



Manual do usuário do gateway de volumes

AWS Storage Gateway



Versão da API 2013-06-30

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Storage Gateway: Manual do usuário do gateway de volumes

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

As marcas comerciais e imagens comerciais 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 desprestígie a Amazon. Todas as outras marcas comerciais que não pertencem à Amazon pertencem a seus respectivos proprietários, que podem ou não ser afiliados, patrocinados pela Amazon ou ter conexão com ela.

Table of Contents

.....	x
O que é o gateway de volumes?	1
Gateway de volumes	1
Você é um usuário iniciante do Storage Gateway?	2
Como funciona o gateway de volumes	2
Gateways de volume	2
Definição de preço	7
Planejar a implantação do gateway	8
Conceitos básicos	10
Inscreva-se para AWS Storage Gateway	10
AWS Regiões	11
Requisitos	11
Requisitos de hardware e armazenamento	11
Requisitos de rede e firewall	14
Hipervisores compatíveis e requisitos de host	24
Iniciadores iSCSI compatíveis	26
Acessando AWS Storage Gateway	27
Como usar o dispositivo de hardware	28
AWS Regiões suportadas	29
Configuração do dispositivo de hardware	29
Como montar em rack e conectar o seu equipamento de hardware à alimentação	30
Dimensões do dispositivo de hardware	31
Como configurar parâmetros de rede	36
Como ativar o dispositivo de hardware	39
Criar um gateway	40
Como configurar um endereço IP para o gateway	41
Como configurar o gateway	43
Como remover um gateway	43
Como excluir o dispositivo de hardware	44
Como criar um gateway	45
Visão geral: ativação do gateway	45
Configurar um gateway	45
Conecte-se a AWS	45
Analisar e ativar	45

Visão geral: configuração do gateway	46
Visão geral: recursos de armazenamento	46
Como criar um gateway de volume	46
Como criar um gateway	46
Como criar um volume	52
Como usar seu volume	56
Fazer backup de seus volumes	66
Como ativar o gateway em uma nuvem privada virtual	71
Como criar um endpoint da VPC para o Storage Gateway	72
Como gerenciar seu gateway	74
Como gerenciar seu gateway de volume	74
Como editar as informações do gateway	76
Como adicionar um volume	76
Como ampliar o tamanho de um volume	76
Como clonar um volume	77
Visualização de uso do volume	81
Redução da quantidade de armazenamento faturado em um volume	81
Exclusão de um volume	82
Mover seus volumes para um gateway diferente	82
Como criar um único snapshot	85
Como editar uma programação de snapshots	85
Como excluir snapshots	86
Noções básicas sobre transições e status de volumes	99
Como mover seus dados para um novo gateway	112
Como mover os volumes armazenados para um novo gateway de volumes armazenado	112
Como mover os volumes em cache para uma nova máquina virtual do gateway de volumes em cache	115
Como monitorar o Storage Gateway	119
Noções básicas de métricas de gateway	119
Dimensões das métricas do Storage Gateway	125
Monitorar o buffer de upload	126
Monitorar um armazenamento em cache	129
Entendendo os CloudWatch alarmes	131
Criação de CloudWatch alarmes recomendados	133
Criando um CloudWatch alarme personalizado	134
Como monitorar um gateway de volume	136

Obter os logs de integridade do gateway de volume	136
Usando o Amazon CloudWatch Metrics	138
Como medir o desempenho entre seu aplicativo e o gateway	139
Como medir o desempenho entre o gateway e a AWS	142
Noções básicas de métricas de volume	146
Como manter seu gateway	153
Encerramento da VM do gateway	153
Como iniciar e interromper um gateway de volumes	154
Como gerenciar discos locais	155
Como determinar o volume de armazenamento do disco local	155
Dimensionamento do buffer de upload	157
Dimensionamento do armazenamento em cache	159
Adicionar um buffer de upload ou armazenamento em cache	159
Como gerenciar largura de banda	160
Como alterar o controle de utilização da largura de banda por meio do console do Storage Gateway	161
Programando o controle de utilização da largura de banda	162
Usando o AWS SDK for Java	164
Usando o AWS SDK for .NET	166
Usando o AWS Tools for Windows PowerShell	168
Como gerenciar atualizações de gateway	169
Ativar ou desativar as atualizações de manutenção	170
Modificar o cronograma da janela de manutenção do gateway	171
Como executar tarefas de manutenção no console local	172
Realizar tarefas no console local da VM do	172
Como realizar tarefas no console local do EC2	191
Acessar o console local do gateway	197
Como configurar adaptadores de rede para seu gateway	202
Como excluir seu gateway e remover recursos	207
Como excluir um gateway usando o console do Storage Gateway	207
Como remover recursos de um gateway implantado no local	208
Como remover recursos de um gateway implantado em uma instância do Amazon EC2	209
Performance	210
Como otimizar o desempenho de um gateway	210
Configuração recomendada	210
Como adicionar recursos ao seu gateway	211

Otimizar as configurações iSCSI	214
Como adicionar recursos ao seu ambiente de aplicativos	214
Como usar o VMware High Availability com o Storage Gateway	215
Configurar o cluster do vSphere VMware HA	216
Baixe a imagem .ova do console do Storage Gateway	218
Implantar o gateway	218
(Opcional) Adicionar opções de substituição para outras VMs no cluster	218
Ativar o gateway.	219
Teste a configuração do VMware High Availability	220
Segurança	221
Proteção de dados	222
Criptografia de dados	223
Como configurar a autenticação CHAP	224
Identity and Access Management	227
Público	227
Autenticando com identidades	228
Gerenciando acesso usando políticas	232
Como o AWS Storage Gateway funciona com o IAM	234
Exemplos de políticas baseadas em identidade	242
Solução de problemas	245
Registro e Monitoramento	247
Informações do Storage Gateway em CloudTrail	247
Como entender as entradas dos arquivos de log do Storage Gateway	248
Validação de conformidade	250
Resiliência	251
Infrastructure Security	252
AWS Melhores práticas de segurança	252
Como solucionar problemas do gateway	253
Solução de problemas: problemas off-line no gateway	253
Verifique o firewall ou proxy associado	254
Verifique se há uma inspeção contínua de SSL ou pacotes profundos do tráfego do seu gateway	254
Verifique se há uma queda de energia ou falha de hardware no host do hipervisor	254
Verifique se há problemas com um disco de cache associado	254
Solução de problemas: problemas de ativação do gateway	255
Resolva erros ao ativar seu gateway usando um endpoint público	256

Resolva erros ao ativar seu gateway usando um endpoint Amazon VPC	259
Resolva erros ao ativar seu gateway usando um endpoint público, e há um endpoint VPC do Storage Gateway na mesma VPC	263
Como solucionar questões on-premises de solução de problemas no gateway	264
Ativando AWS Support para ajudar a solucionar problemas em seu gateway	268
Como solucionar problemas de configuração no Microsoft Hyper-V	269
Como solucionar problemas de gateway do Amazon EC2	274
A ativação do gateway não ocorreu após alguns minutos	275
Não é possível encontrar a instância do gateway do EC2 na lista de instâncias	275
Não é possível conectar um volume do Amazon EBS à instância do gateway EC2	276
Não é possível anexar um iniciador a um destino de volume do gateway do EC2	276
Mensagem de nenhum disco disponível quando você tenta adicionar volumes de armazenamento	276
Você precisa remover um disco alocado como espaço de buffer de upload para reduzir o espaço do buffer de upload	276
O throughput de ou para o gateway do EC2 cai para zero	277
Ativando AWS Support para ajudar a solucionar problemas do gateway	277
Conectar-se ao gateway do Amazon EC2 usando o console de série	279
Como solucionar problemas do dispositivo de hardware	279
Como determinar o endereço IP do serviço	279
Como executar uma redefinição de fábrica	279
Como executar uma reinicialização remota	280
Como obter suporte para o Dell iDRAC	280
Como encontrar o número de série do dispositivo de hardware	280
Como obter suporte para dispositivos de hardware	281
Como solucionar problemas em volumes	282
O console informa que seu volume não está configurado	282
O console informa que seu volume é irrecoverável	283
O gateway armazenado em cache é inacessível e você deseja recuperar seus dados	283
O console informa que o status de seu volume é PASS THROUGH	284
Você deseja verificar a integridade do volume e corrigir possíveis erros	284
Seu volume de destino iSCSI não aparece no Console de Gerenciamento de Disco do Windows	285
Você deseja alterar o nome do destino iSCSI do volume	285
O snapshot de volume programado não ocorreu	285
Você precisa remover ou substituir um disco que apresentou falha	285

A taxa de transferência de seu aplicativo para um volume caiu para zero	286
Um disco de cache no gateway depara-se com uma falha	286
O snapshot de um volume mantém-se no status PENDING por mais tempo que o esperado	287
Notificações de integridade de alta disponibilidade	287
Como solucionar problemas de alta disponibilidade	287
Notificações de integridade	288
Indicadores	289
Como recuperar seus dados: práticas recomendadas	289
Como se recuperar de um caso de encerramento inesperado da VM	290
Como recuperar dados de um gateway ou uma VM com falha	291
Como recuperar dados de um volume irrecuperável	291
Como recuperar dados de um disco de cache com falha	292
Como recuperar dados de um sistema de arquivos corrompido	292
Como recuperar dados de um datacenter inacessível	293
Recursos adicionais	295
Configuração do host	295
Configurando o VMware para o Storage Gateway	295
Como sincronizar o horário da VM do gateway	302
Implante um host do Amazon EC2 para o gateway de volumes	304
Implantar um Amazon EC2 com configurações padrão	308
Modifique as opções de metadados da instância do Amazon EC2	311
Gateway de volumes	312
Como remover discos de seu gateway	312
Volumes do EBS para gateways EC2	316
Obter a chave de ativação	317
Linux (curl)	318
Linux (bash/zsh)	319
Microsoft Windows PowerShell	320
Como usar seu console local	320
Como conectar iniciadores iSCSI	321
Como conectar volumes a um cliente Windows	322
Como conectar volumes ou dispositivos de VTL a um cliente Linux	327
Como personalizar as configurações iSCSI	329
Como configurar a autenticação CHAP	337
Usando AWS Direct Connect com o Storage Gateway	347

Requisitos de porta	347
Como conectar seu gateway	354
Como obter um endereço IP em um host do Amazon EC2	355
Noções básicas sobre recursos e IDs de recurso	356
Como trabalhar com IDs de recurso	356
Marcação de atributos	357
Como trabalhar com tags	358
Componentes de código aberto	359
Cotas do Storage Gateway	359
Cotas para volumes	360
Tamanhos de disco local recomendados para seu gateway	360
Referência da API	362
Cabeçalhos de solicitação requeridos	362
Solicitações de assinatura	365
Cálculo de assinatura de exemplo	366
Respostas de erro	367
Exceções	368
Códigos de erro de operação	370
Respostas de erro	390
Operações	392
Histórico do documento	393
Atualizações anteriores	412
Notas da versão	433

A documentação do gateway de arquivos do Amazon S3 foi movida para [O que é o Amazon S3 File Gateway?](#)

A documentação do gateway de arquivos do Amazon FSx foi movida para [O que é o Amazon FSx File Gateway?](#)

A documentação do gateway de fitas foi movida para [O que é o gateway de fitas?](#)

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.

O que é o gateway de volumes?

AWS Storage Gateway conecta um dispositivo de software local ao armazenamento baseado em nuvem para fornecer integração perfeita com os recursos de segurança de dados entre seu ambiente de TI local e a infraestrutura de armazenamento. É possível usar esse serviço para armazenar dados na nuvem da Amazon Web Services e obter um armazenamento escalável e econômico que ajuda a manter a segurança dos dados.

AWS Storage Gateway oferece soluções de armazenamento baseadas em arquivos (Amazon S3 File e Amazon FSx File), baseadas em volume (em cache e armazenadas) e baseadas em fita.

Tópicos

- [Gateway de volumes](#)
- [Você é um usuário iniciante do Storage Gateway?](#)
- [Como funciona o gateway de volumes \(arquitetura\)](#)
- [Precificação do Storage Gateway](#)
- [Planeje sua implantação do Storage Gateway](#)

Gateway de volumes

Gateway de volumes: o gateway de volumes fornece volumes de armazenamento de backup em nuvem que é possível montar como dispositivos Internet Small Computer System Interface (iSCSI) em servidores de aplicações on-premises.

É possível implantar um gateway de volumes on-premises como um dispositivo de VM executado no hipervisor VMware ESXi, KVM ou Microsoft Hyper-V, como um dispositivo de hardware ou na AWS como uma instância do Amazon EC2.

O gateway oferece suporte às seguintes configurações de volume:

- Volumes armazenados em cache: você armazena seus dados no Amazon Simple Storage Service (Amazon S3) e retém no local uma cópia dos subconjuntos de dados acessados com frequência. Os volumes armazenados em cache oferecem uma economia considerável em armazenamento principal e minimizam a necessidade de dimensionar seu armazenamento local. Além disso, você pode manter o acesso de baixa latência aos dados acessados com frequência.

- **Volumes armazenados:** se você precisa acessar todo o seu conjunto de dados com baixa latência, primeiro configure seu gateway on-premises para armazenar todos os seus dados localmente. Em seguida, faça backup assíncrono dos point-in-time snapshots desses dados no Amazon S3. Essa configuração oferece backups externos duradouros e de baixo custo que podem ser recuperados em seu datacenter local ou no Amazon Elastic Compute Cloud (Amazon EC2). Por exemplo, se você precisar de capacidade de substituição para finalidades de recuperação de desastres, poderá recuperar os backups no Amazon EC2.

Documentação: para obter a documentação do gateway de volumes, consulte [Como criar um gateway de volume](#).

Você é um usuário iniciante do Storage Gateway?

Na documentação a seguir, há uma seção de conceitos básicos que abrange informações de configuração comuns a todos os gateways e também seções de configuração específicas ao gateway. A seção de conceitos básicos mostra como implantar, ativar e configurar um gateway de armazenamento. A seção de gerenciamento mostra como gerenciar seu gateway e recursos:

- [Como criar um gateway de volume](#) descreve como criar e usar um gateway de volumes. Mostra como criar volumes de armazenamento e backup de dados nos volumes.
- [Como gerenciar seu gateway](#) descreve como executar tarefas de gerenciamento para seus tipos de gateway e os recursos.

Neste guia, você encontra principalmente instruções sobre como trabalhar com operações de gateway usando o AWS Management Console. Se você quiser executar estas operações de forma programática, consulte [Referência de API do AWS Storage Gateway](#).

Como funciona o gateway de volumes (arquitetura)

A seguir, é possível encontrar uma visão geral sobre a arquitetura da solução do gateway de volumes.

Gateways de volume

Em gateways de volumes, é possível usar volumes em cache ou volumes armazenados.

Tópicos

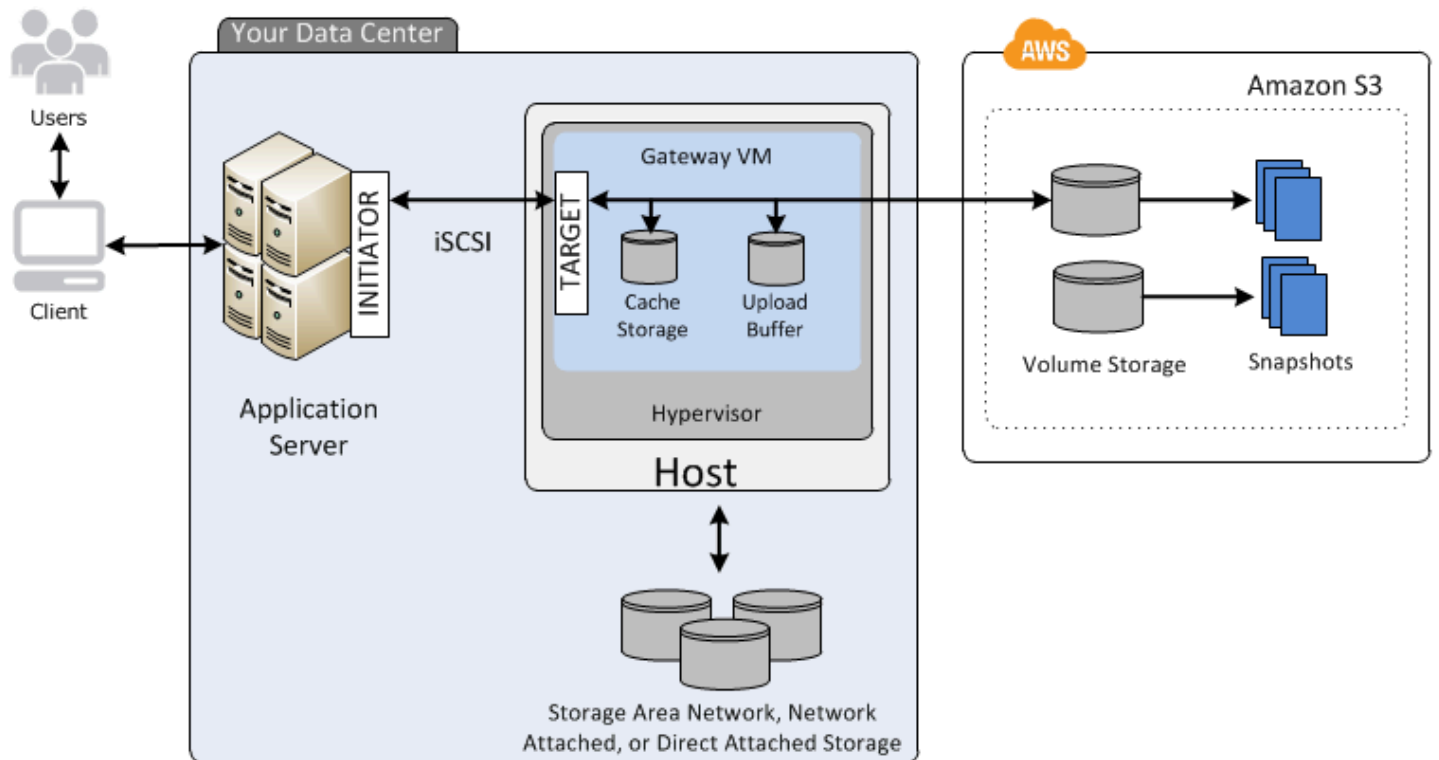
- [Arquitetura de volumes armazenados em cache](#)
- [Arquitetura de volumes armazenados](#)

Arquitetura de volumes armazenados em cache

Ao usar os volumes armazenados em cache, é possível definir o Amazon S3 como armazenamento de dados principal e ao mesmo tempo reter localmente os dados acessados com frequência no Storage Gateway. Os volumes armazenados em cache minimizam a necessidade de redimensionar a infraestrutura de armazenamento local, sem deixar de fornecer aos aplicativos acesso de baixa latência aos dados acessados com frequência. Você pode criar volumes de armazenamento de até 32 TiB e anexá-los como dispositivos iSCSI em seus servidores de aplicativos locais. Seu gateway armazena os dados que você grava nesses volumes no Amazon S3 e retém os dados lidos recentemente no cache de armazenamento e no armazenamento buffer de upload do Storage Gateway on-premises.

Quanto ao tamanho dos volumes armazenados em cache, eles podem variar de 1 GiB a 32 TiB e devem ser arredondados para o GiB mais próximo. Cada gateway configurado para volumes armazenados em cache pode comportar até 32 volumes, o que equivale a um volume total de armazenamento de 1.024 TiB (1 PiB).

