos `TargetKMSServer`. Execute o comando a seguir e verifique se os endereços para esses servidores de AWS KMS estão listados.

```
route print
```

- Verifique se a chave do cliente de AWS KMS está definida. Execute o seguinte comando e verifique a saída.

```
C:\Windows\System32\slmgr.vbs /dlv
```

  Se o resultado contiver o erro Error: product key not found (Erro: chave de produto não encontrada), a chave de cliente do AWS KMS não estará definida. Se a chave de cliente do AWS KMS não estiver definida, procure pela chave de cliente conforme descrito neste artigo da Microsoft: Ativação de cliente e chaves de produto do AWS KMS, e execute o comando a seguir para definir a chave de cliente do AWS KMS.

```
C:\Windows\System32\slmgr.vbs /ipk client_key
```

- Verifique se o sistema tem a hora e o fuso horário corretos. Se você estiver usando um fuso horário diferente do UTC, adicione a seguinte chave de registro e configure-a 1 para garantir que a hora esteja correta: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TimeZoneInformation\RealTimeIsUniversal`.
- Se o Firewall do Windows estiver habilitado, desabilite-o temporariamente usando o seguinte comando.

```
netsh advfirewall set allprofiles state off
```

"O Windows não é genuíno (0x80070005)"

As instâncias do Windows usam a ativação do AWS KMS no Windows. Se uma instância não conseguir concluir o processo de ativação, ela relatará que a cópia do Windows não é genuína.

Tente as sugestões para "Não é possível ativar o Windows".

"Nenhum servidor de licença do servidor terminal disponível para fornecer uma licença"

Por padrão, o Windows Server é licenciado para dois usuários simultâneos por meio do Remote Desktop. Se você precisar fornecer a mais de dois usuários acesso simultâneo à sua instância do Windows por meio do Remote Desktop, compre uma licença de acesso de cliente (CAL) do Remote Desktop Services e instale as funções Remote Desktop Session Host e Remote Desktop Licensing Server.

Verifique se há os seguintes problemas:

- Você excedeu o número máximo de sessões simultâneos de RDP.
- Você instalou a função Windows Remote Desktop Services.
- O licenciamento expirou. Se o licenciamento expirou, você não poderá se conectar à sua instância do Windows como um usuário. É possível tentar o seguinte:
  - Conecte-se à instância da linha de comando usando um parâmetro `/admin`, por exemplo:

    ```
    mstsc /v:instance /admin
    ```

    Para obter mais informações, consulte o seguinte artigo da Microsoft: Acessar a área de trabalho remota por meio da linha de comando.
  - Interrompa a instância, desanexe seus volumes do Amazon EBS e anexe-os a outra instância na mesma zona de disponibilidade para recuperar os dados.

“Algumas configurações são gerenciadas pela sua organização”

As instâncias executadas a partir das AMIs mais recentes do Windows Server podem exibir uma mensagem do Windows Update informando “Algumas configurações são gerenciadas por sua organização”. Essa mensagem aparece como resultado de alterações no Windows Server e não afeta o comportamento do Windows Update nem sua capacidade de gerenciar as configurações de atualização.

Como remover o aviso

1. Abra `gpedit.msc` e navegue até Configuração do Computador, Modelos Administrativos, Componentes do Windows, Atualizações do Windows. Edite Configurar a atualização automática e defina-a como habilitada.

2. Em um prompt de comando, atualize a política de grupo usando gpupdate /force.
3. Feche e reabra as configurações do Windows Update. Você verá a mensagem acima sobre as configurações serem gerenciadas por sua organização, seguida por "Baixaremos automaticamente as atualizações, exceto em conexões limitadas (em que taxas podem ser cobradas). Nesse caso, faremos automaticamente download dessas atualizações necessárias para manter o Windows funcionando sem problemas.
4. Retorne para `gpedit.msc` e defina a política de grupo como não configurada. Execute gpupdate /force novamente.
5. Feche o prompt de comando e aguarde alguns minutos.
6. Reabra as configurações do Windows Update. Você não deve ver a mensagem “Algumas configurações são gerenciadas pela sua organização”

Solucionar problemas com instâncias do Windows do Amazon EC2

Veja a seguir dicas de solução de problemas para ajudar na resolução de problemas com instâncias do Windows do Amazon EC2.

Problemas

- Não é possível conectar o AWS Systems Manager Sessions Manager a uma instância do Windows Server 2025
- Os volumes do EBS não são inicializados no Windows Server 2016 e 2019
- Inicialize uma instância do EC2 Windows no Directory Services Restore Mode (DSRM)
- A instância perde a conectividade de rede ou as tarefas agendadas não são executadas quando esperado
- Não foi possível obter o resultado do console
- Windows Server 2012 R2 não disponível na rede
- Colisão de assinatura em disco

Não é possível conectar o AWS Systems Manager Sessions Manager a uma instância do Windows Server 2025

Você pode encontrar um problema ao conectar o AWS Systems Manager Sessions Manager a uma instância do Windows Server 2025. Para resolver esse problema, faça logon na instância, navegue

até `Settings > Apps > Optional Features` e adicione`WMIC`. Reinicie o serviço SSM Agent ou reinicialize a instância e Sessions Manager deverá se conectar.

Também é possível usar o seguinte comando do PowerShell para realizar a mesma ação:

```
Start-Process -FilePath "$env:SystemRoot\system32\Dism.exe" -ArgumentList @('/
Online', '/Add-Capability', '/CapabilityName:WMIC~~~~') -Wait; Restart-Service -Name
 AmazonSSMAgent
```

Os volumes do EBS não são inicializados no Windows Server 2016 e 2019

Instâncias criadas nas Imagens de máquina da Amazon (AMIs) para Windows Server 2016 e 2019 usam o agente EC2Launch v1 para uma variedade de tarefas de inicialização, incluindo a inicialização de volumes do EBS. Por padrão, o EC2Launch v1 não inicializa volumes secundários. No entanto, é possível configurar o EC2Launch v1 para inicializar esses discos automaticamente, como mostrado a seguir.

Mapear letras de unidade a volumes

1. Conecte-se à instância para configurar e abrir o arquivo `C:\ProgramData\Amazon\EC2-Windows\Launch\Config\DriveLetterMappingConfig.json` em um editor de texto.
2. Especifique as configurações do volume da seguinte maneira:

   ```
   {
   "driveLetterMapping": [
    {
      "volumeName": "sample volume",
      "driveLetter": "H"
    }]
   }
   ```
3. Salve as alterações e feche o arquivo.
4. Abra o Windows PowerShell e use o seguinte comando para executar o script do EC2Launch v1 que inicializa os discos:

   ```
   PS C:\>  C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeDisks.ps1
   ```

   Para inicializar os discos sempre que a instância for inicializada, adicione o sinalizador `-Schedule` da seguinte forma:

```
PS C:\>  C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeDisks.ps1 -
Schedule
```

O agente EC2Launch v1 pode executar scripts de inicialização de instâncias, como `initializeDisks.ps1` em paralelo com o script `InitializeInstance.ps1`. Se o script `InitializeInstance.ps1` reinicializar a instância, ele poderá interromper outras tarefas agendadas que são executadas na inicialização da instância. Para evitar possíveis conflitos, recomendamos que você adicione lógica ao seu script `initializeDisks.ps1` para garantir que a inicialização da instância tenha sido concluída primeiro.

> **Note**
>
> Se o script EC2Launch não inicializar os volumes, verifique se os volumes estão online. Se os volumes estiverem offline, execute o comando a seguir para colocar todos os discos online.
>
> ```
> PS C:\> Get-Disk | Where-Object IsOffline -Eq $True | Set-Disk -IsOffline
>  $False
> ```

Inicialize uma instância do EC2 Windows no Directory Services Restore Mode (DSRM)

Se uma instância que estiver executando o Microsoft Active Directory tiver uma falha do sistema ou outros problemas críticos, você poderá solucionar problemas na instância inicializando em uma versão especial do modo seguro denominado Directory Services Restore Mode (DSRM). No DSRM, você pode reparar ou recuperar o Ative Directory.

Suporte a drivers para DSRM

A forma como você habilita o DSRM e faz a inicialização na instância depende dos drivers que a instância estiver executando. No console do EC2, você pode visualizar os detalhes de versão do driver para uma instância no log do sistema. As tabelas a seguir mostram quais drivers são compatíveis com o DSRM.

Versões do driver	DSRM com suporte?	Próximas etapas
Citrix PV 5.9	Não	Restaure a instância de um backup. Você não pode habilitar o DSRM.
AWS PV 7.2.0	Não	Embora o DSRM não tenha suporte para esse driver, você ainda pode desanexar o volume raiz da instância , criar um snapshot do volume ou criar uma AMI dele e anexá-la a outra instância na mesma zona de disponibi lidade que um volume secundário. Em seguida, você pode habilitar o DSRM (como descrito nesta seção).
AWS PV 7.2.2 e posteriores	Sim	Desanexe o volume raiz, anexe-o a outra instância e habilite o DSRM (como descrito nesta seção).
Redes avançadas	Sim	Desanexe o volume raiz, anexe-o a outra instância e habilite o DSRM (como descrito nesta seção).

Para obter informações sobre como habilitar as redes aperfeiçoadas, consulte the section called “Elastic Network Adapter (ENA)”. Para obter informações sobre como atualizar drivers PV da AWS, consulte Upgrade PV drivers on Windows instances.

Configurar uma instância para ser inicializada no DSRM

As instâncias do EC2 Windows não têm conectividade de rede antes que o sistema operacional seja executado. Por esse motivo, você não pode pressionar o botão F8 no teclado para selecionar uma opção de inicialização. Você deve usar um dos seguintes procedimentos para inicializar uma instância do EC2 Windows Server no DSRM.

Se você suspeitar que o Active Directory foi danificado e a instância ainda estiver em execução, você poderá configurar a instância para fazer a inicialização no DSRM usando a caixa de diálogo Configurações do sistema ou o prompt de comando.

Para inicializar uma instância online no DSRM usando a caixa de diálogo Configurações do sistema

1. Na caixa de diálogo Executar, digite `msconfig` e pressione Enter.
2. Escolha a guia Inicializar.

3. Em Opções de inicialização, escolha Inicialização segura.
4. Escolha Reparo do Active Directory e escolha OK. O sistema solicita que você reinicialize o servidor.

Para inicializar uma instância online no DSRM usando a linha de comando

Em uma janela do prompt de comando, execute o comando a seguir:

```
bcdedit /set safeboot dsrepair
```

Se uma instância estiver offline e inacessível, você deverá desanexar o volume raiz e anexá-lo a outra instância para habilitar o modo DSRM.

Para inicializar uma instância offline no DSRM

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Localize e selecione a instância afetada. Escolha Instance state (Estado da instância) e Stop instance (Interromper instância).
4. Escolha Launch instances (Executar instância) e crie uma instância temporária na mesma zona de disponibilidade que a instância afetada. Escolha um tipo de instância que use uma versão diferente do Windows. Por exemplo, se sua instância for o Windows Server 2016, escolha uma instância do Windows Server 2019.

   > **Important**
   >
   > Se você não criar a instância na mesma zona de disponibilidade que a instância afetada, não conseguirá associar o volume do dispositivo raiz da instância afetada à nova instância.

5. No painel de navegação, escolha Volumes.
6. Localize o volume do dispositivo raiz da instância afetada. Separe o volume e associe-o à instância temporária criada anteriormente. Associe-a com o nome do padrão do dispositivo (xvdf).
7. Use a Área de Trabalho Remota para conectar-se à instância temporária e use em utilitário Gerenciamento de Disco para disponibilizar o volume para uso.

8. Abra um prompt de comando e execute o seguinte comando. Substitua D pela letra real de unidade do volume secundário que você acabou de anexar:

```
bcdedit /store D:\Boot\BCD /set {default} safeboot dsrepair
```

9. No utilitário de Gerenciamento de Disco, escolha a unidade que você associou anteriormente, abra o menu contextual (botão direito do mouse) e escolha Offline.
10. No console do EC2, separe o volume afetado de instância temporária e reanexe-o à sua instância original com o nome de dispositivo `/dev/sda1`. Você deve especificar o nome desse dispositivo para designar o volume como volume do dispositivo raiz.
11. Inicie a instância.
12. Depois que a instância passar nas verificações de integridade no console do EC2, conecte-se à instância usando o Remote Desktop e verifique se ela é inicializada no modo DSRM.
13. (Opcional) Exclua ou interrompa a instância temporária que você criou nesse procedimento.

A instância perde a conectividade de rede ou as tarefas agendadas não são executadas quando esperado

Se você reiniciar sua instância e perder a conectividade de rede, é possível que a instância tenha o horário errado.

Por padrão, as instâncias do Windows usam o tempo universal coordenado (UTC). Se você definir o horário de sua instância como outro fuso horário e, em seguida, reiniciá-la, ocorrerá um desvio no horário, e a instância perderá temporariamente seu endereço IP. A instância recuperará a conectividade de rede, mas isso pode levar várias horas. A quantidade de tempo que leva para a instância recuperar a rede de conectividade depende da diferença entre o UTC e o outro fuso horário.

Esse mesmo problema no horário também pode fazer com que as tarefas agendadas não sejam executadas no horário esperado. Nesse caso, as tarefas agendadas não são executadas quando esperado porque a instância tem o horário incorreto.

Para usar um fuso horário diferente do UTC de forma persistente, você deve definir a chave de Registro RealTimeIsUniversal. Sem essa chave, a instância usará o UTC depois de reiniciá-la.

Para resolver problemas no horário que causam a perda da conectividade de rede

1. Certifique-se de que você esteja executando os drivers PV recomendados. Para obter mais informações, consulte the section called “Atualizar drivers de PV”.
2. Verifique se a chave de Registro a seguir existe e está definida como 1: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TimeZoneInformation \RealTimeIsUniversal

Não foi possível obter o resultado do console

Para instâncias do Windows, o console da instância exibe o resultado das tarefas realizadas durante o processo de inicialização do Windows. Se o Windows for inicializado com êxito, a última mensagem registrada será `Windows is Ready to use`. Você também pode exibir mensagens de log de eventos no console, mas esse recurso pode não estar habilitado por padrão, dependendo da sua versão do Windows. Para obter mais informações, consulte the section called “Agentes de inicialização do Windows”.

Para obter a saída do console da instância usando o console do Amazon EC2, selecione a instância e escolha Actions (Ações), Monitor and troubleshoot (Monitorar e solucionar problemas), Get system log (Obter log do sistema). Para obter a saída do console usando a linha de comando, use um dos seguintes comandos: get-console-output (AWS CLI) ou Get-EC2ConsoleOutput (AWS Tools for Windows PowerShell).

Para instâncias executadas no Windows Server 2012 R2 e anteriores, se a saída do console estiver vazia, poderá indicar um problema com o serviço EC2Config, como um arquivo de configuração desconfigurado ou que o Windows não foi inicializado corretamente. Para corrigir o problema, faça download e instale a versão mais recente do EC2Config. Para obter mais informações, consulte the section called “Instalar o EC2Config”.

Windows Server 2012 R2 não disponível na rede

Para obter informações sobre como solucionar problemas de uma instância do Windows Server 2012 R2 que não está disponível na rede, consulte Windows Server 2012 R2 loses network and storage connectivity after an instance reboot.

Colisão de assinatura em disco

Você pode conferir e resolver colisões de assinatura em disco usando o EC2Rescue para Windows Server. Como alternativa, você pode resolver problemas de assinatura em disco manualmente realizando as etapas a seguir.

> **Warning**
>
> O procedimento a seguir descreve como editar o Registro do Windows usando o Editor do Registro. Se você não estiver familiarizado com o Registro do Windows ou como fazer alterações com segurança usando o Editor do Registro, consulteConfigure the Registry (Configurar o Registro).

1. Abra um prompt de comando, digite regedit.exe e pressione Enter.
2. No Editor do Registro, escolha HKEY_LOCAL_MACHINE no menu contextual (clique com o botão direito do mouse), depois escolha Localizar.
3. Digite Windows Boot Manager e escolha Localizar Próxima.
4. Escolha a chave chamada `11000001`. Essa chave é irmã da chave que você localizou na etapa anterior.
5. No painel direito, selecione `Element` e escolha Modificar no menu de contexto (clique com o botão direito do mouse).
6. Localize a assinatura de disco de quatro bytes no deslocamento 0x38 nos dados. Esta é a assinatura do Boot Configuration Database (BCD). Inverta os bytes para criar a assinatura de disco e anote-a. Por exemplo, a assinatura de disco representada pelos seguintes dados é `E9EB3AA5`:

   ```
   ...
   0030  00 00 00 00 01 00 00 00
   0038  A5 3A EB E9 00 00 00 00
   0040  00 00 00 00 00 00 00 00
   ...
   ```

7. Em uma janela do prompt de comando, execute o comando a seguir para iniciar o Microsoft DiskPart.

   ```
   diskpart
   ```

8. Execute o comando `select disk` DiskPart e especifique o número do disco para o volume com a colisão da assinatura do disco.

> **Tip**
>
> Para verificar o número do disco do volume com a colisão da assinatura do disco, use o utilitário de Gerenciamento de disco. Abra um prompt de comando, digite `compmgmt.msc` e pressione Enter. No painel de navegação à esquerda, clique duas vezes em Gerenciamento de disco. No utilitário de Gerenciamento de disco, verifique o número do disco do volume off-line com a colisão de assinatura do disco.

```
DISKPART> select disk 1
Disk 1 is now the selected disk.
```

9. Execute o comando DiskPart a seguir para obter a assinatura do disco.

```
DISKPART>  uniqueid disk
Disk ID: 0C764FA8
```

10. Se a assinatura de disco mostrada na etapa anterior não corresponder à assinatura de disco que você anotou anteriormente, use o seguinte comando DiskPart para alterar a assinatura de disco para que ela corresponda:

```
DISKPART> uniqueid disk id=E9EB3AA5
```

Redefinir a senha de administrador do Windows para uma instância do Windows do Amazon EC2

Caso não consiga mais se conectar à sua instância do Windows do Amazon EC2 porque a senha do administrador do Windows foi esquecida ou expirou, você poderá redefinir a senha.

> **Note**
>
> Existe um documento de automação do AWS Systems Manager que aplica automaticamente as etapas manuais necessárias para redefinir a senha do administrador local. Para obter

mais informações, consulte Redefinir senhas e chaves SSH em instâncias do EC2 no Guia do usuário do AWS Systems Manager.

Os métodos manuais para redefinir a senha de administrador usam o EC2Launch v2, o EC2Config ou o EC2Launch.

- Para todas as AMIs do Windows compatíveis que incluem o agente EC2Launch v2, use o EC2Launch v2.
- Para AMIs do Windows anteriores ao Windows Server 2016, você pode usar o serviço EC2Config.
- Para AMIs do Windows Server 2016 e posterior, use o serviço EC2Launch.

Esses procedimentos também descrevem como se conectar a uma instância se você perder o par de chaves que foi usado para criar a instância. O Amazon EC2 usa uma chave pública para criptografar uma parte dos dados, como uma senha, e uma chave privada para descriptografar os dados. As chaves pública e privada são conhecidas como par de chaves. Com instâncias do Windows, você usa um par de chaves para obter a senha do administrador e faz login usando o RDP.

> **Note**
>
> Se você desabilitou a conta de administrador local na instância e sua instância estiver configurada para o Systems Manager, você também poderá reabilitar e redefinir sua senha de administrador local usando EC2Rescue e o Run Command. Para obter mais informações, consulte Use EC2Rescue for Windows Server with Systems Manager Run Command.

Sumário

- Redefinir a senha de administrador do Windows para uma instância do EC2 usando o EC2Launch v2
- Redefinir a senha de administrador do Windows para uma instância do EC2 usando o EC2Launch
- Redefinir a senha de administrador do Windows para uma instância do EC2 usando o EC2Config

Redefinir a senha de administrador do Windows para uma instância do EC2 usando o EC2Launch v2

Se você perdeu a senha de administrador do Windows e está usando uma AMI compatível do Windows que inclua o agente EC2Launch v2, poderá usar o EC2Launch v2 para gerar uma nova senha.

Se estiver usando uma AMI do Windows Server 2016 ou posterior que não inclua o agente EC2Launch v2, consulte Redefinir a senha de administrador do Windows para uma instância do EC2 usando o EC2Launch.

Se estiver usando uma AMI do Windows Server anterior a 2016 que não inclua o agente EC2Launch v2, consulte Redefinir a senha de administrador do Windows para uma instância do EC2 usando o EC2Config.

> **Note**
>
> Se você desabilitou a conta de administrador local na instância e sua instância estiver configurada para o Systems Manager, você também poderá reabilitar e redefinir sua senha de administrador local usando EC2Rescue e o Run Command. Para obter mais informações, consulte Use EC2Rescue for Windows Server with Systems Manager Run Command.

> **Note**
>
> Existe um documento de automação do AWS Systems Manager que aplica automaticamente as etapas manuais necessárias para redefinir a senha do administrador local. Para obter mais informações, consulte Redefinir senhas e chaves SSH em instâncias do EC2 no Guia do usuário do AWS Systems Manager.

Para redefinir a senha de administrador do Windows usando o EC2Launch v2, é necessário fazer o seguinte:

- Etapa 1: verificar se o agente EC2Launch v2 está em execução
- Etapa 2: Desanexar o volume raiz da instância
- Etapa 3: Anexar o volume a uma instância temporária
- Etapa 4: Excluir o arquivo .run-once

- Etapa 5: Reiniciar a instância original

Etapa 1: verificar se o agente EC2Launch v2 está em execução

Antes de tentar redefinir a senha de administrador, verifique se o agente EC2Launch v2 está instalado e em execução. O agente EC2Launch v2 será utilizado para redefinir a senha de administrador posteriormente nesta seção.

Verificar se o agente EC2Launch v2 está em execução

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias) e selecione a instância que precisa de redefinição da senha. Essa instância é denominada original neste procedimento.
3. Escolha Actions (Ações), Monitor and troubleshoot (Monitorar e solucionar problemas), Get system log Obter log do sistema.
4. Localize a entrada do EC2 Launch, por exemplo, Launch: EC2Launch v2 service v2.0.124 (Launch: serviço EC2Launch v2 v2.0.124). Se essa entrada for exibida, o serviço EC2Launch v2 estará em execução.

   Se a saída do log do sistema estiver vazia ou se o agente EC2Launch v2 não estiver em execução, solucione os problemas da instância usando o serviço Instance Console Screenshot. Para ter mais informações, consulte Fazer uma captura de tela de uma instância inacessível.

Etapa 2: Desanexar o volume raiz da instância

Não será possível usar o EC2Launch v2 para redefinir uma senha de administrador se o volume no qual a senha está armazenada estiver anexado a uma instância como o volume raiz. Você precisa desanexar o volume da instância original antes de anexá-lo a uma instância temporária como um volume secundário.

Para desanexar o volume raiz da instância

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância que requer uma redefinição de senha e escolha Estado da instância e Parar instância. Depois que o status da instância for alterado para Stopped (Parado), siga para a próxima etapa.

4. (Opcional) Se você tiver a chave privada especificada ao iniciar esta instância, continue para a próxima etapa. Caso contrário, use as etapas a seguir para substituir a instância por uma nova que você executa com um novo par de chaves.

   a. Crie um par de chaves usando o console do Amazon EC2. Para dar ao seu novo par de chaves um nome exatamente igual ao do par de chaves perdido, primeiro exclua o par de chaves existente.

   b. Selecione a instância a ser substituída. Anote o tipo de instância, a VPC, a sub-rede, o grupo de segurança e a função do IAM da instância.

   c. Com a instância selecionada, escolha Ações, Imagem e modelos, Criar imagem. Digite um nome e uma descrição para a imagem e depois escolha Create image (Criar imagem).

   d. No painel de navegação, selecione AMIs. Aguarde até que o status da imagem mude para disponível. Em seguida, selecione a imagem e escolha Iniciar instância a partir da AMI.

   e. Preencha os campos para iniciar uma instância, certificando-se de selecionar o mesmo tipo de instância, VPC, sub-rede, grupo de segurança e perfil do IAM da instância a ser substituída e escolha Iniciar instância.

   f. Quando solicitado, escolha o par de chaves que você criou para a nova instância e escolha Iniciar instância.

   g. (Opcional) Se a instância original tiver um endereço IP elástico associado, transfira-o para a nova instância. Se a instância original tiver volumes do EBS além do volume raiz, transfira-os para a nova instância.

5. Desanexe o volume raiz da instância original da seguinte forma:

   a. Selecione a instância original e escolha a guia Armazenamento. Anote o nome do dispositivo raiz em Nome de dispositivo raiz. Encontre o volume com este nome de dispositivo em Dispositivo de blocos e anote o ID do volume.

   b. No painel de navegação, escolha Volumes.

   c. Na lista de volumes, selecione o volume que você anotou como dispositivo raiz e escolha Ações e Desanexar volume. Após o status do volume mudar para available (disponível), vá para a próxima etapa.

6. Se você criou uma nova instância para substituir a instância original, é possível encerrar a instância original agora. A instância não é mais necessária. Nas etapas remanescentes deste procedimento, todas as referências à instância original se aplicam à nova instância que você criou.

Etapa 3: Anexar o volume a uma instância temporária

Em seguida, execute uma instância temporária e anexe o volume a ela como um volume secundário. Esta é a instância usada para modificar o arquivo de configuração.

Para executar uma instância temporária e anexar o volume

1. Inicie a instância temporária da seguinte forma:

   a. No painel de navegação, escolha Instances (Instâncias), Launch instances (Iniciar instâncias) e, em seguida, selecione uma AMI.

   > **Important**
   >
   > Para evitar colisões de assinatura de disco, você deve selecionar uma AMI para uma versão diferente do Windows. Por exemplo, se a instância original executar o Windows Server 2019, inicie a instância temporária usando a AMI básica do Windows Server 2016.

   b. Selecione um tipo de instância padrão e, a seguir, escolha Next: Configure Instance Details (Próximo: Configurar detalhes da instância).

   c. Na página Configure Instance Details (Configurar os detalhes da instância), em Subnet (Sub-rede), selecione a mesma zona de disponibilidade que a instância original e escolha Review and Launch (Revisar e iniciar).

   > **Important**
   >
   > A instância temporária deve estar na mesma zona de disponibilidade que a instância original. Se sua instância temporária estiver em uma zona de disponibilidade diferente, você não poderá anexar o volume raiz da instância original a ela.

   d. Na página Review Instance Launch, escolha Launch.

   e. Quando solicitado, crie um par de chaves, faça download para um local seguro no computador e escolha Launch Instances (Iniciar instâncias).

2. Anexe o volume à instância temporária como um volume secundário da seguinte forma:

a. No painel de navegação, selecione Volumes, selecione o volume que você desanexou da instância original e escolha Actions (Ações), Attach Volume (Anexar volume).

b. Na caixa de diálogo Attach Volume (Anexar volume), em Instances (Instâncias), comece a digitar o nome ou ID da instância temporária e selecione-a na lista.

c. Em Device (Dispositivo), digite **`xvdf`** (se já não estiver lá) e escolha Attach (Anexar).

Etapa 4: Excluir o arquivo .run-once

Agora, você deve excluir o arquivo `.run-once` do volume off-line anexado à instância. Isso instrui o EC2Launch v2 a executar todas as tarefas com uma frequência de `once`, o que inclui a definição da senha de administrador. O caminho do arquivo no volume secundário que você anexou será semelhante a `D:\ProgramData\Amazon\EC2Launch\state\.run-once`.

Excluir o arquivo .run-once

1. Abra o utilitário Gerenciamento de Disco e coloque a unidade on-line usando estas instruções: Make an Amazon EBS volume available for use.
2. Localize o arquivo `.run-once` no disco que você colocou on-line.
3. Exclua o arquivo .run-once.

> **Important**
>
> Todos os scripts definidos para uma execução serão acionados por essa ação.

Etapa 5: Reiniciar a instância original

Depois de excluir o arquivo `.run-once`, anexe novamente o volume à instância original como o volume raiz e conecte-se à instância usando seu par de chaves para recuperar a senha do administrador.

1. Reanexe o volume à instância original da seguinte forma:

   a. No painel de navegação, selecione Volumes, selecione o volume que você desanexou da instância temporária e escolha Actions (Ações), Attach Volume (Anexar volume).

b. Na caixa de diálogo Attach Volume (Anexar volume), em Instances (Instâncias), comece a digitar o nome ou ID da instância original e selecione-a.

c. Em Device (Dispositivo), digite **/dev/sda1**.

d. Escolha Associar. Após o status do volume mudar para `in-use`, vá para a próxima etapa.

2. No painel de navegação, escolha Instances (Instâncias). Selecione a instância original e escolha Instance state (Estado da instância) e Start instance (Iniciar instância). Após o estado da instância mudar para `Running`, vá para a próxima etapa.

3. Recupere a nova senha de administrador do Windows usando a chave privada do novo par de chaves e conecte-se à instância. Para obter mais informações, consulte Conectar-se à instância do Windows no usando RDP.

> **Important**
>
> A instância recebe um novo endereço IP público depois de você a interrompe e a inicia. Não deixe de se conectar à instância usando o nome DNS público atual. Para obter mais informações, consulte Alterações do estado de instâncias do Amazon EC2.

4. (Opcional) Você pode encerrar a instância temporária se não tiver utilização adicional para ela. Selecione a instância temporária e escolha Instance state (Estado da instância) e Terminate instance (Encerrar instância).

Redefinir a senha de administrador do Windows para uma instância do EC2 usando o EC2Launch

Se você esqueceu a senha de administrador do Windows e está usando uma AMI do Windows Server 2016 ou posterior, poderá usar a ferramenta EC2Rescue, que utiliza o serviço EC2Launch para gerar uma nova senha.

Caso esteja usando uma AMI do Windows Server 2016 ou posterior que não inclua o agente EC2Launch v2, você pode usar o EC2Launch para gerar uma nova senha.

Se você estiver usando uma AMI do Windows Server anterior ao Windows Server 2016, consulte Redefinir a senha de administrador do Windows para uma instância do EC2 usando o EC2Config.

> **Warning**
>
> Quando você interrompe uma instância, os dados em todos os volumes de armazenamento de instâncias são apagados. Para manter dados longe dos volumes de armazenamento de instância, faça backup no armazenamento persistente.

> **Note**
>
> Se você desabilitou a conta de administrador local na instância e sua instância estiver configurada para o Systems Manager, você também poderá reabilitar e redefinir sua senha de administrador local usando EC2Rescue e o Run Command. Para obter mais informações, consulte Use EC2Rescue for Windows Server with Systems Manager Run Command.

> **Note**
>
> Existe um documento de automação do AWS Systems Manager que aplica automaticamente as etapas manuais necessárias para redefinir a senha do administrador local. Para obter mais informações, consulte Redefinir senhas e chaves SSH em instâncias do EC2 no Guia do usuário do AWS Systems Manager.

Para redefinir sua senha de administrador do Windows usando o EC2Launch, você precisa fazer o seguinte:

- Etapa 1: Desanexar o volume raiz da instância
- Etapa 2: Anexar o volume a uma instância temporária
- Etapa 3: Redefinir a senha de administrador
- Etapa 4: Reiniciar a instância original

Etapa 1: Desanexar o volume raiz da instância

Você não poderá usar o EC2Launch para redefinir uma senha de administrador se o volume no qual a senha está armazenada estiver anexado a uma instância como o volume raiz. Você precisa desanexar o volume da instância original antes de anexá-lo a uma instância temporária como um volume secundário.