Na solução de volumes armazenados em cache, o Storage Gateway armazena todos os dados de aplicações on-premises em um volume de armazenamento no Amazon S3. O diagrama a seguir oferece uma visão geral da implantação de volumes armazenados em cache.



Depois de instalar o dispositivo de software Storage Gateway — a VM — em um host em seu datacenter e ativá-lo, você o usa AWS Management Console para provisionar volumes de armazenamento apoiados pelo Amazon S3. Você também pode provisionar volumes de armazenamento programaticamente usando a API Storage Gateway ou as bibliotecas do AWS SDK. Em seguida, você pode montar esses volumes de armazenamento nos servidores de aplicativos locais como dispositivos iSCSI.

Você pode ainda alocar discos locais à VM. Esses discos locais servem às seguintes finalidades:

- Discos para uso pelo gateway como armazenamento em cache — à medida que seus aplicativos gravam dados nos volumes de armazenamento AWS, o gateway primeiro armazena os dados nos discos locais usados para armazenamento em cache. Em seguida, o gateway faz upload dos dados no Amazon S3. O armazenamento em cache funciona como um armazenamento on-premises duradouro que aguarda para fazer upload de dados do buffer para o Amazon S3.

O armazenamento em cache também permite que o gateway armazene localmente os dados de aplicativo acessados recentemente para oferecer acesso de baixa latência. Quando a sua aplicação solicita dados, o gateway verifica os dados no armazenamento em cache antes de verificar no Amazon S3.

Você pode usar as orientações a seguir para determinar o espaço em disco a ser alocado para o armazenamento em cache. Em geral, você deve alocar pelo menos 20% do tamanho de armazenamento de arquivos existente ao armazenamento em cache. O armazenamento em cache também deve ser maior do que o buffer de upload. Esta última orientação ajuda a garantir que o armazenamento em cache seja suficientemente grande para armazenar permanentemente no buffer de upload todos os dados dos quais ainda não foi feito upload para o Amazon S3.

- Discos usados pelo gateway como buffer de upload: para se preparar para fazer upload para o Amazon S3, o gateway também armazena dados de entrada em uma área de preparação, chamada de buffer de upload. Seu gateway carrega esses dados de buffer por meio de uma conexão criptografada Secure Sockets Layer (SSL) AWS, onde são armazenados criptografados no Amazon S3.

É possível realizar backups incrementais, chamados snapshots, de seus volumes de armazenamento no Amazon S3. Esses point-in-time snapshots também são armazenados no Amazon S3 como snapshots do Amazon EBS. Ao obter um novo snapshot, somente os dados alterados desde o último snapshot são armazenados. Quando o snapshot é feito, o gateway carrega as alterações até o ponto do snapshot e cria o novo snapshot usando o Amazon EBS. Você pode iniciar os snapshots de forma programada ou fazê-los uma única vez. Um único volume é compatível com o enfileiramento de vários snapshots em rápida sucessão, mas cada snapshot deve terminar de ser criado antes que o próximo possa ser obtido. Ao excluir um snapshot, são removidos somente os dados dos quais nenhum outro snapshot necessita. Para obter informações sobre snapshots do Amazon EBS, consulte [Snapshots do Amazon EBS](#).

É possível restaurar um snapshot do Amazon EBS em um volume de armazenamento do gateway se precisar recuperar um backup de seus dados. Alternativamente, para snapshots com tamanho máximo de 16 TiB, é possível usá-los como ponto de partida para um novo volume do Amazon EBS. Em seguida, é possível anexar esse novo volume do Amazon EBS a uma instância do Amazon EC2.

Todos os dados do gateway de volumes armazenados em cache e todos os dados de snapshot são mantidos no Amazon S3 e criptografados em repouso por meio da criptografia do lado do servidor (SSE). No entanto, não é possível acessar esses dados com a API do Amazon S3 ou outras ferramentas como o Amazon S3 Management Console.

Arquitetura de volumes armazenados

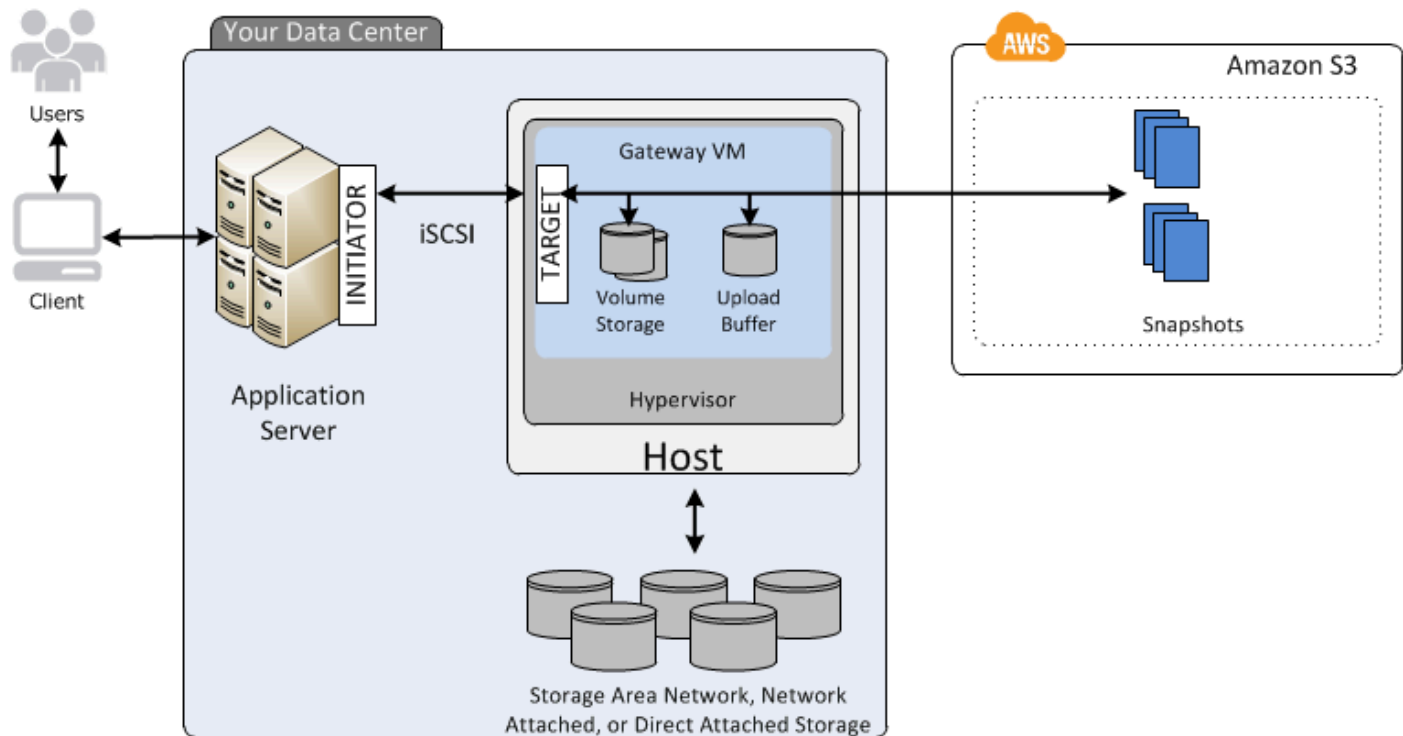
Ao usar volumes armazenados, você pode armazenar seus dados primários localmente e, ao mesmo tempo, fazer backup desses dados de forma assíncrona em. AWS Esses volumes armazenados

oferecem aos aplicativos locais acesso de baixa latência aos conjuntos de dados. Ao mesmo tempo, elas oferecem backups externos duráveis. Você pode criar volumes de armazenamento e montá-los como dispositivos iSCSI em seus servidores de aplicativos locais. Os dados gravados nos volumes armazenados são armazenados em seu hardware de armazenamento local. Esses dados são copiados de forma assíncrona para o Amazon S3 como snapshots do Amazon Elastic Block Store (Amazon EBS).

O tamanho dos volumes armazenados pode variar de 1 GiB a 16 TiB e deve ser arredondado para o GiB mais próximo. Cada gateway configurado para volumes armazenados pode comportar até 32 volumes e um volume total de armazenamento de 512 TiB (0,5 PiB).

No caso dos volumes armazenados, o armazenamento em volume é mantido localmente em seu datacenter. Ou seja, você pode armazenar todos os dados de aplicativo em seu hardware de armazenamento local. Depois, usando atributos que ajudam a manter a segurança dos dados, o gateway faz upload dos dados para a nuvem do Amazon Web Services para assim oferecer backups econômicos e agilidade na recuperação de desastres. Esta solução é ideal quando você deseja manter os dados on-premises porque precisa ter acesso de baixa latência a todos os dados e também quando deseja manter os backups na AWS.

O diagrama a seguir oferece uma visão geral da implantação de volumes armazenados.



Depois de instalar o dispositivo de software do Storage Gateway (a VM) em um host no datacenter e ativá-lo, será possível criar volumes de armazenamento do gateway. Em seguida, mapeie para discos de armazenamento direto (DAS) ou os discos de rede de armazenamento (SAN) no local. Você pode começar com discos novos ou discos que já contenham dados. Você pode então montar esses volumes em seus servidores de aplicativos locais como dispositivos iSCSI. Quando seus aplicativos locais gravam e leem dados do volume de armazenamento de um gateway, esses dados são armazenados e recuperados do disco atribuído ao volume.

Para preparar os dados para fazer upload para o Amazon S3, o gateway também armazena dados de entrada em uma área de preparação, chamada buffer de upload. Você pode usar discos locais DAS ou SAN para armazenamento funcional. O gateway faz upload desses dados do buffer por meio de uma conexão Secure Sockets Layer (SSL) criptografada para o serviço do Storage Gateway em execução na nuvem da Amazon Web Services Cloud. Em seguida, o serviço armazena os dados criptografados no Amazon S3.

Você pode realizar backups incrementais, chamados snapshots, de seus volumes de armazenamento. O gateway armazena esses snapshots no Amazon S3 como snapshots do Amazon EBS. Ao obter um novo snapshot, somente os dados alterados desde o último snapshot são armazenados. Quando o snapshot é feito, o gateway carrega as alterações até o ponto do snapshot e cria o novo snapshot usando o Amazon EBS. Você pode iniciar os snapshots de forma programada ou fazê-los uma única vez. Um único volume é compatível com o enfileiramento de vários snapshots em rápida sucessão, mas cada snapshot deve terminar de ser criado antes que o próximo possa ser obtido. Ao excluir um snapshot, somente os dados que não são necessários para qualquer outro snapshot são removidos.

É possível restaurar um snapshot do Amazon EBS em um volume de armazenamento do gateway on-premises se precisar recuperar um backup de seus dados. Também é possível usar um snapshot como ponto de partida para um novo volume do Amazon EBS, que então poderá se anexar a uma instância do Amazon EC2.

Precificação do Storage Gateway

Para obter informações atuais sobre preços, consulte [Preços](#) na página de AWS Storage Gateway detalhes.

Planeje sua implantação do Storage Gateway

Ao usar o dispositivo de software Storage Gateway, você pode conectar sua infraestrutura de aplicativos local existente a um armazenamento em AWS nuvem escalável e econômico que fornece recursos de segurança de dados.

Para implantar o Storage Gateway, primeiro você precisa resolver as duas seguintes questões:

1. Seu tipo de gateway: este guia aborda o tipo de gateway a seguir.

- **Gateway de volumes:** ao usar gateways de volumes, é possível criar volumes de armazenamento na nuvem da Amazon Web Services. Seus aplicativos locais podem acessá-los como destinos Internet Small Computer System Interface (iSCSI). Existem duas opções – volumes armazenados em cache e volumes armazenados.
 - Com volumes em cache, você armazena dados de volume AWS, com uma pequena parte dos dados acessados recentemente no cache local. Esta abordagem permite acesso de baixa latência ao seu conjunto de dados frequentemente acessado. Ele também fornece acesso contínuo a todo o conjunto de dados armazenado em AWS. Ao usar volumes em cache, você pode dimensionar seus recursos de armazenamento sem precisar provisionar hardware adicional.
 - Com volumes armazenados, você armazena todo o conjunto de dados de volume no local e armazena point-in-time backups periódicos (instantâneos) nele. Nesse modelo, seu armazenamento local é primário, oferecendo acesso de baixa latência a todo o seu conjunto de dados. O armazenamento em AWS é o backup que você pode restaurar no caso de um desastre em seu data center.

Tanto para volumes armazenados em cache quanto para volumes armazenados, você pode tirar point-in-time instantâneos de seus volumes do Volume Gateway na forma de snapshots do Amazon EBS. Também é possível usar um snapshot como o ponto de partida para um novo volume do Amazon EBS, que então poderá se anexar a uma instância do Amazon EC2. Usando esta abordagem, é possível fornecer dados de suas aplicações on-premises para suas aplicações executadas no Amazon EC2 se precisar de capacidade computacional adicional sob demanda para processamento de dados ou capacidade de substituição para fins de recuperação de desastres. Isto permite que você faça cópias de versionamento dos volumes com eficiência de espaço para proteção de dados, recuperação, migração e várias outras necessidades de transferência de dados.

Para obter informações sobre a criação de um volume com base em um snapshot do Amazon EBS, consulte [Como criar um volume](#).

Para uma visão geral da arquitetura dos gateways de volumes, consulte [Arquitetura de volumes em cache](#) e [Arquitetura de volumes armazenados](#).

2. Opção de hospedagem — Você pode executar o Storage Gateway localmente como um dispositivo de VM ou dispositivo de hardware, ou como uma instância do AWS Amazon EC2. Para ter mais informações, consulte [Requisitos](#). Se seu datacenter ficar off-line e você não tiver um host disponível, poderá implantar um gateway em uma instância do EC2. O Storage Gateway fornece uma imagem de máquina da Amazon (AMI) que contém a imagem da VM do gateway.

Além disso, quando você configurar um host para implantar um dispositivo de software de gateway, precisará reservar armazenamento suficiente para VM do gateway.

Antes de passar para a etapa seguinte, procure primeiro fazer o seguinte:

- Para um gateway implantado on-premises, escolha o tipo de host VM e configure-o. Suas opções são VMware ESXi Hypervisor, Microsoft Hyper-V e Linux Kernel-based Virtual Machine (KVM). Se você implantar o gateway com um firewall subjacente, precisará garantir que determinadas portas possam ser acessadas pela VM do gateway. Para ter mais informações, consulte [Requisitos](#).

Conceitos básicos

Nesta seção, é possível encontrar instruções para começar a usar o Storage Gateway. Para começar, primeiro você se inscreve no AWS. Se for um novo usuário, é recomendável ler a seção sobre regiões e requisitos.

Tópicos

- [Inscreva-se para AWS Storage Gateway](#)
- [AWS Regiões](#)
- [Requisitos](#)
- [Acessando AWS Storage Gateway](#)

Inscreva-se para AWS Storage Gateway

Para usar o Storage Gateway, você precisa de uma conta da Amazon Web Services que ofereça acesso a todos os recursos, fóruns, suporte e relatórios de uso da AWS. Você não será cobrado por nenhum desses serviços, a menos que usar algum deles. Se já tiver uma conta da Amazon Web Services, ignore esta etapa.

Para cadastrar uma conta da Amazon Web Services

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

Parte do procedimento de inscrição envolve receber uma chamada telefônica e digitar um código de verificação no teclado do telefone.

Quando você se inscreve em um Conta da AWS, um Usuário raiz da conta da AWS é criado. O usuário-raiz tem acesso a todos os Serviços da AWS e recursos na conta. Como prática recomendada de segurança, atribua o acesso administrativo a um usuário e use somente o usuário-raiz para executar [tarefas que exigem acesso de usuário-raiz](#).

Para obter informações sobre precificação, consulte [Precificação](#) na página de detalhes do Storage Gateway.

AWS Regiões

O Storage Gateway armazena dados de volume, instantâneo, fita e arquivo na AWS região em que seu gateway está ativado. Os dados do arquivo são armazenados na AWS região em que seu bucket do Amazon S3 está localizado. Você seleciona uma AWS região no canto superior direito do Storage Gateway Management Console antes de começar a implantar seu gateway.

- Storage Gateway — Para AWS regiões suportadas e uma lista de endpoints de AWS serviço que você pode usar com o Storage Gateway, consulte [AWS Storage Gateway Endpoints](#) and Quotas no. Referência geral da AWS
- Dispositivo de hardware Storage Gateway — Para AWS regiões suportadas que você pode usar com o dispositivo de hardware, consulte Regiões do dispositivo de [AWS Storage Gateway hardware](#) no. Referência geral da AWS

Requisitos

A menos que especificado de outra forma, os seguintes requisitos são comuns a todas as configurações de gateway.

Tópicos

- [Requisitos de hardware e armazenamento](#)
- [Requisitos de rede e firewall](#)
- [Hypervisores compatíveis e requisitos de host](#)
- [Iniciadores iSCSI compatíveis](#)

Requisitos de hardware e armazenamento

Esta seção descreve os requisitos mínimos de hardware e a configuração para o gateway e a quantidade mínima de espaço em disco para alocar ao armazenamento necessário.

Requisitos de hardware de VMs.

Ao implementar o gateway, você deve ter certeza de que o hardware subjacente no qual está implantando a VM do gateway é capaz de oferecer os seguintes recursos mínimos:

- Quatro processadores virtuais designados para a VM.

- Para o gateway de volumes , seu hardware deve dedicar as seguintes quantidades de RAM:
 - 16 GiB de RAM reservada para gateways com tamanho de cache de até 16 TiB
 - 32 GiB de RAM reservada para gateways com tamanho de cache de 16 TiB a 32 TiB
 - 32 GiB de RAM reservada para gateways com tamanho de cache de 16 TiB a 64 TiB
- 80 GB de espaço em disco para instalação da imagem da VM e dados do sistema.

Para ter mais informações, consulte [Como otimizar o desempenho de um gateway](#). Para obter informações sobre como o hardware afeta o desempenho da VM do gateway, consulte [AWS Storage Gateway cotas](#).

Requisitos para tipos de instância do Amazon EC2

Ao implantar seu gateway no Amazon Elastic Compute Cloud (Amazon EC2), o tamanho da instância deve ser pelo menos xlarge para que o gateway funcione. No entanto, para a família de instâncias otimizadas para computação, o tamanho deve ser pelo menos 2xlarge.

Para o Volume Gateway , sua instância do Amazon EC2 deve dedicar as seguintes quantidades de RAM, dependendo do tamanho do cache que você planeja usar para seu gateway:

- 16 GiB de RAM reservada para gateways com tamanho de cache de até 16 TiB
- 32 GiB de RAM reservada para gateways com tamanho de cache de 16 TiB a 32 TiB
- 32 GiB de RAM reservada para gateways com tamanho de cache de 16 TiB a 64 TiB

Use um dos seguintes tipos de instância recomendados para o seu tipo de gateway.

Recomendado para volumes armazenados em cache e tipos de gateway de fitas

- Família de instâncias de uso geral: tipos de instância m4, m5 ou m6.

Note

Não recomendamos o uso do tipo de instância m4.16xlarge.

- Família de instâncias otimizadas para computação: tipos de instância c4, c5 ou c6. Selecione o tamanho da instância 2xlarge ou superior para atender aos requisitos necessários de RAM.
- Família de instâncias otimizadas para memória: tipos de instância r3, r5 ou r6.

- Família de instâncias otimizadas para armazenamento: tipos de instância i3 ou i4.

Requisitos de armazenamento

Além de 80 GB de espaço em disco para a VM, você também precisará de outros discos para o gateway.

A tabela a seguir recomenda tamanhos para armazenamento em disco local para o gateway implantado.

Tipo de gateway	Cache (mínimo)	Cache (máximo)	Buffer de upload (mínimo)	Buffer de upload (máximo)	Outros discos locais necessários
Gateway de volumes em cache	150 GiB	64 TiB	150 GiB	2 TiB	—
Gateway de volumes armazenado	—	—	150 GiB	2 TiB	Um ou mais para volume ou volumes armazenados

Note

É possível configurar uma ou mais unidades locais para seu cache e buffer de upload, até a capacidade máxima.

Ao adicionar cache ou fazer upload de buffer para um gateway existente, é importante criar novos discos no host (instância do hipervisor ou do Amazon EC2). Não altere o tamanho de discos existentes caso os discos tenham sido alocados anteriormente como um cache ou um buffer de upload.

Para obter informações sobre cotas de gateway, consulte [AWS Storage Gateway cotas](#).

Requisitos de rede e firewall

Seu gateway requer acesso à Internet, redes locais, Domain Name Service (DNS), firewalls, roteadores, servidores etc. A seguir, você pode encontrar informações sobre as portas necessárias e sobre como permitir acesso por meio de firewalls e routers.

Note

Em alguns casos, você pode implantar o Storage Gateway no Amazon EC2 ou usar outros tipos de implantação (inclusive no local) com políticas de segurança de rede que restringem os intervalos de AWS endereços IP. Nesses casos, seu gateway pode ter problemas de conectividade do serviço quando os valores do intervalo de AWS IP são alterados. Os valores do intervalo de endereços AWS IP que você precisa usar estão no subconjunto de serviços da Amazon para a AWS região em que você ativa seu gateway. Para obter os valores atuais de intervalo de IPs, consulte [Intervalos de endereços IP da AWS](#) na Referência geral da AWS.

Note

Os requisitos de largura de banda da rede variam com base na quantidade de dados carregados e baixados pelo gateway. É necessário um mínimo de 100 Mbps para baixar, ativar e atualizar o gateway com êxito. Os padrões de transferência de dados determinarão a largura de banda necessária para suportar a workload. Em alguns casos, é possível implantar o Storage Gateway no Amazon EC2 ou usar outros tipos de implantação

Tópicos

- [Requisitos de porta](#)
- [Requisitos de rede e firewall para o Storage Gateway Hardware Appliance](#)
- [Permitindo AWS Storage Gateway acesso por meio de firewalls e roteadores](#)
- [Como configurar os grupos de segurança para a instância de gateway do Amazon EC2](#)

Requisitos de porta

O Storage Gateway exige que determinadas portas tenham permissão para sua operação. A ilustração a seguir mostra as portas que você precisa permitir para cada tipo de gateway. Algumas

portas são necessárias por todos os tipos de gateway e outras são exigidas por tipos de gateway específicos. Para obter mais informações sobre os requisitos de porta, consulte [Requisitos de porta](#).

Portas comuns para todos os tipos de gateway

As portas a seguir são comuns e necessárias a todos os tipos de gateway.

Protocolo	Port	Direction	Origem	Destino	Como usar
TCP	443 (HTTPS)	Saída	Storage Gateway	AWS	Para comunicação do Storage Gateway com o endpoint do AWS serviço. Para obter informações sobre endpoints de serviço, consulte Permitindo AWS Storage Gateway acesso por meio de firewalls e roteadores .
TCP	80 (HTTP)	Entrada	O host a partir do qual você se conecta ao AWS Management Console.	Storage Gateway	Por sistemas locais para obter a chave de ativação do Storage Gateway. A porta 80 só é usada

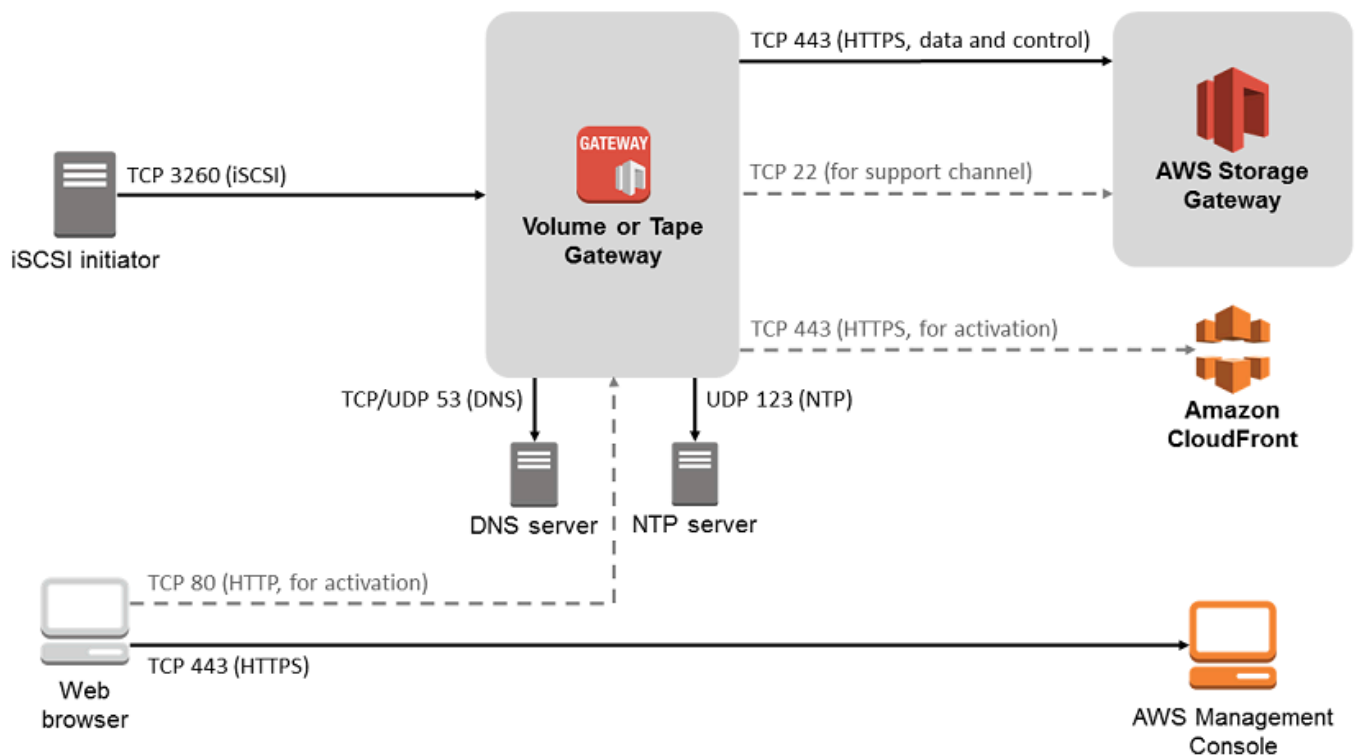
Protocolo	Port	Direction	Origem	Destino	Como usar
					<p>durante a ativação do dispositivo do Storage Gateway.</p> <p>O Storage Gateway não exige que a porta 80 seja acessível publicamente. O nível necessário de acesso à porta 80 depende da configuração da rede. Se você ativar o gateway pelo Storage Gateway Management Console, o host pelo qual se conecta ao console deverá ter acesso à porta 80 do gateway.</p>

Protocolo	Port	Direction	Origem	Destino	Como usar
TCP/UDP	53 (DNS)	Saída	Storage Gateway	Servidor Domain Name Service (DNS – Serviço do nome de domínio)	Para a comunicação entre o agente do Storage Gateway e o servidor DNS.
TCP	22 (Canal de suporte)	Saída	Storage Gateway	AWS Support	Permite AWS Support acessar seu gateway para ajudá-lo a solucionar problemas de gateway. Você não precisa dessa porta aberta para a operação normal do gateway, mas ela é necessária para a solução de problemas.

Protocolo	Port	Direction	Origem	Destino	Como usar
UDP	123 (NTP)	Saída	Cliente NTP	Servidor NTP	Usado por sistemas locais para sincronizar a hora da VM com a hora do host.

Portas para volume e gateways de fitas

A ilustração a seguir mostra as portas a serem abertas para o gateway de volumes.



Além das portas comuns, o gateway de fitas precisam da porta a seguir.

Protocolo	Port	Direction	Origem	Destino	Como usar
TCP	3260 (iSCSI)	Entrada	Iniciadores iSCSI	Storage Gateway	Por sistemas locais para se conectar a destinos iSCSI expostos pelo gateway.

Para obter informações detalhadas sobre os requisitos de porta, consulte [Requisitos de porta](#) na seção Recursos adicionais do Storage Gateway.

Requisitos de rede e firewall para o Storage Gateway Hardware Appliance

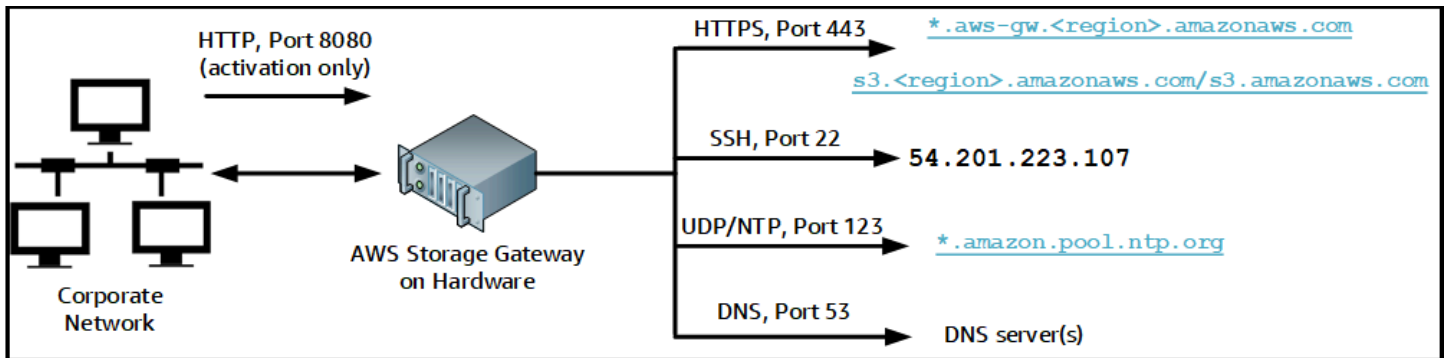
Cada Storage Gateway Hardware Appliance requer os seguintes serviços de rede:

- Acesso à internet: em uma rede sempre disponível de conexão com a Internet por meio de uma interface de rede no servidor.
- DNS services: serviços DNS para comunicação entre o dispositivo de hardware e o servidor DNS.
- Sincronização de horário: um serviço Amazon NTP de horário configurado automaticamente deve ser acessível.
- Endereço IP: um DHCP ou endereço IPv4 estático atribuído. Você não pode atribuir um endereço IPv6.

Há cinco portas de rede físicas na parte traseira do servidor Dell PowerEdge R640. Da esquerda para a direita (atrás do servidor), essas portas são as seguintes:

1. iDRAC
2. em1
3. em2
4. em3
5. em4

Você pode usar a porta iDRAC para gerenciamento de servidor remoto.



Um dispositivo de hardware requer as portas a seguir para operar.

Protocolo	Port	Direction	Origem	Destino	Como usar
SSH	22	Saída	Equipamento de hardware	54.201.223.107	Canal de suporte
DNS	53	Saída	Equipamento de hardware	Servidores DNS	Resolução de nome
UDP/NTP	123	Saída	Equipamento de hardware	*.amazon.pool.ntp.org	Sincronização de horário
HTTPS	443	Saída	Equipamento de hardware	*.amazonaws.com	Transferência de dados
HTTP	8080	Entrada	AWS	Equipamento de hardware	Ativação (apenas brevemente)

Para executar como projetado, um dispositivo de hardware requer configurações de rede e de firewall da seguinte forma:

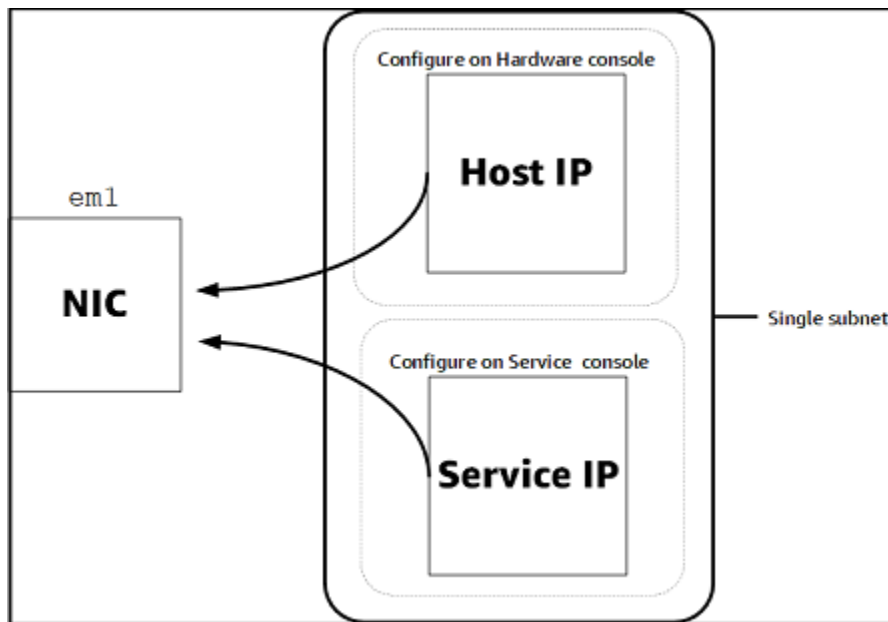
- Configure todas as interfaces de rede conectadas no console de hardware.
- Certifique-se de que cada interface de rede esteja em uma sub-rede exclusiva.

- Forneça a todas as interfaces de rede conectadas o acesso de saída aos endpoints listados no diagrama anterior.
- Configure pelo menos uma interface de rede para oferecer suporte ao dispositivo de hardware. Para ter mais informações, consulte [Como configurar parâmetros de rede](#).

Note

Para ver uma ilustração mostrando a parte posterior do servidor com suas portas, consulte [Como montar em rack o seu equipamento de hardware e conectá-lo à alimentação](#)

Todos os endereços IP na mesma interface de rede (NIC), seja para um gateway ou um host, devem estar na mesma sub-rede. A ilustração a seguir mostra o esquema de endereçamento.



Para obter mais informações sobre como ativar e configurar um dispositivo de hardware, consulte [Como usar o Storage Gateway Hardware Appliance](#)

Permitindo AWS Storage Gateway acesso por meio de firewalls e roteadores

Seu gateway requer acesso aos seguintes endpoints de serviço para se comunicar AWS. Se usar um firewall ou roteador para filtrar ou limitar o tráfego de rede, você deverá configurar o firewall e o roteador para permitir a comunicação externa com a AWS nesses endpoints de serviço.

Note

Se você configurar endpoints de VPC privados para seu Storage Gateway usar para conexão e transferência de dados de e para AWS, seu gateway não exigirá acesso à Internet pública. Para obter mais informações, consulte [Como ativar um gateway em uma nuvem privada virtual](#).

Important

Dependendo da AWS região do seu gateway, substitua a *região* no endpoint do serviço pela string de região correta.

O seguinte endpoint de serviço é exigido por todos os gateways para operações de head-bucket.

```
s3.amazonaws.com:443
```

Os endpoints de serviço a seguir são exigidos por todos os gateways para operações de caminho de controle (anon-cp, client-cp, proxy-app) e caminho de dados (dp-1).

```
anon-cp.storagegateway.região.amazonaws.com:443  
client-cp.storagegateway.região.amazonaws.com:443  
proxy-app.storagegateway.região.amazonaws.com:443  
dp-1.storagegateway.região.amazonaws.com:443
```

Veja a seguir o endpoint de serviço do gateway necessário para fazer chamadas de API.

```
storagegateway.região.amazonaws.com:443
```

O exemplo a seguir é um endpoint de serviço do gateway na região Oeste dos EUA (Oregon) (da us-west-2).

```
storagegateway.us-west-2.amazonaws.com:443
```

O endpoint de serviço do Amazon S3, mostrado a seguir, é usado somente pelos gateways de arquivos. O Gateway de Arquivos necessita deste endpoint para acessar o bucket do S3 para o qual o compartilhamento de arquivos está mapeado.

```
bucketname.s3.region.amazonaws.com
```

O exemplo a seguir é um endpoint de serviço do S3 na região Leste dos EUA (Ohio) (us-east-2).

```
s3.us-east-2.amazonaws.com
```

Note

Se seu gateway não conseguir determinar a AWS região em que seu bucket do S3 está localizado, esse endpoint de serviço assume como padrão. `s3.us-east-1.amazonaws.com` Recomendamos permitir acesso à região Leste dos EUA (Norte da Virgínia) (us-east-1), além das regiões da AWS em que o gateway esteja ativado e em que o bucket do S3 esteja localizado.

Veja a seguir os endpoints de serviço do S3 para as regiões AWS GovCloud (US).

```
s3-fips-us-gov-west-1.amazonaws.com (AWS GovCloud (US-West) Region (FIPS))  
s3-fips.us-gov-east-1.amazonaws.com (AWS GovCloud (US-East) Region (FIPS))  
s3.us-gov-west-1.amazonaws.com (AWS GovCloud (US-West) Region (Standard))  
s3.us-gov-east-1.amazonaws.com (AWS GovCloud (US-East) Region (Standard))
```

O exemplo a seguir é um endpoint de serviço FIPS para um bucket S3 na região AWS GovCloud (Oeste dos EUA).

```
bucket-name.s3-fips-us-gov-west-1.amazonaws.com
```

Uma VM do Storage Gateway está configurada para usar os servidores NTP a seguir.

```
0.amazon.pool.ntp.org  
1.amazon.pool.ntp.org  
2.amazon.pool.ntp.org  
3.amazon.pool.ntp.org
```

- Storage Gateway — Para AWS regiões suportadas e uma lista de endpoints de AWS serviço que você pode usar com o Storage Gateway, consulte [AWS Storage Gateway endpoints](#) e cotas no. Referência geral da AWS

- Dispositivo de hardware do Storage Gateway — Para AWS regiões suportadas que você pode usar com o dispositivo de hardware, consulte as regiões do dispositivo de [hardware do Storage Gateway](#) no. Referência geral da AWS

Como configurar os grupos de segurança para a instância de gateway do Amazon EC2

Um grupo de segurança controla o tráfego para sua instância de gateway do Amazon EC2. Ao configurar um grupo de segurança, recomendamos o seguinte:

- O security group não deve permitir conexões de entrada da Internet externa. Ele deve permitir que apenas instâncias dentro do security group do gateway comuniquem-se com o gateway. Se você precisar permitir que as instâncias conectem-se ao gateway de fora desse security group, é recomendável permitir conexões somente nas portas 3260 (para conexões iSCSI) e 80 (para ativação).
- Se você deseja ativar seu gateway em um host do EC2 fora do grupo de segurança do gateway, permita conexões de entrada na porta 80 do endereço IP desse host. Se não conseguir determinar a ativação de endereço IP do host, poderá abrir a porta 80, ativar seu gateway e fechar o acesso na porta 80 assim que a ativação for concluída.
- Permita o acesso à porta 22 somente se você estiver usando AWS Support para fins de solução de problemas. Para ter mais informações, consulte [Você quer ajudar AWS Support a solucionar problemas do seu gateway EC2](#).