Para desanexar o volume raiz da instância

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância que requer uma redefinição de senha e escolha Estado da instância e Parar instância. Depois que o status da instância for alterado para Stopped (Parado), siga para a próxima etapa.
4. (Opcional) Se você tiver a chave privada especificada ao iniciar esta instância, continue para a próxima etapa. Caso contrário, use as etapas a seguir para substituir a instância por uma nova que você executa com um novo par de chaves.

   a. Crie um par de chaves usando o console do Amazon EC2. Para dar ao seu novo par de chaves um nome exatamente igual ao do par de chaves perdido, primeiro exclua o par de chaves existente.

   b. Selecione a instância a ser substituída. Anote o tipo de instância, a VPC, a sub-rede, o grupo de segurança e a função do IAM da instância.

   c. Com a instância selecionada, escolha Ações, Imagem e modelos, Criar imagem. Digite um nome e uma descrição para a imagem e depois escolha Create image (Criar imagem).

   d. No painel de navegação, selecione AMIs. Aguarde até que o status da imagem mude para disponível. Em seguida, selecione a imagem e escolha Iniciar instância a partir da AMI.

   e. Preencha os campos para iniciar uma instância, certificando-se de selecionar o mesmo tipo de instância, VPC, sub-rede, grupo de segurança e perfil do IAM da instância a ser substituída e escolha Iniciar instância.

   f. Quando solicitado, escolha o par de chaves que você criou para a nova instância e escolha Iniciar instância.

   g. (Opcional) Se a instância original tiver um endereço IP elástico associado, transfira-o para a nova instância. Se a instância original tiver volumes do EBS além do volume raiz, transfira-os para a nova instância.

5. Desanexe o volume raiz da instância original da seguinte forma:

   a. Selecione a instância original e escolha a guia Armazenamento. Anote o nome do dispositivo raiz em Nome de dispositivo raiz. Encontre o volume com este nome de dispositivo em Dispositivo de blocos e anote o ID do volume.

   b. No painel de navegação, escolha Volumes.

c. Na lista de volumes, selecione o volume que você anotou como dispositivo raiz e escolha Ações e Desanexar volume. Após o status do volume mudar para available (disponível), vá para a próxima etapa.

6. Se você criou uma nova instância para substituir a instância original, é possível encerrar a instância original agora. A instância não é mais necessária. Nas etapas remanescentes deste procedimento, todas as referências à instância original se aplicam à nova instância que você criou.

Etapa 2: Anexar o volume a uma instância temporária

Em seguida, execute uma instância temporária e anexe o volume a ela como um volume secundário. Esta é a instância que você usa para executar o EC2Launch.

Para executar uma instância temporária e anexar o volume

1. Inicie a instância temporária da seguinte forma:

   a. No painel de navegação, escolha Instances (Instâncias), Launch instances (Iniciar instâncias) e, em seguida, selecione uma AMI.

   > **Important**
   >
   > Para evitar colisões de assinatura de disco, você deve selecionar uma AMI para uma versão diferente do Windows. Por exemplo, se a instância original executar o Windows Server 2019, inicie a instância temporária usando a AMI básica do Windows Server 2016.

   b. Selecione um tipo de instância padrão e, a seguir, escolha Next: Configure Instance Details (Próximo: Configurar detalhes da instância).

   c. Na página Configure Instance Details (Configurar os detalhes da instância), em Subnet (Sub-rede), selecione a mesma zona de disponibilidade que a instância original e escolha Review and Launch (Revisar e iniciar).

   > **Important**
   >
   > A instância temporária deve estar na mesma zona de disponibilidade que a instância original. Se sua instância temporária estiver em uma zona de

disponibilidade diferente, você não poderá anexar o volume raiz da instância original a ela.

d. Na página Review Instance Launch, escolha Launch.

e. Quando solicitado, crie um par de chaves, faça download para um local seguro no computador e escolha Launch Instances (Iniciar instâncias).

2. Anexe o volume à instância temporária como um volume secundário da seguinte forma:

a. No painel de navegação, selecione Volumes, selecione o volume que você desanexou da instância original e escolha Actions (Ações), Attach Volume (Anexar volume).

b. Na caixa de diálogo Attach Volume (Anexar volume), em Instances (Instâncias), comece a digitar o nome ou ID da instância temporária e selecione-a na lista.

c. Em Device (Dispositivo), digite **`xvdf`** (se já não estiver lá) e escolha Attach (Anexar).

Etapa 3: Redefinir a senha de administrador

Em seguida, conecte-se à instância temporária e use o EC2Launch para redefinir a senha do administrador.

Para redefinir a senha de administrador

1. Conecte-se à instância temporária e use a ferramenta EC2Rescue for Windows Server na instância para redefinir a senha de administrador, da seguinte maneira:

a. Faça download do arquivo zip EC2Rescue for Windows Server, extraia o conteúdo e execute EC2Rescue.exe.

b. Na tela License Agreement (Contrato de licença), leia o contrato de licença e, se você aceitar os termos, escolha I Agree (Eu aceito).

c. Na tela Welcome to EC2Rescue for Windows Server (Bem-vindo ao EC2Rescue for Windows Server), escolha Next (Avançar).

d. Na tela Select mode (Selecionar modo), escolha Offline instance (Instância offline).

e. Na tela Select a disk (Selecionar um disco), selecione o dispositivo xvdf e, em seguida, Next (Avançar).

f. Confirme a seleção do disco e escolha Yes.

g. Depois que o volume for carregado, escolha OK.

h. Na tela Select Offline Instance Option (Selecionar opção de instância offline), escolha Diagnose and Rescue (Diagnosticar e recuperar).

i. Na tela Summary (Resumo), leia as informações e escolha Next (Avançar).

j. Na tela Detected possible issues (Problemas possíveis detectados), selecione Reset Administrator Password (Redefinir senha do administrador) e escolha Next (Avançar).

k. Na tela Confirm (Confirmar), escolha Rescue (Recuperar), OK.

l. Na tela Done (Concluído), escolha Finish (Concluir).

m. Feche a ferramenta EC2Rescue for Windows Server, desconecte-se da instância temporária e, em seguida, retorne para o console do Amazon EC2.

2. Desanexe o volume (`xvdf`) secundário da instância temporária da seguinte forma:

a. No painel de navegação, escolha Instances (Instâncias) e selecione a instância temporária.

b. Na guia Storage (Armazenamento) da instância temporária, observe o ID do volume do EBS listado como xvdf.

c. No painel de navegação, escolha Volumes.

d. Na lista de volumes, selecione o volume anotado na etapa anterior e selecione Actions (Ações) e Detach Volume (Desanexar volume). Após o status do volume mudar para available (disponível), vá para a próxima etapa.

Etapa 4: Reiniciar a instância original

Depois de redefinir a senha do administrador usando o EC2Launch, reconecte o volume à instância original como o volume raiz e conecte-se à instância usando seu par de chaves para recuperar a senha do administrador.

Para reiniciar a instância original

1. Reanexe o volume à instância original da seguinte forma:

a. No painel de navegação, selecione Volumes, selecione o volume que você desanexou da instância temporária e escolha Actions (Ações), Attach Volume (Anexar volume).

b. Na caixa de diálogo Attach Volume (Anexar volume), em Instances (Instâncias), comece a digitar o nome ou ID da instância original e selecione-a.

c. Em Device (Dispositivo), digite **`/dev/sda1`**.

d. Escolha Associar. Após o status do volume mudar para `in-use`, vá para a próxima etapa.

2. No painel de navegação, escolha Instances (Instâncias). Selecione a instância original e escolha Instance state (Estado da instância) e Start instance (Iniciar instância). Após o estado da instância mudar para `Running`, vá para a próxima etapa.
3. Recupere a nova senha de administrador do Windows usando a chave privada do novo par de chaves e conecte-se à instância. Para obter mais informações, consulte Conectar-se à instância do Windows no usando RDP.
4. (Opcional) Você pode encerrar a instância temporária se não tiver utilização adicional para ela. Selecione a instância temporária e escolha Instance state (Estado da instância) e Terminate instance (Encerrar instância).

Redefinir a senha de administrador do Windows para uma instância do EC2 usando o EC2Config

Se você perdeu a senha de administrador do Windows e está usando uma AMI do Windows anterior ao Windows Server 2016, poderá usar o agente EC2Config para gerar uma nova senha.

Se você estiver usando uma AMI do Windows Server 2016 ou posterior, consulte Redefinir a senha de administrador do Windows para uma instância do EC2 usando o EC2Launch, ou poderá usar a ferramenta EC2Rescue, que utiliza o serviço EC2Launch para gerar uma nova senha.

> **Note**
>
> Se você desabilitou a conta de administrador local na instância e sua instância estiver configurada para o Systems Manager, você também poderá reabilitar e redefinir sua senha de administrador local usando EC2Rescue e o Run Command. Para obter mais informações, consulte Use EC2Rescue for Windows Server with Systems Manager Run Command.

> **Note**
>
> Existe um documento de automação do AWS Systems Manager que aplica automaticamente as etapas manuais necessárias para redefinir a senha do administrador local. Para obter mais informações, consulte Redefinir senhas e chaves SSH em instâncias do EC2 no Guia do usuário do AWS Systems Manager.

Para redefinir sua senha de administrador do Windows usando o EC2Config, você precisa fazer o seguinte:

- Etapa 1: Verificar se o serviço do EC2Config está em execução
- Etapa 2: Desanexar o volume raiz da instância
- Etapa 3: Anexar o volume a uma instância temporária
- Etapa 4: Modificar o arquivo de configuração
- Etapa 5: Reiniciar a instância original

Etapa 1: Verificar se o serviço do EC2Config está em execução

Antes de tentar redefinir a senha de administrador, verifique se o serviço EC2Config está instalado e em execução. Você utilizará o serviço EC2Config para redefinir a senha de administrador posteriormente nesta seção.

Para verificar se o serviço do EC2Config está em execução

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias) e selecione a instância que precisa de redefinição da senha. Essa instância é denominada original neste procedimento.
3. Escolha Actions (Ações), Monitor and troubleshoot (Monitorar e solucionar problemas), Get system log Obter log do sistema.
4. Encontre a entrada agente do EC2, por exemplo, EC2 Agent: Ec2Config service v3.18.1118 (Agente do EC2: serviço Ec2Config v3.18.1118). Se você vir essa entrada, o serviço EC2Config estará em execução.

   Se a saída do log do sistema estiver vazia, ou se o serviço EC2Config não estiver em execução, solucione os problemas da instância usando o serviço Instance Console Screenshot. Para ter mais informações, consulte Fazer uma captura de tela de uma instância inacessível.

Etapa 2: Desanexar o volume raiz da instância

Você não poderá usar o EC2Config para redefinir uma senha de administrador se o volume no qual a senha está armazenada estiver anexado a uma instância como o volume raiz. Você precisa desanexar o volume da instância original antes de anexá-lo a uma instância temporária como um volume secundário.

Para desanexar o volume raiz da instância

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância que requer uma redefinição de senha e escolha Estado da instância e Parar instância. Depois que o status da instância for alterado para Stopped (Parado), siga para a próxima etapa.
4. (Opcional) Se você tiver a chave privada especificada ao iniciar esta instância, continue para a próxima etapa. Caso contrário, use as etapas a seguir para substituir a instância por uma nova que você executa com um novo par de chaves.

   a. Crie um par de chaves usando o console do Amazon EC2. Para dar ao seu novo par de chaves um nome exatamente igual ao do par de chaves perdido, primeiro exclua o par de chaves existente.

   b. Selecione a instância a ser substituída. Anote o tipo de instância, a VPC, a sub-rede, o grupo de segurança e a função do IAM da instância.

   c. Com a instância selecionada, escolha Ações, Imagem e modelos, Criar imagem. Digite um nome e uma descrição para a imagem e depois escolha Create image (Criar imagem).

   d. No painel de navegação, selecione AMIs. Aguarde até que o status da imagem mude para disponível. Em seguida, selecione a imagem e escolha Iniciar instância a partir da AMI.

   e. Preencha os campos para iniciar uma instância, certificando-se de selecionar o mesmo tipo de instância, VPC, sub-rede, grupo de segurança e perfil do IAM da instância a ser substituída e escolha Iniciar instância.

   f. Quando solicitado, escolha o par de chaves que você criou para a nova instância e escolha Iniciar instância.

   g. (Opcional) Se a instância original tiver um endereço IP elástico associado, transfira-o para a nova instância. Se a instância original tiver volumes do EBS além do volume raiz, transfira-os para a nova instância.

5. Desanexe o volume raiz da instância original da seguinte forma:

   a. Selecione a instância original e escolha a guia Armazenamento. Anote o nome do dispositivo raiz em Nome de dispositivo raiz. Encontre o volume com este nome de dispositivo em Dispositivo de blocos e anote o ID do volume.

   b. No painel de navegação, escolha Volumes.

c. Na lista de volumes, selecione o volume que você anotou como dispositivo raiz e escolha Ações e Desanexar volume. Após o status do volume mudar para available (disponível), vá para a próxima etapa.

6. Se você criou uma nova instância para substituir a instância original, é possível encerrar a instância original agora. A instância não é mais necessária. Nas etapas remanescentes deste procedimento, todas as referências à instância original se aplicam à nova instância que você criou.

Etapa 3: Anexar o volume a uma instância temporária

Em seguida, execute uma instância temporária e anexe o volume a ela como um volume secundário. Esta é a instância usada para modificar o arquivo de configuração.

Para executar uma instância temporária e anexar o volume

1. Inicie a instância temporária da seguinte forma:

   a. No painel de navegação, escolha Instances (Instâncias), Launch instances (Iniciar instâncias) e, em seguida, selecione uma AMI.

   > **Important**
   >
   > Para evitar colisões de assinatura de disco, você deve selecionar uma AMI para uma versão diferente do Windows. Por exemplo, se a instância original executar o Windows Server 2019, inicie a instância temporária usando a AMI básica do Windows Server 2016.

   b. Selecione um tipo de instância padrão e, a seguir, escolha Next: Configure Instance Details (Próximo: Configurar detalhes da instância).

   c. Na página Configure Instance Details (Configurar os detalhes da instância), em Subnet (Sub-rede), selecione a mesma zona de disponibilidade que a instância original e escolha Review and Launch (Revisar e iniciar).

   > **Important**
   >
   > A instância temporária deve estar na mesma zona de disponibilidade que a instância original. Se sua instância temporária estiver em uma zona de

disponibilidade diferente, você não poderá anexar o volume raiz da instância original a ela.

d. Na página Review Instance Launch, escolha Launch.

e. Quando solicitado, crie um par de chaves, faça download para um local seguro no computador e escolha Launch Instances (Iniciar instâncias).

2. Anexe o volume à instância temporária como um volume secundário da seguinte forma:

a. No painel de navegação, selecione Volumes, selecione o volume que você desanexou da instância original e escolha Actions (Ações), Attach Volume (Anexar volume).

b. Na caixa de diálogo Attach Volume (Anexar volume), em Instances (Instâncias), comece a digitar o nome ou ID da instância temporária e selecione-a na lista.

c. Em Device (Dispositivo), digite **`xvdf`** (se já não estiver lá) e escolha Attach (Anexar).

Etapa 4: Modificar o arquivo de configuração

Depois de anexar o volume à instância temporária como um volume secundário, modifique o plug-in `Ec2SetPassword` no arquivo de configuração.

Para modificar o arquivo de configuração

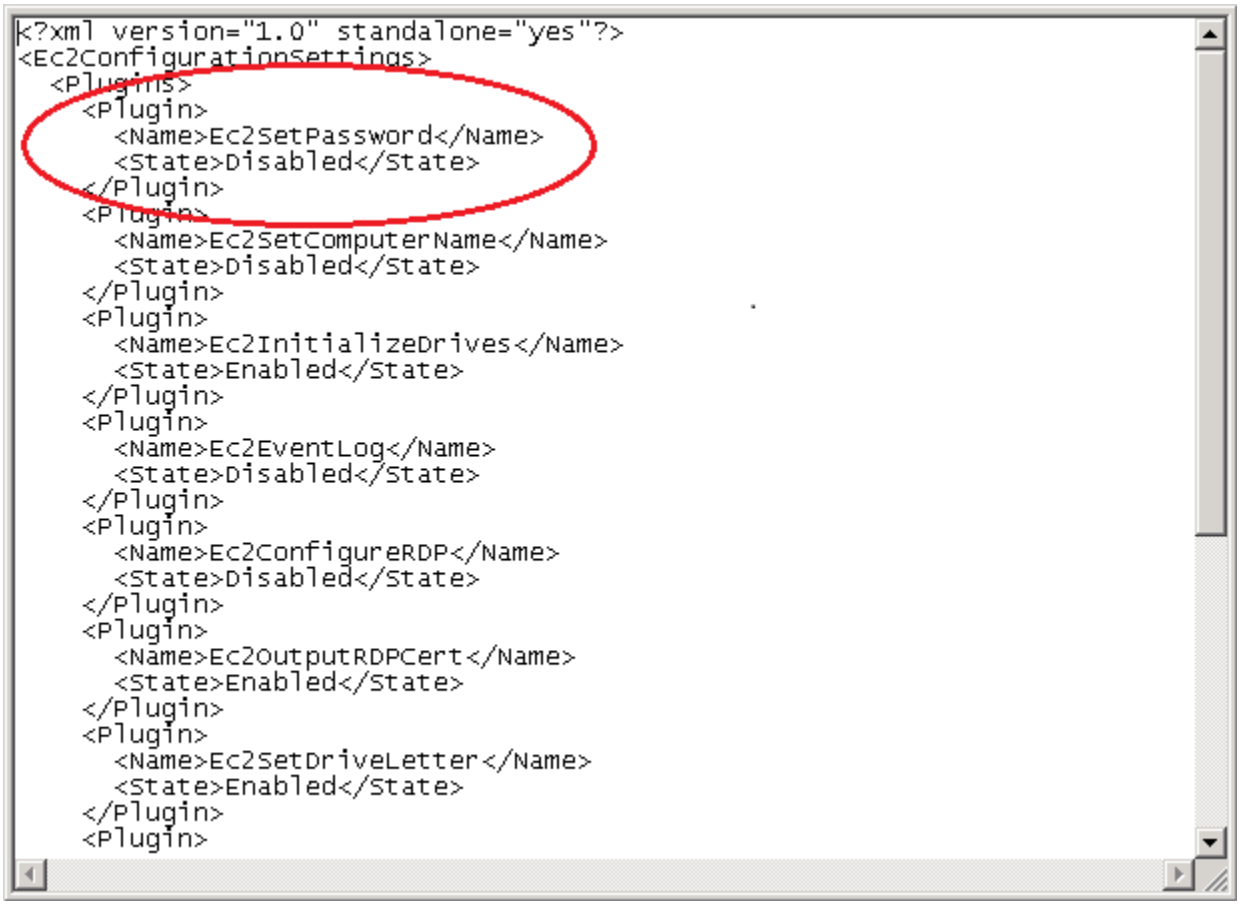
1. Na instância temporária, modifique o arquivo de configuração no volume secundário da seguinte maneira:

a. Execute a instância temporária e conecte-se a ela.

b. Use as instruções a seguir para ativar a unidade online: Disponibiliar o volume do Amazon EBS para uso.

c. Navegue até o volume secundário e abra `\Program Files\Amazon \Ec2ConfigService\Settings\config.xml` usando um editor de texto, como o Bloco de notas.

d. Na parte superior do arquivo, localize o plugin com o nome `Ec2SetPassword`, como mostrado no screenshot. Altere o estado de `Disabled` para `Enabled` e salve o arquivo.



2. Depois de modificar o arquivo de configuração, desconecte o volume secundário da instância temporária da seguinte maneira:

   a. Usando o utilitário Disk Management (Gerenciamento de disco), desative o volume.

   b. Desconecte-se da instância temporária e volte para o console Amazon EC2.

   c. No painel de navegação, selecione Volumes, selecione o volume e escolha Actions (Ações), Detach Volume (Desanexar volume). Quando o status do volume mudar para available (disponível), vá para a próxima etapa.

Etapa 5: Reiniciar a instância original

Depois de modificar o arquivo de configuração, reconecte o volume à instância original como o volume raiz e conecte-se à instância usando seu par de chaves para recuperar a senha do administrador.

1. Reanexe o volume à instância original da seguinte forma:

a. No painel de navegação, selecione Volumes, selecione o volume que você desanexou da instância temporária e escolha Actions (Ações), Attach Volume (Anexar volume).

b. Na caixa de diálogo Attach Volume (Anexar volume), em Instances (Instâncias), comece a digitar o nome ou ID da instância original e selecione-a.

c. Em Device (Dispositivo), digite **`/dev/sda1`**.

d. Escolha Associar. Após o status do volume mudar para `in-use`, vá para a próxima etapa.

2. No painel de navegação, escolha Instances (Instâncias). Selecione a instância original e escolha Instance state (Estado da instância) e Start instance (Iniciar instância). Após o estado da instância mudar para `Running`, vá para a próxima etapa.

3. Recupere a nova senha de administrador do Windows usando a chave privada do novo par de chaves e conecte-se à instância. Para obter mais informações, consulte Conectar-se à instância do Windows no usando RDP.

> **Important**
>
> A instância recebe um novo endereço IP público depois de você a interrompe e a inicia. Não deixe de se conectar à instância usando o nome DNS público atual. Para obter mais informações, consulte Alterações do estado de instâncias do Amazon EC2.

4. (Opcional) Você pode encerrar a instância temporária se não tiver utilização adicional para ela. Selecione a instância temporária e escolha Instance state (Estado da instância) e Terminate instance (Encerrar instância).

Solucionar problemas de Sysprep com instâncias do Windows do Amazon EC2

Se você tiver problemas ou receber mensagens de erro durante as preparações da imagem, veja os logs a seguir. A localização do log depende se você está executando EC2Config, EC2Launch v1 ou EC2Launch v2 com Sysprep.

- `%WINDIR%\Panther\Unattendgc`(EC2Config, EC2Launch v1 e EC2Launch v2)
- `%WINDIR%\System32\Sysprep\Panther`(EC2Config, EC2Launch v1 e EC2Launch v2)
- `C:\Program Files\Amazon\Ec2ConfigService\Logs\Ec2ConfigLog.txt` (somente EC2Config)

- `C:\ProgramData\Amazon\Ec2Config\Logs` (somente EC2Config)
- `C:\ProgramData\Amazon\EC2-Windows\Launch\Log\EC2Launch.log` (somente EC2Launch v1)
- `%ProgramData%\Amazon\EC2Launch\log\agent.log` (somente EC2Launch v2)

Se você receber uma mensagem de erro durante a preparação de imagem com Sysprep, o SO poderá não ser alcançável. Para analisar os arquivos de log, é preciso primeiro parar a instância, associar o volume do dispositivo raiz a outra instância íntegra como volume secundário e analisar os logs mencionados anteriormente no volume secundário. Para obter mais informações sobre a finalidade dos arquivos de log por nome, consulte Arquivos de log relacionados à configuração do Windows na documentação da Microsoft.

Se você encontrar erros no arquivo de log Unattendgc, use a Ferramenta de pesquisa de erro da Microsoft para obter mais detalhes sobre o erro. O problema a seguir relatado no arquivo de log Unattendgc é geralmente o resultado de um ou mais perfis de usuário corrompidos na instância:

```
Error [Shell Unattend] _FindLatestProfile failed (0x80070003) [gle=0x00000003]
Error [Shell Unattend] CopyProfile failed (0x80070003) [gle=0x00000003]
```

Há duas opções para resolver o problema:

Opção 1

Use o Regedit na instância para pesquisar pela chave a seguir. Verifique se não há chaves do registro de perfil para um usuário excluído.

`[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\ProfileList\`

Opção 2

1. Edite o arquivo relevante da seguinte forma:

   - Windows Server 2012 R2 e anterior – Edite o arquivo de resposta do EC2Config (`C:\Program Files\Amazon\Ec2ConfigService\sysprep2008.xml`).
   - Windows Server 2016 e 2019 – Edite o arquivo de resposta unattend.xml (`C:\ProgramData\Amazon\EC2-Windows\Launch\Sysprep\Unattend.xml`).
   - Windows Server 2022 – Edite o arquivo de resposta unattend.xml (`C:\ProgramData\Amazon\EC2Launch\sysprep\unattend.xml`).

2. Fazer `<CopyProfile>true</CopyProfile>` alteração `<CopyProfile>false</CopyProfile>`.
3. Execute novamente o Sysprep. Observe que essa mudança de configuração excluirá o perfil de usuário do administrador incorporado após o Sysprep concluir.

Solucionar problemas de instâncias danificadas do Amazon EC2 no Linux usando o EC2Rescue

O EC2Rescue para Linux é uma ferramenta de código aberto fácil de usar que pode ser executada em uma instância do Amazon EC2 no Linux para diagnosticar e corrigir problemas comuns usando sua biblioteca de mais de cem módulos. Os módulos são arquivos YAML que contêm um script BASH ou Python e os metadados necessários.

Alguns casos de uso generalizados para instâncias do EC2Rescue para Linux incluem:

- Como coletar logs do syslog e do gerenciador de pacotes
- Como coletar dados de utilização de recursos
- Diagnosticar e corrigir parâmetros problemáticos conhecidos do kernel e problemas comuns do OpenSSH

> **Note**
>
> O runbook `AWSSupport-TroubleshootSSH` do AWS Systems Manager Automation instala o EC2Rescue para Linux e, em seguida, usa a ferramenta para verificar ou tentar corrigir problemas comuns que impedem uma conexão SSH a uma instância do Linux. Para obter mais informações, consulte AWSSupport-TroubleshootSSH.

Se você estiver usando uma instância do Windows, consulte the section called “EC2Rescue para instâncias do Windows”.

Tópicos

- Instalar o EC2Rescue para uma instância do Amazon EC2 no Linux
- Executar comandos do EC2Rescue em uma instância do Amazon EC2 no Linux
- Desenvolver módulos do EC2Rescue para instâncias do Amazon EC2 no Linux

Instalar o EC2Rescue para uma instância do Amazon EC2 no 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+
  - SUSE Linux Enterprise Server 12+
  - RHEL 7+
  - Ubuntu 16.04+
- Requisitos de software:
  - Python 2.7.9+ ou 3.2+

Instalar o EC2Rescue

O runbook `AWSSupport-TroubleshootSSH` instala oEC2Rescue para Linux e, em seguida, usa a ferramenta para verificar ou tentar corrigir problemas comuns que impedem uma conexão remota a uma máquina Linux via SSH. Para obter mais informações e para executar essa automação, consulte Suporte-TroubleshootSSH.

Se o seu sistema tem a versão necessária do Python, você pode instalar a compilação padrão. Caso contrário, você pode instalar a compilação do pacote, incluindo uma cópia mínima do Python.

Para instalar a compilação padrão

1. Em uma instância Linux de trabalho, faça download da ferramenta EC2Rescue para Linux:

   ```
   curl -O https://s3.amazonaws.com/ec2rescuelinux/ec2rl.tgz
   ```

2. (Opcional) Verifique a assinatura do arquivo de instalação do EC2Rescue para Linux. Para obter mais informações, consulte (Opcional) Verifique a assinatura de EC2Rescue para Linux.
3. Faça download do arquivo hash sha256:

   ```
   curl -O https://s3.amazonaws.com/ec2rescuelinux/ec2rl.tgz.sha256
   ```

4. Verifique a integridade do tarball:

```
sha256sum -c ec2rl.tgz.sha256
```

5. Desembale o tarball:

```
tar -xzvf ec2rl.tgz
```

6. Verifique instalação listando o arquivo de ajuda:

```
cd ec2rl-<version_number>
./ec2rl help
```

Para instalar a compilação do pacote

Para obter um link para download e uma lista de limitações, consulte EC2Rescue para Linux no GitHub.

(Opcional) Verifique a assinatura de EC2Rescue para Linux

Veja a seguir o processo recomendado para verificação da validade do pacote do EC2Rescue para Linux para sistemas operacionais Linux.

Sempre que baixar um aplicativo da Internet, recomendamos que você autentique a identidade do fornecedor do software e verifique se o aplicativo não foi alterado ou corrompido desde que foi publicado. Isso protege você contra a instalação de uma versão do aplicativo que contenha um vírus ou outro código mal-intencionado.

Se depois de executar as etapas neste tópico, você determinar que o software do EC2Rescue para Linux está alterado ou corrompido, não execute o arquivo de instalação. Em vez disso, entre em contato com o Amazon Web Services.

Os arquivos do EC2Rescue para Linux para os sistemas operacionais baseados em Linux são assinados usando o GnuPG, uma implementação de código aberto do padrão OpenPGP (Pretty Good Privacy) para assinaturas digitais seguras. O GnuPG (também conhecido como GPG) fornece autenticação e verificação de integridade por meio de uma assinatura digital. A AWS publica uma chave pública e assinaturas que você pode usar para verificar o pacote EC2Rescue para Linux que foi obtido por download. Para obter mais informações sobre o PGP e o GnuPG (GPG), consulte https://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

- Autenticar e importar a chave pública
- Verificar a assinatura do pacote

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 prompt 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)
   ```

> **Tip**
>
> Se você vir um erro informando que o comando não pôde ser encontrado, instale o utilitário GnuPG com `apt-get install gnupg2` (Linux baseado em Debian) ou `yum install gnupg2` (Linux baseado em Red Hat).

Verificar a assinatura do pacote

Depois de instalar as ferramentas do GPG, autenticar e importar a chave pública do EC2Rescue para Linux e verificar se a chave pública do EC2Rescue para Linux é confiável, você estará pronto para verificar a assinatura do script de instalação do EC2Rescue para Linux.

Para verificar o script de instalação da assinatura do EC2Rescue para Linux

1. Em um prompt de comando, execute o comando a seguir para baixar o arquivo de assinatura para o script de instalação:

   ```
   curl -O https://s3.amazonaws.com/ec2rescuelinux/ec2rl.tgz.sig
   ```

2. Verifique a assinatura executando o comando a seguir em um prompt no diretório onde você salvou o `ec2rl.tgz.sig` e o arquivo de instalação EC2Rescue para Linux. Ambos os arquivos devem estar presentes.

   ```
   gpg2 --verify ./ec2rl.tgz.sig
   ```

   A saída deve parecer com algo semelhante ao seguinte:

   ```
   gpg: Signature made Thu 12 Jul 2018 01:57:51 AM UTC using RSA key ID 6991ED45
   gpg: Good signature from "ec2autodiag@amazon.com <EC2 Rescue for Linux>"
   gpg: WARNING: This key is not certified with a trusted signature!
   gpg:          There is no indication that the signature belongs to the owner.
   Primary key fingerprint: E528 BCC9 0DBF 5AFA 0F6C  C36A F780 4843 2FAE 2A1C
        Subkey fingerprint: 966B 0D27 85E9 AEEC 1146  7A9D 8851 1153 6991 ED45
   ```

   Se a saída contém a frase `Good signature from "ec2autodiag@amazon.com <EC2 Rescue for Linux>"`, isso significa que a assinatura foi confirmada com êxito e você pode dar continuidade à execução do script de instalação do EC2Rescue para Linux.

Se a saída inclui a frase `BAD signature`, verifique se você executou o procedimento corretamente. Se você continuar a receber essa resposta, entre em contato com o Amazon Web Services e não execute o arquivo de instalação que baixou anteriormente.

Veja a seguir os detalhes sobre as advertências que talvez sejam exibidas:

- WARNING: This key is not certified with a trusted signature! There is no indication that the signature belongs to the owner. Isso se refere ao seu nível pessoal de confiança de que você tem uma chave pública autêntica para o EC2Rescue para Linux. A situação ideal seria você visitar um escritório do Amazon Web Services e receber uma chave em pessoa. No entanto, é mais frequente você baixá-la de um site. Nesse caso, o site é um Amazon Web Services.
- gpg2: no ultimately trusted keys found. Isso significa que a chave específica não é "essencialmente confiável" (por você ou por outras pessoas que você confia).

Para obter mais informações, consulte https://www.gnupg.org/.

Executar comandos do EC2Rescue em uma instância do Amazon EC2 no Linux

O EC2Rescue é uma ferramenta de linha de comandos. Depois de instalar o EC2Rescue em sua instância do Linux, você pode obter ajuda geral sobre como usar a ferramenta executando `./ec2rl help`. Você pode visualizar os módulos disponíveis executando `./ec2rl list` e obter ajuda sobre um módulo específico executando `./ec2rl help` *`module_name`*.

Veja a seguir as tarefas comuns que você pode realizar para começar a usar essa ferramenta.

Tarefas

- Executar módulos do EC2Rescue
- Fazer upload dos resultados do módulo do EC2Rescue
- Criar backups de uma instância do Amazon EC2 no Linux

Executar módulos do EC2Rescue

Para executar todos os módulos do EC2Rescue

Use o comando ./ec2rl run sem especificar nenhum parâmetro adicional. Alguns módulos exigem o acesso raiz. Se você não for um usuário-raiz, use sudo ao executar o comando.

```
./ec2rl run
```

Para executar um módulo específico do EC2Rescue

Use o comando ./ec2rl run, e para `--only-modules`, especifique o nome do módulo a ser executado. Alguns módulos exigem argumentos para usá-los.

```
./ec2rl run --only-modules=module_name --arguments
```

Por exemplo, para executar o módulo dig para consultar o domínio `amazon.com`, use o comando a seguir.

```
./ec2rl run --only-modules=dig --domain=amazon.com
```

Para exibir os resultados de um módulo do EC2Rescue

Execute o módulo e, em seguida, exiba o arquivo de log em `cat /var/tmp/ec2rl/`*`logfile_location`*. Por exemplo, o arquivo de log do módulo dig pode ser encontrado no seguinte local:

```
cat /var/tmp/ec2rl/timestamp/mod_out/run/dig.log
```

Fazer upload dos resultados do módulo do EC2Rescue

Se o Suporte tiver solicitado os resultados de um módulo do EC2Rescue, você pode fazer o upload do arquivo de log usando a ferramenta do EC2Rescue. Você pode fazer o upload dos resultados em um local fornecido pelo Suporte ou em um bucket do Amazon S3 que você possui.

Para fazer o upload dos resultados em um local fornecido pelo Suporte

Use o comando ./ec2rl upload. Para `--upload-directory`, especifique o local do arquivo de log. Para `--support-url`, especifique o URL fornecido pelo Suporte.

```
./ec2rl upload --upload-directory=/var/tmp/ec2rl/logfile_location --support-
url="url_provided_by_aws_support"
```

Para fazer o upload dos resultados em um bucket do Amazon S3

Use o comando ./ec2rl upload. Para `--upload-directory`, especifique o local do arquivo de log. Para `--presigned-url`, especifique um URL pré-assinado para o bucket do S3. Para obter mais informações sobre como gerar pre-signed URLs para o Amazon S3, consulte Fazer upload de objetos usando pre-signed URLs.

```
./ec2rl upload --upload-directory=/var/tmp/ec2rl/logfile_location --presigned-
url="presigned_s3_url"
```

Criar backups de uma instância do Amazon EC2 no Linux

Você pode usar o EC2Rescue para fazer backup da sua instância do Linux criando uma AMI ou criando snapshots dos volumes anexados.

Criar uma AMI

Use o comando `./ec2rl run`, e para `--backup`, especifique `ami`.

```
./ec2rl run --backup=ami
```

Para criar snapshots multivolume de todos os volumes anexados

Use o comando `./ec2rl run`, e para `--backup`, especifique `allvolumes`.

```
./ec2rl run --backup=allvolumes
```

Para criar um snapshot de um volume anexado específico

Use o comando `./ec2rl run`, e para `--backup`, especifique o ID do volume para backup.

```
./ec2rl run --backup=vol-01234567890abcdef
```

Desenvolver módulos do EC2Rescue para instâncias do Amazon EC2 no Linux

Os módulos são gravados em YAML, um padrão de serialização de dados. O arquivo YAML de um módulo consiste em um único documento, representando o módulo e seus atributos.

Adicionar atributos de módulo

A tabela a seguir lista os atributos de módulo disponíveis.

Atributo	Descrição
name	O nome do módulo. O nome precisa ter 18 caracteres ou menos.
versão	O número da versão do módulo.
title	Um título curto e descritivo para o módulo. Esse valor precisa ter 50 caracteres ou menos.

helptext	A descrição estendida do módulo. Cada linha precisa ter 75 caracteres ou menos. Se o módulo utilizar argumentos, obrigatórios ou opcionais, inclua-os no valor helptext.
	
	Por exemplo:
	
	`helptext: !!str |`
	`  Collect output from ps for system analysis`
	`  Consumes --times= for number of times to repeat`
	`  Consumes --period= for time period between repetition`

posicionamento	O estágio no qual o módulo deve ser executado. Valores com suporte: • pré-diagnóstico • executar • pós-diagnóstico
linguagem	A linguagem em que o código do módulo está escrito. Valores com suporte: • bash • python

Atributo	Descrição
	Note O código Python deve ser compatível com o Python 2.7.9+ e o Python 3.2+.
correção	Indica se o módulo dá suporte a correão. Os valores compatíveis são `True` ou `False`. Os padrões do módulo de `False` se estiver ausente, tornando-o um atributo opcional para esses módulos que não dão suporte a correção.
conteúdo	A totalidade do código do script.
restrição	O nome do objeto que contém os valores de limite.
domínio	Um descritor de como o módulo é agrupado ou classificado. O conjunto de módulos incluídos usa os seguintes domínios: • aplicativo • net • os • desempenho

Atributo	Descrição
classe	Um descritor do tipo da tarefa executada pelo módulo. O conjunto de módulos incluídos usa as seguintes classes: • 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	A lista de distribuições Linux às quais esse módulo oferece suporte. O conjunto de módulos usa as seguintes distribuições: • 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	Os executáveis de software usados no módulo. Esse atributo deve especificar o software que não é instalado por padrão. A lógica do EC2Rescue para Linux garante que esses programas estejam presentes e executáveis antes de executar o módulo.

Atributo	Descrição
pacote	O pacote de software de origem para um executável. Esse atributo deve fornecer detalhes estendidos sobre o pacote com o software, incluindo uma URL para fazer download ou obter mais informações.
sudo	Indica se o acesso raiz é necessário para executar o módulo. Não é necessário implementar verificações sudo no script do módulo. Se o valor for verdadeiro, a lógica do EC2Rescue para Linux só executará o módulo quando o usuário que estiver executando tiver acesso raiz.
perfimpact	Indica se o módulo pode ter impacto significativo no desempenho no ambiente no qual ele está sendo execução. Se o valor for verdadeiro e o argumento `--perfimpact=true` não estiver presente, o módulo será ignorado.
parallelexclusive	Especifica um programa que exija exclusividade mútua. Por exemplo, todos os módulos que especificam "bpf" executados de maneira serial.

Adicionar variáveis de ambiente

A tabela a seguir lista as variáveis de ambiente disponíveis.

Variável de ambiente	Descrição
`EC2RL_CALLPATH`	O caminho para `ec2rl.py`. Esse caminho pode ser usado para encontrar o diretório lib e utilizar os módulos Python do fornecedor.

Variável de ambiente	Descrição
EC2RL_WORKDIR	O diretório tmp principal para a ferramenta de diagnóstico. Valor padrão: /var/tmp/ec2rl .
EC2RL_RUNDIR	O diretório no qual a saída é armazenada. Valor padrão: /var/tmp/ec2rl/<date&timestamp> .
EC2RL_GATHEREDDIR	O diretório raiz para colocar os dados de módulo reunidos. Valor padrão:/var/tmp/ec2rl/<date&timestamp>/mod_out/gathered/ .
EC2RL_NET_DRIVER	O driver em uso na primeira interface de rede não virtual, ordenada alfabeticamente, na instância. Exemplos: • xen_netfront • ixgbevf • ena
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: • default-hvm • default-paravirtual

Variável de ambiente	Descrição
`EC2RL_INTERFACES`	Uma lista enumerada de interfaces no sistema. O valor é uma string que contém nomes, como `eth0eth1`, etc. É gerada pelo `functions .bash` e está disponível somente para os módulos que a originaram.

Usar sintaxe de YAML

Os seguintes itens devem ser observados ao construir os arquivos YAML do módulo:

- O hífen triplo (`---`) denota o início explícito de um documento.
- A tag `!ec2rlcore.module.Module` indica para o analisador YAML qual construtor chamar ao criar o objeto do fluxo de dados. Você pode localizar o construtor no arquivo `module.py`.
- A tag `!!str` diz para o analisador YAML não tentar determinar o tipo de dados e, em vez disso, interpretar o conteúdo como um literal de string.
- O caractere pipe (`|`) informa ao analisador YAML que o valor é um escalar de estilo literal. Nesse caso, o analisador inclui todos os espaços em branco. É importante para os módulos porque o recuo e os caracteres de nova linha são mantidos.
- O recuo padrão YAML é dois espaços, que podem ser vistos nos exemplos a seguir. Certifique-se de manter o recuo padrão (por exemplo, quatro espaços para Python) para o script e, em seguida, defina o recuo de dois espaços para todo o conteúdo no arquivo do módulo.

Exemplos de módulos

Exemplo 1 (`mod.d/ps.yaml`):

```
--- !ec2rlcore.module.Module
# Module document. Translates directly into an almost-complete Module object
name: !!str ps
path: !!str
version: !!str 1.0
title: !!str Collect output from ps for system analysis
helptext: !!str |
  Collect output from ps for system analysis
  Requires --times= for number of times to repeat
```

```
  Requires --period= for time period between repetition
placement: !!str run
package:
  - !!str
language: !!str bash
content: !!str |
  #!/bin/bash
  error_trap()
  {
      printf "%0.s=" {1..80}
      echo -e "\nERROR: "$BASH_COMMAND" exited with an error on line ${BASH_LINENO[0]}"
      exit 0
  }
  trap error_trap ERR

  # read-in shared function
  source functions.bash
  echo "I will collect ps output from this $EC2RL_DISTRO box for $times times every
 $period seconds."
  for i in $(seq 1 $times); do
      ps auxww
      sleep $period
  done
constraint:
  requires_ec2: !!str False
  domain: !!str performance
  class: !!str collect
  distro: !!str alami ubuntu rhel suse
  required: !!str period times
  optional: !!str
  software: !!str
  sudo: !!str False
  perfimpact: !!str False
  parallelexclusive: !!str
```

Solucionar problemas de uma instância Amazon EC2 Windows danificada usando o EC2Rescue

O EC2Rescue for Windows Server é uma ferramenta fácil de usar que você executa em uma instância do Windows Server do Amazon EC2 para diagnosticar e solucionar os possíveis problemas. A ferramenta é valiosa para coletar arquivos de log e solucionar problemas e também

para pesquisar proativamente possíveis áreas de preocupação. Ele pode até examinar volumes raiz do Amazon EBS de outras instâncias e coletar logs relevantes para solucionar problemas de instâncias do Windows Server que usam esse volume. Veja a seguir alguns problemas comuns que o EC2Rescue pode resolver:

- Problemas de conectividade da instância devido a firewall, ao Remote Desktop Protocol (RDP) ou à configuração da interface de rede
- Problemas de inicialização do sistema operacional devido a um erro de parada, loop de inicialização ou registro corrompido
- Problemas que podem precisar de análise avançada de logs e solução de problemas

O EC2Rescue para Windows Server tem dois módulos diferentes:

- Um módulo coletor de dados que coleta dados de todas as diferentes fontes
- Um módulo analisador que analisa os dados coletados em relação a uma série de regras predefinidas para identificar problemas e fornecer sugestões

A ferramenta EC2Rescue para Windows Server apenas é executada em instâncias do Amazon EC2 executando o Windows Server 2012 e versões posteriores. Quando a ferramenta é iniciada, ela verifica se está sendo executada em uma instância do Amazon EC2.

> **Note**
>
> O runbook de automação `AWSSupport-ExecuteEC2Rescue` do AWS Systems Manager usa a ferramenta EC2Rescue para solucionar problemas e, quando possível, reparar problemas comuns de conectividade com a instância do EC2 especificada. Para obter mais informações e executar essa automação, consulte >AWSSupport-ExecuteEC2Rescue.

Se você estiver usando uma instância do Linux, consulte the section called “EC2Rescue para instâncias do Linux”.

Tópicos

- Solucionar problemas em instâncias danificadas do Windows com a GUI do EC2Rescue
- Solucionar problemas em instâncias danificadas do Windows com a CLI do EC2Rescue

- Solucionar problemas em instâncias danificadas do Windows com o EC2Rescue e o Systems Manager

Solucionar problemas em instâncias danificadas do Windows com a GUI do EC2Rescue

O EC2Rescue para Windows Server pode executar as seguintes análises em instâncias offl-ine:

Opção	Descrição

Diagnostico e resgate	O EC2Rescue for Windows Server pode detectar e resolver problemas com as seguintes configurações de serviço:
	• Hora do sistema
	  • RealTimeisUniversal: detecta se a chave do registro `RealTimeisUniversal` está habilitada. Se estiver desabilitada, a hora do sistema Windows derivará quando o fuso horário estiver definido como um valor diferente de UTC.
	• Firewall do Windows
	  • Domain networks (Redes de domínio): detecta se o perfil do Firewall do Windows está habilitado ou desabilitado.
	  • Private networks (Redes privadas): detecta se o perfil do Firewall do Windows está habilitado ou desabilitado.
	  • Guest or public networks (Redes públicas ou de convidado): detecta se o perfil do Firewall do Windows está habilitado ou desabilitado.
	• Desktop remoto

Opção	Descrição
	• Service Start (Início do serviço): detecta se o serviço Área de Trabalho Remota está habilitado. • Remote Desktop Connections (Conexões da Área de Trabalho Remota): detecta se essa opção está habilitada. • TCP Port (Porta TCP): detecta a porta em que o serviço Área de Trabalho Remota está ouvindo. • EC2Config (Windows Server 2012 R2 e anteriores) • Installation (Instalação): detecta qual versão do EC2Config está instalada. • Service Start (Início do serviço): detecta se o serviço EC2Config está habilitado. • Ec2SetPassword: gera uma nova senha de administrador. • Ec2HandleUserData: permite que você execute um script de dados de usuário na próxima inicialização da instância. • EC2Launch (Windows Server 2016 e posterior) • Installation (Instalação): detecta qual versão do EC2Launch está instalada. • Ec2SetPassword: gera uma nova senha de administrador. • Interface de rede

Opção	Descrição
	• DHCP Service Startup (Inicialização do serviço DHCP): detecta se o serviço DHCP está habilitado. • Ethernet detail (Detalhes da Ethernet): exibe informações sobre a versão do driver de rede, se detectado. • DHCP on Ethernet (DHCP na Ethernet): detecta se o DHCP está habilitado. • Status da assinatura no disco • Signature on disk (Assinatura em disco) e Signature on Boot Configuration Database (BCD) (Assinatura em banco de dados de configuração de inicialização): detectam se a assinatura no disco e a assinatura no BCD são iguais. Se os valores forem diferentes, o EC2Rescue tentará substituir a assinatura no disco pela assinatura no BCD.
Restaurar	Execute uma das seguintes ações: • Last Known Good Configuration (Última configuração válida conhecida): tenta inicializar a instância no estado inicializável mais recente conhecido. • Restore registry from backup (Restaurar registro do backup): restaura o registro de `\Windows\System32\config\RegBack` .
Capturar logs	Permite que você capture logs na instância para análise.

O EC2Rescue for Windows Server pode coletar os seguintes dados de instâncias ativas e offline:

Item	Descrição
Log de eventos	Coleta logs da aplicação, do sistema e de eventos do EC2Config.
Registro	Coleta os hives `SYSTEM` e `SOFTWARE`.
Log do Windows Update	Coleta arquivos de log gerados pelo Windows Update. **Note** No Windows Server 2016 e posterior, o log é coletado no formato Event Tracing for Windows (ETW, Rastreamento de Eventos para Windows).
Log do Sysprep	Coleta os arquivos de log gerados pela ferramenta de Preparação do sistema Windows.
Log de configuração do driver	Coleta os logs da SetupAPI do Windows (`setupapi.dev.log` e `setupapi.setup.log`).
Configuração da inicialização	Coleta o hive `HKEY_LOCAL_MACHINE\BCD00000000`.
Despejo de memória	Coleta todos os arquivos de despejo de memória existentes na instância.
Arquivo do EC2Config	Coleta os arquivos de log gerados pelo serviço EC2Config.
Arquivo do EC2Launch	Coleta os arquivos de log gerados pelos scripts do EC2Launch.

Item	Descrição
Arquivo do SSM Agent	Coleta arquivos de log gerados pelo SSM Agent e pelos logs do Patch Manager.
Arquivo ElasticGPUs do EC2	Recolhe os logs de eventos relacionados a GPUs elásticas.
ECS	Coleta logs relacionados ao Amazon ECS.
CloudEndure	Coleta arquivos de log relacionados ao agente CloudEndure.
AWS Replication Agent para arquivos de log MGN ou DRS	Coleta arquivos de log relacionados ao AWS Application Migration Service ou AWS Elastic Disaster Recovery.

EC2Rescue for Windows Server pode coletar os seguintes dados adicionais de instâncias ativas:

Item	Descrição
Informações do sistema	Coleta MSInfo32.
Resultado da política de grupo	Coleta um relatório de políticas de grupo.

Analisar uma instância offline

A opção Offline Instance é útil para a depuração de problemas de inicialização com instâncias do Windows.

Para executar uma ação em uma instância off-line

1. Em uma instância do Windows Server em execução, faça download da ferramenta EC2Rescue for Windows Server e extraia os arquivos.

   É possível executar o seguinte comando do PowerShell para baixar o EC2Rescue sem alterar a configuração de segurança aprimorada do Internet Explorer (ESC):

```
Invoke-WebRequest https://s3.amazonaws.com/ec2rescue/windows/EC2Rescue_latest.zip -
OutFile $env:USERPROFILE\Desktop\EC2Rescue_latest.zip
```

Esse comando fará download do arquivo .zip do EC2Rescue para a área de trabalho do usuário atualmente conectado.

> **Note**
>
> Se você receber um erro ao baixar o arquivo e estiver usando o Windows Server 2016 ou anterior, talvez seja necessário habilitar o TLS 1.2 para seu terminal PowerShell. É possível habilitar o TLS 1.2 para a sessão atual do PowerShell com o comando a seguir e tentar novamente:
>
> ```
> [Net.ServicePointManager]::SecurityProtocol =
>  [Net.SecurityProtocolType]::Tls12
> ```

2. Pare a instância com falha, se ela ainda não estiver parada.
3. Desanexe o volume raiz do EBS da instância com falha e anexe o volume a uma instância do Windows em funcionamento que tenha a EC2Rescue for Windows Server instalada.
4. Execute a ferramenta EC2Rescue for Windows Server na instância em funcionamento e escolha Offline Instance.
5. Selecione o disco do volume recém-montado e escolha Next.
6. Confirme a seleção do disco e escolha Yes.
7. Escolha a opção de instância off-line a ser executada e escolha Next.

A ferramenta EC2Rescue for Windows Server verifica o volume e coleta informações para solução de problemas com base nos arquivos de log selecionados.

Coletar dados de uma instância ativa

É possível coletar logs e outros dados de uma instância ativa.

Para coletar dados de uma instância ativa

1. Conecte-se à sua instância do Windows.

2. Faça download da ferramenta EC2Rescue for Windows Server na instância do Windows e extraia os arquivos.

   É possível executar o seguinte comando do PowerShell para baixar o EC2Rescue sem alterar a configuração de segurança aprimorada do Internet Explorer (ESC):

   ```
   Invoke-WebRequest https://s3.amazonaws.com/ec2rescue/windows/EC2Rescue_latest.zip -
   OutFile $env:USERPROFILE\Desktop\EC2Rescue_latest.zip
   ```

   Esse comando fará download do arquivo .zip do EC2Rescue para a área de trabalho do usuário atualmente conectado.

   > **Note**
   >
   > Se você receber um erro ao baixar o arquivo e estiver usando o Windows Server 2016 ou anterior, talvez seja necessário habilitar o TLS 1.2 para seu terminal PowerShell. É possível habilitar o TLS 1.2 para a sessão atual do PowerShell com o comando a seguir e tentar novamente:
   >
   > ```
   > [Net.ServicePointManager]::SecurityProtocol =
   >  [Net.SecurityProtocolType]::Tls12
   > ```

3. Abra a aplicação da EC2Rescue for Windows Server e aceite o contrato de licença.
4. Escolha Next, Current instance, Capture logs.
5. Selecione os itens de dados a serem coletados e escolha Collect.... Leia o aviso e escolha Yes para continuar.
6. Escolha um nome de arquivo e um local do arquivo ZIP e escolha Save.
7. Depois que a EC2Rescue for Windows Server for concluída, escolha Open Containing Folder para visualizar o arquivo ZIP.
8. Escolha Finish.

Solucionar problemas em instâncias danificadas do Windows com a CLI do EC2Rescue

A interface de linha de comando (CLI) do EC2Rescue for Windows Server permite executar um plug-in do EC2Rescue for Windows Server (conhecido como “ação”) de forma programada.

O ferramenta EC2Rescue for Windows Server tem dois modos de execução:

- /online — Permite agir na instância em que o EC2Rescue for Windows Server está instalado, como coletar arquivos de log.
- /offline:<device_id>—Permite agir no volume raiz offline que está associado a uma instância separada do Amazon EC2 do Windows em que você instalou o EC2Rescue for Windows Server.

Faça download da ferramenta EC2Rescue for Windows Server na instância do Windows e extraia os arquivos. É possível visualizar o arquivo de ajuda usando o seguinte comando:

```
EC2RescueCmd.exe /help
```

O EC2Rescue for Windows Server pode executar as seguintes ações na instância do Windows do Amazon EC2:

- Ação de coleta
- Ação de salvamento
- Ação de restauração

Ação de coleta

> **Note**
>
> É possível coletar todos os logs, um grupo inteiro de log ou um log individual dentro de um grupo.

O EC2Rescue for Windows Server pode coletar os seguintes dados de instâncias ativas e offline.

Grupo de logs	Logs disponíveis	Descrição
`all`		Coleta todos os logs disponíveis.
`eventlog`	• `'Application'` • `'System'` • `'EC2ConfigService'`	Coleta logs da aplicação, do sistema e de eventos do EC2Config.
`memory-dump`	• `'Memory Dump File'` • `'Mini Dump Files'`	Coleta todos os arquivos de despejo de memória existentes na instância.
`ec2config`	• `'Log Files'` • `'Configuration Files'`	Coleta os arquivos de log gerados pelo serviço EC2Config.
`ec2launch`	• `'Logs'` • `'Config'`	Coleta os arquivos de log gerados pelos scripts do EC2Launch.
`ssm-agent`	• `'Log Files'` • `'Patch Baseline Logs'` • `'InstanceData'`	Coleta arquivos de log gerados pelo Agente SSM e pelos logs do Patch Manager.
`sysprep`	`'Log Files'`	Coleta os arquivos de log gerados pela ferramenta de Preparação do sistema Windows.
`driver-setup`	• `'SetupAPI Log Files'` • `'DPInst Log File'` • `'AWS PV Setup Log File'`	Coleta os logs da SetupAPI do Windows (`setupapi.dev.log` e `setupapi.setup.log`).
`registry`	• `'SYSTEM'` • `'SOFTWARE'`	Coleta os hives `SYSTEM` e `SOFTWARE`.

Grupo de logs	Logs disponíveis	Descrição
	• 'BCD'	
egpu	• 'Event Log' • 'System Files'	Recolhe os logs de eventos relacionados a GPUs elásticas .
boot-config	'BCDEDIT Output'	Coleta o hive HKEY_LOCAL_MACHINE\BCD00000000 .
windows-update	'Log Files'	Coleta arquivos de log gerados pelo Windows Update. **Note** No Windows Server 2016 e posterior , o log é coletado no formato Event Tracing for Windows (ETW, Rastreamento de Eventos para Windows).
cloudendure	• 'Migrate Script Logs' • 'Driver Logs' • 'CloudEndure File List'	Coleta arquivos de log relacionados ao agente CloudEndure.

O EC2Rescue for Windows Server pode coletar os seguintes dados adicionais de instâncias ativas.

Grupo de logs	Logs disponíveis	Descrição
`system-info`	`'MSInfo32 Output'`	Coleta `MSInfo32`.
`gpresult`	`'GPResult Output'`	Coleta um relatório de políticas de grupo.

As seguintes opções estão disponíveis:

- /output:<outputFilePath>: localização do caminho de arquivo de destino obrigatório para salvar arquivos de log coletados no formato zip.
- /no-offline: atributo opcional usado no modo offline. Não define o volume offline após completar a ação.
- /no-fix-signature: atributo opcional usado no modo offline. Não conserta uma possível colisão de assinatura de disco após concluir a ação.

Exemplos

A seguir, exemplos usando a CLI do EC2Rescue for Windows Server.

Exemplos de modo online

Coleta todos os logs disponíveis:

```
EC2RescueCmd /accepteula /online /collect:all /output:<outputFilePath>
```

Coleta somente um grupo específico de log:

```
EC2RescueCmd /accepteula /online /collect:ec2config /output:<outputFilePath>
```

Coleta logs individuais dentro de um grupo de log:

```
EC2RescueCmd /accepteula /online /collect:'ec2config.Log Files,driver-setup.SetupAPI
 Log Files' /output:<outputFilePath>
```

Exemplos de modo offline

Coleta todos os logs disponíveis de um volume do EBS. O volume é especificado pelo valor device_id.

```
EC2RescueCmd /accepteula /offline:xvdf /collect:all /output:<outputFilePath>
```

Coleta somente um grupo específico de log:

```
EC2RescueCmd /accepteula /offline:xvdf /collect:ec2config /output:<outputFilePath>
```

Ação de salvamento

O EC2Rescue for Windows Server pode detectar e resolver problemas com as seguintes configurações de serviço:

Grupo de serviço	Ações disponíveis	Descrição
`all`		
`system-time`	`'RealTimeIsUniversal'`	Hora do sistema • RealTimeisUniversal: detecta se a chave do registro `RealTimeisUniversal` está habilitada. Se estiver desabilitada, a hora do sistema Windows derivará quando o fuso horário estiver definido como um valor diferente de UTC.
`firewall`	• `'Domain networks'` • `'Private networks'` • `'Guest or public networks'`	Firewall do Windows • Domain networks (Redes de domínio): detecta se o perfil do Firewall do Windows

Grupo de serviço	Ações disponíveis	Descrição
		está habilitado ou desabilitado. • Private networks (Redes privadas): detecta se o perfil do Firewall do Windows está habilitado ou desabilitado. • Guest or public networks (Redes públicas ou de convidado): detecta se o perfil do Firewall do Windows está habilitado ou desabilitado.
rdp	• `'Service Start'` • `'Remote Desktop Connections'` • `'TCP Port'`	Desktop remoto • Service Start (Início do serviço): detecta se o serviço Área de Trabalho Remota está habilitado. • Remote Desktop Connections (Conexões da Área de Trabalho Remota): detecta se essa opção está habilitada. • TCP Port (Porta TCP): detecta a porta em que o serviço Área de Trabalho Remota está ouvindo.

Grupo de serviço	Ações disponíveis	Descrição
`ec2config`	• `'Service Start'` • `'Ec2SetPassword'` • `'Ec2HandleUserData'`	EC2Config • Service Start (Início do serviço): detecta se o serviço EC2Config está habilitado. • Ec2SetPassword: gera uma nova senha de administr ador. • Ec2HandleUserData: permite que você execute um script de dados de usuário na próxima inicializ ação da instância.
`ec2launch`	`'Reset Administrator Password'`	Gera uma nova senha de administrador do Windows.
`network`	`'DHCP Service Startup'`	Interface de rede • DHCP Service Startup (Inicialização do serviço DHCP): detecta se o serviço DHCP está habilitado.

As seguintes opções estão disponíveis:

- /level:<level>: atributo opcional para o nível de verificação que a ação deve acionar. Os valores permitidos são: `information`, `warning`, `error`, `all`. Por padrão, ele é definido como `error`.
- /check-only atributo opcional que gera um relatório, mas não faz nenhuma modificação no volume offline.

> **Note**
>
> Se o EC2Rescue para Windows Server detectar uma possível colisão de assinatura de disco, ele corrigirá a assinatura após a conclusão do processo off-line por padrão, mesmo quando você usa a opção `/check-only`. Use a opção `/no-fix-signature` para evitar a correção.

- /no-offline atributo opcional que impede que o volume seja definido como offline após concluir a ação.
- /no-fix-signature: atributo opcional que não corrige uma possível colisão de assinatura de disco após concluir a ação.

Exemplos de salvamento

A seguir, exemplos usando a CLI do EC2Rescue for Windows Server. O volume é especificado usando o valor device_id.

Tentar corrigir todos os problemas identificados em um volume:

```
EC2RescueCmd /accepteula /offline:xvdf /rescue:all
```

Tentar corrigir todos os problemas dentro de um grupo de serviço em um volume:

```
EC2RescueCmd /accepteula /offline:xvdf /rescue:firewall
```

Tentar corrigir um item específico dentro de um grupo de serviço em um volume:

```
EC2RescueCmd /accepteula /offline:xvdf /rescue:rdp.'Service Start'
```

Especificar vários problemas para tentar corrigir em um volume:

```
EC2RescueCmd /accepteula /offline:xvdf /rescue:'system-
time.RealTimeIsUniversal,ec2config.Service Start'
```

Ação de restauração

O EC2Rescue for Windows Server pode detectar e resolver problemas com as seguintes configurações de serviço:

Grupo de serviço	Ações disponíveis	Descrição
Restaurar a última boa configuração conhecida	`lkgc`	Last Known Good Configura tion (Última configuração válida conhecida): tenta inicializar a instância no estado inicializável mais recente conhecido.
Restaurar o registro do Windows do backup mais recente	`regback`	Restore registry from backup (Restaurar registro do backup): restaura o registro de `\Windows\System32\ config\RegBack` .

As seguintes opções estão disponíveis:

- /no-offline—Atributo opcional que impede que o volume seja definido offline após concluir a ação.
- /no-fix-signature—Atributo opcional que não corrige uma possível colisão de assinatura de disco após concluir a ação.

Exemplos de restauração

A seguir, exemplos usando a CLI do EC2Rescue for Windows Server. O volume é especificado usando o valor device_id.

Restaurar a última boa configuração conhecida em um volume:

```
EC2RescueCmd /accepteula /offline:xvdf /restore:lkgc
```

Restaurar o último backup de registro do Windows em um volume:

```
EC2RescueCmd /accepteula /offline:xvdf /restore:regback
```

Solucionar problemas em instâncias danificadas do Windows com o EC2Rescue e o Systems Manager

SuporteO fornece um documento Run Command do Systems Manager para interagir com a instância habilitada para Systems Manager a fim de executar o EC2Rescue for Windows Server. O documento Run Command é chamado `AWSSupport-RunEC2RescueForWindowsTool`.

Este documento Run Command do Systems Manager realiza as seguintes tarefas:

- Baixa e verifica o EC2Rescue for Windows Server.
- Importa um módulo do PowerShell para facilitar a interação com a ferramenta.
- Executa EC2RescueCmd com o comando e os parâmetros fornecidos.

O documento Run Command do Systems Manager aceita três parâmetros:

- Comando—A EC2Rescue for Windows Server ação. Os valores atuais permitidos são:
  - ResetAccess—Restaura a senha do administrador local. A senha de administrador local da instância atual será restaurada e uma senha gerada aleatoriamente será armazenada com segurança no Parameter Store como `/EC2Rescue/Password/<INSTANCE_ID>`. Se você selecionar essa ação e não fornecer um parâmetro, as senhas serão criptografadas automaticamente com a chave padrão Chave do KMS. Opcionalmente, você pode especificar um ID de chave Chave do KMS em Parameters (Parâmetros) para criptografar a senha com sua própria chave.
  - CollectLogs—Executa o EC2Rescue for Windows Server com a ação `/collect:all`. Se você selecionar essa ação, `Parameters` deverá incluir um nome de bucket Amazon S3 no qual carregar os logs.
  - FixAlll—Executa o EC2Rescue for Windows Server com a ação `/rescue:all`. Se você selecionar essa ação, `Parameters` deverá incluir o nome de dispositivo de bloco para salvar.
- Parameters—Os parâmetros do PowerShell para passar para o comando especificado.

Requisitos

Para executar a ação ResetAccess, sua instância do Amazon EC2 deve ter uma política anexada que conceda permissões para gravar a senha criptografada no Parameter Store. Após anexar a política, aguarde alguns minutos antes de tentar redefinir a senha de uma instância depois de ter anexado esta política ao perfil do IAM relacionado.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ssm:PutParameter"
      ],
      "Resource": [
        "arn:aws:ssm:us-east-1:111122223333:parameter/EC2Rescue/
Passwords/<instanceid>"
      ]
    }
  ]
}
```