Em alguns casos, é possível usar uma instância do Amazon EC2 como iniciador (isto é, para se conectar aos destinos de iSCSI no gateway implantado no Amazon EC2). Nesse caso, recomendamos uma abordagem de duas etapas:

1. Você deve executar a instância do iniciador no mesmo security group do seu gateway.
2. Você deve configurar o acesso para que o iniciador possa se comunicar com seu gateway.

Para obter informações sobre quais portas abrir para seu gateway, consulte [Requisitos de porta](#).

Hipervisores compatíveis e requisitos de host

Você pode executar o Storage Gateway no local como um dispositivo de máquina virtual (VM), um dispositivo de hardware físico ou como uma instância do AWS Amazon EC2.

Note

Quando um fabricante termina o suporte geral para uma versão do hipervisor, o Storage Gateway também termina o suporte para a versão desse hipervisor. Para obter informações detalhadas sobre o suporte para versões específicas de um hipervisor, consulte a documentação do fabricante.

O Storage Gateway é compatível com as seguintes versões de hipervisor e hosts:

- VMware ESXi Hypervisor (versões 7.0 ou 8.0): uma versão gratuita do VMware está disponível no [site da VMware](#). Para esta configuração, você precisa também de um cliente VMware vSphere para se conectar ao host.
- Microsoft Hyper-V Hypervisor (versões 2012 R2, 2016, 2019 ou 2022): uma versão gratuita e independente do Hyper-V está disponível no [Centro de Download da Microsoft](#). Para esta configuração, você precisará de um Microsoft Hyper-V Manager em um computador cliente Microsoft Windows para se conectar ao host.
- Máquina virtual baseada em kernel (KVM) do Linux: uma tecnologia de virtualização gratuita e de código aberto. O KVM está incluído em todas as versões do Linux versão 2.6.20 e mais recentes. O Storage Gateway é testado e compatível nas distribuições CentOS/RHEL 7.7, Ubuntu 16.04 LTS e Ubuntu 18.04 LTS. Qualquer outra distribuição do Linux moderna poderá funcionar, mas não garantimos o funcionamento nem o desempenho. Recomendamos esta opção se você já tiver um ambiente de KVM em funcionamento e já estiver familiarizado com o funcionamento da KVM.
- Instância do EC2: o Storage Gateway fornece uma imagem de máquina da Amazon (AMI) que contém a imagem da VM do gateway. Somente arquivos, volumes armazenados em cache e gateways de fitas podem ser implantados no Amazon EC2. Para obter informações sobre como implantar um gateway no Amazon EC2, consulte [Como implantar uma instância do Amazon EC2 para hospedar seu gateway de volumes](#).
- Storage Gateway Hardware Appliance: o Storage Gateway fornece um dispositivo de hardware físico como uma opção de implantação on-premises para locais com uma infraestrutura de máquina virtual limitada.

Note

O Storage Gateway não oferece suporte à recuperação de um gateway de uma VM criada por meio de um snapshot ou clonada de outra VM do gateway ou de uma AMI do Amazon

EC2. Se a sua VM de gateway não funciona corretamente, ative um novo gateway e recupere os seus dados de outro. Para ter mais informações, consulte [Como se recuperar de um caso de encerramento inesperado da máquina virtual](#).

O Storage Gateway não oferece suporte à memória dinâmica nem à expansão da memória virtual.

Iniciadores iSCSI compatíveis

Ao implantar um volume em cache ou um gateway de volumes armazenado, é possível criar volumes de armazenamento iSCSI no gateway.

Para estabelecer conexão com esses dispositivos iSCSI, o Storage Gateway oferece suporte para os seguintes iniciadores iSCSI:

- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows 10
- Windows 8.1
- Red Hat Enterprise Linux 5
- Red Hat Enterprise Linux 6
- Red Hat Enterprise Linux 7
- VMware ESX Initiator, que fornece uma alternativa ao uso de iniciadores nos sistemas operacionais convidados de suas VMs

Important

O Storage Gateway não é compatível com o Microsoft Multipath de E/S (MPIO) de clientes Windows.

O Storage Gateway permite a conexão de vários hosts com um mesmo volume quando os hosts coordenam o acesso por meio do Windows Server Failover Clustering (WSFC). No entanto, você não pode conectar vários hosts com o mesmo volume (por exemplo, compartilhando um sistema de arquivos sem cluster NTFS/ext4) se não usar o WSFC.

Acessando AWS Storage Gateway

É possível usar o [Storage Gateway Management Console](#) para executar várias tarefas de configuração e gerenciamento de gateway. A seção Conceitos básicos e várias outras seções deste guia usam o console para mostrar a funcionalidade de gateway.

Para permitir o acesso do navegador ao console do Storage Gateway, certifique-se de que seu navegador tenha acesso ao endpoint da API do Storage Gateway. Para obter mais informações, consulte [Endpoints e cotas do Storage Gateway](#), na Referência geral da AWS .

Além disso, você pode usar a AWS Storage Gateway API para configurar e gerenciar programaticamente seus gateways. Para obter mais informações sobre a API, consulte [Referência de API para o Storage Gateway](#).

Você também pode usar os AWS SDKs para desenvolver aplicativos que interajam com o Storage Gateway. Os AWS SDKs para Java, .NET e PHP encapsulam a API subjacente do Storage Gateway para simplificar as tarefas de programação. Para obter informações sobre como fazer download de bibliotecas de SDKs, consulte [Bibliotecas de códigos de exemplo](#).

Como usar o Storage Gateway Hardware Appliance

O Storage Gateway Hardware Appliance é um dispositivo de hardware físico com o software Storage Gateway pré-instalado em uma configuração de servidor validada. É possível gerenciar seu equipamento de hardware na página Visão geral do dispositivo de hardware no console do AWS Storage Gateway .

Cada dispositivo de hardware é um servidor 1U de alto desempenho que pode ser implantado em seu datacenter ou on-premises dentro do seu firewall corporativo. Ao comprar e ativar o dispositivo de hardware, o processo de ativação associa o dispositivo de hardware com sua conta da Amazon Web Services. Após a ativação, seu dispositivo de hardware será exibido no console como um gateway na página Visão geral do dispositivo de hardware. É possível configurar o dispositivo de hardware como um tipo de gateway de arquivos, gateway de fitas ou gateway de volumes. O procedimento usado para implantar e ativar esses tipos de gateway em um equipamento de hardware é o mesmo utilizado em plataformas virtuais.

Nas seções a seguir, você encontrará instruções sobre como pedir, instalar, configurar, ativar, iniciar e usar um Storage Gateway Hardware Appliance.

Tópicos

- [AWS Regiões suportadas](#)
- [Configuração do dispositivo de hardware](#)
- [Como montar em rack o seu equipamento de hardware e conectá-lo à alimentação](#)
- [Como configurar parâmetros de rede](#)
- [Como ativar o dispositivo de hardware](#)
- [Criar um gateway](#)
- [Como configurar um endereço IP para o gateway](#)
- [Como configurar o gateway](#)
- [Como remover um gateway do dispositivo de hardware](#)
- [Como excluir o dispositivo de hardware](#)

AWS Regiões suportadas

Para obter uma lista dos Regiões da AWS locais onde o Storage Gateway Hardware Appliance está disponível para ativação e uso, consulte [Regiões do Storage Gateway Hardware Appliance](#) no. Referência geral da AWS

Configuração do dispositivo de hardware

Depois de receber seu dispositivo de hardware Storage Gateway, você usa o console do dispositivo de hardware para configurar a rede para fornecer uma conexão sempre ativa e ativar seu dispositivo. AWS A ativação associa seu dispositivo à conta da Amazon Web Services que é usada durante o processo de ativação. Depois que ele for ativado, execute um arquivo, volume, ou gateway de fitas no console do Storage Gateway.

Note

É sua responsabilidade garantir que o firmware do dispositivo de hardware esteja up-to-date.

Para instalar e configurar o dispositivo de hardware

1. Monte o dispositivo em rack e conecte-o à energia e à rede. Para ter mais informações, consulte [Como montar em rack o seu equipamento de hardware e conectá-lo à alimentação](#).
2. Defina os endereços do Protocolo de Internet versão 4 (IPv4) para o dispositivo de hardware (host) e o Storage Gateway (o serviço). Para ter mais informações, consulte [Como configurar parâmetros de rede](#).
3. Ative o dispositivo de hardware no console Página de visão geral do dispositivo de hardware na AWS região de sua escolha. Para ter mais informações, consulte [Como ativar o dispositivo de hardware](#).
4. Instale o Storage Gateway em seu dispositivo de hardware. Para ter mais informações, consulte [Como configurar o gateway](#).

Os gateways são instalados no dispositivo de hardware do mesmo modo que no VMware ESXi, no Microsoft Hyper-V, na máquina virtual baseada em kernel (KVM) do Linux ou no Amazon EC2.

Aumento do armazenamento em cache utilizável

É possível aumentar o armazenamento utilizável no dispositivo de hardware de 5 TB para 12 TB. Isso fornece um cache maior para acesso de baixa latência aos dados de entrada. AWS Se você comprou o modelo de 5 TB, pode aumentar o armazenamento utilizável para 12 TB comprando cinco SSDs de 1,92 TB (unidades de estado sólido).

É possível adicioná-los ao dispositivo de hardware antes de ativá-lo. Se você já tiver ativado o dispositivo de hardware e deseja aumentar o armazenamento utilizável no dispositivo de 12 TB, faça o seguinte:

1. Redefina o dispositivo de hardware para as configurações de fábrica. Entre em contato com Amazon Web Services Support para obter instruções sobre como fazer isso.
2. Adicione cinco SSDs de 1,92 TB ao dispositivo.

Opções da placa da interface de rede

Dependendo do modelo do dispositivo que você solicitou, ele pode vir com uma placa de rede de cobre 10G-Base-T ou uma placa de rede 10G DA/SFP+.

- Configuração da NIC 10G-Base-T:
 - Use cabos CAT6 para 10G ou CAT5(e) para 1G
- Configuração de NIC 10G DA/SFP+:
 - Use cabos de conexão direta de cobre Twinax de até cinco metros
 - Módulos ópticos SFP+ compatíveis com Dell/Intel (SR ou LR)
 - Transceptor de cobre SFP/SFP+ para 1G-Base-T ou 10G-Base-T

Como montar em rack o seu equipamento de hardware e conectá-lo à alimentação

Depois de tirar o Storage Gateway Hardware Appliance da embalagem, siga as instruções contidas na caixa para montar o servidor no rack. O dispositivo tem um formato de 1U e cabe em um rack padrão de 19 polegadas compatível com a Comissão Eletrotécnica Internacional (IEC).

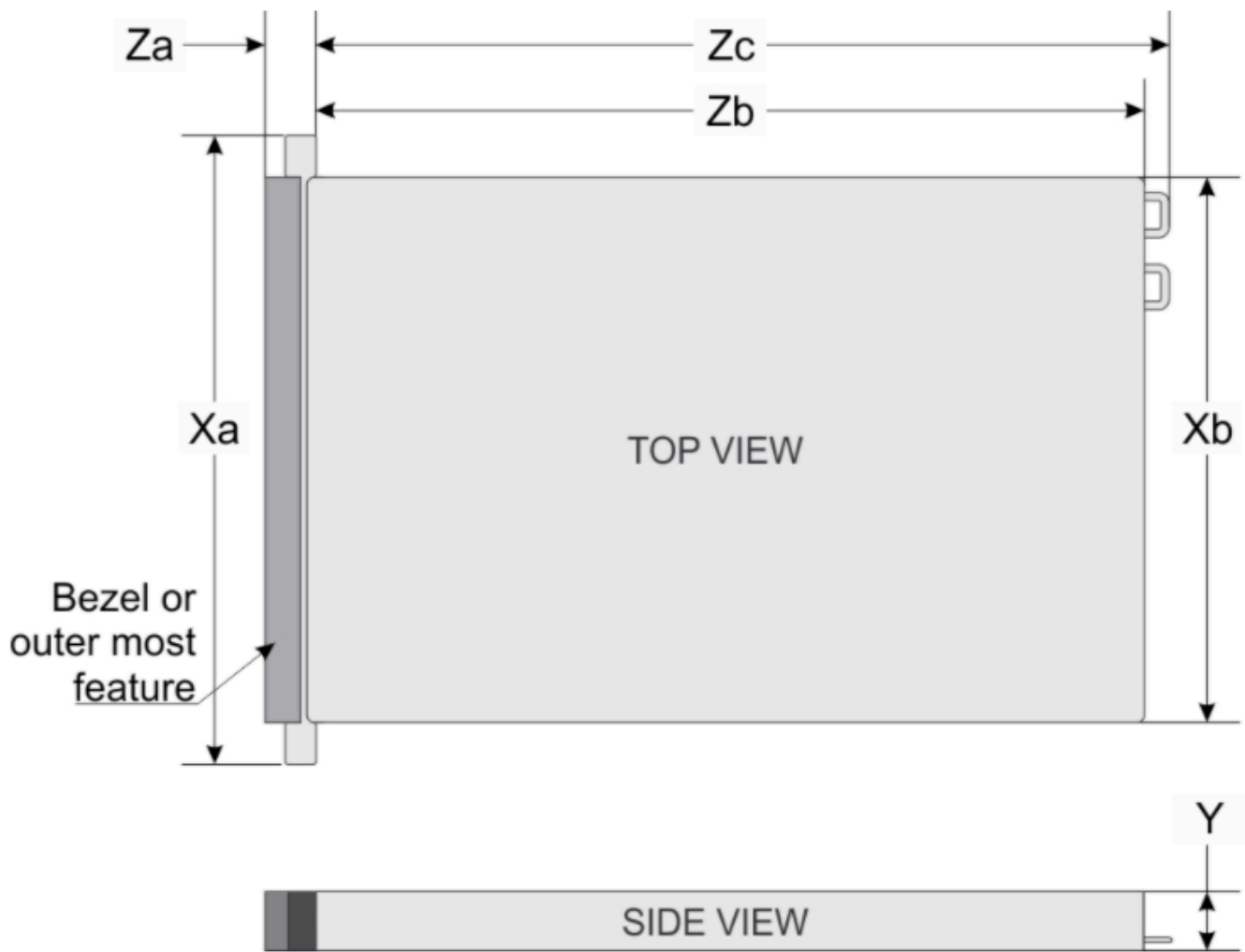
Para instalar e configurar o dispositivo de hardware, você precisa dos seguintes componentes:

- Cabos de alimentação: 1 (necessário); 2 (recomendado).

- Cabeamento de rede compatível (dependendo de qual placa de interface de rede, NIC, está incluída no dispositivo de hardware). O módulo óptico Twinax Copper DAC, SFP+ (compatível com Intel) ou transceptor de cobre SFP para Base-T.
- Teclado e monitor, ou uma solução de switch de teclado, vídeo e mouse (KVM).

Dimensões do dispositivo de hardware

dimensões do dispositivo de hardware, incluindo suportes de montagem e moldura.



System	Xa	Xb	Y	Za (with bezel)	Za (without bezel)	Zb*	Zc
10 x 2.5-inches	482.0 mm (18.97-inches)	434.0 mm (17.08-inches)	42.8 mm (1.68-inches)	35.84 mm (1.41-inches)	22.0 mm (0.87-inches)	733.82 mm (29.61-inches)	772.67 mm (30.42-inches)

dimensões do dispositivo de hardware, incluindo suportes de montagem e moldura.

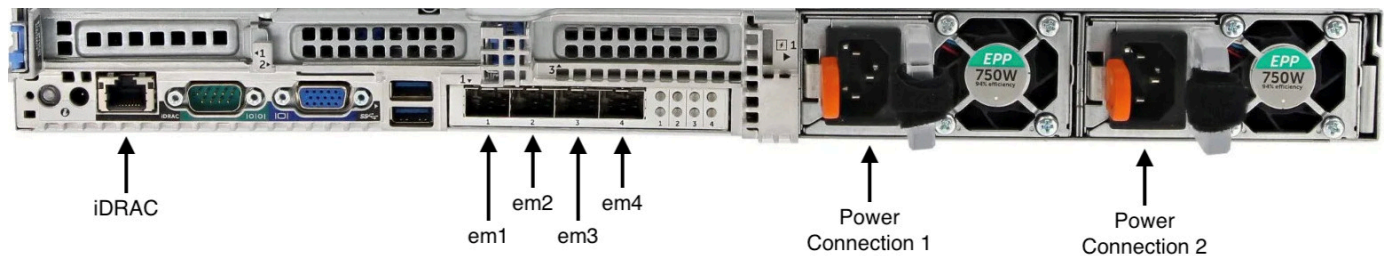
Para conectar o dispositivo de hardware à rede

Note

Antes de executar o procedimento a seguir, verifique se você atende a todos os requisitos para o Storage Gateway Hardware Appliance como descrito em [Requisitos de rede e firewall para o Storage Gateway Hardware Appliance](#).

1. Conecte um cabo de alimentação para cada uma das duas fontes. É possível conectar a apenas uma fonte de alimentação, mas recomendamos ligações com ambas as fontes.

Na imagem a seguir, você pode ver o dispositivo de hardware com diferentes conexões. parte traseira do dispositivo de hardware com etiquetas de rede e conector de alimentação.



parte traseira do dispositivo de hardware com etiquetas de rede e conector de alimentação.

2. Conecte um cabo Ethernet à porta em1 para garantir conexão permanente à Internet. A porta em1 é a primeira das quatro portas de rede física na parte traseira, da esquerda para a direita.

Note

O dispositivo de hardware não é compatível com o entroncamento de VLAN. Configure a porta de switch à qual você está conectando o dispositivo de hardware como uma porta de VLAN não truncada.

3. Conecte o teclado e o monitor.
4. Pressione o botão Power (Ligar no painel frontal, conforme mostrado na imagem a seguir. dispositivo de hardware frontal com etiqueta de botão liga/desliga.



dispositivo de hardware frontal com etiqueta de botão liga/desliga.

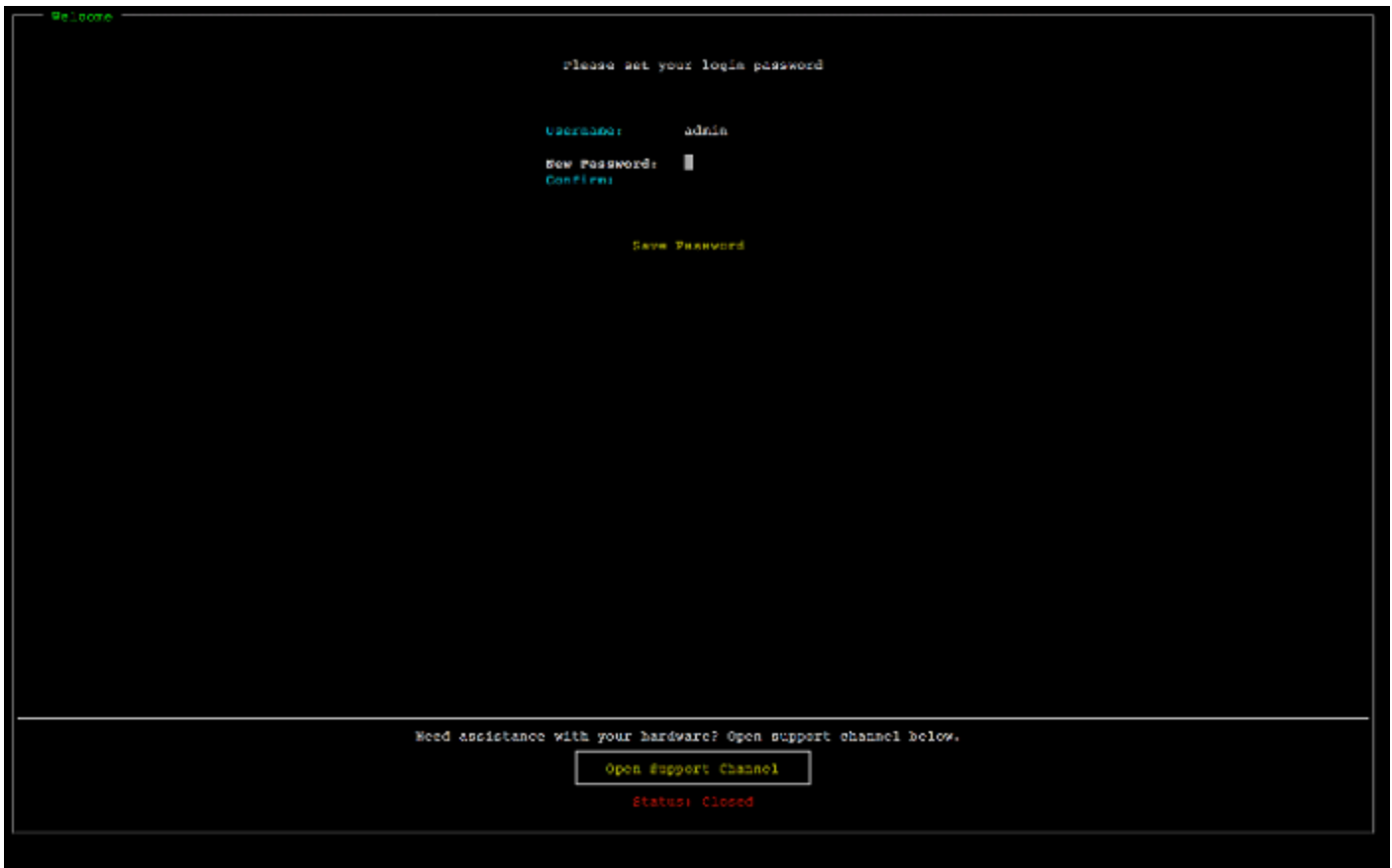
Depois que o servidor é inicializado, o console de hardware é exibido na tela. O console de hardware apresenta uma interface de usuário específica AWS que você pode usar para configurar os parâmetros iniciais da rede. Configure esses parâmetros para conectar o dispositivo à AWS e abrir um canal de suporte para usar o Amazon Web Services Support quando precisar solucionar problemas.

Para trabalhar com o console do hardware, digite o texto no teclado e use as teclas Up, Down, Right e Left Arrow para mover a tela na direção indicada. Use a tecla Tab para percorrer os itens na tela. Em algumas configurações, você pode usar a tecla Shift+Tab para mover sequencialmente para trás. Use a tecla Enter para salvar seleções ou para escolher um botão na tela.

Como definir uma senha pela primeira vez

1. Para Set Password (Definir senha), digite uma e, em seguida, pressione Down arrow.
2. Para Confirm (Confirmar), digite novamente e, em seguida, escolha Save Password (Salvar senha).

tela de diálogo de configuração de senha do console do dispositivo de hardware.



tela de diálogo de configuração de senha do console do dispositivo de hardware.

Nesse momento você visualiza o console do hardware, que mostra o seguinte:
menu principal do console do dispositivo de hardware mostrando conexões e opções de menu.



menu principal do console do dispositivo de hardware mostrando conexões e opções de menu.

Próxima etapa

[Como configurar parâmetros de rede](#)

Como configurar parâmetros de rede

Depois que o servidor é inicializado, você pode inserir a primeira senha no console de hardware, como descrito em [Como montar em rack o seu equipamento de hardware e conectá-lo à alimentação](#).

Em seguida, no console de hardware, siga as etapas a seguir para configurar os parâmetros de rede e conectar o dispositivo de hardware à AWS.

Para definir o endereço de rede

1. Escolha Configure Network (Configurar rede) e pressione Enter. A tela Configure Network (Configurar rede), mostrada a seguir, é exibida.
console do dispositivo de hardware configura a tela de rede.



console do dispositivo de hardware configura a tela de rede.

2. Para IP Address (Endereço IP), insira um endereço IPv4 válido de uma das fontes a seguir:

- Use o endereço IPv4 atribuído pelo servidor Dynamic Host Configuration Protocol (DHCP) para sua porta de rede física.

Se você fizer isso, anote este endereço IPv4 para uso posterior na etapa de ativação.

- Atribua um endereço IPv4 estático. Para fazer isso, escolha Static (Estático) na seção em1 e pressione Enter para ver a tela de configuração do IP estático mostrada a seguir.

A seção em1 é exibida na parte superior esquerda do grupo de configurações de porta.

Depois de inserir um endereço IPv4 válido, pressione Down arrow ou Tab.

Note

Se você configurar qualquer outra interface, ela deverá fornecer a mesma conexão sempre ativa com os AWS endpoints listados nos requisitos.

o console do dispositivo de hardware configura a NIC para a tela IP estática.



o console do dispositivo de hardware configura a NIC para a tela IP estática.

3. Para Subnet (Sub-rede), insira uma máscara de sub-rede válida e pressione `Down arrow`.
4. Para Gateway, insira o endereço IPv4 do gateway da sua rede e pressione `Down arrow`.
5. Para DNS1, insira o endereço IPv4 do servidor do seu DNS e pressione `Down arrow`.
6. (Opcional) Para DNS2, insira um segundo endereço IPv4 e pressione `Down arrow`. Se o servidor DNS principal ficar indisponível, a atribuição de um segundo DNS oferecerá redundância adicional.
7. Escolha `Save` (Salvar) e pressione `Enter` para salvar a configuração do seu endereço IPv4 estático para o dispositivo.

Para encerrar a sessão do console de hardware

1. Para voltar à página principal, escolha `Back` (Voltar).
2. Para retornar à tela de login, escolha `Logout` (Encerrar sessão).

Próxima etapa

[Como ativar o dispositivo de hardware](#)

Como ativar o dispositivo de hardware

Depois de configurar seu endereço IP, você insere esse endereço IP na página Hardware do AWS Storage Gateway console para ativar seu dispositivo de hardware. O processo de ativação confirma que o dispositivo de hardware tem as credenciais de segurança apropriadas e registra o dispositivo na sua conta da AWS .

Você pode optar por ativar seu dispositivo de hardware em qualquer um dos compatíveis Regiões da AWS. Para obter uma lista das regiões suportadas Regiões da AWS, consulte [Regiões do dispositivo de hardware do Storage Gateway](#) no Referência geral da AWS.

Para ativar o dispositivo de hardware do Storage Gateway

1. Abra o [Console de Gerenciamento da AWS Storage Gateway](#) e faça login com as credenciais da conta que você deseja usar para ativar o hardware.

Note

Para somente ativar, o seguinte deve acontecer:

- Seu navegador deve estar na mesma rede que o seu dispositivo de hardware.
- O firewall deve permitir acesso HTTP na porta 8080 no dispositivo para o tráfego de entrada.

2. Selecione Hardware no menu de navegação no lado esquerdo da página.
3. Escolha Ativar dispositivo.
4. Em Endereço IP, insira o endereço IP que você configurou para o dispositivo de hardware e escolha Conectar.

Consulte mais informações sobre como configurar o endereço IP em [Como configurar parâmetros de rede](#).

5. Em Nome, insira um nome para o dispositivo de hardware. Os nomes podem ter até 255 caracteres e não podem conter barras.

6. Em Fuso horário do dispositivo de hardware, insira o fuso horário local com base no qual a maior parte da workload do gateway será gerada e, depois, escolha Próximo.

O fuso horário controla quando ocorrem atualizações de hardware, com o horário 2h00 usado como horário programado padrão para fazer atualizações. Idealmente, se o fuso horário estiver definido corretamente, as atualizações ocorrerão fora da janela local de dias úteis por padrão.

7. Revise os parâmetros de ativação na seção Detalhes do dispositivo de hardware. Você pode escolher Anterior para voltar e fazer alterações, se necessário. Caso contrário, escolha Ativar para finalizar a ativação.

Um banner é exibido na página Visão geral de dispositivos de hardware, indicando que o dispositivo de hardware foi ativado com sucesso.

Nesse momento, o dispositivo está associado à sua conta. A próxima etapa é configurar e iniciar um Gateway de Arquivos do S3, Gateway de Arquivos do FSx, Gateway de Fitos ou Gateway de Volumes no novo dispositivo.

Próxima etapa

[Criar um gateway](#)

Criar um gateway

É possível criar um gateway de arquivos do S3, gateway de arquivos, gateway de fitas ou gateway de volumes do FSx no dispositivo de hardware.

Para criar um gateway no dispositivo de hardware

1. Faça login AWS Management Console e abra o console do Storage Gateway em <https://console.aws.amazon.com/storagegateway/home>.
2. Escolha Hardware.
3. Selecione o dispositivo de hardware ativado no qual você deseja criar o gateway e escolha Criar gateway.
4. Siga os procedimentos descritos em [Como criar seu gateway](#) para instalar, conectar e configurar o tipo de gateway escolhido.

Ao terminar de criar seu gateway no console do Storage Gateway, o software Storage Gateway começa a ser instalado automaticamente no dispositivo de hardware. Pode levar de cinco a 10 minutos para que um gateway seja exibido como on-line no console.

Para atribuir um endereço IP estático ao gateway instalado, configure as interfaces de rede do gateway para serem utilizadas pelos seus aplicativos.

Próxima etapa

[Como configurar um endereço IP para o gateway](#)

Como configurar um endereço IP para o gateway

Antes de ativar seu dispositivo de hardware, você atribuiu um endereço IP à interface de rede física. Agora que ativou o equipamento e iniciou o Storage Gateway nele, você precisa atribuir outro endereço IP à máquina virtual do Storage Gateway que é executada no dispositivo de hardware. Para atribuir um endereço IP estático a um gateway instalado no dispositivo de hardware, configure o endereço IP no console local do gateway. Seus aplicativos (como o cliente NFS ou SMB, o iniciador iSCSI e assim por diante) se conectam a esse endereço IP. Você pode acessar o console local do gateway do console do dispositivo de hardware.

Para configurar o endereço IP dispositivo para trabalhar com aplicativos

1. No console de hardware, escolha Open Service Console (Abrir console de serviço) para abrir a tela de login do console local do gateway.
2. Insira a senha de login do host local e pressione `Enter`.

A conta padrão é `admin` e a senha padrão é `password`.

3. Altere a senha padrão. Escolha Actions (Ações) e, depois, Set Local Password (Definir senha local). Insira suas novas credenciais na caixa de diálogo Set Local Password (Definir senha local).
4. (Opcional) Defina as configurações de proxy. Para obter instruções, consulte [the section called "Como definir a senha do console local no console do Storage Gateway"](#).
5. Navegue até a página de configurações de rede do console local do gateway, como mostrado a seguir.
página de configuração do console local do gateway mostrando opções, incluindo configuração de rede.

```
AWS Storage Gateway Configuration
#####
## Currently connected network adapters:
##
## eth0: 10.0.0.45
#####

1: SOCKS Proxy Configuration
2: Network Configuration
3: Test Network Connectivity
4: System Time Management
5: Gateway Console
6: View System Resource Check (0 Errors)

0: Stop AWS Storage Gateway

Press "x" to exit session

Enter command: _
```

página de configuração do console local do gateway mostrando opções, incluindo configuração de rede.

6. Digite 2 para acessar a página Network Configuration (Configuração de rede) mostrada a seguir. página de configuração de rede do console local do gateway com opções de DHCP e IP estático.

```
AWS Storage Gateway Network Configuration

1: Describe Adapter
2: Configure DHCP
3: Configure Static IP
4: Reset all to DHCP
5: Set Default Adapter
6: View DNS Configuration
7: View Routes

Press "x" to exit

Enter command: _
```

página de configuração de rede do console local do gateway com opções de DHCP e IP estático.

7. Configure um endereço IP estático ou DHCP para a porta de rede no dispositivo de hardware para apresentar um gateway de arquivo, volume ou fita para as aplicações. Esse endereço IP deve estar presente na mesma sub-rede que o endereço IP usado durante a ativação do dispositivo de hardware.

Para sair do console local do gateway

- Pressione a tecla `Crtl+] (colchete de fechamento)`. O console de hardware é exibido.

Note

A tecla precedente é a única forma de sair do console local do gateway.

Próxima etapa

[Como configurar o gateway](#)

Como configurar o gateway

Depois de ativar e configurar seu dispositivo de hardware, ele é exibido no console. Agora você pode criar o tipo de gateway que quiser. Continue a instalação na página Configurar gateway para seu tipo de gateway. Para obter instruções, consulte [Como configurar o gateway de volumes](#).

Como remover um gateway do dispositivo de hardware

Para remover um software de gateway de seu dispositivo de hardware, use o procedimento a seguir. Depois de fazer isso, o software do gateway é desinstalado do seu dispositivo de hardware.

Para remover um gateway a partir de um dispositivo de hardware

1. Na página Hardware do console do Storage Gateway, escolha o dispositivo de hardware que você deseja excluir.
2. Em Actions, selecione Remove Gateway. Uma caixa de diálogo de confirmação é exibida.
3. Verifique se você deseja remover o software de gateway do dispositivo de hardware especificado, digite a palavra remover na caixa de confirmação e escolha Remover.

Note

Depois de remover o software do gateway, você não poderá desfazer a ação. Para determinados tipos de gateway, você pode perder dados na exclusão, especialmente os dados em cache. Para mais informações sobre como deletar um gateway, consulte [Como excluir seu gateway usando o console do AWS Storage Gateway e como limpar os recursos associados](#).

A remoção de um gateway não exclui o dispositivo de hardware do console. O dispositivo de hardware permanece para futuras implantações do gateway.

Como excluir o dispositivo de hardware

Se você não precisar mais de um equipamento de hardware Storage Gateway que já tenha ativado, você pode excluir o equipamento completamente da sua AWS conta.

Note

Para mover seu equipamento para uma AWS conta diferente ou Região da AWS, você deve primeiro excluí-lo usando o procedimento a seguir e, em seguida, abrir o canal de suporte do gateway e entrar em contato AWS Support para realizar uma reinicialização suave. Para obter mais informações, consulte [Ativando o AWS Support acesso para ajudar a solucionar problemas do gateway](#) hospedado no local.

Para excluir do dispositivo de hardware

1. Se você tiver instalado um gateway no dispositivo de hardware, primeiro remova o gateway antes de excluir o dispositivo. Para obter instruções sobre como remover um gateway do seu dispositivo de hardware, consulte [Como remover um gateway do dispositivo de hardware](#).
2. Na página Hardware do console do Storage Gateway, escolha o dispositivo de hardware que você deseja excluir.
3. Em Actions (Ações), escolha Delete Appliance (Excluir dispositivo). Uma caixa de diálogo de confirmação é exibida.
4. Verifique se você deseja excluir os dispositivos de hardware especificados, digite a palavra excluir na caixa de confirmação e escolha Excluir.

Quando você excluir o dispositivo de hardware, todos os recursos associados ao gateway que está instalado no dispositivo também serão excluídos, exceto os dados no próprio dispositivo de hardware.

Como criar um gateway

Os tópicos de visão geral desta página fornecem uma sinopse de alto nível de como funciona o processo de criação do Storage Gateway. Para obter step-by-step os procedimentos para criar um tipo específico de gateway usando o console do Storage Gateway, consulte [Criando um gateway de volume](#).

Visão geral: ativação do gateway

A ativação do gateway envolve configurar seu gateway, conectá-lo e AWS, em seguida, revisar suas configurações e ativá-lo.

Configurar um gateway

Para configurar seu Storage Gateway, primeiro você escolhe o tipo de gateway que deseja criar e a plataforma host na qual executará o dispositivo virtual do gateway. Em seguida, você baixa o modelo de dispositivo virtual de gateway para a plataforma de sua escolha e o implanta em seu ambiente on-premises. Você também pode implantar seu Storage Gateway como um dispositivo de hardware físico que você solicita de seu revendedor preferido ou como uma instância do Amazon EC2 em AWS seu ambiente de nuvem. Ao implantar o dispositivo de gateway, você aloca espaço em disco físico local no host de virtualização.

Conecte-se a AWS

A próxima etapa é conectar seu gateway com a AWS. Para fazer isso, primeiro você escolhe o tipo de endpoint de serviço que deseja usar para comunicações entre o dispositivo virtual do gateway e AWS os serviços na nuvem. Este endpoint pode ser acessado pela Internet pública ou somente de dentro da sua Amazon VPC, onde você tem controle total sobre a configuração de segurança da rede. O endereço IP do gateway ou sua chave de ativação é especificado, que pode ser obtido ao se conectar ao console local no dispositivo de gateway.

Analisar e ativar

Neste ponto, você terá a oportunidade de revisar as opções de gateway e conexão escolhidas e fazer alterações, se necessário. Quando tudo estiver configurado da forma como deseja, é possível ativar o gateway. Antes de começar a usar seu gateway ativado, você precisará configurar alguns ajustes adicionais e criar seus recursos de armazenamento.

Visão geral: configuração do gateway

Depois de ativar o Storage Gateway, você precisa fazer algumas configurações adicionais. Nesta etapa, você aloca o armazenamento físico provisionado na plataforma host do gateway para ser usado como cache ou buffer de upload pelo dispositivo de gateway. Em seguida, você define as configurações para ajudar a monitorar a integridade do seu gateway usando Amazon CloudWatch Logs e CloudWatch alarmes e adiciona tags para ajudar a identificar o gateway, se desejar. Antes de começar a usar seu gateway ativado e configurado, você precisará criar seus recursos de armazenamento.

Visão geral: recursos de armazenamento

Depois de ativar e configurar o Storage Gateway, você precisa criar recursos de armazenamento em nuvem para que ele os use. Dependendo do tipo de gateway criado, você usará o console do Storage Gateway para criar volumes, fitas ou compartilhamentos de arquivos do Amazon S3 ou Amazon FSx e associá-los a ele. Cada tipo de gateway usa seus respectivos recursos para emular o tipo relacionado de infraestrutura de armazenamento em rede e transfere os dados que você grava para a nuvem da AWS .

Como criar um gateway de volume

Nesta seção, é possível encontrar instruções sobre como criar e usar um gateway de volumes.

Tópicos

- [Como criar um gateway](#)
- [Como criar um volume](#)
- [Como usar seu volume](#)
- [Fazer backup de seus volumes](#)

Como criar um gateway

Nesta seção, é possível encontrar instruções sobre como fazer download, implantar e ativar um gateway de volumes.