Se você estiver usando uma chave do KMS personalizada, e não a chave do KMS padrão, use esta política em vez disso.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ssm:PutParameter"
      ],
      "Resource": [
        "arn:aws:ssm:us-east-1:111122223333:parameter/EC2Rescue/
Passwords/<instanceid>"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms:Encrypt"
```

```
      ],
      "Resource": [
        "arn:aws:kms:us-east-1:111122223333:key/<kmskeyid>"
      ]
    }
  ]
}
```

Visualização do JSON do documento

O procedimento apresentado a seguir descreve como visualizar o JSON deste documento.

Para visualizar o JSON para o documento Run Command do Systems Manager

1. Abra o console AWS Systems Manager em https://console.aws.amazon.com/systems-manager/.
2. No painel de navegação, expanda Ferramentas de gerenciamento de alterações e selecione Documentos.
3. Na barra de pesquisa, insira `AWSSupport-RunEC2RescueForWindowsTool`, e, em seguida, selecione o documento `AWSSupport-RunEC2RescueForWindowsTool`.
4. Escolha a guia Conteúdo.

Exemplos

Veja alguns exemplos sobre como usar o documento Run Command do Systems Manager para executar o EC2Rescue for Windows Server usando a AWS CLI. Para obter mais informações sobre o envio de comandos com a AWS CLI, consulte send-command.

Exemplos

- Tentar corrigir todos os problemas identificados em um volume raiz offline
- Coletar logs da instância atual do Windows do Amazon EC2
- Redefinir a senha do administrador local

Tentar corrigir todos os problemas identificados em um volume raiz offline

Tente corrigir todos os problemas identificados em um volume raiz off-line associado a uma instância do Windows do Amazon EC2:

```
aws ssm send-command --instance-ids "i-0cb2b964d3e14fd9f" --document-name "AWSSupport-
RunEC2RescueForWindowsTool" --parameters "Command=FixAll, Parameters='xvdf'" --output
 text
```

Coletar logs da instância atual do Windows do Amazon EC2

Colete todos os logs da instância atual do Windows do Amazon EC2 online e carregue-os em um bucket do Amazon S3:

```
aws ssm send-command --instance-ids "i-0cb2b964d3e14fd9f" --document-name "AWSSupport-
RunEC2RescueForWindowsTool" --parameters "Command=CollectLogs, Parameters='amzn-s3-
demo-bucket'" --output text
```

Redefinir a senha do administrador local

Os seguintes exemplos mostram os métodos que você pode usar para restaurar a senha de administrador local. A saída fornece um link para o Parameter Store, onde você encontra a senha segura gerada aleatoriamente para usar o RDP para sua instância do Windows do Amazon EC2 como administrador local.

Restaurar a senha de administrador local de uma instância online usando a chave padrão AWS KMS key alias/aws/ssm:

```
aws ssm send-command --instance-ids "i-0cb2b964d3e14fd9f" --document-name "AWSSupport-
RunEC2RescueForWindowsTool" --parameters "Command=ResetAccess" --output text
```

Restaurar a senha de administrador local de uma instância online usando uma Chave do KMS:

```
aws ssm send-command --instance-ids "i-0cb2b964d3e14fd9f" --document-name "AWSSupport-
RunEC2RescueForWindowsTool" --parameters "Command=ResetAccess, Parameters=a133dc3c-
a2g4-4fc6-a873-6c0720104bf0" --output text
```

> **Note**
>
> Nesse exemplo, a Chave do KMS é `a133dc3c-a2g4-4fc6-a873-6c0720104bf0`.

EC2 Serial Console para instâncias do

Com o Console de Série do EC2, você tem acesso à porta serial da instância do Amazon EC2, que pode ser usada para solucionar problemas de lançamento, configuração de rede e outros problemas. O console de série não exige que sua instância tenha recursos de rede. Com o console de série, você pode inserir comandos para uma instância como se o teclado e o monitor estivessem conectados diretamente à porta serial da instância. A sessão do console de série tem a duração do período de reinicialização e de parada da instância. Durante a reinicialização, você pode visualizar todas as mensagens de inicialização desde o início.

O acesso ao console de série não está disponível por padrão. Sua organização deve conceder acesso da conta ao console de série e configurar políticas do IAM para conceder aos usuários acesso ao console de série. O acesso ao console serial pode ser controlado em um nível granular usando IDs de instância, tags de recursos e outras alavancas do IAM. Para obter mais informações, consulte Configurar o acesso ao Console de Série do EC2.

O console de série pode ser acessado usando o console do EC2 ou a AWS CLI.

O console de série está disponível sem qualquer custo adicional.

Tópicos

- Pré-requisitos do Console de Série do EC2
- Configurar o acesso ao Console de Série do EC2
- Conectar-se ao Console de Série do EC2
- Desconecte-se do Console de Série do EC2
- Solução de problemas da instância do Amazon EC2 usando o Console de Série do EC2

Pré-requisitos do Console de Série do EC2

Para se conectar ao Console de Série do EC2 e usar a ferramenta de sua escolha para solucionar problemas, os seguintes pré-requisitos devem ser atendidos:

- Regiões da AWS
- Zonas do Wavelength e AWS Outposts
- Zonas Locais
- Tipos de instância
- Concessão de acesso

- Suporte para cliente baseado em navegador
- Estado da instância
- Amazon EC2 Systems Manager
- Configurar a ferramenta de solução de problemas escolhida

Regiões da AWS

Disponibilidade em todas as Regiões da AWS, exceto Ásia-Pacífico (Taipei).

Zonas do Wavelength e AWS Outposts

Sem compatibilidade.

Zonas Locais

Compatível em todas as zonas locais.

Tipos de instância

Tipos de instâncias compatíveis:

- Linux
  - Todas as instâncias virtualizadas criadas no Nitro System.
  - Todas instâncias bare metal, exceto:
    - Uso geral: `a1.metal`, `mac1.metal`, `mac2.metal`
    - Computação acelerada: `g5g.metal`
    - Otimizadas para memória: `u-6tb1.metal`, `u-9tb1.metal`, `u-12tb1.metal`, `u-18tb1.metal`, `u-24tb1.metal`
- Windows

  Todas as instâncias virtualizadas criadas no Nitro System. Não há suporte para instâncias bare metal.

Concessão de acesso

Você deve concluir as tarefas de configuração para conceder acesso ao Console de Série do EC2. Para obter mais informações, consulte Configurar o acesso ao Console de Série do EC2.

Suporte para cliente baseado em navegador

Para se conectar ao console de sérieUsando o cliente com base em navegador, seu navegador deve suportar WebSocket. Se o navegador não suportar WebSocket, conecte-se ao console de sérieUsando sua própria chave e um cliente SSH.

Estado da instância

Deve ser `running`.

Você não poderá se conectar ao console de série se a instância estiver no estado `pending`, `stopping`, `stopped`, `shutting-down` ou `terminated`.

Para obter mais informações sobre os estados da instância, consulte Alterações do estado de instâncias do Amazon EC2.

Amazon EC2 Systems Manager

Se a instância usar o Amazon EC2 Systems Manager, o SSM Agent versão 3.0.854.0 ou posterior deve ser instalado na instância. Para obter mais informações sobre o SSM Agent, consulte Trabalhar com o SSM Agent no Guia do usuário do AWS Systems Manager.

Configurar a ferramenta de solução de problemas escolhida

Para solucionar problemas da instância usando console de série, você pode usar o GRUB ou o SysRq nas instâncias do Linux e o Special Admin Console (SAC) nas instâncias do Windows. Antes de usar essas ferramentas, é necessário executar as etapas de configuração em cada instância em que elas serão usadas.

Use as instruções para o sistema operacional da sua instância para configurar a ferramenta de solução de problemas escolhida.

(Instâncias do Linux) Configurar o GRUB

Para configurar o GRUB, escolha um dos seguintes procedimentos com base na AMI que foi usada para executar a instância.

Amazon Linux 2

Para configurar o GRUB em uma instância do Amazon Linux 2

1. Conectar-se à instância do Linux usando SSH

2. Adicione ou altere as seguintes opções em `/etc/default/grub`:

   - Defina `GRUB_TIMEOUT=1`.
   - Adicionar `GRUB_TERMINAL="console serial"`.
   - Adicionar `GRUB_SERIAL_COMMAND="serial --speed=115200"`.

   Veja a seguir um exemplo de `/etc/default/grub`. É possível precisar alterar a configuração com base na configuração do seu sistema.

   ```
   GRUB_CMDLINE_LINUX_DEFAULT="console=tty0 console=ttyS0,115200n8 net.ifnames=0
    biosdevname=0 nvme_core.io_timeout=4294967295 rd.emergency=poweroff rd.shell=0"
   GRUB_TIMEOUT=1
   GRUB_DISABLE_RECOVERY="true"
   GRUB_TERMINAL="console serial"
   GRUB_SERIAL_COMMAND="serial --speed=115200"
   ```

3. Aplique a configuração atualizada executando o comando a seguir.

   ```
   [ec2-user ~]$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
   ```

Ubuntu

Para configurar o GRUB em uma instância do Ubuntu

1. Conecte-se à sua instância.
2. Adicione ou altere as seguintes opções em `/etc/default/grub.d/50-cloudimg-settings.cfg`:

   - Defina `GRUB_TIMEOUT=1`.
   - Adicionar `GRUB_TIMEOUT_STYLE=menu`.
   - Adicionar `GRUB_TERMINAL="console serial"`.
   - Remover `GRUB_HIDDEN_TIMEOUT`.
   - Adicionar `GRUB_SERIAL_COMMAND="serial --speed=115200"`.

   Veja a seguir um exemplo de `/etc/default/grub.d/50-cloudimg-settings.cfg`. É possível precisar alterar a configuração com base na configuração do seu sistema.

```
# Cloud Image specific Grub settings for Generic Cloud Images
# CLOUD_IMG: This file was created/modified by the Cloud Image build process

# Set the recordfail timeout
GRUB_RECORDFAIL_TIMEOUT=0

# Do not wait on grub prompt
GRUB_TIMEOUT=1
GRUB_TIMEOUT_STYLE=menu

# Set the default commandline
GRUB_CMDLINE_LINUX_DEFAULT="console=tty1 console=ttyS0
 nvme_core.io_timeout=4294967295"

# Set the grub console type
GRUB_TERMINAL="console serial"
GRUB_SERIAL_COMMAND="serial --speed 115200"
```

3. Aplique a configuração atualizada executando o comando a seguir.

```
[ec2-user ~]$ sudo update-grub
```

RHEL

Para configurar o GRUB em uma instância do RHEL

1. Conecte-se à sua instância.
2. Adicione ou altere as seguintes opções em `/etc/default/grub`:
   - Remover `GRUB_TERMINAL_OUTPUT`.
   - Adicionar `GRUB_TERMINAL="console serial"`.
   - Adicionar `GRUB_SERIAL_COMMAND="serial --speed=115200"`.

   Veja a seguir um exemplo de `/etc/default/grub`. É possível precisar alterar a configuração com base na configuração do seu sistema.

```
GRUB_TIMEOUT=1
GRUB_DISTRIBUTOR="$(sed 's, release .*$,,g' /etc/system-release)"
GRUB_DEFAULT=saved
```

```
GRUB_DISABLE_SUBMENU=true
GRUB_CMDLINE_LINUX="console=tty0 console=ttyS0,115200n8 net.ifnames=0
 rd.blacklist=nouveau nvme_core.io_timeout=4294967295 crashkernel=auto"
GRUB_DISABLE_RECOVERY="true"
GRUB_ENABLE_BLSCFG=true
GRUB_TERMINAL="console serial"
GRUB_SERIAL_COMMAND="serial --speed=115200"
```

3. Aplique a configuração atualizada executando o comando a seguir.

```
[ec2-user ~]$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg --update-bls-cmdline
```

Para o RHEL 9.2 e anteriores, use o comando a seguir.

```
[ec2-user ~]$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

CentOS

Para instâncias executadas usando uma AMI do CentOS, o GRUB é configurado para o console de série por padrão.

Veja a seguir um exemplo de `/etc/default/grub`. Sua configuração pode ser diferente com base na configuração do sistema.

```
GRUB_TIMEOUT=1
GRUB_DISTRIBUTOR="$(sed 's, release .*$,,g' /etc/system-release)"
GRUB_DEFAULT=saved
GRUB_DISABLE_SUBMENU=true
GRUB_TERMINAL="serial console"
GRUB_SERIAL_COMMAND="serial --speed=115200"
GRUB_CMDLINE_LINUX="console=tty0 crashkernel=auto console=ttyS0,115200"
GRUB_DISABLE_RECOVERY="true"
```

(Instâncias do Linux) Configurar o SysRq

Para configurar o SysRq, habilite os comandos do SysRq para o ciclo de inicialização atual. Para tornar a configuração persistente, você também pode habilitar os comandos SysRq para inicializações subsequentes.

Para habilitar todos os comandos SysRq para o ciclo de inicialização atual

1. Conecte-se à sua instância.
2. Execute o seguinte comando.

```
[ec2-user ~]$ sudo sysctl -w kernel.sysrq=1
```

Essa configuração será limpa na próxima reinicialização.

Para habilitar todos os comandos do SysRq para inicializações subsequentes

1. Crie o arquivo `/etc/sysctl.d/99-sysrq.conf` e abra-o no seu editor favorito.

```
[ec2-user ~]$ sudo vi /etc/sysctl.d/99-sysrq.conf
```

2. Adicione a seguinte linha.

```
kernel.sysrq=1
```

3. Reinicie a instância para aplicar as alterações.

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

4. No prompt de `login`, insira o nome do usuário com a senha que você configurou anteriormente e, em seguida, pressione Enter.
5. No prompt `Password`, insira a senha e, a seguir, pressione Enter.

(Instâncias do Windows) Habilitar o SAC e o menu de inicialização

> **Note**
>
> Se você habilitar o SAC em uma instância, os serviços do EC2 que dependem de recuperação de senha não funcionarão no console do Amazon EC2. Os agentes de execução do Windows no Amazon EC2 (EC2Config, EC2Launch v1 e EC2Launch v2) dependem do console de série para executar várias tarefas. Essas tarefas não são executadas com êxito quando você habilita o SAC em uma instância. Para obter mais informações sobre o Windows nos agentes de inicialização do Amazon EC2, consulte the section called “Configuração da instância do Windows”. Se você habilitar o SAC, poderá

desabilitá-lo posteriormente. Para obter mais informações, consulte Desabilitar o SAC e o menu de inicialização.

Use um dos métodos a seguir para habilitar o SAC e o menu de inicialização em uma instância.

PowerShell

Para habilitar o SAC e o menu de inicialização em uma instância do Windows

1. Conecte-se à sua instância e execute as seguintes etapas na linha de comando do PowerShell.
2. Habilite o SAC.

```
bcdedit /ems '{current}' on
bcdedit /emssettings EMSPORT:1 EMSBAUDRATE:115200
```

3. Habilite o menu de inicialização.

```
bcdedit /set '{bootmgr}' displaybootmenu yes
bcdedit /set '{bootmgr}' timeout 15
bcdedit /set '{bootmgr}' bootems yes
```

4. Aplique a configuração atualizada reinicializando a instância.

```
shutdown -r -t 0
```

Command prompt

Para habilitar o SAC e o menu de inicialização em uma instância do Windows

1. Conecte-se à sua instância e execute as seguintes etapas no prompt de comando.
2. Habilite o SAC.

```
bcdedit /ems {current} on
bcdedit /emssettings EMSPORT:1 EMSBAUDRATE:115200
```

3. Habilite o menu de inicialização.

```
bcdedit /set {bootmgr} displaybootmenu yes
bcdedit /set {bootmgr} timeout 15
bcdedit /set {bootmgr} bootems yes
```

4. Aplique a configuração atualizada reinicializando a instância.

```
shutdown -r -t 0
```

Configurar o acesso ao Console de Série do EC2

Para configurar o acesso ao console de série, você deve conceder acesso ao console de série no nível da conta e, em seguida, configurar políticas do IAM para conceder acesso aos seus usuários. Para instâncias do Linux, você também deve configurar um usuário baseado em senha em cada instância com a finalidade de que os usuários possam usar o console de série para obter a solução de problemas.

O Console de Série do EC2 usa uma conexão de porta serial virtual para interagir com uma instância. Essa conexão é independente da VPC da instância, de modo que você poderá trabalhar com o sistema operacional da instância e executar ferramentas de solução de problemas mesmo se houver falhas de inicialização ou problemas de configuração de rede. Como essa conexão fica fora da rede VPC, a Console de Série do EC2 não usa o grupo de segurança da instância nem a ACL de rede da sub-rede para autorizar tráfego para a instância.

Antes de começar

Verifique se os pré-requisitos são atendidos.

Conteúdo

- Níveis de acesso ao Console de Série do EC2
- Gerenciar o acesso da conta ao Console de Série do EC2
- Configurar políticas do IAM para acesso ao Console de Série do EC2
- Definição de uma senha do usuário do sistema operacional em uma instância do Linux

Níveis de acesso ao Console de Série do EC2

Por padrão, não há acesso ao console de série no nível da conta. Você precisa explicitamente conceder acesso ao console de série no nível da conta. Para obter mais informações, consulte Gerenciar o acesso da conta ao Console de Série do EC2.

É possível usar uma política de controle de serviços (SCP) para permitir o acesso ao console de série dentro de sua organização. Em seguida, você pode ter controle de acesso granular no nível de usuário usando uma política do IAM para controlar o acesso. Usando uma combinação de políticas de SCP e do IAM, você tem diferentes níveis de controle de acesso ao console de série.

Nível da organização

É possível usar uma política de controle de serviços (SCP) para permitir o acesso ao console de série para contas de membros dentro da sua organização. Para obter mais informações sobre SCPs, consulte Políticas de controle de serviço no Guia do usuário do AWS Organizations.

Nível da instância

É possível configurar as políticas de acesso ao console de série usando as construções IAM PrincipalTag e ResourceTag e especificando instâncias pelo ID delas. Para obter mais informações, consulte Configurar políticas do IAM para acesso ao Console de Série do EC2.

Nível de usuário

É possível configurar o acesso no nível do usuário configurando uma política do IAM para permitir ou negar a um usuário especificado a permissão para enviar a chave pública SSH ao serviço de console de série de uma instância específica. Para obter mais informações, consulte Configurar políticas do IAM para acesso ao Console de Série do EC2.

Nível do sistema operacional (somente para instâncias do Linux)

É possível definir uma senha de usuário no nível do SO convidado. Isso fornece acesso ao console de série para alguns casos de uso. No entanto, para monitorar os logs, você não precisa de um usuário com senha. Para obter mais informações, consulte Definição de uma senha do usuário do sistema operacional em uma instância do Linux.

Gerenciar o acesso da conta ao Console de Série do EC2

Por padrão, não há acesso ao console de série no nível da conta. Você precisa explicitamente conceder acesso ao console de série no nível da conta.

Essa configuração é definida no nível da conta, diretamente na conta ou usando uma política declarativa. Ela deve ser configurada em cada Região da AWS onde você desejar conceder acesso ao console serial. O uso de uma política declarativa permite que você aplique a configuração em várias regiões simultaneamente, bem como em várias contas simultaneamente. Quando uma política declarativa está em uso, você não pode modificar a configuração diretamente em uma conta. Este tópico descreve como ajustar a configuração diretamente em uma conta. Para obter informações sobre o uso de políticas declarativas, consulte Políticas declarativas no Guia do usuário do AWS Organizations.

Sumário

- Conceder permissão a usuários para gerenciar acesso à conta
- Exibir status de acesso da conta no console de série
- Conceder acesso da conta ao console serial
- Negar acesso da conta ao console de série

Conceder permissão a usuários para gerenciar acesso à conta

Para permitir que os usuários gerenciem o acesso da conta ao Console de Série do EC2, você precisa conceder a eles as permissões necessárias do IAM.

A política a seguir concede permissões para visualizar o status da conta e para permitir e impedir o acesso da conta ao Console de Série do EC2.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:GetSerialConsoleAccessStatus",
                "ec2:EnableSerialConsoleAccess",
                "ec2:DisableSerialConsoleAccess"
            ],
            "Resource": "*"
        }
    ]
```

```
}
```

Para obter mais informações, consulte Criar políticas do IAM no Guia do usuário do IAM.

Exibir status de acesso da conta no console de série

Console

Para visualizar o status do acesso da conta ao console serial

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha EC2 Dashboard (Painel do EC2).
3. Em Account attributes (Atributos de conta), escolha EC2 Serial Console (Console serial do EC2).
4. Na guia Console serial do EC2, o valor de Acesso ao Console serial do EC2 é Permitido ou Impedido.

AWS CLI

Para visualizar o status do acesso da conta ao console serial

Use o comando get-serial-console-access-status.

```
aws ec2 get-serial-console-access-status
```

O seguinte é um exemplo de saída. Um valor de `true` indica que a conta tem permissão para acessar o console serial.

```
{
    "SerialConsoleAccessEnabled": true,
    "ManagedBy": "account"
}
```

O campo `ManagedBy` indica a entidade que definiu a configuração. Os valores possíveis são `account` (configurados diretamente) ou `declarative-policy`. Para obter mais informações, consulte Políticas declarativas no Guia do Usuário do AWS Organizations.

PowerShell

Para visualizar o status do acesso da conta ao console serial

Use o cmdlet Get-EC2SerialConsoleAccessStatus.

```
Get-EC2SerialConsoleAccessStatus -Select *
```

O seguinte é um exemplo de saída. Um valor de `True` indica que a conta tem permissão para acessar o console serial.

```
ManagedBy SerialConsoleAccessEnabled
--------- --------------------------
account   True
```

O campo `ManagedBy` indica a entidade que definiu a configuração. Os valores possíveis são `account` (configurados diretamente) ou `declarative-policy`. Para obter mais informações, consulte Políticas declarativas no Guia do Usuário do AWS Organizations.

Conceder acesso da conta ao console serial

Console

Para conceder acesso da conta ao console serial

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha EC2 Dashboard (Painel do EC2).
3. Em Account attributes (Atributos de conta), escolha EC2 Serial Console (Console serial do EC2).
4. Escolha Gerenciar.
5. Para permitir acesso de todas as instâncias da conta ao console de série do EC2, marque a caixa de seleção Permitir.
6. Selecione Atualizar.

AWS CLI

Para conceder acesso da conta ao console serial

Use o comando enable-serial-console-access.

```
aws ec2 enable-serial-console-access
```

O seguinte é um exemplo de saída.

```
{
    "SerialConsoleAccessEnabled": true
}
```

PowerShell

Para conceder acesso da conta ao console serial

Use o cmdlet Enable-EC2SerialConsoleAccess.

```
Enable-EC2SerialConsoleAccess
```

O seguinte é um exemplo de saída.

```
True
```

Negar acesso da conta ao console de série

Console

Para negar acesso da conta ao console serial

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha EC2 Dashboard (Painel do EC2).
3. Em Account attributes (Atributos de conta), escolha EC2 Serial Console (Console serial do EC2).
4. Escolha Gerenciar.
5. Para evitar o acesso de todas as instâncias da conta ao console de série do EC2, desmarque a caixa de seleção Permitir.
6. Selecione Atualizar.

AWS CLI

Para negar acesso da conta ao console serial

Use o comando disable-serial-console-access.

```
aws ec2 disable-serial-console-access
```

O seguinte é um exemplo de saída.

```
{
    "SerialConsoleAccessEnabled": false
}
```

PowerShell

Para negar acesso da conta ao console serial

Use o cmdlet Disable-EC2SerialConsoleAccess.

```
Disable-EC2SerialConsoleAccess
```

O seguinte é um exemplo de saída.

```
False
```

Configurar políticas do IAM para acesso ao Console de Série do EC2

Por padrão, seus usuários não têm acesso ao console de série. Sua organização deve configurar políticas do IAM para conceder aos usuários o acesso necessário. Para obter mais informações, consulte Criar políticas do IAM no Guia do usuário do IAM.

Para acessar o console de série, crie um documento de política JSON que inclua a ação `ec2-instance-connect:SendSerialConsoleSSHPublicKey`. Essa ação concede a um usuário permissão para enviar a chave pública para o serviço de console de série, que inicia uma sessão de console de série. Recomendamos restringir o acesso a instâncias do EC2 específicas. Caso contrário, todos os usuários com essa permissão poderão se conectar ao console de série de todas as instâncias do EC2.

Políticas de exemplo do IAM.

- Permitir explicitamente o acesso ao console de série
- Explicitamente negar acesso ao console de série

- Usar tags de recursos para controlar o acesso ao console de série

Permitir explicitamente o acesso ao console de série

Por padrão, ninguém tem acesso ao console de série. Para conceder acesso ao console de série, é preciso configurar uma política para permitir explicitamente o acesso. Recomendamos configurar uma política que restrinja o acesso a instâncias específicas.

A política a seguir permite o acesso ao console de série de uma instância específica, identificada pelo ID da instância.

Observe que as ações `DescribeInstances`, `DescribeInstanceTypes` e `GetSerialConsoleAccessStatus` não são compatíveis com permissões no nível do recurso e, portanto, todos os recursos, indicados por * (asterisco), devem ser especificados para essas ações.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowDescribeInstances",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceTypes",
                "ec2:GetSerialConsoleAccessStatus"
            ],
             "Resource": "*"
        },
        {
            "Sid": "AllowinstanceBasedSerialConsoleAccess",
            "Effect": "Allow",
            "Action": [
                "ec2-instance-connect:SendSerialConsoleSSHPublicKey"
            ],
            "Resource": "arn:aws:ec2:us-
east-1:111122223333:instance/i-0598c7d356eba48d7"
        }
    ]
}
```

Explicitamente negar acesso ao console de série

A política do IAM a seguir permite o acesso ao console de série de todas as instâncias, denotado pelo * (asterisco) e nega explicitamente o acesso ao console de série de uma instância específica, identificado por seu ID.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowSerialConsoleAccess",
            "Effect": "Allow",
            "Action": [
                "ec2-instance-connect:SendSerialConsoleSSHPublicKey",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceTypes",
                "ec2:GetSerialConsoleAccessStatus"
            ],
            "Resource": "*"
        },
        {
            "Sid": "DenySerialConsoleAccess",
            "Effect": "Deny",
            "Action": [
                "ec2-instance-connect:SendSerialConsoleSSHPublicKey"
            ],
            "Resource": "arn:aws:ec2:us-
east-1:111122223333:instance/i-0598c7d356eba48d7"
        }
    ]
}
```

Usar tags de recursos para controlar o acesso ao console de série

É possível usar tags de recursos para controlar o acesso ao console de série de uma instância.

O controle de acesso por atributo é uma estratégia de autorização que define permissões de acordo com tags que podem ser anexadas a usuários e a recursos da AWS. Por exemplo, a política a seguir só permite que um usuário inicie uma conexão de console de série para uma instância se a tag de

recurso desta instância e a tag da entidade principal tiverem o mesmo valor do `SerialConsole` para a chave de tag.

Para obter mais informações sobre como usar tags para controlar o acesso aos recursos da AWS, consulte Controle do acesso aos recursos da AWS no Guia do usuário do IAM.

Observe que as ações `DescribeInstances`, `DescribeInstanceTypes` e `GetSerialConsoleAccessStatus` não são compatíveis com permissões no nível do recurso e, portanto, todos os recursos, indicados por * (asterisco), devem ser especificados para essas ações.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowDescribeInstances",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceTypes",
                "ec2:GetSerialConsoleAccessStatus"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowTagBasedSerialConsoleAccess",
            "Effect": "Allow",
            "Action": [
                "ec2-instance-connect:SendSerialConsoleSSHPublicKey"
            ],
            "Resource": "arn:aws:ec2:us-east-1:111122223333:instance/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/SerialConsole":
 "${aws:PrincipalTag/SerialConsole}"
                }
            }
        }
    ]
}
```

Definição de uma senha do usuário do sistema operacional em uma instância do Linux

É possível se conectar ao console de série sem uma senha. No entanto, para usar o console de série com a finalidade de solucionar problemas de uma instância do Linux, a instância deve ter um usuário do sistema operacional baseado em senha.

É possível definir a senha para qualquer usuário do sistema operacional, incluindo o usuário raiz. Observe que o usuário raiz pode modificar todos os arquivos, enquanto cada usuário do sistema operacional pode ter permissões limitadas.

Você deve definir uma senha de usuário para cada instância para a qual você usará o console de série. Essa é uma exigência única de cada instância.

> **Note**
>
> Por padrão, as AMIs fornecidas pela AWS não são configuradas com um usuário baseado em senha. Se você tiver executado a instância usando uma AMI que já tenha a senha do usuário raiz configurada, poderá ignorar essas instruções.

Para definir uma senha do usuário do sistema operacional em uma instância do Linux

1. Conecte-se à sua instância. É possível usar qualquer método para se conectar à instância, exceto o método de conexão do Console de Série do EC2.
2. Para definir a senha para um usuário, use o comando passwd. No exemplo a seguir, o usuário é `root`.

   ```
   [ec2-user ~]$ sudo passwd root
   ```

   A seguir está um exemplo de saída.

   ```
   Changing password for user root.
   New password:
   ```

3. No prompt `New password`, digite a nova senha.
4. No prompt, digite novamente a senha.

Conectar-se ao Console de Série do EC2

Você pode se conectar ao console de série da instância do EC2 usando o console do Amazon EC2 ou por SSH. Depois de se conectar ao console de série, você pode usá-lo para solucionar problemas de inicialização, configuração de rede e outros problemas. Para obter mais informações sobre solução de problemas, consulte Solução de problemas da instância do Amazon EC2 usando o Console de Série do EC2.

Considerações

- Há suporte para somente uma conexão ativa do console de série por instância.
- A conexão do console de série geralmente dura uma hora, a menos que você se desconecte. No entanto, durante a manutenção do sistema, o Amazon EC2 desconectará a sessão do console de série.

  A duração da conexão não é determinada pela duração de suas credenciais do IAM. Se as suas credenciais do IAM expirarem, a conexão continuará persistindo até que a duração máxima da conexão do console serial seja atingida. Ao usar a experiência de console do Console de Série do EC2, se as suas credenciais do IAM expirarem, encerre a conexão fechando a página do navegador.
- Demora 30 segundos para derrubar uma sessão depois que você se desconecta do console de série para permitir uma nova sessão.
- Portas do console de série com suporte: `ttyS0` (instâncias do Linux) e `COM1` (instâncias do Windows)
- Quando você se conecta ao console de série, pode observar uma pequena queda na taxa de throughput da instância.

Tópicos

- Conectar-se usando o cliente com base em navegador
- Conectar-se usando sua própria chave e cliente SSH
- Endpoints e impressões digitais do console serial EC2

Conectar-se usando o cliente com base em navegador

É possível se conectar ao console de série da instância do EC2 usando o cliente com base em navegador. Faça isso selecionando a instância no console do Amazon EC2 e escolhendo conectar-

se ao console de série. O cliente com base em navegador lida com as permissões e fornece uma conexão bem-sucedida.