Tópicos

- [Configurar um gateway de volumes](#)

- [Conecte seu gateway de volumes à AWS](#)
- [Analisar as configurações e ativar o gateway de volumes](#)
- [Configure o gateway de volumes](#)

Configurar um gateway de volumes

Para configurar um novo gateway de volumes

1. Abra o AWS Management Console em <https://console.aws.amazon.com/storagegateway/home/> e escolha Região da AWS onde você deseja criar seu gateway.
2. Escolha Criar gateway para abrir a página Configurar gateway.
3. Na seção Configurações de gateway, faça o seguinte:
 - a. Em Gateway name (Nome do gateway), insira um nome para o seu gateway. É possível pesquisar esse nome para encontrar seu gateway nas páginas de listagem no console do Storage Gateway.
 - b. Em Fuso horário do gateway, escolha o fuso horário local da parte do mundo em que você deseja implantar seu gateway.
4. Na seção Opções de gateway, em Tipo de gateway, escolha Gateway de volumes e o tipo de volume que seu gateway usará. Você pode escolher entre as seguintes opções:
 - Volumes em cache: armazena os dados primários no Amazon S3 e retém os dados acessados com frequência localmente no cache para um acesso mais rápido.
 - Volumes armazenados: armazena todos os seus dados localmente enquanto faz backup deles de forma assíncrona no Amazon S3. Os gateways que usam esse tipo de volume não podem ser implantados no Amazon EC2.
5. Na seção Opções de plataforma, faça o seguinte:
 - a. Em Plataforma host, escolha a plataforma na qual você deseja implantar seu gateway e siga as instruções específicas da plataforma exibidas na página do console do Storage Gateway para configurar a plataforma host. Você pode escolher entre as seguintes opções:
 - VMware ESXi: baixe, implante e configure a máquina virtual de gateway usando o VMware ESXi.
 - Microsoft Hyper-V: baixe, implante e configure a máquina virtual de gateway usando o Microsoft Hyper-V.

- Linux KVM: baixe, implante e configure a máquina virtual de gateway usando o Linux KVM.
 - Amazon EC2: configure e execute uma instância do Amazon EC2 para hospedar seu gateway. Esta opção não está disponível para gateways de volume armazenado.
 - Dispositivo de hardware - Solicite um dispositivo de hardware físico dedicado AWS para hospedar seu gateway.
- b. Em Confirmar configuração do gateway, marque a caixa de seleção para confirmar que você executou as etapas de implantação da plataforma host escolhida. Esta etapa não se aplica à plataforma host do dispositivo de hardware.
6. Escolha Próximo para continuar.

Agora que seu gateway está configurado, você precisa escolher como deseja se conectar e se comunicar com ele AWS. Para obter instruções, consulte [Conectar seu Volume Gateway AWS](#) a.

Conecte seu gateway de volumes à AWS

Para conectar um novo Volume Gateway ao AWS

1. Conclua o procedimento descrito em [Configurar um gateway de volumes](#), caso ainda não tenha feito isso. Ao terminar, escolha Avançar para abrir a página Conectar-se à página da AWS no console do Storage Gateway.
2. Na seção Opções de endpoint, para Endpoint de serviço, escolha o tipo de endpoint com o qual seu gateway usará para se comunicar. AWS Você pode escolher entre as seguintes opções:
 - Acessível ao público - Seu gateway se AWS comunica pela Internet pública. Se você selecionar essa opção, use a caixa de seleção do endpoint habilitado para FIPS para especificar se a conexão deve estar em conformidade com os padrões FIPS (Padrões Federais de Processamento de Informações).

Note

Se você precisar de módulos criptográficos validados pelo FIPS 140-2 ao acessar AWS por meio de uma interface de linha de comando ou de uma API, use um endpoint compatível com FIPS. Para obter mais informações, consulte [Federal Information Processing Standard \(FIPS – Norma federal de processamento de informações\) 140-2](#).

O endpoint de serviço de FIPS está disponível somente em algumas regiões da AWS . Para obter mais informações, consulte [Endpoints e cotas do Storage Gateway](#) na Referência geral da AWS.

- VPC hospedado: seu gateway se comunica com a AWS por meio de uma conexão privada com sua VPC, permitindo que você controle suas configurações de rede. Se você selecionar essa opção, deverá especificar um endpoint da VPC existente escolhendo seu ID de endpoint da VPC no menu suspenso ou fornecendo o nome DNS ou o endereço IP do endpoint da VPC.
3. Na seção Opções de conexão do gateway, em Opções de conexão, escolha como identificar seu gateway na AWS. Você pode escolher entre as seguintes opções:
- Endereço IP: forneça o endereço IP do seu gateway no campo correspondente. Este endereço IP deve ser público ou acessível de dentro da sua rede atual e você deve ser capaz de se conectar com ele do seu navegador da web.
- É possível obter o endereço IP do gateway fazendo login no console local do gateway a partir do seu cliente hipervisor ou copiando-o da página de detalhes da instância do Amazon EC2.
- Chave de ativação: fornece a chave de ativação do seu gateway no campo correspondente. É possível gerar uma chave de ativação usando o console local do gateway. Escolha esta opção se o endereço IP do seu gateway não estiver disponível.
4. Escolha Próximo para continuar.

Agora que você escolheu como deseja que seu gateway se conecte AWS, você precisa ativar o gateway. Para obter instruções, consulte [Como revisar as configurações e ativar o gateway de volumes](#).


Analisar as configurações e ativar o gateway de volumes

Para ativar um novo gateway de volumes

1. Conclua os procedimentos descritos nos seguintes tópicos, caso ainda não o tenha feito isso:
 - [Configurar um gateway de volumes](#)
 - [Conecte seu Volume Gateway a AWS](#)

Ao terminar, escolha Avançar para abrir a página Revisar e ativar no console do Storage Gateway.

2. Revise os detalhes iniciais do gateway para cada seção na página.
3. Se uma seção contiver erros, escolha Editar para retornar à página de configurações correspondente e fazer as alterações.

 Note

Não é possível modificar as opções do gateway ou as configurações de conexão após a criação do gateway.

4. Escolha Ativar gateway para continuar.

Agora que ativou seu gateway, você precisa realizar a primeira configuração para alocar os discos de armazenamento local e configurar o registro em log. Para obter instruções, consulte [Como configurar o gateway de volumes](#).

Configure o gateway de volumes

Para realizar a primeira configuração em um novo gateway de volumes

1. Conclua os procedimentos descritos nos seguintes tópicos, caso ainda não o tenha feito isso:
 - [Configurar um gateway de volumes](#)
 - [Conecte seu Volume Gateway a AWS](#)
 - [Analisar as configurações e ativar o gateway de volumes](#)

Ao terminar, escolha Avançar para abrir a página Configurar gateway no console do Storage Gateway.

2. Na seção Configurar armazenamento, use os menus suspensos para alocar pelo menos um disco com pelo menos 165 GiB de capacidade para ARMAZENAMENTO EM CACHE e pelo menos um disco com capacidade de pelo menos 150 GiB para BUFFER DE UPLOAD. Os discos locais listados nesta seção correspondem ao armazenamento físico que você provisionou em sua plataforma host.

3. Na seção Grupo de CloudWatch registros, escolha como configurar o Amazon CloudWatch Logs para monitorar a integridade do seu gateway. Você pode escolher entre as seguintes opções:
 - Crie um novo grupo de logs - Configure um novo grupo de logs para monitorar seu gateway.
 - Usar um grupo de logs existente: escolha um grupo de logs existente no menu suspenso correspondente.
 - Desative o registro - Não use o Amazon CloudWatch Logs para monitorar seu gateway.

Note

Para receber os registros de integridade do Storage Gateway, as seguintes permissões devem estar presentes na política de recursos do grupo de registros. Substitua a *seção destacada* pelas informações específicas do grupo de registros ResourceArn para sua implantação.

```
"Sid": "AWSLogDeliveryWrite20150319",
  "Effect": "Allow",
  "Principal": {
    "Service": [
      "delivery.logs.amazonaws.com"
    ]
  },
  "Action": [
    "logs:CreateLogStream",
    "logs:PutLogEvents"
  ],
  "Resource": "arn:aws:logs:eu-west-1:1234567890:log-group:/foo/bar:log-stream:*"
```

O elemento “Recurso” é necessário somente se você quiser que as permissões sejam aplicadas explicitamente a um grupo de registros individual.

4. Na seção de CloudWatch alarmes, escolha como configurar os CloudWatch alarmes da Amazon para notificá-lo quando as métricas do gateway se desviam dos limites definidos. Você pode escolher entre as seguintes opções:
 - Crie os alarmes recomendados pelo Storage Gateway — Crie todos os CloudWatch alarmes recomendados automaticamente quando o gateway for criado. Para obter mais informações sobre os alarmes recomendados, consulte [Compreendendo os CloudWatch alarmes](#).

Note

Esse recurso requer permissões CloudWatch de política, que não são concedidas automaticamente como parte da política de acesso total pré-configurada do Storage Gateway. Certifique-se de que sua política de segurança conceda as seguintes permissões antes de tentar criar CloudWatch alarmes recomendados:

- `cloudwatch:PutMetricAlarm`: criar alarmes
- `cloudwatch:DisableAlarmActions`: desativar as ações de alarme
- `cloudwatch:EnableAlarmActions`: ativar as ações de alarme
- `cloudwatch>DeleteAlarms`: excluir alarmes

- Crie um alarme personalizado — Configure um novo CloudWatch alarme para notificá-lo sobre as métricas do seu gateway. Escolha Criar alarme para definir métricas e especificar ações de alarme no CloudWatch console da Amazon. Para obter instruções, consulte [Como usar CloudWatch alarmes da Amazon](#) no Guia do CloudWatch usuário da Amazon.
 - Sem alarme — Não receba CloudWatch notificações sobre as métricas do seu gateway.
5. (Opcional) Na seção Tags, escolha Adicionar nova tag e, em seguida, insira um par de chaves/valores com distinção entre maiúsculas e minúsculas para ajudá-lo a pesquisar e filtrar seu gateway nas páginas de listagem no console do Storage Gateway. Repita esta etapa para adicionar quantas tags precisar.
 6. Escolha Configurar para concluir a criação do gateway.


Para verificar o status do novo gateway, procure-o na página de Visão geral do Gateway do Storage Gateway.

Agora que criou o gateway, você precisa criar um volume para que ele possa ser usado. Para obter instruções, consulte [Como criar um volume](#).

Como criar um volume

Anteriormente, você alocou discos locais que adicionou ao armazenamento em cache e ao buffer de upload da VM. Agora você criará um volume de armazenamento no qual seus aplicativos lerão e gravarão dados. O gateway mantém os dados recém-acessados do volume armazenados localmente em cache e os dados transferidos de forma assíncrona no Amazon S3. Em relação aos

volumes armazenados, você alocou discos locais que foram adicionados ao buffer de upload da VM e aos dados de seu aplicativo.

 Note

Você pode usar AWS Key Management Service (AWS KMS) para criptografar dados gravados em um volume em cache armazenado no Amazon S3. Atualmente, é possível fazer isso usando a Referência de API do AWS Storage Gateway . Para obter mais informações, consulte [CreateCachediscsiVolume](#) ou [create-cached-iscsi-volume](#)

Para criar um volume


1. Abra o console do Storage Gateway em <https://console.aws.amazon.com/storagegateway/home>.
2. No console do Storage Gateway, escolha Criar volume.
3. Na caixa de diálogo Create volume (Criar volume), escolha um gateway em Gateway.
4. Para os volumes armazenados em cache, digite a capacidade em Capacidade.

Para os volumes armazenados, selecione um valor para Disk ID (ID do disco) na lista.

5. Em Conteúdo do volume, suas opções dependem do tipo de gateway para o qual você está criando o volume.

Para os volumes armazenados em cache, você tem as seguintes opções:

- Create a new empty volume (Criar um novo volume vazio).
- Criar um volume com base em um snapshot do Amazon EBS. Se você escolher esta opção, forneça um valor para EBS snapshot ID (ID do snapshot do EBS).

 Note

O Storage Gateway não é compatível com a criação de volumes em cache a partir de snapshots de volumes do AWS Marketplace .

- Clone from last volume recovery point (Clonar o último ponto de recuperação do volume). Se você escolher essa opção, escolha um ID de volume para Source volume (Volume da origem). Quando não houver nenhum volume na região, esta opção não será exibida.

Para os volumes armazenados, você tem as seguintes opções:


- Create a new empty volume (Criar um novo volume vazio).
 - Create a volume based on a snapshot (Criar um volume com base em um snapshot). Se você escolher esta opção, forneça um valor para EBS snapshot ID (ID do snapshot do EBS).
 - Preserve existing data on the disk (Preservar os dados existentes no disco)
6. Insira um nome em Nome do destino iSCSI.

O nome de destino pode conter letras minúsculas, números, pontos (.) e hífen (-). Esse nome de destino aparece como o nome do iSCSI target node (Nó de destino do iSCSI) na guia Targets (Destinos) da interface do iSCSI Microsoft initiator (Iniciador Microsoft iSCSI) após a descoberta. Por exemplo, o nome target1 aparece como `iqn.1007-05.com.amazon:target1`. Garanta que o nome de destino seja exclusivo globalmente na rede de área de armazenamento (SAN).

7. Verifique se a configuração Network interface (Interface de rede) tem um endereço IP selecionado ou escolha um endereço IP para Network interface (Interface de rede). Em Network interface (Interface de rede), é exibido um endereço IP para cada adaptador configurado para a VM do gateway. Se a VM do gateway estiver configurada para apenas um adaptador de rede, não será exibida nenhuma lista de Network interface (Interface de rede) porque existe apenas um endereço IP.

Seu destino iSCSI estará disponível no adaptador de rede que você escolher.

Se tiver definido seu gateway para usar vários adaptadores de rede, escolha o endereço IP que seus aplicativos de armazenamento usarão para acessar o volume. Para obter mais informações sobre como configurar vários adaptadores de rede, consulte [Como configurar seu gateway para vários NICs](#).

 Note

Depois que você escolher um adaptador de rede, não será possível alterar essa configuração.

8. (Opcional) Em Tags, insira uma chave e um valor para adicionar uma tag ao volume. Uma tag é um par de chave/valor que diferencia maiúsculas de minúsculas e ajuda você a gerenciar, filtrar e pesquisar seus volumes.
9. Escolha Create volume (Criar volume).

Se você tiver criado anteriormente volumes nessa região, eles serão listados no console do Storage Gateway.

A caixa de diálogo Configure CHAP Authentication (Configurar autenticação do CHAP) é exibida. É possível configurar o Challenge-Handshake Authentication Protocol (CHAP) para seu volume nesse momento ou pode escolher Cancelar e configurar o CHAP mais tarde. Para obter mais informações sobre a configuração CHAP, consulte [Configurar a autenticação CHAP para os volumes](#).

The screenshot shows the AWS Storage Gateway console interface. At the top, there is a 'Create volume' button and an 'Actions' dropdown menu. Below this is a search bar with the text 'Filter by ID, type, or other volume attributes.' A table lists several volumes with columns for Volume ID, Status, Type, Used, Size, and Gateway. The volume 'vol-0e0eb15a2996b3094' is selected and highlighted in blue. Below the table, there are two tabs: 'Details' and 'Tags'. The 'Details' tab is active, showing the following information:

Volume ID	vol-0e0eb15a2996b3094 (Cached)	Status	Available
Gateway		Used	14.895 GiB
CHAP authentication	No	Size	20 GiB
Target name	iqn.1997-05.com.amazon:storage:gateway-test-0	Monitoring	Cloudwatch
Initiator	10.0.0.10:10100	Host IP	
		Host port	3260
		Snapshot schedule	-
		Created	9/26/2017, 8:57:34 PM

Se você não quiser configurar o CHAP, poderá começar a usar o volume. Para ter mais informações, consulte [Como usar seu volume](#).

Configurar a autenticação CHAP para os volumes

CHAP oferece proteção contra ataques de playback exigindo autenticação para acessar os destinos de volume de armazenamento. Na caixa de diálogo Configure CHAP Authentication (Configurar autenticação do CHAP), você fornece informações a fim de configurar CHAP para os volumes.

Para configurar CHAP

1. Selecione o volume para o qual você deseja configurar o CHAP.
2. Em Actions (Ações), escolha Configure CHAP authentication (Configurar autenticação do CHAP).
3. Em Nome do iniciador, digite o nome do iniciador.
4. Em Segredo do iniciador, digite a frase secreta que você usou para autenticar o iniciador iSCSI.

5. Em Frase secreta do destino, digite a frase secreta que você usou para autenticar o destino do CHAP mútuo.
6. Escolha Save para salvar as entradas.

Para obter mais informações sobre como configurar a autenticação de CHAP, consulte [Como configurar a autenticação CHAP para destinos iSCSI](#).

Próxima etapa

[Como usar seu volume](#)

Como usar seu volume

A seguir, você pode encontrar instruções sobre como usar seus volumes. Para usar seus volumes, primeiro conecte-se com seus clientes como destinos iSCSI e depois inicialize e formate o volume.

Tópicos

- [Como conectar volumes ao cliente](#)
- [Como inicializar e formatar um volume](#)
- [Como testar um gateway](#)
- [Para onde ir agora?](#)

Como conectar volumes ao cliente

Você pode usar o iniciador iSCSI em seu cliente para se conectar aos seus volumes. No final do procedimento a seguir, os volumes são disponibilizados como dispositivos locais em seu cliente.

Important

Com o Storage Gateway, é possível se conectar a vários hosts com um mesmo volume quando os hosts coordenam o acesso por meio do Windows Server Failover Clustering (WSFC). Não é possível conectar vários hosts ao mesmo volume sem usar o WSFC, por exemplo, compartilhando um sistema de arquivos NTFS/ext4 sem cluster.

Tópicos

- [Como se conectar ao cliente Microsoft Windows](#)

- [Como se conectar ao cliente Red Hat Enterprise Linux](#)

Como se conectar ao cliente Microsoft Windows

O procedimento a seguir mostra um resumo das etapas para você se conectar a um cliente Windows. Para ter mais informações, consulte [Como conectar iniciadores iSCSI](#).

Para se conectar a um cliente Windows

1. Execute o `iscsicpl.exe`.
2. Na caixa de diálogo iSCSI Initiator Properties, escolha a guia Discovery e, em seguida, Discovery Portal.
3. Na caixa de diálogo Discover Target Portal, digite o endereço IP do destino iSCSI para o endereço IP ou nome DNS.
4. Conecte o novo portal de destino ao destino do volume de armazenamento no gateway.
5. Escolha o destino e escolha Connect.
6. Na guia Targets, confirme se o Status do destino está com o valor Connected, que indica que o destino está conectado, e clique em OK.

Como se conectar ao cliente Red Hat Enterprise Linux

O procedimento a seguir mostra um resumo das etapas para você se conectar a um cliente Red Hat Enterprise Linux (RHEL). Para ter mais informações, consulte [Como conectar iniciadores iSCSI](#).

Para conectar um cliente Linux a destinos iSCSI

1. Instale o pacote `iscsi-initiator-utils` RPM.

Você pode usar o comando a seguir para instalar o pacote.

```
sudo yum install iscsi-initiator-utils
```

2. Verifique se o daemon iSCSI está em execução.

Para o RHEL 5 ou 6, use o comando a seguir.

```
sudo /etc/init.d/iscsi status
```

Para o RHEL 7, use o comando a seguir.

```
sudo service iscsid status
```

3. Descubra o volume ou o destino dos dispositivos de VTL definidos para um gateway. Use o comando de descoberta a seguir.

```
sudo /sbin/iscsiadm --mode discovery --type sendtargets --portal [GATEWAY_IP]:3260
```

A saída do comando de descoberta será semelhante à saída do exemplo a seguir.

Em gateways de volumes: `[GATEWAY_IP]:3260, 1`
`iqn.1997-05.com.amazon:myvolume`

Em gateway de fitas: `iqn.1997-05.com.amazon:[GATEWAY_IP]-tapedrive-01`

4. Conecte-se a um destino.

Especifique o `[GATEWAY_IP]` e IQN corretos no comando de conexão.