O Console de Série do EC2 funciona a na maioria dos navegadores e suporta entrada de teclado e mouse.

Antes de realizar a conexão, certifique-se de ter concluído os pré-requisitos.

Para se conectar à porta serial da instância usando o cliente com base em navegador (console do Amazon EC2)

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância e escolher Actions (Ações), Monitor and troubleshoot (Monitorar e solucionar problemas), EC2 Serial Console (Console de Série do EC2), Connect (Conectar).

   Ou selecione a instância e escolha Connect (Conectar), EC2 Serial Console (Console de Série do EC2), Connect (Conectar).

   Uma janela de terminal no navegador é aberta.
4. Pressione Enter. Se for exibido um prompt de login, significará que você está conectado ao console de série.

   Se a tela permanecer preta, será possível usar as seguintes informações para ajudar a resolver problemas com a conexão ao console de série:

   - Verifique se você configurou o acesso ao console de série. Para obter mais informações, consulte Configurar o acesso ao Console de Série do EC2.
   - (Somente para instâncias do Linux) Use SysRq para realizar a conexão com o console de série. O SysRq não exige que você se conecte usado o cliente baseado no navegador. Para obter mais informações, consulte (Instâncias do Linux) Usar o SysRq para solucionar problemas na sua instância.
   - (Somente para instâncias do Linux) Reinicie o getty. Se você tiver acesso SSH à instância, conecte-se à instância usando SSH e reinicie o getty usando o comando a seguir.

     ```
     [ec2-user ~]$ sudo systemctl restart serial-getty@ttyS0
     ```
   - Reinicie a instância. É possível reinicializar a instância ao usar SysRq (instâncias do Linux), o console do EC2 ou a AWS CLI. Para obter mais informações, consulte (Instâncias do

Linux) Usar o SysRq para solucionar problemas na sua instância (instâncias do Linux) ou Reinicializar uma instância do Amazon EC2.

5. (Somente para instâncias do Linux) No prompt de `login`, insira o nome do usuário com a senha que você configurou anteriormente e, em seguida, pressione Enter.
6. (Somente para instâncias do Linux) Na prompt de `Password`, insira a senha e, em seguida, pressione Enter.

Conectar-se usando sua própria chave e cliente SSH

É possível usar sua própria chave do SSH e conectar-se à sua instância a partir do cliente SSH de sua escolha enquanto usa a API do console de série. Isso permite que você se beneficie da capacidade do console de série de enviar por push uma chave pública para a instância.

Depois de enviar a chave SSH para a instância, a conexão SSH não está sujeita às políticas do IAM que você configurou para conceder aos usuários acesso ao Console de Série do EC2.

Antes de começar

Verifique se os pré-requisitos são atendidos.

Para se conectar ao console de série de uma instância usando SSH

1. Envie por push a chave pública do SSH para a instância para iniciar uma sessão de console de série

   Use o comando send-serial-console-ssh-public-key para enviar por push a chave pública do SSH para a instância. Isso inicia uma sessão de console de série.

   Se uma sessão de console de série já tiver sido iniciada para essa instância, o comando falhará porque você só pode ter uma sessão aberta de cada vez. Demora 30 segundos para derrubar uma sessão depois que você se desconecta do console de série para permitir uma nova sessão.

   ```
   aws ec2-instance-connect send-serial-console-ssh-public-key \
       --instance-id i-001234a4bf70dec41EXAMPLE \
       --serial-port 0 \
       --ssh-public-key file://my_key.pub \
       --region us-east-1
   ```

2. Conecte-se ao console de série usando sua chave privada

   Use o comando ssh para se conectar ao console de série antes que a chave pública seja removida do serviço de console de série. Você tem 60 segundos antes que ela seja removida.

   Use a chave privada que corresponde à chave pública.

   O formato do nome de usuário é `instance-id.port0`, que inclui o ID da instância e a porta 0. No exemplo a seguir, o nome de usuário é `i-001234a4bf70dec41EXAMPLE.port0`.

   O endpoint do serviço de console de série é diferente para cada região. Veja a Endpoints e impressões digitais do console serial EC2 tabela do endpoint de cada região. No exemplo a seguir, o serviço de console de série está na região *us-east-1*.

   ```
   ssh -i my_key i-001234a4bf70dec41EXAMPLE.port0@serial-console.ec2-instance-connect.us-east-1.aws
   ```

   O exemplo a seguir usa `timeout 3600` para definir que sua sessão SSH seja encerrada após 1 hora. Os processos iniciados durante a sessão podem continuar em execução na sua instância após o término da sessão.

   ```
   timeout 3600 ssh -i my_key i-001234a4bf70dec41EXAMPLE.port0@serial-console.ec2-instance-connect.us-east-1.aws
   ```

3. (Opcional) Verificar a impressão digital

   Quando você se conecta pela primeira vez ao console de série, é solicitado a verificar a impressão digital. É possível comparar a impressão digital do console de série com a impressão digital exibida para verificação. Caso essas impressões digitais não correspondam, alguém pode estar tentando um ataque "man-in-the-middle". Se elas corresponderem, será possível se conectar com confiança ao console de série.

   A seguinte impressão digital corresponde ao serviço de console de série na região us-east-1. Para obter as impressões digitais de cada região, consulte Endpoints e impressões digitais do console serial EC2.

   ```
   SHA256:dXwn5ma/xadVMeBZGEru5l2gx+yI5LDiJaLUcz0FMmw
   ```

   A impressão digital só aparece na primeira vez que você se conecta ao console de série.

4. Pressione Enter. Se for exibido um prompt, significará que você está conectado ao console de série.

   Se a tela permanecer preta, será possível usar as seguintes informações para ajudar a resolver problemas com a conexão ao console de série:

   - Verifique se você configurou o acesso ao console de série. Para obter mais informações, consulte Configurar o acesso ao Console de Série do EC2.
   - (Somente para instâncias do Linux) Use SysRq para realizar a conexão com o console de série. O SysRq não exige que você se conecte usando SSH. Para obter mais informações, consulte (Instâncias do Linux) Usar o SysRq para solucionar problemas na sua instância.
   - (Somente para instâncias do Linux) Reinicie o getty. Se você tiver acesso SSH à instância, conecte-se à instância usando SSH e reinicie o getty usando o comando a seguir.

     ```
     [ec2-user ~]$ sudo systemctl restart serial-getty@ttyS0
     ```

   - Reinicie a instância. É possível reinicializar a instância ao usar SysRq (somente para instâncias do Linux), o console do EC2 ou a AWS CLI. Para obter mais informações, consulte (Instâncias do Linux) Usar o SysRq para solucionar problemas na sua instância (somente para instâncias do Linux) ou Reinicializar uma instância do Amazon EC2.
5. (Somente para instâncias do Linux) No prompt de `login`, insira o nome do usuário com a senha que você configurou anteriormente e, em seguida, pressione Enter.
6. (Somente para instâncias do Linux) Na prompt de `Password`, insira a senha e, em seguida, pressione Enter.

Endpoints e impressões digitais do console serial EC2

A seguir estão os endpoints de serviço e as impressões digitais do EC2 Serial Console. Para se conectar programaticamente ao console de série de uma instância, você usa um endpoint do console de série EC2. Os endpoints e impressões digitais do console serial do EC2 são exclusivos para cada região AWS.

Nome da Região	Região	Endpoint	Impressão digital
Leste dos EUA (Ohio)	us-east-2	serial-console.ec2-instance-connect.us-east-2.aws	SHA256:EhwPkTzRtTY7TRSzz26XbB0/

Nome da Região	Região	Endpoint	Impressão digital
			HvV9jRM7mCZN0xw/d/0
Leste dos EUA (Norte da Virgínia)	us-east-1	serial-console.ec2-instance-connect.us-east-1.aws	SHA256:dXwn5ma/xadVMeBZGEru5l2gx+yI5LDiJaLUcz0FMmw
Oeste dos EUA (Norte da Califórnia)	us-west-1	serial-console.ec2-instance-connect.us-west-1.aws	SHA256:OHldlcMET8u7QLSX3jmRTRAPFHVtqbyoLZBMUCqiH3Y
Oeste dos EUA (Oregon)	us-west-2	serial-console.ec2-instance-connect.us-west-2.aws	SHA256:EMCIe23TqKaBI6yGHainqZcMwqNkDhhAVHa1O2JxVUc
África (Cidade do Cabo)	af-south-1	ec2-serial-console.af-south-1.api.aws	SHA256:RMWWZ2fVePeJUqzjO5jL2KIgXsczoHlz21Ed00biiWI
Ásia-Pacífico (Hong Kong)	ap-east-1	ec2-serial-console.ap-east-1.api.aws	SHA256:T0Q1lpiXxChoZHplnAkjbP7tkm2xXViC9bJFsjYnifk
Ásia-Pacífico (Hyderabad)	ap-south-2	ec2-serial-console.ap-south-2.api.aws	SHA256:WJgPBSwV4/shN+OPITValoewAuYj15DVW845JEhDKRs
Ásia-Pacífico (Jacarta)	ap-southeast-3	ec2-serial-console.ap-southeast-3.api.aws	SHA256:5ZwgrCh+lfns32XITqL/4O0zIfbx4bZgsYFqy3o8mIk

Nome da Região	Região	Endpoint	Impressão digital
Ásia-Pacífico (Malásia)	ap-southeast-5	ec2-serial-console.ap-southeast-5.api.aws	SHA256:cQXTHQMRcqRdIjmAGoAMBSExeoRobYyRwT67yTjnEiA
Ásia-Pacífico (Melbourne)	ap-southeast-4	ec2-serial-console.ap-southeast-4.api.aws	SHA256:Avaq27hFgLvjn5gTSShZ0oV7h90p0GG46wfOeT6ZJvM
Ásia-Pacífico (Mumbai)	ap-south-1	serial-console.ec2-instance-connect.ap-south-1.aws	SHA256:oBLXcYmklqHHEbliARxEgH8IsO51rezTPiSM35BsU40
Ásia-Pacífico (Osaka)	ap-northeast-3	ec2-serial-console.ap-northeast-3.api.aws	SHA256:Am0/jiBKBnBuFnHr9aXsgEV3G8Tu/vVHFXE/3UcyjsQ
Ásia-Pacífico (Seul)	ap-northeast-2	serial-console.ec2-instance-connect.ap-northeast-2.aws	SHA256:FoqWXNX+DZ++GuNTztg9PK49WYMqBX+FrcZM2dSrqrI
Ásia-Pacífico (Singapura)	ap-southeast-1	serial-console.ec2-instance-connect.ap-southeast-1.aws	SHA256:PLFNn7WnCQDHx3qmwLu1Gy/O8TUX7LQgZuaC6L45CoY

Nome da Região	Região	Endpoint	Impressão digital
Ásia-Pacífico (Sydney)	ap-southeast-2	serial-console.ec2-instance-connect.ap-southeast-2.aws	SHA256:yFvMwUK9lEUQjQTRoXXzuN+cW9/VSe9W984Cf5Tgzo4
Ásia-Pacífico (Tailândia)	ap-southeast-7	ec2-serial-console.ap-southeast-7.api.aws	SHA256:KCAZiRYrR1Q2lqsg7vTwixWmvc2wmjVT31XRgSdEfDY
Ásia-Pacífico (Tóquio)	ap-northeast-1	serial-console.ec2-instance-connect.ap-northeast-1.aws	SHA256:RQfsDCZTOfQawewTRDV1t9Em/HMrFQe+CRlIOT5um4k
Canadá (Central)	ca-central-1	serial-console.ec2-instance-connect.ca-central-1.aws	SHA256:P2O2jOZwmpMwkpO6YW738FIOTHdUTyEv2gczYMMO7s4
Oeste do Canadá (Calgary)	ca-west-1	ec2-serial-console.ca-west-1.api.aws	SHA256:s3rc8lI2xhbhr3iedjJNxGAFLPGOLjx7IxxXrGckk6Q
China (Pequim)	cn-north-1	ec2-serial-console.cn-north-1.api.amazonwebservices.com.cn	SHA256:2gHVFy4H7uU3+WaFUxD28v/ggMeqjvSlgngpgLgGT+Y

Nome da Região	Região	Endpoint	Impressão digital
China (Ningxia)	cn-northwest-1	ec2-serial-console.cn-northwest-1.api.amazonwebservices.com.cn	SHA256:TdgrNZkiQOdVfYEBUhO4SzUA09VWI5rYOZGTogpwmiM
Europa (Frankfurt)	eu-central-1	serial-console.ec2-instance-connect.eu-central-1.aws	SHA256:aCMFS/yIcOdOlkXvOl8AmZ1Toe+bBnrJJ3Fy0k0De2c
Europa (Irlanda)	eu-west-1	serial-console.ec2-instance-connect.eu-west-1.aws	SHA256:h2AaGAWO4Hathhtm6ezs3Bj7udgUxi2qTrHjZAwCW6E
Europa (Londres)	eu-west-2	serial-console.ec2-instance-connect.eu-west-2.aws	SHA256:a69rd5CE/AEG4Amm53I6lkD1ZPvS/BCV3tTPW2RnJg8
Europa (Milão)	eu-south-1	ec2-serial-console.eu-south-1.api.aws	SHA256:lC0kOVJnpgFyBVrxn0A7n99ecLbXSX95cuuS7X7QK30
Europa (Paris)	eu-west-3	serial-console.ec2-instance-connect.eu-west-3.aws	SHA256:q8ldnAf9pymeNe8BnFVngY3RPAr/kxswJUzfrlxeEWs
Europa (Espanha)	eu-south-2	ec2-serial-console.eu-south-2.api.aws	SHA256:GoCW2DFRlu669QNxqFxEcsR6fZUz/4F4n7T45ZcwoEc

Nome da Região	Região	Endpoint	Impressão digital
Europa (Estocolmo)	eu-north-1	serial-console.ec2-instance-connect.eu-north-1.aws	SHA256:tkGFFUVUDvocDiGSS3Cu8Gdl6w2uI32EPNpKFKLwX84
Europa (Zurique)	eu-central-2	ec2-serial-console.eu-central-2.api.aws	SHA256:8Ppx2mBMf6WdCw0NUlzKfwM4/IfRz4OaXFutQXWp6mk
Israel (Tel Aviv)	il-central-1	ec2-serial-console.il-central-1.api.aws	SHA256:JR6q8v6kNNPi8+QSFQ4dj5dimNmZPTgwgsM1SNvtYyU
México (Central)	mx-central-1	ec2-serial-console.mx-central-1.api.aws	SHA256:BCuVl13iQNk+CcVnt18Ef4p2ZHUrBBAOxlFetB32GS0
Oriente Médio (Barém)	me-south-1	ec2-serial-console.me-south-1.api.aws	SHA256:nPjLLKHu2QnLdUq2kVArsoK5xvPJOMRJKCBzCDqC3k8
Oriente Médio (Emirados Árabes Unidos)	me-central-1	ec2-serial-console.me-central-1.api.aws	SHA256:zpb5duKiBZ+l0dFwPeyykB4MPBYhI/XzXNeFSDKBvLE
América do Sul (São Paulo)	sa-east-1	serial-console.ec2-instance-connect.sa-east-1.aws	SHA256:rd2+/32Ognjew1yVIemENaQzC+Botbih62OqAPDq1dI

Nome da Região	Região	Endpoint	Impressão digital
AWS GovCloud (Leste dos EUA)	us-gov-east-1	serial-console.ec2-instance-connect.us-gov-east-1.amazonaws.com	SHA256:tIwe19GWsoyLClrtvu38YEEh+DHIkqnDcZnmtebvF28
AWS GovCloud (Oeste dos EUA)	us-gov-west-1	serial-console.ec2-instance-connect.us-gov-west-1.amazonaws.com	SHA256:kfOFRWLaOZfB+utbd3bRf8OlPf8nGO2YZLqXZiIw5DQ

Desconecte-se do Console de Série do EC2

Se você não precisa mais estar conectado ao Console de Série do EC2 da sua instância, pode se desconectar dele. Quando você se desconecta do console de série, as sessões de shell em execução na instância continuarão sendo executadas. Se desejar encerrar a sessão do shell, será necessário encerrá-la antes de se desconectar do console de série.

Considerações

- A conexão do console de série geralmente dura uma hora, a menos que você se desconecte. No entanto, durante a manutenção do sistema, o Amazon EC2 desconectará a sessão do console de série.
- Demora 30 segundos para derrubar uma sessão depois que você se desconecta do console de série para permitir uma nova sessão.

A forma de se desconectar do console de série depende do cliente.

Cliente com base em navegador

Para se desconectar do console de série, feche a janela de terminal no navegador do console de série.

Cliente OpenSSH padrão

Para se desconectar do console de série, use o comando a seguir para fechar a conexão SSH. Esse comando deve ser executado imediatamente após uma nova linha.

```
~.
```

O comando que você usa para fechar uma conexão SSH pode ser diferente, dependendo do cliente SSH que você está usando.

Solução de problemas da instância do Amazon EC2 usando o Console de Série do EC2

Ao usar o Console de Série do EC2, você pode solucionar problemas de inicialização, configuração de rede e outros problemas ao se conectar à porta serial da instância.

Use as instruções para o sistema operacional da sua instância e para a ferramenta que você configurou em sua instância.

Ferramentas

- (Instâncias do Linux) Usar o GRUB para solucionar problemas na sua instância
- (Instâncias do Linux) Usar o SysRq para solucionar problemas na sua instância
- (Instâncias do Windows) Usar o SAC para solucionar problemas na sua instância

Pré-requisitos

Antes de começar, certifique-se de ter concluído os pré-requisitos, incluindo a configuração da ferramenta de solução de problemas escolhida por você.

(Instâncias do Linux) Usar o GRUB para solucionar problemas na sua instância

O GNU GRUB (abreviatura de GNU GRand Unified Bootloader) é o carregador de inicialização padrão para a maioria dos sistemas operacionais Linux. No menu do GRUB, você pode selecionar em qual kernel inicializar ou modificar entradas de menu para alterar a forma como o kernel irá inicializar. Isso pode ser útil ao solucionar problemas de uma instância com falha.

O menu do GRUB é exibido durante o processo de inicialização. O menu não é acessível via SSH normal, mas você pode acessá-lo usando o Console de Série do EC2.

É possível inicializar no modo de usuário único ou no modo de emergência. O modo de usuário único inicializará o kernel em um nível de execução inferior. Por exemplo, ele pode montar o sistema de arquivos, mas não ativar a rede, dando a você a oportunidade de realizar a manutenção necessária

para corrigir a instância. O modo de emergência é semelhante ao modo de usuário único, exceto que o kernel é executado no nível de execução mais baixo possível.

Para inicializar no modo de usuário único

1. Connect (Conecte-se) ao console de série da instância.
2. Execute a instância usando o seguinte comando.

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

3. Durante a reinicialização, quando o menu do GRUB aparecer, pressione qualquer tecla para interromper o processo de inicialização.
4. No menu do GRUB, use as teclas de seta para selecionar o kernel para inicializar e pressione e no teclado.
5. Use as teclas de seta para posicionar o cursor na linha que contém o kernel. A linha começa com um `linux` ou `linux16`, dependendo da AMI usada para executar a instância. Para o Ubuntu, duas linhas começam com `linux`, que devem ser modificadas na próxima etapa.
6. No final da linha, adicione a palavra `single`.

   Veja um exemplo a seguir para Amazon Linux 2.

```
linux /boot/vmlinuz-4.14.193-149.317.amzn2.aarch64 root=UUID=d33f9c9a-\
dadd-4499-938d-ebbf42c3e499 ro  console=tty0 console=ttyS0,115200n8 net.ifname\
s=0 biosdevname=0 nvme_core.io_timeout=4294967295 rd.emergency=poweroff rd.she\
ll=0 single
```

7. Pressione Ctrl+X para inicializar no modo de usuário único.
8. No prompt de `login`, insira o nome do usuário com a senha que você configurou anteriormente e, em seguida, pressione Enter.
9. No prompt `Password`, insira a senha e, a seguir, pressione Enter.

Para inicializar no modo de emergência

Siga as mesmas etapas do modo de usuário único, mas, na etapa 6, adicione a palavra `emergency` em vez de `single`.

(Instâncias do Linux) Usar o SysRq para solucionar problemas na sua instância

A chave System Request (SysRq), que, às vezes, é denominada “SysRq mágica”, pode ser usada para enviar diretamente ao kernel um comando, fora de um shell, e o kernel responderá, independentemente do que o kernel está fazendo. Por exemplo, se a instância tiver parado de responder, será possível usar a chave SysRq para dizer ao kernel para falhar ou reiniciar. Para obter mais informações, consulte Chave SysRq mágica na Wikipédia.

É possível usar comandos SysRq no cliente com base em navegador do Console de Série do EC2 ou em um cliente SSH. O comando que enviará uma solicitação de interrupção é diferente para cada cliente.

Para usar o SysRq, escolha um dos seguintes procedimentos com base no cliente que você está usando.

Browser-based client

Para usar o SysRq no cliente com base em navegador do console de série

1. Connect (Conecte-se) ao console de série da instância.
2. Para enviar uma solicitação de interrupção, pressione `CTRL+0` (zero). Se o teclado suportá-la, você também poderá enviar uma solicitação de interrupção usando a tecla Pause ou Break.

   ```
   [ec2-user ~]$ CTRL+0
   ```

3. Para emitir um comando do SysRq, pressione a tecla no teclado que corresponde ao comando requerido. Por exemplo, para exibir uma lista de comandos do SysRq, pressione h.

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

   O comando h gera algo semelhante ao seguinte.

   ```
   [ 1169.389495] sysrq: HELP : loglevel(0-9) reboot(b) crash(c) terminate-all-
   tasks(e) memory-full-oom-kill(f) kill-all-tasks(i) thaw-filesystems
   (j) sak(k) show-backtrace-all-active-cpus(l) show-memory-usage(m) nice-all-RT-
   tasks(n) poweroff(o) show-registers(p) show-all-timers(q) unraw(r
   ) sync(s) show-task-states(t) unmount(u) show-blocked-tasks(w) dump-ftrace-
   buffer(z)
   ```

SSH client

Para usar o SysRq em um cliente SSH

1. Connect (Conecte-se) ao console de série da instância.
2. Para enviar uma solicitação de interrupção, pressione ~B (til, seguido de maiúsculas B).

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

3. Para emitir um comando do SysRq, pressione a tecla no teclado que corresponde ao comando requerido. Por exemplo, para exibir uma lista de comandos do SysRq, pressione h.

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

O comando h gera algo semelhante ao seguinte.

```
[ 1169.389495] sysrq: HELP : loglevel(0-9) reboot(b) crash(c) terminate-all-
tasks(e) memory-full-oom-kill(f) kill-all-tasks(i) thaw-filesystems
(j) sak(k) show-backtrace-all-active-cpus(l) show-memory-usage(m) nice-all-RT-
tasks(n) poweroff(o) show-registers(p) show-all-timers(q) unraw(r
) sync(s) show-task-states(t) unmount(u) show-blocked-tasks(w) dump-ftrace-
buffer(z)
```

> **Note**
>
> O comando que você usa para enviar uma solicitação de interrupção pode ser diferente, dependendo do cliente SSH que você está usando.

(Instâncias do Windows) Usar o SAC para solucionar problemas na sua instância

O recurso Special Admin Console (SAC) do Windows fornece uma maneira de solucionar problemas de uma instância do Windows. Ao se conectar ao console de série da instância e usando o SAC, você pode interromper o processo de inicialização e inicializar o Windows no modo de segurança.

> **Note**
>
> Se você habilitar o SAC em uma instância, os serviços do EC2 que dependem de recuperação de senha não funcionarão no console do Amazon EC2. Os agentes de

execução do Windows no Amazon EC2 (EC2Config, EC2Launch v1 e EC2Launch v2) dependem do console de série para executar várias tarefas. Essas tarefas não são executadas com êxito quando você habilita o SAC em uma instância. Para obter mais informações sobre o Windows nos agentes de inicialização do Amazon EC2, consulte the section called “Configuração da instância do Windows”. Se você habilitar o SAC, poderá desabilitá-lo posteriormente. Para obter mais informações, consulte Desabilitar o SAC e o menu de inicialização.

Tarefas

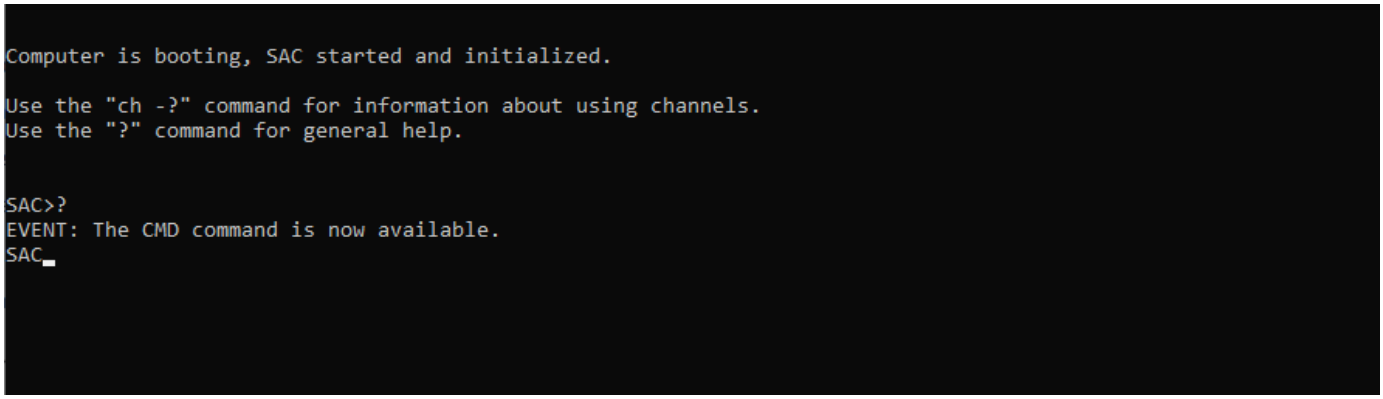
- Usar o SAC
- Usar o menu de inicialização
- Desabilitar o SAC e o menu de inicialização

Usar o SAC

Para usar o SAC

1. Conecte-se ao console de série.

   Se o SAC estiver habilitado na instância, o console de série exibirá o prompt SAC>.

2. Para exibir os comandos do SAC, insira ? e, em seguida, pressione Enter.

   Saída esperada

```
SAC>?
ch                    Channel management commands.  Use ch -? for more help.
cmd                   Create a Command Prompt channel.
d                     Dump the current kernel log.
f                     Toggle detailed or abbreviated tlist info.
? or help             Display this list.
i                     List all IP network numbers and their IP addresses.
i <#> <ip> <subnet> <gateway> Set IPv4 addr., subnet and gateway.
id                    Display the computer identification information.
k <pid>               Kill the given process.
l <pid>               Lower the priority of a process to the lowest possible.
lock                  Lock access to Command Prompt channels.
m <pid> <MB-allow>    Limit the memory usage of a process to <MB-allow>.
p                     Toggle paging the display.
r <pid>               Raise the priority of a process by one.
s                     Display the current time and date (24 hour clock used).
s mm/dd/yyyy hh:mm    Set the current time and date (24 hour clock used).
t                     Tlist.
restart               Restart the system immediately.
shutdown              Shutdown the system immediately.
crashdump             Crash the system. You must have crash dump enabled.
```

3. Para criar um canal de prompt de comando (como `cmd0001` ou `cmd0002`), insira cmd e pressione Enter.
4. Para ver o canal do prompt de comando, pressioneESCE pressioneTAB.

   Saída esperada

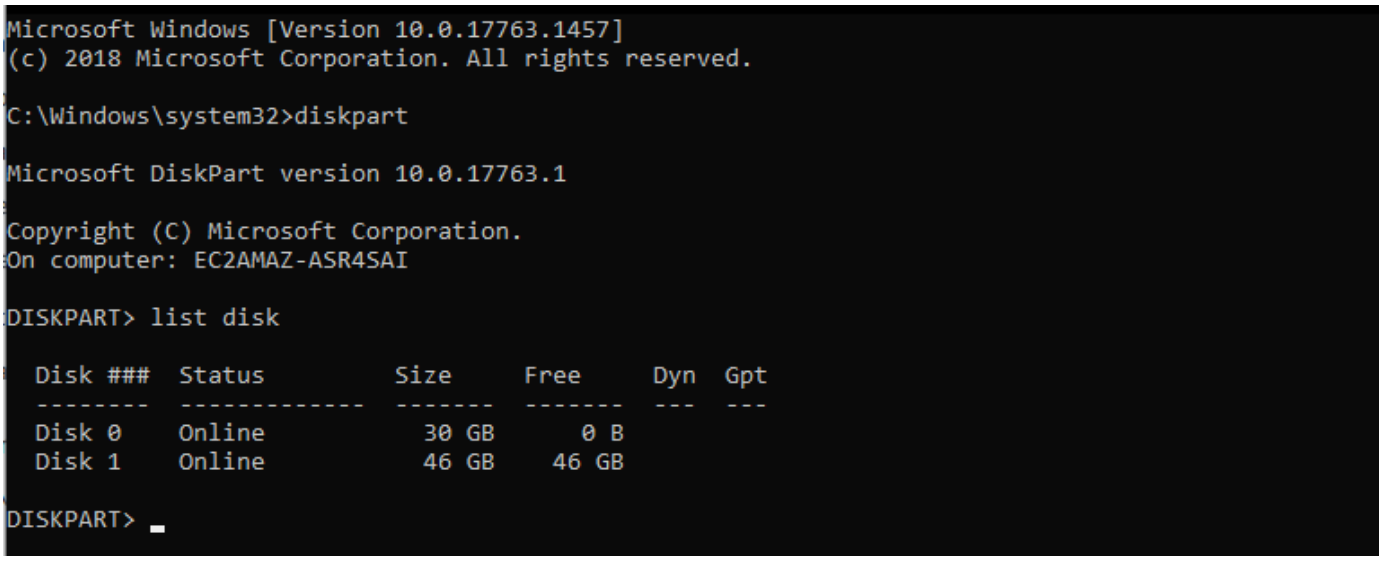
```
Name:                 Cmd0001
Description:          Command
Type:                 VT-UTF8
Channel GUID:         ef9f20a0-1287-11eb-82b0-0e4ba51872e5
Application Type GUID: 63d02271-8aa4-11d5-bccf-00b0d014a2d0

Press <esc><tab> for next channel.
Press <esc><tab>0 to return to the SAC channel.
Use any other key to view this channel.
```

5. Para trocar de canais, pressioneESC+tab+número do canaljunto. Por exemplo, para alternar para o`cmd0002`(se tiver sido criado), pressioneESC+TABA+2.
6. Insira as credenciais exigidas pelo canal do prompt de comando.

```
Please enter login credentials.
Username: Administrator
Domain  : .
Password: *******
```

O prompt de comando é o mesmo shell de comando completo que você obtém em um desktop, mas com a exceção de que ele não permite a leitura de caracteres que já foram emitidos.



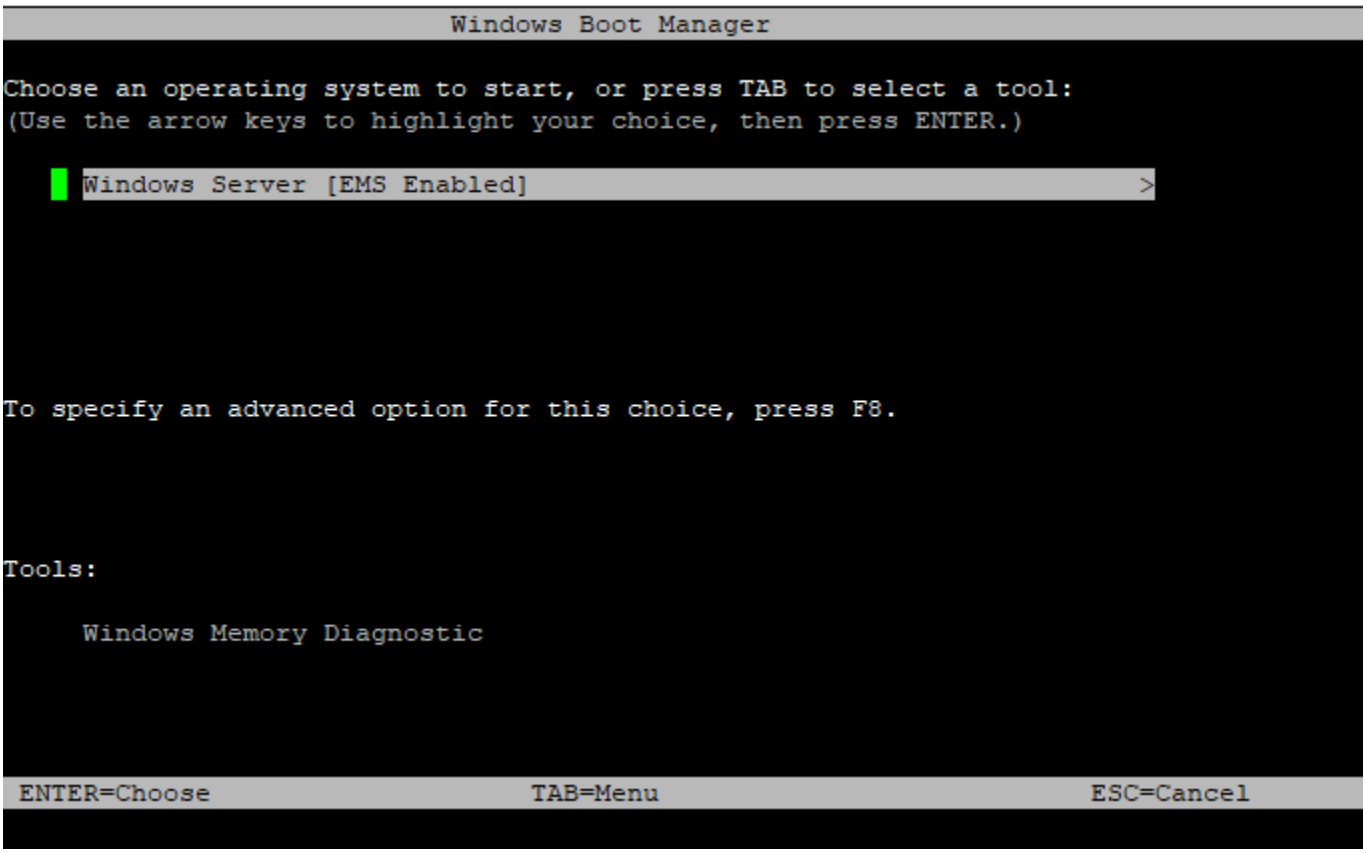
O PowerShell também pode ser usado a partir do prompt de comando.

Observe que talvez seja necessário definir a preferência do progresso para o modo silencioso.

```
PS C:\Windows\system32> $ProgressPreference="SilentlyContinue"
PS C:\Windows\system32> $computerInfo = Get-ComputerInfo
PS C:\Windows\system32> $computerInfo.Csprocessors[0].Name
Intel(R) Xeon(R) Platinum 8124M CPU @ 3.00GHz
PS C:\Windows\system32> $computerInfo.Csprocessors[0].Description
Intel64 Family 6 Model 85 Stepping 4
PS C:\Windows\system32>
```

Usar o menu de inicialização

Se a instância tiver o menu de inicialização habilitado e for reiniciada após a conexão por SSH, você deverá ver o menu de inicialização, como se segue.



Comandos do menu de inicialização

ENTER

Inicia a entrada selecionada do sistema operacional.

TAB

Alterna para o menu Tools (Ferramentas).

ESC

Cancela e reinicia a instância.

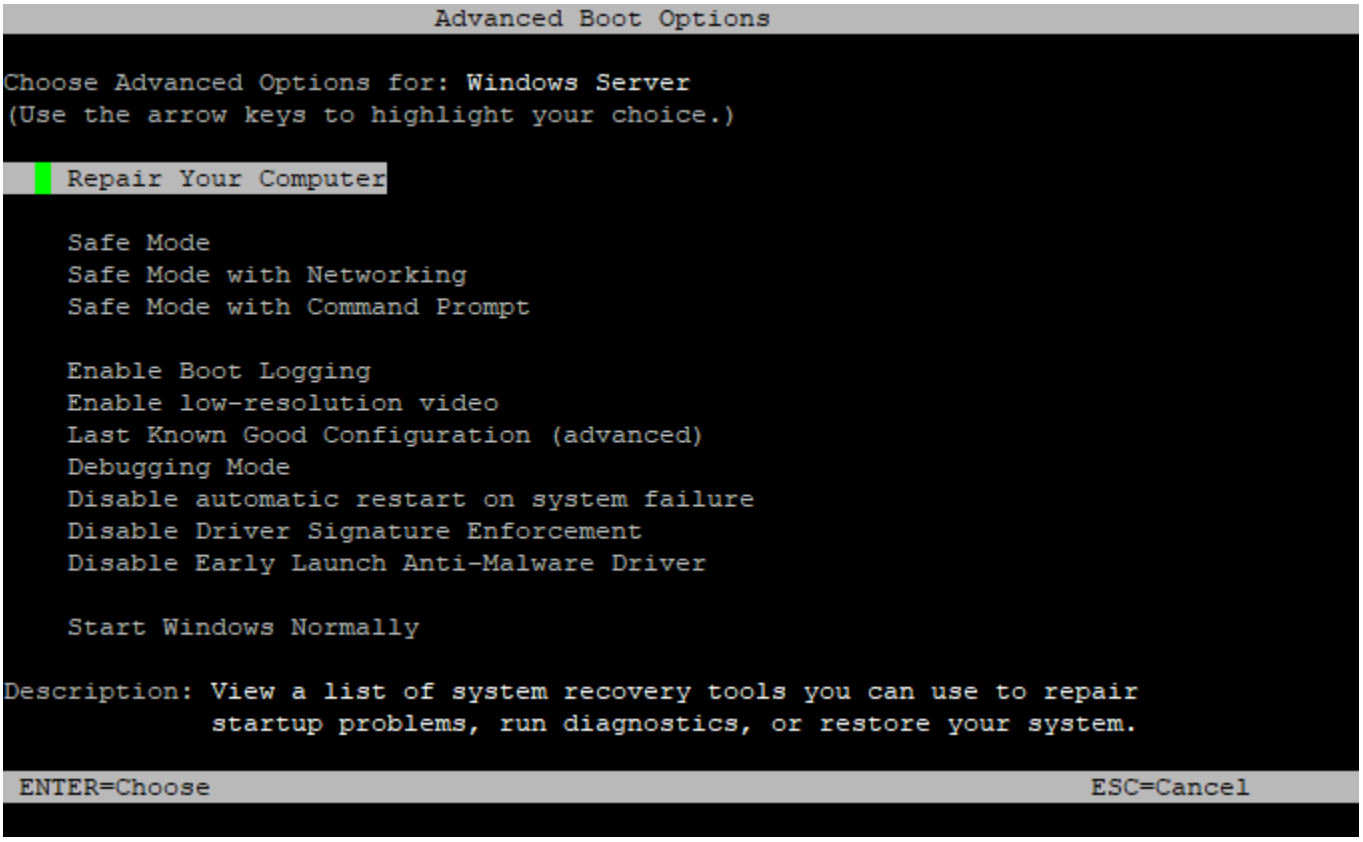
ESC seguido por 8

Equivalente a pressionar F8. Mostra opções avançadas para o item selecionado.

Tecla ESC + seta para a esquerda

Volta para o menu de inicialização inicial.

A tecla ESC por si só não leva você de volta ao menu principal porque o Windows está aguardando para ver se uma sequência de escape está em andamento.



Desabilitar o SAC e o menu de inicialização

Se você habilitar o SAC e o menu de inicialização, poderá desabilitar esses recursos posteriormente.

Use um dos métodos a seguir para desabilitar o SAC e o menu de inicialização em uma instância.

PowerShell

Para desabilitar o SAC e o menu de inicialização em uma instância do Windows

1. Conecte-se à sua instância e execute as seguintes etapas na linha de comando do PowerShell.
2. Primeiro, desabilite o menu de inicialização alterando o valor para `no`.

```
bcdedit /set '{bootmgr}' displaybootmenu no
```

3. Em seguida, desabilite o SAC alterando o valor para `off`.

```
bcdedit /ems '{current}' off
```

4. Aplique a configuração atualizada reinicializando a instância.

```
shutdown -r -t 0
```

Command prompt

Para desabilitar o SAC e o menu de inicialização em uma instância do Windows

1. Conecte-se à sua instância e execute as seguintes etapas no prompt de comando.
2. Primeiro, desabilite o menu de inicialização alterando o valor para `no`.

```
bcdedit /set {bootmgr} displaybootmenu no
```

3. Em seguida, desabilite o SAC alterando o valor para `off`.

```
bcdedit /ems {current} off
```

4. Aplique a configuração atualizada reinicializando a instância.

```
shutdown -r -t 0
```

Enviar uma interrupção para diagnóstico para depurar uma instância inacessível do Amazon EC2

> **Warning**
>
> As interrupções de diagnóstico são destinadas ao uso de usuários avançados. O uso incorreto pode ter um impacto negativo sobre sua instância. Enviar uma interrupção de diagnóstico para uma instância pode acionar uma instância para travar e reinicializar, o que pode levar à perda de dados.

É possível enviar uma interrupção de diagnóstico para uma instância inacessível ou que não responde com a finalidade de acionar manualmente um kernel panic para uma instância do Linux ou um erro de parada (comumente chamado de erro de tela azul) para uma instância do Windows.

Instâncias do Linux

Os sistemas operacionais Linux normalmente falham e reinicializam quando ocorre um pânico de kernel. O comportamento específico do sistema operacional depende de sua configuração. Um pânico de kernel também pode ser usado para fazer com que o kernel do sistema operacional da instância execute tarefas, como a geração de um arquivo de despejo de falha. É possível usar as informações no arquivo de despejo da falha para conduzir uma análise de causa raiz e depurar a instância. Os dados do despejo da falha são gerados localmente pelo sistema operacional na própria instância.

Instâncias do Windows

Em geral, os sistemas operacionais Windows falham e reinicializam quando ocorre um erro de parada, mas o comportamento específico depende de sua configuração. Um erro de parada também pode fazer com que o sistema operacional grave informações de depuração, como um despejo de memória de kernel, em um arquivo. É possível usar essas informações para conduzir análises de causa raiz para depurar a instância. Os dados do despejo da memória são gerados localmente pelo sistema operacional na própria instância.

Antes de enviar uma interrupção de diagnóstico para sua instância, recomendamos que você consulte a documentação do seu sistema operacional e, em seguida, faça as alterações de configuração necessárias.

Tópicos

- Tipos de instâncias compatíveis
- Pré-requisitos
- Enviar uma interrupção para diagnóstico

Tipos de instâncias compatíveis

A interrupção do diagnóstico é compatível com todos os tipos de instância baseadas em Nitro, exceto as que são ativadas pelos processadores AWS Graviton. Para obter mais informações, consulte Instances built on the AWS Nitro System e AWS Graviton.

Pré-requisitos

Antes de usar uma interrupção para diagnóstico, configure o sistema operacional da instância. Isso garantirá que o sistema operacional execute as ações necessárias quando ocorrer um kernel panic (instâncias do Linux) ou um erro de parada (instâncias do Windows).

Instâncias do Linux

Para configurar o Amazon Linux 2 ou o Amazon Linux 2023 para gerar um despejo de falha quando ocorrer um pânico de kernel

1. Conecte-se à sua instância.
2. Instale kexec e kdump.

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

3. Configure o kernel para reservar uma quantidade de memória para o kernel secundário. A quantidade de memória a ser reservada depende da memória disponível total de sua instância. Abra o arquivo `/etc/default/grub` usando o editor de texto de sua preferência, localize a linha que começa com `GRUB_CMDLINE_LINUX_DEFAULT` e adicione o parâmetro `crashkernel` no seguinte formato: `crashkernel=`*`memory_to_reserve`*. Por exemplo, para reservar `256MB`, modifique o arquivo `grub` da seguinte forma:

```
GRUB_CMDLINE_LINUX_DEFAULT="crashkernel=256M console=tty0 console=ttyS0,115200n8
 net.ifnames=0 biosdevname=0 nvme_core.io_timeout=4294967295 rd.emergency=poweroff
 rd.shell=0"
GRUB_TIMEOUT=0
GRUB_DISABLE_RECOVERY="true"
```

4. Salve as alterações e feche o arquivo `grub`.
5. Recompile o arquivo de configuração do GRUB2.

```
[ec2-user ~]$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

6. Em instâncias com base em processadores Intel e AMD, o comando `send-diagnostic-interrupt` envia uma interrupção não mascarável (NMI - non-maskable interrupt) desconhecida para a instância. É necessário configurar o kernel para falhar quando receber a NMI desconhecida. Abra o arquivo `/etc/sysctl.conf` usando o editor de texto de sua preferência e adicione o seguinte.

```
kernel.unknown_nmi_panic=1
```

7. Reinicialize e reconecte-se a sua instância.
8. Verifique se o kernel foi inicializado com o parâmetro `crashkernel` correto.

```
$ grep crashkernel /proc/cmdline
```

A saída do seguinte exemplo indica uma configuração bem-sucedida.

```
BOOT_IMAGE=/boot/vmlinuz-4.14.128-112.105.amzn2.x86_64 root=UUID=a1e1011e-
e38f-408e-878b-fed395b47ad6 ro crashkernel=256M console=tty0 console=ttyS0,115200n8
 net.ifnames=0 biosdevname=0 nvme_core.io_timeout=4294967295 rd.emergency=poweroff
 rd.shell=0
```

9. Verifique se o serviço kdump está em execução.

```
[ec2-user ~]$ systemctl status kdump.service
```

A saída do seguinte exemplo mostrará o resultado se o kdump estiver em execução.

```
kdump.service - Crash recovery kernel arming
   Loaded: loaded (/usr/lib/systemd/system/kdump.service; enabled; vendor preset:
 enabled)
   Active: active (exited) since Fri 2019-05-24 23:29:13 UTC; 22s ago
  Process: 2503 ExecStart=/usr/bin/kdumpctl start (code=exited, status=0/SUCCESS)
 Main PID: 2503 (code=exited, status=0/SUCCESS)
```

> **Note**
>
> Por padrão, o arquivo de dump da falha é salvo em `/var/crash/`. Para alterar o local, modifique o arquivo `/etc/kdump.conf` usando o editor de texto de sua preferência.

Para configurar o SUSE Linux Enterprise, o Ubuntu ou o Red Hat Enterprise Linux

Em instâncias com base em processadores Intel e AMD, o comando `send-diagnostic-interrupt` envia uma interrupção não mascarável (NMI - non-maskable interrupt) desconhecida para a instância. É necessário configurar o kernel para falhar quando ele receber a NMI desconhecida. Para fazer isso, ajuste o arquivo de configuração para o seu sistema operacional. Para obter mais informações sobre como configurar o kernel para falhar, consulte a documentação do sistema operacional.

- SUSE Linux Enterprise

- Ubuntu
- Red Hat Enterprise Linux (RHEL)

Instâncias do Windows

Para configurar o Windows para gerar um despejo de memória quando ocorrer um erro de parada.

1. Conecte-se à sua instância.
2. Abra o Control Panel (Painel de controle) e escolha System (Sistema), Advanced system settings (Configurações avançadas do sistema).
3. Na caixa de diálogo System Properties (Propriedades do sistema), escolha a guia Advanced (Avançado).
4. Na seção Startup and Recovery (Inicialização e recuperação), escolha Settings... (Configurações...).
5. Na seção System failure (Falha do sistema), defina as configurações conforme necessário e escolha OK.

Para obter mais informações sobre como configurar os erros de parada do Windows, consulte Visão geral das opções do arquivo de despejo de memória do Windows.

Enviar uma interrupção para diagnóstico

Depois de concluir as alterações necessárias na configuração, é possível enviar uma interrupção de diagnóstico para a instância usando a AWS CLI ou a API do Amazon EC2.

AWS CLI

Para enviar uma interrupção para diagnóstico para sua instância

Use o comando send-diagnostic-interrupt.

```
aws ec2 send-diagnostic-interrupt --instance-id i-1234567890abcdef0
```

PowerShell

Para enviar uma interrupção para diagnóstico para sua instância

Use o cmdlet Send-EC2DiagnosticInterrupt.