Use o comando a seguir.

```
sudo /sbin/iscsiadm --mode node --targetname  
iqn.1997-05.com.amazon:[ISCSI_TARGET_NAME] --portal [GATEWAY_IP]:3260,1 --login
```

5. Verifique se o volume está anexado à máquina do cliente (o iniciador). Para fazer isso, use o comando a seguir.

```
ls -l /dev/disk/by-path
```

A saída do comando será semelhante à saída do exemplo a seguir.

```
lrwxrwxrwx. 1 root root 9 Apr 16 19:31 ip-[GATEWAY_IP]:3260-iscsi-  
iqn.1997-05.com.amazon:myvolume-lun-0 -> ../../sda
```

Depois que configurar seu iniciador, é altamente recomendável que você personalize suas configurações iSCSI, tal como examinado em [Como personalizar suas configurações iSCSI Linux](#).

Como inicializar e formatar um volume

Depois de usar o iniciador iSCSI em seu cliente para se conectar aos seus volumes, deverá inicializar e formatar seu volume.

Tópicos

- [Como inicializar e formatar seu volume no Microsoft Windows](#)
- [Como inicializar e formatar seu volume no Red Hat Enterprise Linux](#)

Como inicializar e formatar seu volume no Microsoft Windows

Use o procedimento a seguir para inicializar e formatar seu volume no Windows.

Para inicializar e formatar seu volume de armazenamento

1. Inicie o **diskmgmt.msc** para abrir o console Disk Management (Gerenciamento de disco).
2. Na caixa de diálogo Inicialize Disk (Iniciar disco), inicialize o volume como uma partição MBR (Master Boot Record). Ao selecionar o estilo de partição, você deve levar em conta o tipo de volume ao qual está se conectando – armazenado em cache ou armazenado –, tal como mostrado na tabela a seguir.

Estilo de partição	Use nas condições a seguir
MBR (Master Boot Record)	<ul style="list-style-type: none">• Se seu gateway for um volume armazenado e o tamanho máximo do volume de armazenamento for 1 TiB.• Se seu gateway for um volume armazenado em cache e o tamanho do volume de armazenamento for inferior a 2 TiB.
GPT (GUID Partition Table)	Se o tamanho do volume de armazenamento de seu gateway for 2 TiB ou superior.

3. Crie um volume simples:
 - a. Abra o volume on-line para inicializá-lo. Todos os volumes disponíveis são exibidos no console de gerenciamento de disco.
 - b. Abra o menu de contexto (clique com o botão direito do mouse) do disco e escolha New Simple Volume (Novo volume simples).

⚠ Important

Tenha cuidado para não formatar o disco errado. Verifique se o disco que você está formatando tem o mesmo tamanho do disco local alocado à VM do gateway e se o respectivo status é Unallocated (Não atribuído).

- c. Especifique o tamanho máximo de disco.
- d. Atribua a letra ou o caminho da unidade ao seu volume e formate-o escolhendo Perform a quick format (Realizar formatação rápida).

⚠ Important

Recomendamos que você use Perform a quick format (Realizar formatação rápida) para volumes armazenados em cache. Isso resulta em menos E/S de inicialização, menor tamanho inicial de snapshot e tempo mais rápido para um volume utilizável. Ele também evita o uso de volume armazenado em cache espaço para o processo de formatação completa.

ℹ Note

O tempo necessário para formatar o volume depende do tamanho do volume. O processo pode levar alguns minutos para ser concluído.

Como inicializar e formatar seu volume no Red Hat Enterprise Linux

Use o procedimento a seguir para inicializar e formatar seu volume no Red Hat Enterprise Linux (RHEL).

Para inicializar e formatar seu volume de armazenamento

1. Altere o diretório para a pasta /dev.
2. Execute o comando `sudo cfdisk`.
3. Identifique seu novo volume usando o seguinte comando. Para encontrar novos volumes, você pode relacionar a estrutura de partição de seus volumes.

```
$ lsblk
```

Um erro "unrecognized volumes label" referente ao novo volume não particionado é exibido.

4. Inicialize seu novo volume. Ao selecionar o estilo de partição, você deve levar em conta o tipo e tamanho de volume ao qual está se conectando – armazenado em cache ou armazenado –, tal como mostrado na tabela a seguir.

Estilo de partição	Use nas condições a seguir
MBR (Master Boot Record)	<ul style="list-style-type: none"> • Se seu gateway for um volume armazenado e o tamanho máximo do volume de armazenamento for 1 TiB. • Se seu gateway for um volume armazenado em cache e o tamanho do volume de armazenamento for inferior a 2 TiB.
GPT (GUID Partition Table)	Se o tamanho do volume de armazenamento de seu gateway for 2 TiB ou superior.

Para partição MBR, use o comando a seguir: `sudo parted /dev/your volume mklabel msdos`

Para partição GPT, use o comando a seguir: `sudo parted /dev/your volume mklabel gpt`

5. Crie uma partição usando o seguinte comando.

```
sudo parted -a opt /dev/your volume mkpart primary file system 0% 100%
```

6. Atribua uma letra de unidade à partição e crie um sistema de arquivos usando o seguinte comando.

```
sudo mkfs -L datapartition /dev/your volume
```

7. Monte o sistema de arquivos usando o seguinte comando.


```
sudo mount -o defaults /dev/your volume /mnt/your directory
```

Como testar um gateway

A configuração de seu gateway de volumes é testada ao realizar as seguintes tarefas:

1. Grave dados no volume.
2. Faça um snapshot.
3. Restaure o snapshot para outro volume.

Você verifica a configuração de um gateway fazendo um backup instantâneo do seu volume e armazenando o instantâneo nele. AWS Em seguida, restaure o snapshot para outro volume. Seu gateway copia os dados do snapshot especificado AWS para o novo volume.

 Note

A restauração de dados de volumes do Amazon Elastic Block Store (Amazon EBS) que são criptografados não é suportada.

Para criar um snapshot do Amazon EBS de um volume de armazenamento no Microsoft Windows

1. Em um computador com Windows, copie alguns dados para o volume de armazenamento mapeado.

O volume de dados copiados não importa para esta demonstração. Um arquivo pequeno é suficiente para demonstrar o processo de restauração.

2. No painel de navegação do console do Storage Gateway, escolha Volumes.
3. Selecione o volume de armazenamento que você criou para o gateway.

Esse gateway deve ter somente um volume de armazenamento. Ao selecionar o volume, suas propriedades são exibidas.

4. Em Actions (Ações), escolha Create EBS Snapshot (Criar snapshot do EBS) para criar um snapshot do volume.

Dependendo do volume de dados no disco e da largura de banda do upload, pode levar alguns segundos para a conclusão do snapshot. Tome nota do ID do volume com o qual você cria um snapshot. Você usará o ID para localizar o snapshot.

5. Na caixa de diálogo Create EBS Snapshot (Criar snapshot do EBS), forneça uma descrição para o snapshot.

6. (Opcional) Em Tags, insira uma chave e um valor para adicionar tags ao snapshot. Uma tag é um par de chave/valor que diferencia maiúsculas de minúsculas e ajuda você a gerenciar, filtrar e pesquisar seus snapshots.
7. Escolha Create Snapshot (Criar snapshot). O snapshot é armazenado como um snapshot do Amazon EBS. Anote o ID do snapshot. O número de snapshots criados para seu volume é exibido na coluna de snapshots.
8. Em Snapshots do EBS, escolha o link do volume para o qual você criou o snapshot e veja o snapshot do EBS no console do Amazon EC2.

Como restaurar um snapshot para outro volume

Consulte [Como criar um volume](#).

Para onde ir agora?

Nas seções anteriores, você criou e provisionou um gateway e em seguida conectou o host ao volume de armazenamento do gateway. Você adicionou dados ao volume iSCSI do gateway, obteve um snapshot e o restaurou para um novo volume e conectou-se a esse novo volume e confirmou se os dados estavam ali.

Assim que concluir este exercício, considere o seguinte:

- Se tiver intenção de continuar a usar seu gateway, deverá obter informações sobre como dimensionar apropriadamente o buffer de upload para cargas de trabalho reais. Para ter mais informações, consulte [Como dimensionar o volume de armazenamento do gateway para cargas de trabalho reais](#).
- Se não tiver intenção de continuar a usar seu gateway, pense na possibilidade de excluir o gateway para evitar cobranças. Para ter mais informações, consulte [Limpar os recursos dos quais não necessita](#).

Outras seções deste guia incluem informações sobre como fazer o seguinte:

- Para saber mais sobre volumes de armazenamento e como gerenciá-los (consulte [Como gerenciar seu gateway](#)).
- Para solucionar problemas de gateway (consulte [Solução de problemas em seu gateway](#)).
- Para otimizar o gateway (consulte [Como otimizar o desempenho de um gateway](#)).

- Para saber mais sobre as métricas do Storage Gateway e saber como monitorar o desempenho do gateway, consulte [Como monitorar o Storage Gateway](#).
- Para saber mais sobre como configurar destinos de iSCSI do gateway para armazenar dados, consulte [Como conectar volumes a um cliente Windows](#).

Para saber mais sobre como dimensionar seu volume de armazenamento do gateway de volumes para workloads reais e limpar recursos que você não precisa, consulte as seções a seguir.

Como dimensionar o volume de armazenamento do gateway para cargas de trabalho reais

A essa altura, você tem um gateway simples e funcional. No entanto, as suposições usadas para criar o gateway não são adequadas para as cargas de trabalho reais. Se desejar usar esse gateway para cargas de trabalho reais, precisará fazer duas coisas:

1. Dimensionar adequadamente o buffer de upload.
2. Configurar o monitoramento do buffer de upload, se ainda não tiver feito isso.

A seguir você pode encontrar informações sobre como executar essas tarefas. Se tiver ativado um gateway para volumes armazenados em cache, precisará também dimensionar o armazenamento em cache para cargas de trabalho reais.

Para dimensionar o buffer de upload e o armazenamento em cache para uma configuração de gateway de armazenamento em cache

- Use a fórmula mostrada em [Como determinar o tamanho do buffer de upload para alocar](#) para dimensionar o buffer de upload. É altamente recomendável reservar pelo menos 150 GiB para o buffer de upload. Se a fórmula do buffer de upload gerar um valor inferior a 150 GiB, use 150 GiB como valor alocado ao buffer de upload.

A fórmula do buffer de upload leva em consideração a diferença entre a taxa de transferência do aplicativo para o gateway e a taxa de transferência do gateway para AWS, multiplicada pelo tempo que você espera gravar dados. Por exemplo, suponha que seus aplicativos gravem dados de texto no gateway a uma taxa de 40 MB por segundo durante 12 horas por dia e a taxa de transferência de rede seja de 12 MB por segundo. Supondo um fator de compressão de 2:1 para os dados de texto, a fórmula específica que você precisa alocar em torno de 675 GiB de espaço do buffer de upload.

Para dimensionar o buffer de upload para uma configuração armazenada

- Use a fórmula examinada em [Como determinar o tamanho do buffer de upload para alocar](#). É altamente recomendável reservar pelo menos 150 GiB para seu buffer de upload. Se a fórmula do buffer de upload gerar um valor inferior a 150 GiB, use 150 GiB como valor alocado ao buffer de upload.

A fórmula do buffer de upload leva em consideração a diferença entre a taxa de transferência do aplicativo para o gateway e a taxa de transferência do gateway para AWS, multiplicada pelo tempo que você espera gravar dados. Por exemplo, suponha que seus aplicativos gravem dados de texto no gateway a uma taxa de 40 MB por segundo durante 12 horas por dia e a taxa de transferência de rede seja de 12 MB por segundo. Supondo um fator de compressão de 2:1 para os dados de texto, a fórmula especifica que você precisa alocar em torno de 675 GiB de espaço do buffer de upload.

Para monitorar o buffer de upload

1. Abra o console do Storage Gateway em <https://console.aws.amazon.com/storagegateway/home>.
2. Escolha a guia Gateway e, em seguida, Details. Depois, localize o campo Upload Buffer Used para ver o buffer de upload atual do seu gateway.
3. Defina um ou mais alarmes para notificá-lo sobre o uso do buffer de upload.

É altamente recomendável que você crie um ou mais alarmes de buffer de upload no console da Amazon CloudWatch. Por exemplo, você pode definir um alarme para um nível de uso sobre o qual você deseja ser avisado e um alerta para um nível de uso que, se superado, é um motivo para agir. Essa ação pode ser ampliar o espaço do buffer de upload. Para ter mais informações, consulte [Para definir um alarme com limite superior para o buffer de upload de um gateway](#).

Limpar os recursos dos quais não necessita

Se você criou o gateway como exercício de exemplo ou um teste, pense na possibilidade de limpá-lo para evitar encargos inesperados ou desnecessários.

Para limpar os recursos dos quais você não necessita

1. Exclua todos os snapshots. Para obter instruções, consulte [Excluir um snapshot](#).

2. Se você não pretende continuar usando o gateway, exclua-o. Para ter mais informações, consulte [Como excluir seu gateway usando o console do AWS Storage Gateway e como limpar os recursos associados](#).
3. Exclua a VM do Storage Gateway do host on-premises. Se tiver criado seu gateway em uma instância do Amazon EC2, encerre a instância.

Fazer backup de seus volumes

Ao usar o Storage Gateway, é possível ajudar a proteger suas aplicações de negócios on-premises que usam os volumes do Storage Gateway para o armazenamento de backup em nuvem. É possível fazer backup dos volumes do Storage Gateway on-premises usando o programador de snapshots nativo no Storage Gateway ou no AWS Backup. Em ambos os casos, os backups de volume do Storage Gateway são armazenados como snapshots do Amazon EBS na Amazon Web Services.

Tópicos

- [Como usar o Storage Gateway para fazer backup dos volumes](#)
- [Usando AWS Backup para fazer backup de seus volumes](#)

Como usar o Storage Gateway para fazer backup dos volumes

É possível usar o Storage Gateway Management Console para fazer backup de seus volumes tirando snapshots do Amazon EBS e armazenando os snapshots na Amazon Web Services. É possível tirar um snapshot ad hoc (uma única vez) ou configurar uma programação de snapshots que seja gerenciada pelo Storage Gateway. É possível restaurar o snapshot para um novo volume posteriormente usando o console do Storage Gateway. Para obter informações sobre como fazer backup e gerenciar o seu backup no Storage Gateway, consulte os seguintes tópicos:

- [Como testar um gateway](#)
- [Como criar um único snapshot](#)
- [Como clonar um volume](#)

Usando AWS Backup para fazer backup de seus volumes

AWS Backup é um serviço de backup centralizado que torna fácil e econômico fazer backup dos dados do seu aplicativo em vários AWS serviços, tanto na Amazon Web Services Cloud quanto no local. Isso ajuda você a atender aos requisitos comerciais e regulatórios de conformidade de backup.

AWS Backup simplifica a proteção AWS de seus volumes de armazenamento, bancos de dados e sistemas de arquivos, fornecendo um local central onde você pode fazer o seguinte:

- Configure e audite os AWS recursos dos quais você deseja fazer backup.
- Automatizar a programação de backups.
- Definir políticas de retenção.
- Monitorar todas as atividades recentes de backup e restauração.

Como o Storage Gateway se integra ao AWS Backup, ele permite que os clientes AWS Backup façam backup de aplicativos comerciais locais que usam volumes do Storage Gateway para armazenamento baseado em nuvem. AWS Backup suporta backup e restauração de volumes armazenados e em cache. Para obter informações sobre AWS Backup, consulte a AWS Backup documentação. Para obter informações sobre AWS Backup, consulte [O que é AWS Backup?](#) no Guia do AWS Backup usuário.

Você pode gerenciar as operações de backup e recuperação dos volumes do Storage Gateway AWS Backup e evitar a necessidade de criar scripts personalizados ou gerenciar point-in-time backups manualmente. Com AWS Backup, você também pode monitorar seus backups de volume locais junto com seus AWS recursos na nuvem a partir de um único AWS Backup painel. Você pode usar AWS Backup para criar um backup único sob demanda ou definir um plano de backup que seja gerenciado em. AWS Backup

Os backups de volume do Storage Gateway retirados AWS Backup são armazenados no Amazon S3 como snapshots do Amazon EBS. Você pode ver os backups de volume do Storage Gateway no AWS Backup console ou no console do Amazon EBS.

Você pode restaurar facilmente os volumes do Storage Gateway que são gerenciados por meio AWS Backup de qualquer gateway local ou gateway na nuvem. Também é possível restaurar esse volume para um volume do Amazon EBS que pode ser usado com instâncias do Amazon EC2.

Benefícios do uso AWS Backup para fazer backup de volumes do Storage Gateway

Os benefícios de usar AWS Backup para fazer backup de volumes do Storage Gateway são que você pode atender aos requisitos de conformidade, evitar sobrecarga operacional e centralizar o gerenciamento de backup. AWS Backup permite que você faça o seguinte:

- Definir políticas personalizáveis de backups programados que atendam aos seus requisitos de backup.

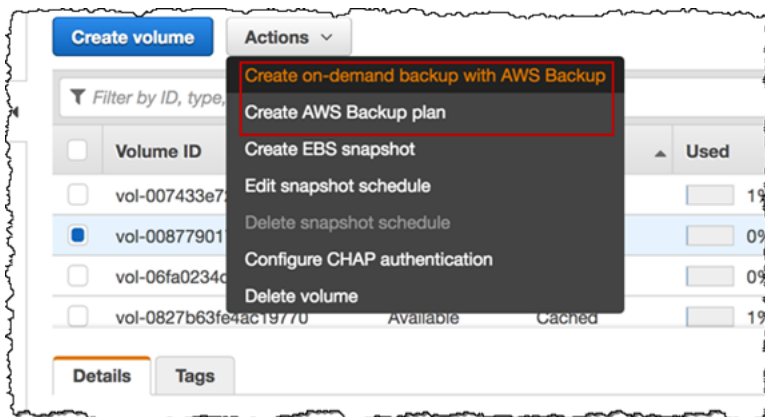
- Defina regras de retenção e expiração de backup para que você não precise mais desenvolver scripts personalizados ou gerenciar manualmente os point-in-time backups de seus volumes.
- Gerencie e monitore backups em vários gateways e outros AWS recursos a partir de uma visão central.

Para usar AWS Backup para criar backups de seus volumes

Note

AWS Backup exige que você escolha uma função AWS Identity and Access Management (IAM) que AWS Backup consuma. Você precisa criar essa função porque ela AWS Backup não a cria para você. Você também precisa criar uma relação de confiança AWS Backup entre essa função do IAM. Para obter informações sobre como fazer isso, consulte Guia do usuário do AWS Backup . Para obter informações sobre como fazer isso, consulte [Como criar um plano de backup](#) no Guia do usuário do AWS Backup .

1. Abra o console do Storage Gateway e selecione Volumes no painel de navegação à esquerda.
2. Em Ações, escolha Criar backup sob demanda com AWS Backup ou Criar plano AWS de backup.



Se você quiser criar um backup sob demanda do volume do Storage Gateway, escolha Criar backup sob demanda com. AWS Backup Você é direcionado para o AWS Backup console.