```
Send-EC2DiagnosticInterrupt -InstanceId i-1234567890abcdef0
```

Histórico de documentos do Guia do usuário do Amazon EC2

A tabela apresentada a seguir descreve adições importantes ao Guia do usuário do Amazon EC2 a partir de 2019. Além disso, atualizamos o guia com frequência para abordar os comentários enviados por você.

Alteração	Descrição	Data
Virtualização aninhada	Você pode executar hiperviso res, como Hyper-V e KVM, dentro de instâncias virtualiz adas do Amazon EC2.	16 de fevereiro de 2026
Reservas de capacidade interruptível	As reservas de capacidade interruptível ajudam você a disponibilizar temporariamente a capacidade não utilizada para outras workloads em sua conta.	21 de novembro de 2025
Topologia das instâncias P6-B	É possível obter informaçõ es sobre a topologia das instâncias `p6-b300.48xlarge` .	18 de novembro de 2025
Ancestralidade da AMI	Agora você pode rastrear a origem de uma AMI obtendo uma lista de todas as AMIs ancestrais.	12 de novembro de 2025
Topologia da reserva de capacidade	Antes de iniciar as instância s, é possível usar a API DescribeCapacityReservation Topology para descrever o local em que a capacidade reservada será alocada na	28 de outubro de 2025

	hierarquia da rede, em relação às outras alocações.	
Otimize as CPUs para economizar licenças	Agora é possível configurar CPUs ativas para economizar nos custos de licenciamento de instâncias do Windows e do SQL Server incluídas na licença.	15 de outubro de 2025
Novo EC2 Capacity Manager	O Amazon EC2 adicionou o EC2 Capacity Manager, que permite que você monitore, analise e gerencie seu uso de capacidade ao longo de instâncias sob demanda, instâncias spot e reservas de capacidade, em um único local.	15 de outubro de 2025
AWSEC2CapacityManagerServiceRolePolicy: nova política gerenciada	O Amazon EC2 adicionou a política gerenciada AWSEC2CapacityManagerServiceRolePolicy para permitir que você gerencie recursos de capacidade e se integre com o AWS Organizations em seu nome.	15 de outubro de 2025
`GPUPowerUtilization` Métrica	Nova métrica `GPUPowerUtilization` para instâncias com computação acelerada.	13 de outubro de 2025

Compatibilidade com IPv6 do EC2 Instance Connect Endpoint	O EC2 Instance Connect Endpoint agora é compatível com conectividade IPv6. Agora você pode configurar os EC2 Instance Connect Endpoints para serem compatíveis com pilha dupla ou somente IPv6 para conexão com instâncias com endereços IPv6.	2.º de outubro de 2025
AMIs permitidas: novos parâmetros	AMIs permitidas, um atributo que permite limitar a detecção e o uso de AMIs em sua Conta da AWS, agora são compatíveis com quatro novos parâmetros: códigos de produto de AWS Marketplace, nomes de AMIs, período máximo desde a depreciação da AMI e idade máxima de AMIs.	25 de setembro de 2025
Estatísticas de performance detalhadas para volumes de armazenamento de instância	O Amazon EC2 fornece em tempo real estatísticas de performance de alta resolução para os volumes de armazenamento de instância NVMe anexados a instâncias baseadas no Nitro.	16 de setembro de 2025

Atualizações do host dedicado do Amazon EC2 Mac	Os hosts dedicados do Amazon EC2 Mac são compatíveis com a recuperação automática do host dedicado e com a manutenção do host com base na reinicialização.	28 de agosto de 2025
Cópias de AMIs para zonas locais	Agora você pode copiar AMIs baseadas no Amazon EBS de e para zonas locais.	28 de agosto de 2025
AmazonEC2ImageReferencesAccessPolicy: nova política gerenciada	O Amazon EC2 adicionou a política gerenciada AmazonEC2ImageReferencesAccessPolicy para fornecer permissão para escanear todos os tipos de recursos compatíveis com a API DescribeImageReferences do EC2.	26 de agosto de 2025

Relatórios de uso de AMIs	Se você compartilhar suas imagens de máquina da Amazon (AMI) com outras Contas da AWS, seja com Contas da AWS específic as, organizações, unidades organizacionais (UOs) ou publicamente, será possível ver como essas AMIs são usadas criando relatórios de uso de AMIs. Os relatório s fornecem visibilidade sobre quais Contas da AWS estão usando suas AMIs em modelos de inicialização ou instâncias do EC2, e quantas instâncias ou modelos de inicialização estão referenci ando cada AMI.	26 de agosto de 2025
Referências de AMIs	É possível identificar seus recursos da AWS que referenciam imagens de máquina da Amazon (AMIs) específicas, independe ntemente de as AMIs serem públicas ou privadas ou de quem as possui. Essa visibilid ade ajuda você a garantir que seus recursos usem as mais recentes AMIs compatíveis.	26 de agosto de 2025
Modificar o endpoint do EC2 Instance Connect	É possível modificar o endpoint do EC2 Instance Connect usando o AWS CLI ou um SDK.	14 de agosto de 2025

Aprimoramentos no compartilhamento de reservas de capacidade	É possível compartilhar as reservas de capacidade que você criou nos grupos de posicionamento de cluster.	12 de agosto de 2025
Política gerenciada atualizada para o endpoint do EC2 Instance Connect	Para oferecer suporte à modificação dos endpoints do EC2 Instance Connect existente, o Amazon EC2 atualizou essa política `Ec2InstanceConnectEndpoint` para adicionar permissões para atribuir e cancelar a atribuição de endereços IPv6 e modificar grupos de segurança em interfaces de rede criadas pelo endpoint do EC2 Instance Connect. O Amazon EC2 também atualizou essa política para substituir o operador de condição `Null` pelo operador de condição `StringLike` .	31 de julho de 2025
Topologia da instância: suporte a região adicional	A API DescribeInstanceTopology agora está disponível na região Ásia-Pacífico (Melbourne).	31 de julho de 2025
Forçar finalização	Agora você pode forçar a finalização da sua instância.	31 de julho de 2025
Topologia da instância: suporte a região adicional	A API DescribeInstanceTopology agora está disponível em AWS GovCloud (US-West) .	24 de julho de 2025

Ignorar o desligamento do sistema operacional durante o encerramento da instância	É possível ignorar o desligamento normal do sistema operacional (SO) ao encerrar uma instância.	23 de julho de 2025
Ignorar o desligamento do sistema operacional durante a parada da instância	É possível ignorar o desligamento normal do sistema operacional (SO) ao parar uma instância.	23 de julho de 2025
Blocos de capacidade P6-B200 em us-east-1	Os blocos de capacidade P6-B200 agora estão disponíveis em Leste dos EUA (Norte da Virgínia) - `us-east-1` .	23 de julho de 2025
Atualização da política gerenciada para o perfil vinculado ao serviço do EC2 Fast Launch	Para ajudar a evitar recursos órfãos, o Amazon EC2 atualizou essa política para adicionar permissão para descrever volumes, atributos de volume e interfaces de rede, e para excluir volumes e interfaces de rede criados pelo EC2 Fast Launch.	17 de julho de 2025
Console Serial do EC2: suporte a região adicional	O EC2 Serial Console agora também está disponível na Ásia-Pacífico (Tailândia) e no México (Central).	15 de julho de 2025
EC2 Instance Connect: suporte a região adicional	O EC2 Instance Connect agora também está disponível nas regiões Ásia-Pacífico (Tailândia) e México (Centro).	15 de julho de 2025

Carimbo de data e hora de pacotes de hardware	É possível habilitar o carimbo de data e hora de pacotes de hardware na instância do EC2 para adicionar um carimbo de data e hora de precisão de 64 bits em nanossegundos a cada pacote de rede recebido.	23 de junho de 2025
Excluir snapshots durante o cancelamento do registro da AMI	Ao cancelar o registro de uma AMI, é possível excluir automática e simultaneamente os snapshots associados.	28 de maio de 2025
Migração em reinicialização iniciada pelo usuário	Quando sua instância recebe uma notificação de evento de reinicialização programad a do EC2, ela é habilitada por padrão para a migração da instância quando você reinicializa a instância antes do evento.	20 de maio de 2025
Configuração do SIP para instâncias Mac do Amazon EC	É possível configurar as opções da proteção da integridade do sistema (SIP) para instâncias Mac x86 e instâncias Mac com chip Apple.	20 de maio de 2025
Delegação da propriedade do volume raiz	Agora é possível automatizar a delegação da propriedade do volume raiz para o volume raiz do Amazon EBS ao atualizar o sistema operacion al em instâncias Mac com chip Apple.	20 de maio de 2025

Topologia das instâncias P6-B	É possível obter informaçõ es sobre a topologia das instâncias `p6-b200.48xlarge` .	15 de maio de 2025
Atualizadas as políticas gerenciadas para o perfil vinculado ao serviço do EC2 Fast Launch	Atualizada a política de perfil vinculado ao serviço do EC2 Fast Launch com acesso para criar e manter regras de eventos do Amazon EventBridge e outras ações para aprimorar a experiênc ia do EC2 Fast Launch. Para obter mais informações sobre as permissões concedida s pelo perfil vinculado ao serviço, consulte Permissões concedidas pelo `EC2FastLaunchServiceRolePolicy` .	14 de maio de 2025
Atualizadas as políticas gerenciadas para a política de acesso total do EC2 Fast Launch	Atualizada a política de acesso total do EC2 Fast Launch com permissão para as operações Criar e Modificar modelo de inicialização, criar recursos de rede e grupos de segurança, autorizar regras de ingresso e excluir recursos criados pelo EC2 Fast Launch. A política também pode descrever e criar pilhas do CloudFormation, e excluir pilhas criadas pelo EC2 Fast Launch.	14 de maio de 2025

Onboarding simplificado para o EC2 Fast Launch	Atualizado o EC2 Fast Launch para simplificar o processo de onboarding.	14 de maio de 2025
AWS Config Integração do com AMIs permitidas	Use a regra ec2-instance-launched-with-allowed-ami do AWS Config para verificar se as instâncias em execução ou interrompidas foram iniciadas com AMIs que atendem aos seus critérios de AMIs permitidas.	11 de março de 2025
Política AWSEC2CapacityReservationFleetRolePolicy gerenciada atualizada	O Amazon EC2 atualizou a política gerenciada `AWSEC2CapacityReservationFleetRolePolicy` para utilizar o operador de condição `ArnLike` em vez do operador de condição `StringLike` .	3 de março de 2025
Cópias de AMI baseadas no tempo	Agora, você pode solicitar uma duração de conclusão para operações de cópia de AMI baseadas no EBS, para garantir que as cópias da AMI sejam concluídas em um prazo específico.	25 de fevereiro de 2025
Política AmazonEC2 ReadOnlyAccess atualizada	O Amazon EC2 adicionou a operação `GetSecurityGroupsForVpc` à política existente AmazonEC2 ReadOnlyAccess.	27 de dezembro de 2024

Instâncias gerenciadas	Agora é possível visualizar as instâncias gerenciadas do Amazon EC2 no console do EC2.	1.º de dezembro de 2024
Políticas declarativas	Agora é possível usar políticas declarativas para aplicar configurações em nível de conta em várias regiões e contas simultaneamente. Há suporte para as políticas declarativas configurarem o acesso ao Console de Série do EC2, AMIs permitidas, padrões do IMDS e configurações de bloqueio de acesso público para VPCs, AMIs e snapshots. Para obter mais informações, consulte Políticas declarativas no Guia do usuário do AWS Organizations, bem como a documentação específica para cada atributo com suporte.	1.º de dezembro de 2024
AMIs permitidas	Agora é possível controlar a descoberta e o uso de AMIs no Amazon EC2 especificando os critérios que as AMIs devem atender.	1.º de dezembro de 2024
Blocos de capacidade instantânea	Agora você pode reservar blocos de capacidade para ML, que podem começar em 30 minutos.	21 de novembro de 2024

Reservas de capacidade com data futura	Agora você pode solicitar reservas de capacidade para uma data futura.	21 de novembro de 2024
Estender bloco de capacidade	Agora você pode estender a duração dos blocos de capacidade existentes.	21 de novembro de 2024
6 Blocos de capacidade de seis meses	Agora você pode reservar blocos de capacidade para ML por até seis meses (182 dias).	21 de novembro de 2024
Conjuntos de filtros salvos	Agora você pode criar grupos personalizados de filtros e reutilizá-los para visualizar com eficiência seus recursos do EC2.	20 de novembro de 2024
Proteção de performance	Ao usar a seleção do tipo de instância baseada em atributos para a frota do EC2 ou frota spot, agora você pode habilitar a proteção de performance para garantir que os tipos de instância seleciona dos sejam semelhantes ou excedam uma linha de base de performance especificada.	20 de novembro de 2024
Somente reservas de capacidade	Agora você pode especific ar que as instâncias serão executadas somente em uma reserva de capacidade ou um grupo de recursos de reserva de capacidade.	20 de novembro de 2024

Identificar a AMI de origem	Agora você pode identificar a AMI de origem usada para criar uma AMI.	13 de novembro de 2024
Dividir a capacidade	É possível dividir a capacidade de uma reserva de capacidade existente e criar uma nova.	30 de outubro de 2024
Mover capacidade	Agora você pode mover a capacidade de uma reserva de capacidade para outra.	30 de outubro de 2024
Tutoriais para iniciantes	Dois novos tutoriais para iniciantes: Executar minha primeira instância do EC2 e Executar uma instância de teste do EC2 e conectar-se a ela.	21 de outubro de 2024
Suporte ao Windows Server	Adiciona suporte ao Windows Server 2025.	16 de outubro de 2024
EC2 Global View	O EC2 Global View agora permite que você visualize reservas de capacidade e blocos de capacidade na conta em todas as regiões.	16 de outubro de 2024

Manutenção de host de migração em tempo real	Os hosts dedicados do Amazon EC2 agora são compatíveis com a manutenção de host de migração em tempo real, que migra automaticamente as instâncias compatíveis de um host dedicado danificado para um host dedicado de substituição sem interrompê-las e reiniciá-las.	15 de outubro de 2024
Atribuição de faturamento para reservas de capacidade compartilhadas	Agora você pode atribuir o faturamento de qualquer capacidade disponível de uma reserva de capacidade compartilhada a uma conta de consumidor que pertença à mesma organização da AWS.	14 de outubro de 2024
Relógio de hardware PTP: suporte regional adicional	O relógio de hardware PTP agora também está disponível no Leste dos EUA (Ohio) e Ásia-Pacífico (Malásia).	23 de setembro de 2024
O EC2 Instance Connect é compatível com o IPv6	Agora é possível usar o EC2 Instance Connect para se conectar ao endereço IPv6 público da instância.	23 de setembro de 2024
Listas de prefixos do EC2 Instance Connect	Agora você pode selecionar uma lista de prefixos gerenciados para endereços IPv4 ou IPv6 ao criar regras em seus grupos de segurança para permitir tráfego SSH do serviço EC2 Instance Connect.	23 de setembro de 2024

Novos recursos para gerenciar reservas de capacidade sob demanda	Agora você pode dividir sua reserva de capacidade, mover a capacidade entre reservas de capacidade e modificar o atributo de elegibilidade da instância de sua reserva de capacidade.	14 de agosto de 2024
Compatibilidade com hibernação para C6g, C6gn, C6gd, C7g, C7gd, M6g, M6gd, M7g, M7gd, R6g e R6gd	Coloque em hibernação suas instâncias recém-iniciadas em execução nos tipos de instância C6g, C6gn, C6gd, C7g, C7gd, M6g, M6gd, M7g, M7gd, R6g e R6gd.	30 de julho de 2024
Compatibilidade com hibernação para AMIs compatíveis com instâncias do tipo Graviton	Coloque em hibernação as instâncias recém-iniciadas em uma AMI do Amazon Linux ou em uma AMI do Ubuntu que sejam compatíveis com instâncias do tipo Graviton.	30 de julho de 2024
Tipos de instância adicionais compatíveis com o Credential Guard	Agora é possível habilitar o Credential Guard para instâncias C7i, C7-flex, M7i, M7i-flex, R7i, R7i-flex e T3.	26 de junho de 2024
Assistente de seleção de tipo de instância do EC2: parâmetros adicionais	Agora, o assistente de seleção de tipo de instância do EC2 fornece parâmetros adicionais para você especificar requisitos mais detalhados para a workload.	5 de junho de 2024

Nova política gerenciada para o EC2 Fast Launch	Adicionada a política de EC2FastLaunchFullAccess para realizar ações de API relacionadas ao atributo EC2 Fast Launch em uma instância .	14 de maio de 2024
Proteção contra cancelamento de registro da AMI	É possível ativar a proteção contra cancelamento de registro em uma AMI para evitar sua exclusão acidental ou mal-intencionada.	23 de abril de 2024
Relógio de hardware PTP: suporte ao tipo de instância	O relógio de hardware PTP agora está disponível nos tipos de instância M7a, M7g, M7i, R7a e R7i.	22 de abril de 2024
Adição de considerações de performance sobre o Nitro para redes aprimoradas	Esta página se concentra em considerações de rede para ajudar no ajuste de performance de instâncias do Amazon EC2 baseadas no Nitro.	4 de abril de 2024
Nova política gerenciada para snapshots do EBS baseados no VSS	O VSS do Amazon EC2 tem uma nova política gerenciada pelo IAM disponível que você pode adicionar à sua função do perfil de instância para garantir que as permissões permaneçam atualizadas e sigam as práticas recomendadas.	28 de março de 2024

Relógio de hardware PTP: Leste dos EUA (Norte da Virgínia)	O relógio de hardware PTP agora está disponível na região Leste dos EUA (Norte da Virgínia).	26 de março de 2024
Definir o IMDSv2 como o padrão da conta	É possível definir todas as execuções de novas instâncias do EC2 em sua conta para usar o Instance Metadata Service Version 2 (IMDSv2) por padrão.	25 de março de 2024
Marcar novas AMIs do Linux criadas com base em um snapshot	Ao criar uma AMI do Linux com base em um snapshot, é possível marcar a nova AMI.	7 de março de 2024
Marcar novas AMIs e snapshots ao copiar	Ao copiar uma AMI, é possível marcar a nova AMI e os novos snapshots com as mesmas tags ou com tags diferentes.	7 de março de 2024
Remoção de páginas do AWS Management Pack	O AWS Management Pack foi usado, principalmente, com o Windows Server 2012 e com versões anteriores. Não há mais suporte para essas versões da plataforma do sistema operacional herdadas. Para gerenciar e solucionar problemas relacionados à sua frota de servidores em execução na AWS e on-premises, consulte AWS Systems Manager Fleet Manager.	12 de fevereiro de 2024

EC2 Instance Connect pré-instalado em AMIs do macOS	Agora, o EC2 Instance Connect vem pré-instalado nas AMIs do macOS Sonoma 14.2.1 ou posterior, macOS Ventura 13.6.3 ou posterior e macOS Monterey 12.7.2 ou posterior.	26 de janeiro de 2024
EC2 Instance Connect support for CentOS, macOS, and RHEL	Agora é possível instalar o EC2 Instance Connect em AMIs compatíveis do CentOS, do macOS e do RHEL.	6 de dezembro de 2023
Compatibilidade com hibernação de C7a, C7i, R7a, R7i e R7iz	Coloque em hibernação as instâncias recém-iniciadas em execução nos tipos de instância C7a, C7i, R7a, R7i e R7iz.	1.º de dezembro de 2023
Seletor de tipo de instância do EC2 Amazon Q	O seletor de tipo de instância do EC2 Amazon Q considera o caso de uso, o tipo de workload e a preferência do fabricante da CPU, e também como você prioriza preço e performance. Depois, ele usa esses dados para fornecer orientações e sugestões sobre os tipos de instância do Amazon EC2 que são mais adequados para as novas workloads.	28 de novembro de 2023
Nível gratuito do EC	É possível acompanhar o seu uso do nível gratuito do EC2 no painel do EC2.	26 de novembro de 2023

Console-to-Code	O Console-to-Code pode ajudar você a começar a usar o seu código de automação. O Console-to-Code registra as suas ações feitas no console e depois usa IA generativa para sugerir código no formato de infraestrutura como código de sua preferência. É possível usar o código como ponto de partida, personalizando-o para deixá-lo pronto para produção no seu caso de uso específico.	26 de novembro de 2023
Tempos limites configuráveis de rastreamento de conexão ociosa	As conexões do grupo de segurança que permanece m ociosas podem levar à exaustão do rastreamento da conexão e fazer com que as conexões não sejam rastreadas e os pacotes sejam descartados. Você agora pode definir em segundos o tempo limite para rastreame nto de conexões do grupo de segurança em uma interface de rede do Elastic.	17 de novembro de 2023
Relógio PTP físico	As instâncias compatíve is agora têm um relógio Precision Time Protocol (PTP) físico. O relógio PTP físico é compatível tanto com uma conexão NTP como com uma conexão PTP direta.	16 de novembro de 2023

Alterar o tipo de instância de uma instância habilitada para hibernação	Você não pode alterar o tipo de instância de uma instância habilitada para hibernação quando ela está no estado `stopped`.	16 de novembro de 2023
Topologia da instância	É possível usar a API DescribeInstanceTopology para detectar a localização das suas instâncias e depois usar essas informações para otimizar trabalhos de HPC e ML executando-os em instâncias fisicamente mais próximas umas das outras.	13 de novembro de 2023
Compatibilidade com AMI compartilhada do EC2 Fast Launch	Agora você pode habilitar o EC2 Fast Launch em uma AMI que seja compartilhada com você. Quando você habilita o EC2 Fast Launch em uma AMI compartilhada, snapshots pré-provisionados para uma inicialização mais rápida são criados na sua conta.	6 de novembro de 2023
Blocos de capacidade para ML	Você agora pode reservar instâncias de GPU para uma data futura a fim de lidar com workloads de machine learning (ML) de curta duração.	31 de outubro de 2023

Hibernação de instância spot	Agora você pode colocar instâncias spot em hibernação usando a mesma experiência de hibernação e as mesmas famílias de instâncias que estão atualmente disponíveis para instâncias sob demanda.	24 de outubro de 2023
Configurações padrão de bloquear acesso público para AMIs	O bloqueio do acesso público para AMIs agora é habilitado por padrão em todas as contas novas e nas contas existentes sem AMIs públicas.	20 de outubro de 2023
Amazon EC2 Global View	A Visualização Global do Amazon EC2 é compatível com tipos de recursos adicionais e opções de exibição personalizáveis.	18 de outubro de 2023
Suporte à hibernação para o Ubuntu 22.04.2 LTS (Jammy Jellyfish)	Hiberne suas instâncias executadas recentemente pela AMI do Ubuntu 22.04.2 LTS (Jammy Jellyfish).	16 de outubro de 2023
Desabilitar uma AMI	É possível desabilitar uma AMI para evitar que ela seja usada em execuções de instâncias.	12 de outubro de 2023
Verificações de status do EBS anexado	É possível usar as verificações de status do EBS anexado para monitorar se os volumes do Amazon EBS anexados a uma instância estão acessíveis.	11 de outubro de 2023

Suporte de hibernação para o Red Hat Enterprise Linux 9	Coloque em hibernação as instâncias recém-iniciadas que foram executadas na AMI do Red Hat Enterprise Linux 9.	2 de outubro de 2023
Suporte de hibernação para o Microsoft Windows Server 2022	Coloque em hibernação as instâncias recém-iniciadas que foram executadas no AMI do Microsoft Windows Server 2022.	2 de outubro de 2023
Suporte para hibernação do AL2023	Coloque em hibernação as instâncias recém-iniciadas que foram executadas na AMI do AL2023.	2 de outubro de 2023
Iniciar a interrupção das instâncias spot em uma frota spot	É possível selecionar uma Frota Spot no console da Amazon EC2 e iniciar uma interrupção das Instância s Spot na frota para testar como as aplicações nas suas Instâncias Spot lidam com a interrupção.	21 de setembro de 2023
Bloqueie o acesso público às AMIs	É possível ativar o bloqueio de acesso público para AMIs no nível da conta para bloquear qualquer tentativa de tornar suas AMIs públicas.	12 de setembro de 2023
Compatibilidade com hibernação para M7i e M7i-flex	Hiberne as instâncias recém-iniciadas em execução nos tipos de instância M7i e M7i-flex.	22 de agosto de 2023

O EC2-Classic foi descontinuado	Com o EC2-Classic, suas instâncias do EC2 executadas em uma única rede simples compartilhada com outros clientes. A Amazon VPC substitui o EC2-Classic. Com a Amazon VPC, suas instâncias são executadas em uma nuvem privada virtual (VPC) que é isolada logicamente na conta da AWS.	8 de agosto de 2023
Hosts dedicados	É possível alocar hosts dedicados em ativos de hardware específicos em um Outpost.	20 de junho de 2023
Endpoint do EC2 Instance Connect	Agora é possível conectar-se a uma instância via SSH ou RDP sem exigir que a instância tenha um endereço IPv4 público.	13 de junho de 2023
IMDS Package Analyzer	Agora você pode usar o IMDS Packet Analyzer para identificar origens de chamadas IMDSv1 em suas instâncias do EC2.	1.º de junho de 2023
Instâncias bare metal do Console de Série do EC	O Console de Série do EC2 agora oferece suporte à conectividade com a porta de série de instâncias bare metal selecionadas.	11 de abril de 2023

Cotas do modelo de execução	É possível visualizar as cotas para os modelos de execução e as versões de modelos de execução no console do Service Quotas e usando a CLI do Service Quotas.	3 de abril de 2023
Notificações de utilização da reserva de capacidade	O AWS Health enviará notificações quando a utilizaçã o da capacidade para reservas de capacidade em sua conta estiver abaixo de 20%.	3 de abril de 2023
Grupos de Reserva de capacidade	É possível adicionar reservas de capacidade compartilhadas com você aos grupos de reserva de capacidade de sua propriedade.	30 de março de 2023
Modificar opções de metadados da instância	É possível usar o console Amazon EC2 para modificar as opções de metadados da instância.	20 de março de 2023
Atualizações do sistema operacional macOS no local	Agora, é possível realizar atualizações do sistema operacional no local em instâncias M1 do Mac.	14 de março de 2023
UEFI preferencial	Agora, é possível criar uma única AMI que suporte ambos os modos de inicialização, Unified Extensible Firmware Interface (UEFI) e BIOS legado.	3 de março de 2023

Modificar uma AMI para IMDSv2	Modifique sua AMI existente de modo que as instância s iniciadas a partir da AMI exijam o IMDSv2 por padrão.	28 de fevereiro de 2023
Segurança baseada na virtualização do Windows - Credential Guard	É possível habilitar o Credential Guard, um recurso de segurança baseada em virtualização (VBS), em instâncias compatíveis do Amazon EC2.	31 de janeiro de 2023
Nova política gerenciada para endpoint de conexão de instância do EC	Adicionada a política `Ec2InstanceConnect Endpoint` , que está anexada ao perfil vinculado ao serviço AWSServiceRoleForE C2InstanceConnect, para permitir que o Amazon EC2 execute ações em seu nome quando você criar um endpoint de conexão de instância do EC2.	24 de janeiro de 2023
Alias de AMI em modelos de inicialização	É possível especificar um parâmetro AWS Systems Manager em vez do ID da AMI nos modelos de inicialização para evitar ter que atualizar os modelos toda vez que o ID da AMI for alterada.	19 de janeiro de 2023
Compatibilidade com hibernação para C6i, I3en e M6i	Hiberne as instâncias recém-iniciadas em execução nos tipos de instância C6i, I3en e M6i.	19 de dezembro de 2022

Prevenção de gravação interrompida	Melhore a performance das workloads de banco de dados relacional com uso intenso de E/S e reduza a latência sem afetar negativamente a resiliência dos dados com a prevenção a gravação interrompida, um recurso de armazenamento de blocos.	29 de novembro de 2022
ENA Express	Aumente o throughput e minimize a latência final do tráfego de rede entre instâncias do EC2 com o ENA Express.	28 de novembro de 2022
Copiar as tags de AMI	Ao copiar uma AMI, você pode copiar as tags de AMI definidas pelo usuário ao mesmo tempo.	18 de novembro de 2022
Tamanho de AMI para armazenamento e restauração	O tamanho de uma AMI (antes da compactação) que pode ser armazenada e restaurada de e em um bucket do Amazon S3 agora pode ser de até 5.000 GB.	16 de novembro de 2022
priceCapacityOptimized Estratégia de alocação para instâncias spot	Uma frota spot que usa a estratégia de alocação `priceCapacityOptimized` examina o preço e a capacidade para selecionar os grupos de instâncias spot com menor probabilidade de interrupção e com o menor preço mais possível.	10 de novembro de 2022

price-capacity-optimized Estratégia de alocação para instâncias spot	Uma frota do EC2 que usa a estratégia de alocação `price-capacity-optimized` em preço e capacidade para selecionar os grupos de instâncias spot com menor probabilidade de interrupção e com o menor preço possível.	10 de novembro de 2022
Cancelar o compartilhamento de uma AMI com sua conta	Se uma AMI tiver sido compartilhada com sua Conta da AWS e você não quiser mais compartilhá-la com sua conta, poderá remover sua conta das permissões de execução da AMI.	4 de novembro de 2022
Transferir endereços IP elásticos	Agora, é possível transferir endereços IP elásticos de uma Conta da AWS para outra.	31 de outubro de 2022
Substituir volume raiz	É possível substituir o volume raiz do Amazon EBS por uma instância em execução usando uma AMI.	27 de outubro de 2022
Conectar automaticamente a instância ao banco de dados	Use o recurso de conexão automática para conectar rapidamente uma ou mais instâncias do EC2 a um banco de dados do RDS para permitir o tráfego entre elas.	10 de outubro de 2022
Cotas de AMI	As cotas já se aplicam à criação e ao compartilhamento de AMIs.	10 de outubro de 2022

Configurar AMI para o IMDSv2	Configure a AMI de modo que as instâncias iniciadas a partir da AMI exijam o IMDSv2 por padrão.	3 de outubro de 2022
Iniciar interrupção de instância spot	É possível selecionar uma instância spot no console do Amazon EC2 e iniciar uma interrupção para poder testar como as aplicações nessas instâncias spot lidam com interrupções.	26 de setembro de 2022
Provedor de AMI verificado	No console do Amazon EC2, AMIs públicas de propriedade da Amazon ou de um parceiro verificado da Amazon são marcadas como Provedor verificado.	22 de julho de 2022
Grupos de posicionamento no AWS Outposts	Foi adicionada uma estratégi a de distribuição de host para grupos de posicionamento em um Outpost.	30 de junho de 2022
Hosts dedicados no AWS Outposts	É possível alocar hosts dedicados em AWS Outposts.	31 de maio de 2022
Proteção de instâncias contra interrupção	Para impedir que sua instância seja interrompida acidental mente, habilite a proteção contra a interrupção da instância.	24 de maio de 2022

UEFI Secure Boot	O UEFI Secure Boot baseia-se no longo processo de inicialização segura do Amazon EC2 e fornece defesa adicional em profundidade que ajuda os clientes a proteger o software contra ameaças que persistem durante as reinicializações.	10 de maio de 2022
NitroTPM	O Nitro Trusted Platform Module (NitroTPM) é um dispositivo virtual fornecido pelo AWS Nitro System que está em conformidade com a especificação TPM 2.0.	10 de maio de 2022
Eventos de alteração de estado de AMI	O Amazon EC2 agora gera um evento quando uma AMI muda de estado. É possível usar o Amazon EventBridge para detectar e reagir a esses eventos.	9 de maio de 2022
Descrever as chaves públicas	É possível consultar a chave pública e a data de criação de um par de chaves do Amazon EC2.	28 de abril de 2022
Criar pares de chaves	É possível especificar o formato da chave (PEM ou PPK) ao criar um novo par de chaves.	28 de abril de 2022

Monte sistemas de arquivos Amazon FSx na inicialização	É possível montar um sistema de arquivos Amazon FSx novo ou existente para NetApp ONTAP ou Amazon FSx for OpenZFS na inicialização usando o novo assistente de inicialização de instância.	12 de abril de 2022
Novo assistente de inicializ ação de instância, versão beta	Uma nova e aprimorada experiência de lançamento no console do Amazon EC2, fornecendo uma maneira mais rápida e fácil de iniciar uma instância do EC2.	5 de abril de 2022
Descontinuar automatic amente as AMIs públicas	Por padrão, a data de descontinuação de todas as AMIs públicas é definida como dois anos a partir da data de criação da AMI.	31 de março de 2022
Categoria de metadados de instância: autoescalabilidade/ estado de destino do ciclo de vida	Ao usar grupos do Auto Scaling, é possível acessar o estado de destino do ciclo de vida de uma instância com base nos metadados de instância.	24 de março de 2022
Hora do último início da AMI	`lastLaunchedTime` indica quando sua AMI foi usada pela última vez para iniciar uma instância.	28 de fevereiro de 2022
Chaves ED	Agora há suporte para as chaves ED25519 para EC2 Instance Connect e Console de série do EC2.	20 de janeiro de 2022

Plataformas RHEL adicionais para reservas de capacidade	Plataformas Red Hat Enterprise Linux adicionais para reservas de capacidade sob demanda.	11 de janeiro de 2022
Configure AMIs do Windows para um início mais rápido	Configure AMIs do Windows para iniciar instâncias até 65% mais rápido, usando snapshots pré-provisionados.	10 de janeiro de 2022
Tags de instância em metadados de instância	É possível acessar as tags de uma instância a partir dos metadados da instância.	6 de janeiro de 2022
As Reservas de capacidade não podem ser criadas em grupos de posicionamento de cluster	É possível criar reservas de capacidade em grupos de posicionamento de cluster.	6 de janeiro de 2022
Lançamento antes do término da frota spot	A frota spot pode terminar as instâncias spot que recebem uma notificação de rebalanceamento após o lançamento de novas Instâncias spot de substituição.	4 de novembro de 2021
Lançamento antes do término da frota do EC	A frota do EC2 pode terminar as instâncias spot que recebem uma notificação de rebalanceamento após o início de novas instâncias spot de substituição.	4 de novembro de 2021
Compare os carimbos de data/hora	É possível determinar a hora real de um evento comparando o carimbo de data/hora da instância do Linux do Amazon EC2 com o ClockBound.	2 de novembro de 2021

Compartilhe AMIs com organizações e UOs	Agora é possível compartilhar AMIs com os seguintes recursos da AWS: organizações e unidades organizacionais (UOs).	29 de outubro de 2021
Pontuação de posicionamento de spot	Receba uma recomendação para uma região ou zona de disponibilidade da AWS com base nos requisitos de capacidade spot.	27 de outubro de 2021
Seleção de tipo de instância baseada em atributos para frota spot	Especifique os atributos que uma instância deve ter, e o Amazon EC2 identificará todos os tipos de instância com esses atributos.	27 de outubro de 2021
Seleção de tipo de instância baseada em atributos para frota do EC	Especifique os atributos que uma instância deve ter, e o Amazon EC2 identificará todos os tipos de instância com esses atributos.	27 de outubro de 2021
Frota de reserva de capacidade sob demanda	É possível usar uma frota de reserva de capacidade para iniciar um grupo ou frota de reservas de capacidade.	5 de outubro de 2021
Compatibilidade com hibernação para Ubuntu 20.04 LTS - Focal	Coloque em hibernação suas instâncias recém-iniciadas que foram executadas no Ubuntu 20.04 LTS - Focal AMI.	4 de outubro de 2021
Reservas de Capacidade sob demanda e direcionadas para EC2 Fleet	O EC2 Fleet pode iniciar Instâncias sob demanda nas Reservas de Capacidade `targeted`.	22 de setembro de 2021

Instâncias T3 em hosts dedicados	Suporte para instâncias T3 no host dedicado Amazon EC2.	14 de setembro de 2021
Suporte de hibernação para RHEL, Fedora e CentOS	Coloque em hibernação suas instâncias recém-iniciadas que foram iniciadas a partir de AMIs RHEL, Fedora e CentOS.	9 de setembro de 2021
Amazon EC2 Global View	O Amazon EC2 Global View permite que você visualize VPCs, sub-redes, instância s, grupos de segurança e volumes em várias regiões do AWS em um único console.	1º de setembro de 2021
Suporte à hibernação para C5d, M5d e R5d	Coloque em hibernação suas instâncias recém-iniciadas em execução nos tipos de instância C5d, M5d e R5d.	19 de agosto de 2021
Pares de chaves do Amazon EC	O Amazon EC2 agora é compatível com chaves ED25519 em instâncias Linux e Mac.	17 de agosto de 2021
Prefixos para interfaces de rede	É possível atribuir um intervalo de CIDR IPv4 ou IPv6 privado, de modo automático ou manual, às interfaces de rede.	22 de julho de 2021
Janelas de eventos	É possível definir janelas de eventos personalizadas e semanais para eventos programados que reinicial izam, interrompem ou terminam suas instâncias do Amazon EC2.	15 de julho de 2021

IDs de recursos e suporte a marcação para regras do grupo de segurança	É possível fazer referência a regras de grupo de segurança por ID de recurso. Também é possível adicionar tags a regras de grupos de segurança.	7 de julho de 2021
Descontinuar uma AMI	Agora é possível especificar quando uma AMI é defasada.	11 de junho de 2021
Cobrança do Windows por segundo	O Amazon EC2 cobra por segundo pela utilização baseada em Windows e SQL Server, com cobrança mínima de um minuto.	10 de junho de 2021
Reservas de Capacidade no AWS Outposts	Agora é possível usar as Reservas de Capacidade no AWS Outposts.	24 de maio de 2021
Compartilhamento de reserva de capacidade	Agora é possível compartilhar Reservas de Capacidade criadas em zonas locais e zonas do Wavelength.	24 de maio de 2021
Substituição do volume raiz	Agora é possível usar tarefas de substituição de volume raiz para substituir o volume raiz do EBS para instâncias em execução.	22 de abril de 2021
Armazenar e restaurar uma AMI usando o S3	Armazene AMIs baseadas em EBS no S3 e restaure-as a partir do S3 para permitir a cópia de AMIs entre partições.	6 de abril de 2021

Console serial do EC	Solucione problemas de inicialização e conectividade de rede estabelecendo uma conexão com a porta serial de uma instância.	30 de março de 2021
Modos de inicialização	O Amazon EC2 agora é compatível com a inicializ ação UEFI em determinadas instâncias do EC2 baseadas em AMD e Intel.	22 de março de 2021
Crie um registro de DNS reverso	Agora é possível configurar a pesquisa de DNS reverso para os seus endereços IP elásticos.	3 de fevereiro de 2021
Marcar AMIs e snapshots na criação de AMI	Ao criar uma AMI, é possível marcar a AMI e os snapshots com as mesmas tags, ou pode marcá-los com tags diferentes.	4 de dezembro de 2020
Use o Amazon EventBridge para monitorar eventos de frota spot	Crie regras do EventBridge que acionem ações programát icas em resposta a alteraçõe s e erros de estado de frota spot.	20 de novembro de 2020
Use Amazon EventBridge para monitorar eventos de Frota do EC	Crie regras de EventBridge que acionem ações programát icas em resposta a alterações e erros de estado de Frota do EC2.	20 de novembro de 2020
Excluir frotas de instant	Exclua uma Frota do EC2 do tipo `instant` e encerre todas as instâncias na frota em uma única chamada de API.	18 de novembro de 2020

Suporte à hibernação para T3 e T3a	Hiberne suas instância s recém-executadas em execução em tipos de instância T3 e T3a.	17 de novembro de 2020
Criação rápida do Amazon EFS	É possível criar e montar um sistema de arquivos do Amazon EFS em uma instância na inicialização usando o Amazon EFS Quick Create.	9 de novembro de 2020
Categoria de metadados da instância: events/re commendations/rebalance	O tempo aproximado, em UTC, quando a notificação de recomendação de rebalance amento da instância do EC2 é emitida para a instância.	4 de novembro de 2020
Recomendação de rebalance amento de instâncias do EC	Um sinal que o notifica quando uma instância spot está em risco elevado de interrupção.	4 de novembro de 2020
Reservas de Capacidade em zonas Wavelength	Reservas de Capacidade agora podem ser criadas e usadas em zonas Wavelength.	4 de novembro de 2020
Rebalanceamento de capacidade	Configure a frota spot ou a EC2 Fleet para executar uma instância spot de substitui ção quando o Amazon EC2 emitir uma recomendação de rebalanceamento.	4 de novembro de 2020
Suporte à hibernação para I3, M5ad e R5ad	Hibernar suas instâncias recém-iniciadas em execução nos tipos de instância I3, M5ad e R5ad.	21 de outubro de 2020

Limites de vCPU da instância spot	Os limites da instância spot agora são gerenciados em termos do número de vCPUs que suas instâncias spot em execução estão usando ou usarão até o atendimento de solicitações abertas.	1º de outubro de 2020
Reservas de Capacidade em zonas locais	Reservas de Capacidade agora podem ser criadas e usadas em zonas locais.	30 de setembro de 2020
Suporte à hibernação para M5a e R5a	Hiberne suas instância s recém-executadas em execução nos tipos de instância M5a e R5a.	28 de agosto de 2020
Os metadados da instância fornecem informações de posicionamento e localização da instância	Novos campos de metadados de instância na categoria `placement` : região, nome do placement group, número da partição, ID do host e ID da zona de disponibilidade.	24 de agosto de 2020
Grupos de Reserva de capacidade	É possível usar AWS Resource Groups para criar coleções lógicas de reservas de capacidade e, depois, direcionar execuções de instâncias nesses grupos.	29 de julho de 2020

EC2Launch v2	É possível usar o EC2Launch v2 para executar tarefas durante o startup da instância se uma instância for interrompida e iniciada posteriormente, se uma instância for reiniciada, e também sob demanda. O EC2Launch v2 é compatível com todas as versões do Windows Server e substitui o EC2Launch e o EC2Config.	30 de junho de 2020
Traga seus próprios endereços IPv	É possível trazer parte ou todo o seu intervalo de endereços IPv6 da rede on-premises para sua conta da AWS.	21 de maio de 2020
Inicie instâncias usando um parâmetro do Systems Manager	É possível especificar um parâmetro do AWS Systems Manager em vez de uma AMI ao executar uma instância.	5 de maio de 2020
Personalizar notificações de eventos programados	É possível personalizar notificações de eventos programados para incluir tags na notificação por e-mail.	4 de maio de 2020
Windows Server no Hosts dedicados	É possível usar as AMIs do Windows Server fornecidas pela Amazon para executar as versões mais recentes do Windows Server no Hosts dedicados.	7 de abril de 2020

Interromper e iniciar uma instância spot	Agora é possível interromper suas instâncias spot com base no Amazon EBS e iniciá-las à vontade, em vez de depender do comportamento de interrupção.	13 de janeiro de 2020
Marcação de recursos	É possível marcar gateways da Internet somente de saída, gateways locais, tabelas de rotas de gateway, interfaces virtuais de gateway locais, grupos de interface virtual de gateway local, associações de VPC da tabela de rotas do gateway local e associações de grupo de interface virtual da tabela de rotas do gateway local	10 de janeiro de 2020
Conecte-se à sua instância usando o Gerenciador de sessões	É possível iniciar uma sessão do Gerenciador de sessões com uma instância no console do Amazon EC2.	18 de dezembro de 2019
Hosts dedicados e grupos de recursos de host	Hosts dedicados agora podem ser usados com grupos de recursos de host.	2 de dezembro de 2019
Compartilhamento de host dedicado	Agora é possível compartilhar os hosts dedicados entre contas da AWS.	2 de dezembro de 2019

Especificação de crédito padrão no nível da conta	É possível definir a especificação de crédito padrão por família de instâncias expansíveis no nível da conta, por região da AWS.	25 de novembro de 2019
Descoberta de tipo de instância	É possível encontrar um tipo de instância que atenda às suas necessidades.	22 de novembro de 2019
Hosts dedicados	Agora, é possível configurar um Host dedicado para oferecer suporte a vários tipos de instância em uma família de instâncias.	21 de novembro de 2019
Serviço de metadados da instância versão 2	É possível usar o Serviço de metadados da instância versão 2, que é um método orientado a sessão para solicitação de metadados da instância.	19 de novembro de 2019
Elastic Fabric Adapter	O Adaptador de malha elástica agora pode ser usado com a Intel MPI 2019 Update 6.	15 de novembro de 2019
Suporte à hibernação de instâncias do Windows sob demanda	É possível hibernar instâncias do Windows sob demanda.	14 de outubro de 2019
Compras na fila de instâncias reservadas	É possível colocar a compra de uma Instância reservada na fila até três anos de maneira antecipada.	4 de outubro de 2019

Interrupção do diagnóstico	É possível enviar uma interrupção para diagnóstico a uma instância inacessível ou sem resposta para acionar um pânico de kernel.	14 de agosto de 2019
Estratégia de alocação otimizada por capacidade	Com o uso de EC2 Fleet ou de frota spot, agora é possível executar instâncias spot a partir de grupos spot com a capacidade ideal para o número de instâncias que estão sendo executadas.	12 de agosto de 2019
Compartilhamento de reservas de capacidade sob demanda	Agora é possível compartilhar as Reservas de Capacidade entre contas da AWS.	29 de julho de 2019
Elastic Fabric Adapter	O EFA agora oferece suporte à Open MPI 3.1.4 e à Intel MPI 2019 Update 4.	26 de julho de 2019
EC2 Instance Connect	O EC2 Instance Connect é uma forma simples e segura de conectar-se com suas instâncias usando Secure Shell (SSH).	27 de junho de 2019
Recuperação do host	Reinicie automaticamente suas instâncias em um novo host no caso de uma falha inesperada do hardware em um Host dedicado.	5 de junho de 2019

Snapshots consistentes com a aplicação VSS	Crie snapshots consistentes com a aplicação de todos os volumes do Amazon EBS anexados às instâncias do Windows usando o Run Command do AWS Systems Manager.	13 de maio de 2019
Assistente de realocação de plataformas Windows para Linux para bancos de dados do Microsoft SQL Server	Mover workloads existentes do Microsoft SQL Server de um sistema operacional Windows para Linux. O link atualizado aponta para o Microsoft SQL Server no Guia do usuário do Amazon EC2.	8 de maio de 2019
Atualização automatizada do Windows	Execute atualizações automatizadas de instâncias do EC2 do Windows usando o AWS Systems Manager.	6 de maio de 2019
Elastic Fabric Adapter	É possível anexar um Elastic Fabric Adapter às suas instâncias para acelerar as aplicações de High Performan ce Computing (HPC).	29 de abril de 2019

Para obter informações sobre as liberações de tipo de instância do Amazon EC2, consulte Document history no Guia de tipos de instância do Amazon EC2.

Histórico para 2018 e para os anos anteriores

A tabela apresentada a seguir descreve adições importantes ao Guia do usuário do Amazon EC2 em 2018 e nos anos anteriores.

Recurso	Versão da API	Descrição	Data de lançamento
Grupos de posicionamento de partição	15/11/2016	Os grupos de posicionamento 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.	20 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 do Amazon EC2.	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.	28 de novembro de 2018
O console do Spot recomenda uma frota de instâncias	15/11/2016	O console do Spot recomenda uma frota de instâncias com base na melhor prática do Spot (diversificação de instâncias) para atender às especificações mínimas de hardware (vCPUs, memória e armazenamento) para a necessidade de sua aplicação. Para obter mais informações, consulte Criar uma Frota spot.	20 de novembro de 2018
Novo tipo de solicitação de Frota do EC2: instant	15/11/2016	Agora, o Frota do EC2 oferece suporte a um novo tipo de solicitação, `instant`, que pode ser usada para provisionar capacidade de forma síncrona entre tipos de instâncias e modelos de compra. A solicitação `instant` retorna as instâncias executadas na resposta	14 de novembro de 2018

Recurso	Versão da API	Descrição	Data de lançamento
		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 e de frota spot.	
Informações sobre economias do Spot	15/11/2016	É possível visualizar as economias feitas com o uso de instâncias spot para uma única frota spot ou para todas as instâncias spot. Para obter mais informações, consulte Economia na compra das Instâncias spot.	5 de novembro de 2018
Suporte do console para otimização de opções de CPU	15/11/2016	Ao executar uma instância, é possível otimizar as opções de CPU para atender a workloads ou necessidades de negócios específicas usando o console do Amazon EC2. Para obter mais informações, consulte Opções de CPU para instâncias do Amazon EC2.	31 de outubro de 2018
Suporte do console para criação de um modelo de execução usando uma instância	15/11/2016	É possível 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 informaçõ es, consulte Criar um modelo de execução do Amazon EC2.	30 de outubro de 2018

Recurso	Versão da API	Descrição	Data de lançamento
On-Demand Capacity Reservations	15/11/2016	É possível 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 Reservar capacidade computacional com reservas de capacidade sob demanda do EC2.	25 de outubro de 2018
Traga seus próprios endereços IP (BYOIP)	15/11/2016	É possível trazer parte ou todo o seu intervalo de endereços IPv4 públicos da rede on-premises para sua conta da AWS. Depois de levar o intervalo de endereços para a AWS, ele aparece em sua conta como um grupo de endereços. É possível criar um endereço IP elástico de seu grupo de endereços e usá-lo com seus recursos da AWS. Para obter mais informações, consulte Trazer seus próprios endereços IP (BYOIP) para o Amazon EC2.	23 de outubro de 2018
Tag de Host dedicado na criação e suporte do console	15/11/2016	É possível marcar seus Hosts dedicados na criação e gerenciar as tags de Host dedicado usando o console do Amazon EC2. Para obter mais informações, consulte Alocar um host dedicado do Amazon EC2 para uso em sua conta.	08 de outubro de 2018

Recurso	Versão da API	Descrição	Data de lançamento
Suporte ao console para escalabilidade programada para a frota spot	15/11/2016	Aumentar ou diminuir a capacidade atual da frota com base em data e hora. Para obter mais informações, consulte Escalabilidade programada: escalar a frota spot de acordo com uma programação.	20 de setembro de 2018
Estratégias de alocação para Frotas do EC2	15/11/2016	É possível especificar se a capacidade sob demanda é atendida pelo preço (preço mais baixo primeiro) ou prioridade (prioridade mais alta primeiro). É possível especificar o número de grupos spot para os quais alocar sua capacidade spot de destino. Para obter mais informações, consulte Usar estratégias de alocação para determinar como a frota do EC2 ou a frota spot atende à capacidade spot e sob demanda.	26 de julho de 2018
Estratégias de alocação para Frotas spot	15/11/2016	É possível especificar se a capacidade sob demanda é atendida pelo preço (preço mais baixo primeiro) ou prioridade (prioridade mais alta primeiro). É possível especificar o número de grupos spot para os quais alocar sua capacidade spot de destino. Para obter mais informações, consulte Usar estratégias de alocação para determinar como a frota do EC2 ou a frota spot atende à capacidade spot e sob demanda.	26 de julho de 2018
Automação do ciclo de vida do snapshot	15/11/2016	É possível usar o Amazon Data Lifecycle Manager para automatizar a criação e a exclusão de snapshots para seus volumes do EBS. Para obter mais informações, consulte Amazon Data Lifecycle Manager.	12 de julho de 2018

Recurso	Versão da API	Descrição	Data de lançamento
Opções de CPU em modelos de execução	15/11/2016	Quando você cria um modelo de execução usando as ferramentas da linha de comando, pode otimizar as opções de CPU para se adequarem a workloads ou necessidades de negócios específicos. Para obter mais informações, consulte Criar um modelo de execução do Amazon EC2.	11 de julho de 2018
Marcação de Hosts dedicados	15/11/2016	É possível marcar seus Hosts dedicados.	3 de julho de 2018
Obter a saída mais recente do console	15/11/2016	É possível 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, é possível otimizar as opções de CPU para atender a workloads ou necessidades de negócios específicas: Para obter mais informações, consulte Opções de CPU para instâncias do Amazon EC2.	8 de maio de 2018
EC2 Fleet	15/11/2016	É possível usar a EC2 Fleet para executar um grupo de instâncias em tipos de instância do EC2 e zonas de disponibilidade diferentes, e entre modelos de compra sob demanda, instância reservada e instância spot. Para obter mais informações, consulte Frota do EC2 e frota spot.	2 de maio de 2018

Recurso	Versão da API	Descrição	Data de lançamento
Instâncias sob demanda em Frotas spot	15/11/2016	É possível incluir uma solicitação de capacidade sob demanda na solicitação de frota spot para garantir que você sempre tenha capacidade de instância. Para obter mais informações, consulte Frota do EC2 e frota spot.	2 de maio de 2018
Marcar snapshots do EBS na criação	15/11/2016	É possível aplicar tags a snapshots durante a criação.	2 de abril de 2018
Alterar grupos de posicionamento	15/11/2016	É possível mover uma instância para dentro ou para fora de um grupo de posicionamento, ou alterar o grupo de posicionamento da instância. Para obter mais informações, consulte Alterar o posicionamento para uma instância do EC2.	1 de março de 2018
IDs mais longos de recursos	15/11/2016	É possível habilitar o formato de ID mais longo para outros tipos de recursos.	9 de fevereiro de 2018
Melhorias na performance da rede	15/11/2016	As instâncias de fora de um grupo de posicionamento 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.	24 de janeiro de 2018
Marcar endereços IP elásticos	15/11/2016	É possível marcar seus endereços IP elásticos.	21 de dezembro de 2017

Recurso	Versão da API	Descrição	Data de lançamento
Amazon Time Sync Service	15/11/2016	É possível usar o Amazon Time Sync Service para manter a precisão da hora na instância. Para obter mais informações, consulte Relógio de precisão e sincronização de horas em sua instância do EC2.	29 de novembro de 2017
T2 ilimitada	15/11/2016	As instâncias T2 ilimitadas podem apresentar uma expansão acima da linha de base pelo tempo que for necessário. Para obter mais informações, consulte Instâncias expansíveis.	29 de novembro de 2017
Modelos de execução	15/11/2016	Um modelo de execução pode conter todos ou alguns parâmetros necessários à execução de uma instância, de modo que você não precise especificá-las todas as vezes que executar uma instância. Para obter mais informações, consulte Armazenar os parâmetros de execução de instâncias nos modelos de execução do Amazon EC2.	29 de novembro de 2017
Posicionamento disseminado	15/11/2016	Os grupos de posicionamento de distribuição são recomendados para aplicações com uma pequena quantidade de instâncias críticas que devem ser mantidas separadas umas das outras. Para obter mais informações, consulte Grupos com posicionamento distribuído.	29 de novembro de 2017
Hibernação da instância spot	15/11/2016	O serviço spot pode hibernar instâncias spot em caso de interrupção.	28 de novembro de 2017

Recurso	Versão da API	Descrição	Data de lançamento
Monitoramento do objetivo da frota spot	15/11/2016	É possível configurar políticas de dimensionamento com monitoramento do objetivo para a frota spot. Para obter mais informações, consulte Escalabilidade de rastreamento de destino: escalar a frota spot definindo um valor para uma métrica específica.	17 de novembro de 2017
A frota spot integra-se ao Elastic Load Balancing	15/11/2016	É possível associar um ou mais load balancers a uma frota spot.	10 de novembro de 2017
Mesclagem e divisão do Instâncias reservadas conversíveis	15/11/2016	É possível trocar (mesclar) dois ou mais Instâncias reservadas conversíveis por um novo Instância reservada convertível. Também é possível usar o processo de modificação para dividir um Instância reservada convertível em reservas menores. Para obter mais informações, consulte Trocar Instâncias reservadas conversíveis.	6 de novembro de 2017
Modificar a locação da VPC	15/11/2016	É possível alterar o atributo de locação da instância da VPC de `dedicated` para `default`. Para obter mais informações, consulte Alterar a locação da instância de uma VPC.	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

Recurso	Versão da API	Descrição	Data de lançamento
Parar em interrupção	15/11/2016	É possível especificar se o Amazon EC2 deve parar ou encerrar as Instâncias spot quando elas são interrompidas. Para obter mais informações, consulte Comportamento das interrupções de instâncias spot.	18 de setembro de 2017
Marcar gateways NAT	15/11/2016	É possível marcar o gateway NAT. Para obter mais informações, consulte Marcar seus recursos com tag.	7 de setembro de 2017
Descrições de regras do grupo de segurança	15/11/2016	É possível adicionar descrições às regras do grupo de segurança.	31 de agosto de 2017
Elastic Graphics	15/11/2016	Anexe aceleradores de Elastic Graphics a suas instâncias para acelerar a performance de gráficos de suas aplicações.	29 de agosto de 2017
Recuperar endereços IP elásticos	15/11/2016	Se você liberar um endereço IP elástico para usar em um VPC, poderá recuperá-lo.	11 de agosto de 2017
Marcar instâncias de frota spot	15/11/2016	É possível configurar sua frota spot para marcar automaticamente as instâncias que ela executa.	24 de julho de 2017

Recurso	Versão da API	Descrição	Data de lançamento
Recursos de tags durante a criação	15/11/2016	É possível aplicar tags a instâncias e volumes durante a criação. Para obter mais informações, consulte Marcar seus recursos com tag. Além disso, é possível usar permissões em nível de recurso baseadas em tags para controlar as tags que são aplicadas. Para obter mais informações, consulte ., Conceder permissão para marcar recursos do Amazon EC2 durante a criação.	28 de março 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, é possível modificar o tamanho, o tipo e as IOPS do volume sem desanexar o volume ou parar a instância.	13 de fevereiro de 2017
Anexar uma função da IAM	15/11/2016	É possível anexar, desanexar ou substituir uma função da IAM para uma instância existente. Para obter mais informações, consulte Funções do IAM para Amazon EC2.	9 de fevereiro de 2017
Instâncias spot dedicadas	15/11/2016	É possível executar Instâncias spot em hardware de único locatário em uma nuvem privada virtual (VPC). Para obter mais informações, consulte Executar no hardware de locatário único.	19 de janeiro de 2017
Suporte a IPv6	15/11/2016	É possível 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.	1º de dezembro de 2016

Recurso	Versão da API	Descrição	Data de lançamento
Escalabilidade automática para frota spot		Agora é possível configurar políticas de escalabilidade para a frota spot. Para obter mais informações, consulte Saiba mais sobre escalabilidade automática para frota spot.	1º de setembro de 2016
Elastic Network Adapter (ENA)	01/04/2016	Agora é possível usar o ENA para rede avançada. Para obter mais informações, consulte Redes aperfeiçoadas para instâncias do Amazon EC2.	28 de junho de 2016
Suporte avançado para visualização e modificação de IDs mais longos	01/04/2016	Agora é possível visualizar e modificar as configurações de IDs mais longos para outros usuários do IAM funções do IAM ou usuários root.	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.	21 de junho de 2016
Capturar uma captura de tela do console de uma instância	01/10/2015	Agora é possível obter informações adicionais ao depurar instâncias não acessíveis. Para obter mais informações, consulte Fazer uma captura de tela de uma instância inacessível.	24 de maio de 2016
Dois novos tipos de volume do EBS	01/10/2015	Agora é possível criar HDD otimizado para throughput (st1) e volumes de disco rígido frio (sc1).	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.	23 de março de 2016

Recurso	Versão da API	Descrição	Data de lançamento
Métricas do CloudWatch para frota spot		Agora é possível obter as métricas do CloudWatch para sua frota spot. Para obter mais informações, consulte Monitorar a frota do EC2 ou frota spot usando o CloudWatch.	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.	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, é possível habilitar o formato mais longo de ID para tipos de recursos compatíveis.	13 de janeiro de 2016
Suporte do DNS para o ClassicLink	01/10/2015	É possível 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.	11 de janeiro de 2016
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 do Amazon EC2.	23 de novembro de 2015

Recurso	Versão da API	Descrição	Data de lançamento
Duração da instância spot	01/10/2015	Agora é possível especificar uma duração para Instâncias spot. Bloqueios pontuais não são compatíveis (janeiro de 2023).	6 de outubro de 2015
Solicitação de modificação de frota spot	01/10/2015	Agora é possível modificar a capacidade de destino de sua solicitação de frota spot. Para obter mais informações, consulte Modificar uma solicitação de frota spot.	29 de setembro de 2015
Estratégia diversificada de alocação de frota spot	15/04/2015	Agora é possível alocar instâncias spot em vários grupos spot usando uma única solicitação de frota spot. Para obter mais informações, consulte Usar estratégias de alocação para determinar como a frota do EC2 ou a frota spot atende à capacidade spot e sob demanda.	15 de setembro de 2015
Peso de instâncias de frotas spot	15/04/2015	Agora é possível definir as unidades de capacidade com que cada tipo de instância contribui para a performance de sua aplicação, e ajustar o valor a ser pago por Instâncias spot para cada grupo spot de forma correspondente. Para obter mais informações, consulte Usar ponderação de instâncias para gerenciar o custo e a performance da frota do EC2 ou da frota spot.	31 de agosto de 2015
Nova ação de alarme de reinicialização e nova função do IAM para uso com ações de alarme		Adicionada a ação de alarme de reinicialização e a nova função do IAM para uso com ações de alarme. Para obter mais informações, consulte Criar alarmes para interromper, encerrar, reinicializar ou recuperar uma instância.	23 de julho de 2015

Recurso	Versão da API	Descrição	Data de lançamento
Spot Fleets	15/04/2015	É possível gerenciar uma coleção ou uma frota de instâncias spot em vez de gerenciar solicitações separadas de instância spot. Para obter mais informações, consulte Frota do EC2 e frota spot.	18 de maio de 2015
Migrar endereços IP elásticos para o EC2-Classic	15/04/2015	É possível migrar um endereço IP elástico alocado para uso no EC2-Classic para ser usado em uma VPC.	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
Systems Manager		O Systems Manager permite configurar e gerenciar as instâncias do EC2.	17 de fevereiro de 2015
Systems Manager para Microsoft SCVMM 1.5		Agora é possível usar o Systems Manager para Microsoft SCVMM para executar uma instância e para importar uma VM do SCVMM para o Amazon EC2.	21 de janeiro de 2015

Recurso	Versão da API	Descrição	Data de lançamento
Recuperação automática de instâncias do EC2		É possível 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. Para obter mais informações, consulte Recuperação automática de instâncias.	12 de janeiro de 2015
ClassicLink	01/10/2014	O ClassicLink permite vincular sua instância do EC2-Classic a uma VPC em sua conta. É possível associar grupos de segurança 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.	7 de janeiro de 2015
Notificações de encerramento de instância spot		A melhor maneira de proteger-se contra a interrupção de instância spot é configurar a aplicação para ser tolerante a falhas. Além disso, é possível aproveitar os avisos de encerramento de instância spot, que enviam um aviso dois minutos antes de o Amazon EC2 encerrar a instância spot. Para obter mais informações, consulte Avisos de interrupção de instância spot.	5 de janeiro de 2015

Recurso	Versão da API	Descrição	Data de lançamento
Systems Manager para Microsoft SCVMM		O Systems Manager para Microsoft SCVMM fornece uma interface simples e fácil de usar para gerenciamento de recursos da AWS, como instâncias do EC2, no Microsoft SCVMM.	29 de outubro de 2014
`DescribeVolumes` Suporte à paginação de	01/09/2014	A API `DescribeVolumes` agora oferece suporte à paginação dos resultados com os parâmetros `MaxResults` e `NextToken`. Para obter mais informações, consulte DescribeVolumes no Amazon EC2 API Reference.	23 de outubro de 2014
Adicionado o suporte para Amazon CloudWatch Logs		É possível usar o Amazon CloudWatch Logs para monitorar, armazenar e acessar o sistema, a aplicação e os arquivos de log personalizados em suas instâncias ou em outras origens. Em seguida, é possível recuperar os dados de log associados do CloudWatch Logs usando o console do Amazon CloudWatch, os comandos do CloudWatch Logs na CLI da AWS ou o SDK do CloudWatch Logs.	10 de julho 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

Recurso	Versão da API	Descrição	Data de lançamento
Volumes de Amazon EBS Finalidade geral (SSD)	01/05/2014	Os volumes Finalidade geral (SSD) oferecem armazenamento econômico ideal para uma ampla variedade de workloads. Esses volumes proporcionam latências de milissegundos de um dígito, capacidade de expansão de 3.000 IOPS por períodos estendidos e uma performance básica de 3 IOPS/GiB. Os volumes SSD de uso geral podem variar de tamanho entre 1 GiB e 1 TiB.	16 de junho de 2014
AWS Management Pack		AWSO Management Pack agora oferece suporte para o System Center Operations Manager 2012 R2.	22 de maio de 2014
Amazon EBS encryption	01/05/2014	O Criptografia de Amazon EBS oferece criptografia sem interrupção dos volumes de dados do EBS, bem como de snapshots, eliminando a necessidade de criar e manter uma infraestrutura de gerenciamento de chaves de segurança. A criptografia do EBS ativa a segurança dos dados em repouso, criptografando os dados usando as Chaves gerenciadas pela AWS. A criptografia ocorre nos servidores que hospedam as instância s do EC2, oferecendo criptografia de dados durante seu trânsito entre as instâncias do EC2 e armazenamento do EBS.	21 de maio 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.	28 de janeiro de 2014

Recurso	Versão da API	Descrição	Data de lançamento
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 VM Import/Export User Guide (Manual do usuário para importação/exportação de VMs).	16 de dezembro de 2013
Permissões em nível de recurso para RunInstances	15/10/2013	Agora é possível criar políticas no AWS Identity and Access Management para controlar permissões em nível de recurso para a ação da API RunInstances do Amazon EC2. Para obter mais informações e políticas de exemplo, consulte Identity and Access Management para o Amazon EC2.	20 de novembro de 2013
Execução de uma instância no AWS Marketplace		Agora é possível iniciar uma instância no AWS Marketplace usando o Launch Wizard do Amazon EC2. Para obter mais informações, consulte Executar uma instância do Amazon EC2 em uma AMI do AWS Marketplace.	11 de novembro de 2013
Novo assistente de execução		Há um novo assistente de execução reprojeta do do EC2. Para obter mais informações, consulte Executar uma instância do EC2 usando o assistente de inicialização de instâncias no console.	10 de outubro de 2013
Modificação dos tipos de instância de instâncias reservadas	01/10/2013	Agora é possível modificar o tipo de instância de instâncias reservadas do Linux na mesma família (por exemplo, M1, M2, M3, C1). Para obter mais informações, consulte Modificar a Instâncias reservadas.	09 de outubro de 2013

Recurso	Versão da API	Descrição	Data de lançamento
Modificação de instâncias reservadas do Amazon EC2	15/08/2013	Agora é possível modificar instâncias reservadas em uma região. Para obter mais informações, consulte Modificar a Instâncias reservadas.	11 de setembro de 2013
Atribuição de um endereço IP público	15/07/2013	Agora é possível atribuir um endereço IP público ao executar uma instância em uma VPC. Para obter mais informações, consulte Atribuir um endereço IPv4 público na inicialização.	20 de agosto de 2013
Concessão de permissões em nível de recurso	15/06/2013	O Amazon EC2 oferece suporte aos novos Nomes de recurso da Amazon (ARNs) e a chaves de condição. Para obter mais informações, consulte Políticas baseadas em identidade do Amazon EC2.	8 de julho de 2013
Cópias incrementais de snapshot	01/02/2013	Agora é possível executar cópias incrementais de snapshot.	11 de junho de 2013
AWS Management Pack		O AWS Management Pack vincula as instâncias do Amazon EC2 e os sistemas operacionais Windows ou Linux que são executados nelas. O AWS Management Pack é uma extensão do Microsoft System Center Operations Manager.	8 de maio de 2013
Nova página Tags		Há uma nova página Tags no console do Amazon EC2. Para obter mais informações, consulte Marcar com tag os recursos do Amazon EC2.	04 de abril de 2013

Recurso	Versão da API	Descrição	Data de lançamento
Cópia de uma AMI de uma região para outra	01/02/2013	É possível copiar uma AMI de uma região para outra, o que permite executar instâncias consistentes em mais de uma região da AWS de maneira rápida e fácil. Para obter mais informações, consulte Copiar uma AMI do Amazon EC2.	11 de março de 2013
Execução de instâncias em uma VPC padrão	01/02/2013	Sua conta da AWS é capaz de iniciar instâncias no EC2-Classic ou uma VPC ou somente em uma VPC, dependendo da região. Se você puder executar instâncias somente em uma VPC, criamos uma VPC padrão para você. Quando você executa uma instância, nós a executamos em sua VPC padrão, a menos que você crie uma VPC não padrão e a especifique ao executar a instância.	11 de março de 2013
Cópia de snapshot do EBS	01/12/2012	É possível 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).	17 de dezembro de 2012
Verificações de métricas e status do EBS atualizadas para volumes do Provisioned IOPS SSD	01/10/2012	Atualizadas as métricas do EBS para incluir duas novas métricas para volumes do Provisioned IOPS SSD. Novas verificações de status também adicionadas para volumes do Provisioned IOPS SSD.	20 de novembro de 2012
Status da solicitação de instância spot	01/10/2012	O status da solicitação da instância spot facilita a determinação do estado de suas solicitações spot.	14 de outubro de 2012

Recurso	Versão da API	Descrição	Data de lançamento
Marketplace de instâncias reservadas do Amazon EC2	15/08/2012	O Marketplace de instâncias reservadas correlaciona vendedores que têm instâncias reservadas do Amazon EC2 que não são mais necessárias a compradores que desejam adquirir capacidade adicional. As instâncias reservadas adquiridas e vendidas por meio do Marketplace de instâncias reservadas funcionam como qualquer outra instância reservada, com a exceção de que têm um período de vigência padrão menor que o período de vigência padrão total e podem ser vendidas a preços diferentes.	11 de setembro de 2012
Provisioned IOPS SSD para Amazon EBS	20/07/2012	Os volumes do Provisioned IOPS SSD fornecem alta performance previsível para workloads com uso intensivo de E/S, como aplicações de banco de dados que dependem de tempos de resposta consistentes e rápidos.	31 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: • AWSChaves de acesso da para aplicações que executam em instâncias do Amazon EC2. • Rotação automática das chaves de acesso da AWS na instância do Amazon EC2. • Permissões granulares para aplicações que executam em instâncias do Amazon EC2 que fazem solicitações para seus serviços da AWS.	11 de junho de 2012

Recurso	Versão da API	Descrição	Data de lançamento
Os recursos de instâncias spot que facilitam a familiarização e o manuseio de possíveis interrupções.		Agora é possível gerenciar suas Instâncias spot da seguinte forma: • Especifique o valor que você está disposto a pagar por Instâncias spot usando as configurações de execução de Auto Scaling e configure um cronograma para especificar o valor que você está disposto a pagar por Instâncias spot. Para obter mais informações, consulte Solicitar instâncias spot no Guia do usuário do Amazon EC2 Auto Scaling. • Obter notificações quando as instâncias forem executadas ou encerradas. • Use modelos do CloudFormation para iniciar instâncias spot em uma pilha com recursos da AWS.	7 de junho de 2012
Exportação de instâncias do EC2 e time stamps para verificações de status para o Amazon EC2	01/05/2012	Suporte adicionado para exportar instâncias do Windows Server que você importou originalmente para o EC2. Suporte adicionado para time stamps no status da instância e no status do sistema para indicar a data e a hora em que uma verificação de status falhou.	25 de maio de 2012

Recurso	Versão da API	Descrição	Data de lançamento
Exportação de instâncias do EC2 e time stamps em verificações do status de instâncias e do sistema para a Amazon VPC	01/05/2012	Suporte adicionado para a exportação de instâncias do EC2 ao Citrix Xen, ao Microsoft Hyper-V e ao VMware vSphere. Suporte adicionado para time stamps em verificações de status de instâncias e do sistema.	25 de maio de 2012
AWS Marketplace AMIs	01/04/2012	Suporte adicionado para AMIs do AWS Marketplace.	19 de abril de 2012
Níveis de definição de preço de instâncias reservadas	15/12/2011	Adicionada uma nova seção que discute como beneficiar-se da definição de preço com desconto que está embutido nos níveis de definição de preço de instâncias reservadas.	5 de março de 2012
Interfaces de rede elástica (ENIs) para instâncias do EC2 na Amazon Virtual Private Cloud	01/12/2011	Adicionada nova seção sobre interfaces de rede elástica (ENIs) para instâncias do EC2 em uma VPC. Para obter mais informações, consulte Interfaces de rede elástica.	21 de dezembro de 2011
Novos tipos de ofertas para instâncias reservadas do Amazon EC2	01/11/2011	É possível escolher entre várias ofertas de instâncias reservadas que atendem a seu uso projetado da instância.	01 de dezembro de 2011

Recurso	Versão da API	Descrição	Data de lançamento
Status das instâncias do Amazon EC2	01/11/2011	É possível visualizar detalhes adicionais sobre o status de suas instâncias, incluindo eventos programados planejados pela AWS que podem ter um impacto em suas instâncias. Essas atividades operacionais incluem reinicializações de instâncias necessárias para aplicar atualizações de software ou patches de segurança, ou a baixa de instâncias necessária quando há um problema de hardware. Para obter mais informações, consulte Monitorar o status das instâncias do Amazon EC2.	16 de novembro de 2011
Instâncias spot na Amazon VPC	15/07/2011	Adição de informações sobre o suporte para Instâncias spot na Amazon VPC. Com essa atualização, os usuários podem executar Instâncias spot em uma nuvem privada virtual (VPC). Ao executar Instâncias spot em uma VPC, os usuários de Instâncias spot podem aproveitar os benefícios da Amazon VPC.	11 de outubro de 2011
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 `ImportInstance` e do `ImportVolume`, que agora executarão o upload das imagens no Amazon EC2 depois de criar a tarefa de importação. Além disso, com a introdução do `ResumeImport`, os usuários poderão reiniciar um upload incompleto no ponto em que a tarefa parou.	15 de setembro de 2011

Recurso	Versão da API	Descrição	Data de lançamento
Suporte para importação do formato de arquivo VHD		O VM Import agora pode importar arquivos de imagem de máquina virtual em formato VHD. O formato de arquivo VHD é compatível com as plataformas de virtualização Citrix Xen e Microsoft Hyper-V. Com essa versão, o VM Import agora oferece suporte aos formatos de imagem RAW, VHD e VMDK (compatível com o VMware ESX). Para obter mais informações, consulte o VM Import/Export User Guide (Manual do usuário para importação/exportação de VMs).	24 de agosto de 2011
Atualização do Amazon EC2 VM Import Connector para VMware vCenter		Adicionadas informações sobre a versão 1.1 do Amazon EC2 VM Import Connector para o dispositivo virtual VMware vCenter (conector). Essa atualização inclui suporte de proxy para acesso à Internet, melhor manipulação de erros, barra de progresso de tarefas aprimorada e várias correções de erros.	27 de junho de 2011
Alterações na definição de preço de zonas de disponibilidade de Instâncias spot	15/05/2011	Adição de informações sobre o recurso de definição de preço de zonas de disponibilidade de Instâncias spot. Nessa versão, adicionamos novas opções de definição de preço de zonas de disponibilidade como parte das informações retornadas ao consultar as solicitações de instância spot e o histórico de preços spot. Essas adições facilitam a determinação do preço requerido para executar uma instância spot em uma zona de disponibilidade específica.	26 de maio de 2011

Recurso	Versão da API	Descrição	Data de lançamento
AWS Identity and Access Management		Adicionadas informações sobre o AWS Identity and Access Management (IAM), que permite que os usuários especifiquem quais ações do Amazon EC2 um usuário pode usar com recursos do Amazon EC2 em geral. Para obter mais informações, consulte Identity and Access Management para o Amazon EC2.	26 de abril de 2011
Instâncias dedicadas		Executadas em sua Amazon Virtual Private Cloud (Amazon VPC), as instâncias dedicadas são instâncias isoladas fisicamente no nível do hardware de host. As instâncias dedicadas permitem tirar proveito da Amazon VPC e da Nuvem AWS, com benefícios que incluem provisionamento elástico sob demanda e pagamento apenas pelo que você usa e, ao mesmo tempo, isolando suas instâncias de computação do Amazon EC2 no nível do hardware. Para obter mais informações, consulte Instâncias dedicadas do Amazon EC2.	27 de março de 2011
Atualizações nas instâncias reservadas para o Console de Gerenciamento da AWS		As atualizações no Console de Gerenciamento da AWS facilitam que os usuários visualizem suas instâncias reservadas e comprem instâncias reservadas adicionais, incluindo instâncias reservadas dedicadas.	27 de março de 2011
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 Usar metadados da instância para gerenciar a instância do EC2 e Categorias de metadados da instância.	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 é possível usar o Console de gerenciamento da AWS para forçar o desapego de um volume do Amazon EBS de uma instância.	23 de fevereiro de 2011
Proteção contra encerramento de instância		Agora é possível usar o Console de Gerenciamento da AWS para impedir que uma instância seja encerrada. Para obter mais informações, consulte Alterar proteção contra encerramento de instância.	23 de fevereiro de 2011
VM Import	15/11/2010	Adicionadas informações sobre o VM Import que permite importar uma máquina virtual ou um volume no Amazon EC2. Para obter mais informações, consulte o VM Import/Export User Guide (Manual do usuário para importação/exportação de VMs).	15 de dezembro de 2010
Monitoramento básico para instâncias	31/08/2010	Adicionadas informações sobre o monitoramento básico de instâncias do EC2.	12 de dezembro de 2010

Recurso	Versão da API	Descrição	Data de lançamento
Filtros e tags	31/08/2010	Adicionadas informações sobre recursos de listagem, filtragem e marcação. Para obter mais informações, consulte Encontrar seus recursos do Amazon EC2 e Marcar com tag os recursos do Amazon EC2.	19 de setembro de 2010
Execução de instância idempotente	31/08/2010	Adicionadas informações sobre garantia de idempotência ao executar instâncias.	19 de setembro de 2010
AWS Identity and Access Management para o Amazon EC2		O Amazon EC2 agora se integra ao AWS Identity and Access Management (IAM). Para obter mais informações, consulte Identity and Access Management para o Amazon EC2.	2 de setembro de 2010
Designação de endereço IP da Amazon VPC	15/06/2010	Os usuários do Amazon VPC agora podem especificar o endereço IP para atribuir uma instância executada em uma VPC.	12 de julho de 2010
Monitoramento de Amazon CloudWatch para volumes de Amazon EBS		Monitoramento de Amazon CloudWatch agora está disponível automaticamente para volumes de Amazon EBS.	14 de junho de 2010
Instâncias reservadas com Windows		O Amazon EC2 agora oferece suporte a instâncias reservadas com o Windows.	22 de fevereiro de 2010