Create on-demand backup

Settings

Resource
Specify the AWS resource that you want to backup

Resource type: Volume ID: [Refresh](#)

Backup window

Create Backup now
 Customize backup window

Lifecycle
Specify when this backup is transitioned to cold storage or is expired [Info](#)

Move to cold date
N/A

Expire

Backup Vault

Se você quiser criar um novo AWS Backup plano, escolha Criar plano AWS de backup. Você é direcionado para o AWS Backup console.

Create backup plan

Start options

Choose how you want to begin. [Info](#)

Build a new plan
Enter configuration details to create a new backup plan.

Start from an existing plan
Create a new backup plan based on an existing backup plan, including plans created by AWS.

Define a plan using JSON [Info](#)

Backup plan name

Backup plan name is case sensitive. Must contain from 1 to 63 alphanumeric characters or hyphens.

No AWS Backup console, você pode criar um plano de backup, atribuir um volume do Storage Gateway ao plano de backup e criar um backup. Você também pode executar tarefas de gerenciamento de backups em andamento.

Como descobrir e restaurar seus volumes do AWS Backup

Você pode encontrar e restaurar seus volumes de backup do Storage Gateway a partir do AWS Backup console. Para obter mais informações, consulte o AWS Backup Guia do Usuário. Para obter mais informações, consulte [Pontos de recuperação](#) no Guia do usuário do AWS Backup .

Para localizar e restaurar seus volumes

1. Abra o AWS Backup console e encontre o backup de volume do Storage Gateway que você deseja restaurar. É possível restaurar o backup do volume do Storage Gateway em um volume do Amazon EBS ou em um volume do Storage Gateway. Escolha a opção adequada para os seus requisitos de restauração.
2. Em Tipo de restauração, opte por restaurar um volume do Storage Gateway armazenado ou não em cache e forneça as informações necessárias:
 - Para um volume armazenado, forneça as informações em Gateway name (Nome do gateway), Disk ID (ID do disco) e iSCSI target name (Nome de destino do iSCSI).

Restore backup

Settings

Snapshot ID
snap-068e1ef065c6f2704

Resource type
Specify the type of AWS resource to create when restoring this backup

EBS volume

Storage Gateway volume

Gateway
temp [dropdown]

iSCSI target name
[input field]

1 to 200 characters including a-z, 0-9, and "-;"

- Para um volume armazenado em cache, forneça as informações em Gateway name (Nome do gateway), Capacity (Capacidade) e iSCSI target name (Nome de destino do iSCSI).

Restore backup

Settings

Snapshot ID
snap-068e1ef065c6f2704

Resource type
Specify the type of AWS resource to create when restoring this backup

EBS volume

Storage Gateway volume

Gateway
v-thinstaller-centos-1

Capacity
TiB

iSCSI target name
1 to 200 characters including a-z, 0-9, and "-;"

3. Selecione Restore resource (Restaurar recurso) para restaurar seu volume.

Note

Você não pode usar o console do Amazon EBS para excluir um snapshot criado por AWS Backup

Como ativar o gateway em uma nuvem privada virtual

É possível criar uma conexão privada entre o dispositivo do gateway on-premises e a infraestrutura de armazenamento baseada em nuvem. Você pode usar essa conexão para ativar seu gateway e permitir que ele transfira dados para serviços AWS de armazenamento sem se comunicar pela Internet pública. Usando o serviço Amazon VPC, você pode lançar AWS recursos, incluindo endpoints de interface de rede privada, em uma nuvem privada virtual (VPC) personalizada. Uma

VPC dá controle para que você controle as configurações de rede, como o intervalo de endereços IP, sub-redes, tabelas de rotas e gateways de rede. Para saber mais sobre a Amazon VPC, consulte [O que é Amazon VPC?](#) no Manual do usuário da Amazon VPC.

Para ativar seu gateway em uma VPC, use o console da Amazon VPC para criar um endpoint da VPC para o Storage Gateway, obter o ID do endpoint da VPC, e especifique esse ID de endpoint da VPC ao criar e ativar o gateway. Para obter mais informações, consulte [conectar seu gateway de volume AWS](#) a.

Note

O gateway deve ser ativado na mesma região em que criou o endpoint da VPC para o Storage Gateway

Tópicos

- [Como criar um endpoint da VPC para o Storage Gateway](#)

Como criar um endpoint da VPC para o Storage Gateway

Siga estas instruções para criar um VPC endpoint. Se você já tem um endpoint da VPC para Storage Gateway, é possível usá-lo para ativar seu gateway.

Para criar um endpoint da VPC para o Storage Gateway

1. [Faça login AWS Management Console e abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.](https://console.aws.amazon.com/vpc/)
2. No painel de navegação, selecione Endpoints e Criar endpoint.
3. Na página Criar Endpoint, selecione Serviços da AWS para Categoria de serviço.
4. Em Service Name (Nome do serviço), escolha com .amazonaws.*region*.storagegateway. Por exemplo, com.amazonaws.us-east-2.storagegateway.
5. Para VPC, selecione a VPC e anote as zonas de disponibilidade e sub-redes.
6. Verifique se Enable Private DNS Name (Habilitar nome de DNS privado) não está selecionado.
7. Para Security group (Grupo de segurança), escolha o grupo de segurança que você deseja usar para a VPC. Você pode aceitar o grupo de segurança padrão. Verifique se todas as portas TCP a seguir são permitidas no seu grupo de segurança:

- TCP 443
 - TCP 1026
 - TCP 1027
 - TCP 1028
 - TCP 1031
 - TCP 2222
8. Escolha Criar endpoint. O estado inicial do endpoint é pending (pendente). Quando o endpoint for criado, anote o ID do VPC endpoint que você acabou de criar.
 9. Quando o endpoint for criado, escolha Endpoints e, depois, o novo VPC endpoint.
 10. Na guia Detalhes do endpoint do gateway de armazenamento selecionado, em Nomes DNS, use o primeiro nome DNS que não especifique uma zona de disponibilidade. O nome DNS será semelhante a este: `vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com`

Agora que você tem um VPC endpoint, poderá criar seu gateway. Para obter mais informações, consulte [Como criar um gateway](#).

Como gerenciar seu gateway

O gerenciamento de um gateway inclui tarefas como configuração de armazenamento em cache e espaço do buffer de upload, a utilização de volumes ou fitas virtuais e a realização da manutenção geral. Se você não tiver criado um gateway, consulte [Conceitos básicos](#).

Os lançamentos do software de gateway regularmente incluem atualizações do sistema operacional e patches de segurança que foram validados. Estas atualizações são aplicadas como parte do processo regular de atualização do gateway durante uma janela de manutenção programada e normalmente são lançadas a cada seis meses. Observação: os usuários devem tratar o dispositivo Storage Gateway como uma máquina virtual gerenciada e não devem tentar acessar ou modificar a instância do dispositivo Storage Gateway. A tentativa de instalar ou atualizar qualquer pacote de software usando outros métodos (por exemplo: ferramentas SSM ou Hypervisor) além do mecanismo normal de atualização do gateway pode resultar na interrupção do funcionamento adequado do Gateway.

Tópicos

- [Como gerenciar seu gateway de volume](#)
- [Como mover seus dados para um novo gateway](#)

Como gerenciar seu gateway de volume


A seguir, é possível encontrar informações sobre como gerenciar os recursos do gateway de volumes.

Os volumes armazenados em cache são volumes no Amazon Simple Storage Service (Amazon S3) expostos como destinos iSCSI, nos quais é possível armazenar dados de aplicações. Você pode encontrar informações a seguir sobre como adicionar e excluir volumes para a configuração de armazenamento em cache. Você também pode aprender como adicionar e remover volumes do Amazon Elastic Block Store (Amazon EBS) em gateways do Amazon EC2.

Tópicos

- [Como editar as informações básicas do gateway](#)
- [Como adicionar um volume](#)
- [Como ampliar o tamanho de um volume](#)

- [Como clonar um volume](#)
- [Visualização de uso do volume](#)
- [Redução da quantidade de armazenamento faturado em um volume](#)
- [Exclusão de um volume](#)
- [Mover seus volumes para um gateway diferente](#)
- [Como criar um único snapshot](#)
- [Como editar uma programação de snapshots](#)
- [Excluir um snapshot](#)
- [Noções básicas sobre transições e status de volumes](#)

 Important

Se um volume armazenado em cache mantiver os dados principais no Amazon S3, você deve evitar processos que leiam ou gravem todos os dados no volume inteiro. Por exemplo, não recomendamos o uso de software antivírus que examina todo o volume armazenado em cache. Esse tipo de verificação, seja sob demanda ou programada, faz com que todos os dados armazenados no Amazon S3 sejam baixados localmente para verificação, e isso requer o uso de alta largura de banda. Em vez de realizar uma verificação completa do disco, você pode usar a verificação de vírus em tempo real, ou seja, a verificação de dados à medida que eles são lidos ou gravados no volume armazenado em cache.

Não é possível redimensionar um volume. Para alterar o tamanho de um volume, crie um snapshot do volume e em seguida crie um novo volume armazenado em cache por meio do snapshot. O novo volume pode ser maior do que o volume com base no qual o snapshot foi criado. Para as etapas que descrevem como remover um volume, consulte [Para excluir um volume](#). Para as etapas que descrevem como adicionar um volume e preservar os dados existentes, consulte [Exclusão de um volume](#).

Todos os dados do volume armazenado em cache e todos os dados de snapshot são armazenados no Amazon S3 e criptografados em repouso por meio da criptografia do lado do servidor (SSE). No entanto, não é possível acessar esses dados com a API do Amazon S3 ou outras ferramentas como o Amazon S3 Management Console.

Como editar as informações básicas do gateway

Você pode usar o console do Storage Gateway para editar informações básicas de um gateway existente, incluindo o nome do gateway, o fuso horário e o grupo de CloudWatch registros.

Para editar informações básicas de um gateway existente

1. Abra o console do Storage Gateway em <https://console.aws.amazon.com/storagegateway/home>.
2. Escolha Gateways e escolha o gateway para o qual você deseja editar as informações básicas.
3. No menu suspenso Ações, escolha Editar informações do gateway.
4. Modifique as configurações que você deseja alterar e escolha Salvar.

Note

Alterar o nome de um gateway desconectará todos CloudWatch os alarmes configurados para monitorar o gateway. Para reconectar os alarmes, atualize o GatewayName para cada alarme no CloudWatch console.

Como adicionar um volume

É provável que você precisa adicionar mais volumes ao gateway à medida que as necessidades de seu aplicativo aumentarem. Ao adicionar mais volumes, é preciso levar em conta o tamanho do armazenamento em cache e o buffer de upload alocados ao gateway. O gateway deve ter espaço do buffer e espaço de cache suficientes para os novos volumes. Para ter mais informações, consulte [Como determinar o tamanho do buffer de upload para alocar](#).

É possível adicionar volumes usando o console do Storage Gateway ou a API do Storage Gateway. Para obter informações sobre como usar a API Storage Gateway para adicionar volumes, consulte [CreateCachediSCSIVolume](#). Para obter instruções sobre como adicionar um volume usando o console do Storage Gateway, consulte [Como criar um volume](#).

Como ampliar o tamanho de um volume

É provável que você queira ampliar seu volume, em vez de adicionar mais volumes ao gateway, à medida que as necessidades de seu aplicativo aumentarem. Nesse caso, você pode realizar uma das seguintes ações:

- Criar um snapshot do volume que você deseja ampliar e em seguida usar o snapshot para criar um novo volume de tamanho maior. Para obter informações sobre como criar um snapshot, consulte [Como criar um único snapshot](#). Para obter informações sobre como usar um snapshot para criar um novo volume, consulte [Como criar um volume](#).
- Use o volume armazenado em cache que você deseja ampliar para clonar um novo volume de tamanho maior. Para obter informações sobre como clonar um volume, consulte [Como clonar um volume](#). Para obter informações sobre como criar um volume, consulte [Como criar um volume](#).

Como clonar um volume

Você pode criar um novo volume a partir de qualquer volume em cache existente na mesma AWS região. O novo volume é criado a partir do ponto de recuperação mais recente do volume selecionado. Ponto de recuperação é o momento em que todos os dados do volume são consistentes. Para clonar um volume, você pode escolher a opção Clone from last recovery point na caixa de diálogo Create volume e selecionar o volume a ser usado como origem. A captura de tela a seguir mostra a caixa de diálogo Create volume.

The screenshot shows the 'Create volume' dialog box with the following fields and options:

- Gateway:** GatewayCached1
- Capacity:** 100 GiB
- Volume contents:** Clone from last volume recovery point [Learn more](#)
- Source volume:** vol-3507255e
- iSCSI target name:** iqn.1122-03.com.amazon

Buttons: Cancel, Create volume

Clonar com base em um volume existente é mais rápido e mais econômico do que criar um snapshot do Amazon EBS. A clonagem faz uma byte-to-byte cópia dos dados do volume

de origem para o novo volume, usando o ponto de recuperação mais recente do volume de origem. O Storage Gateway cria pontos de recuperação automaticamente para os volumes armazenados em cache. Para ver quando o último ponto de recuperação foi criado, verifique a `TimeSinceLastRecoveryPoint` métrica na Amazon CloudWatch.

O volume clonado é independente do volume de origem. Ou seja, as alterações feitas em ambos os volumes após a clonagem não afetam umas as outras. Por exemplo, se você excluir o volume de origem, isso não terá nenhum efeito sobre o volume clonado. Você pode clonar um volume de origem em uso ativo enquanto os iniciadores estiverem conectados. Isso não afeta o desempenho do volume de origem. Para obter informações sobre como clonar um volume, consulte [Como criar um volume](#).

Você também pode usar o processo de clonagem em situações de recuperação. Para ter mais informações, consulte [O gateway armazenado em cache é inacessível e você deseja recuperar seus dados](#).

Clonar com base em um ponto de recuperação de volume

O procedimento a seguir mostra como clonar um volume com base em um ponto de recuperação de volume e usar esse volume.

Para clonar e usar um volume de um gateway inacessível

1. Abra o console do Storage Gateway em <https://console.aws.amazon.com/storagegateway/home>.
2. No console do Storage Gateway, escolha Criar volume.
3. Na caixa de diálogo Create volume (Criar volume), escolha um gateway em Gateway.
4. Em Capacity (Capacidade), digite a capacidade de seu volume. A capacidade deve ter pelo menos o mesmo tamanho do volume de origem.
5. Escolha Clone from last recovery point e selecione um ID de volume em Source volume. O volume de origem pode ser qualquer volume em cache na AWS região selecionada.

The screenshot shows the 'Create volume' dialog box with the following fields and options:

- Gateway:** GatewayCached1
- Capacity:** 100 GIB
- Volume contents:** New empty volume, Based on EBS snapshot, Clone from last volume recovery point [Learn more](#)
- Source volume:** vol-3507255e
- iSCSI target name:** iqn.1122-03.com.amazon

Additional text: 'Volumes must not be larger than 32 TiB.' and '1 to 200 characters including a-z, 0-9, and "-,"'.

6. Digite um nome em iSCSI target name (Nome do destino do iSCSI).

O nome de destino pode conter letras minúsculas, números, pontos (.) e hífen (-). Esse nome de destino aparece como o nome do iSCSI target node (Nó de destino do iSCSI) na guia Targets (Destinos) da interface do iSCSI Microsoft initiator (Iniciador Microsoft iSCSI) após a descoberta. Por exemplo, o nome target1 aparece como iqn.1007-05.com.amazon:target1. Garanta que o nome de destino seja exclusivo globalmente na rede de área de armazenamento (SAN).

7. Verifique se a configuração Network interface tem o endereço IP de seu gateway; do contrário, escolha um endereço IP para Network interface.

Se tiver definido seu gateway para usar vários adaptadores de rede, escolha o endereço IP que seus aplicativos de armazenamento usarão para acessar o volume. Cada adaptador de rede definido para um gateway representa um endereço IP que você pode escolher.

Se a VM do gateway estiver configurada para mais de um adaptador de rede, a caixa de diálogo Create volume (Criar volume) exibirá uma lista para Network interface (Interface de rede). Nesta lista, um endereço IP é exibido para cada adaptador configurado para a VM do gateway. Se a VM do gateway estiver configurada para apenas um adaptador de rede, nenhuma lista será exibida porque só existe um endereço IP.

- Escolha Create volume (Criar volume). A caixa de diálogo Configure CHAP Authentication (Configurar autenticação do CHAP) é exibida. Você pode configurar o CHAP posteriormente. Para obter mais informações, consulte [Como configurar a autenticação CHAP para destinos iSCSI](#).

A próxima etapa é conectar o volume ao seu cliente. Para ter mais informações, consulte [Como conectar volumes ao cliente](#).

Como criar um snapshot de recuperação

O procedimento a seguir mostra como criar um snapshot de um ponto de recuperação de volume e usar esse snapshot. Você pode tirar snapshots uma única vez, para uma finalidade específica, ou configurar uma programação de snapshots para o volume.

Para criar e usar um snapshot de recuperação de volume de um gateway inacessível

- Abra o console do Storage Gateway em <https://console.aws.amazon.com/storagegateway/home>.
- No painel de navegação, selecione Gateways da .
- Escolha o gateway inacessível e selecione a guia Details.

Uma mensagem de snapshot de recuperação é exibida na guia.



- Escolha Create recovery snapshot para abrir a caixa de diálogo Create recovery snapshot.
- Na lista de volumes exibida, escolha o volume que você deseja recuperar e em seguida Create snapshots.

O Storage Gateway inicia o processo de snapshot.

- Localize e restaure o snapshot.

Visualização de uso do volume

Ao gravar dados em um volume, é possível visualizar o volume de dados armazenados no volume no Storage Gateway Management Console. A guia Detalhes de cada volume mostra as informações de uso de volume.

Para visualizar o volume de dados gravados em um volume

1. Abra o console do Storage Gateway em <https://console.aws.amazon.com/storagegateway/home>.
2. No painel de navegação, escolha Volumes e o volume desejado.
3. Escolha a guia Detalhes.

Os campos a seguir fornecem informações sobre o volume:

- Tamanho: a capacidade total do volume selecionado.
- Usado: o tamanho dos dados armazenados no volume.

Note

Esses valores não estão disponíveis para os volumes criados antes de 13 de maio de 2015, até você armazenar dados no volume.

Redução da quantidade de armazenamento faturado em um volume

Excluir arquivos do seu sistema de arquivos não necessariamente exclui dados do dispositivo de blocos subjacente ou reduz a quantidade de dados armazenados no volume. Se você deseja reduzir a quantidade de armazenamento cobrada em seu volume, recomendamos sobrescrever seus arquivos com zeros para compactar o armazenamento a uma pequena quantidade de armazenamento real. O Storage Gateway cobra pelo uso do volume com base no armazenamento compactado.

Note

Se você usar uma ferramenta de exclusão segura que substitui os dados em seu volume por dados aleatórios, seu uso não será reduzido. Isso ocorre porque os dados aleatórios não são compactáveis.

Exclusão de um volume

Talvez você precise excluir um volume quando as necessidades de sua aplicação mudarem: por exemplo, se migrar sua aplicação para usar um volume de armazenamento maior. Antes de excluir um volume, verifique se não há nenhum aplicativo gravando no momento no volume. Além disso, confirme se não há snapshots em andamento para o volume. Se houver uma programação de snapshot definida para o volumes, é possível conferir isso na guia Programações de snapshots do console do Storage Gateway. Para ter mais informações, consulte [Como editar uma programação de snapshots](#).

É possível excluir volumes usando o console do Storage Gateway ou a API do Storage Gateway. Para obter informações sobre como usar a API do Storage Gateway para remover volumes, consulte [Excluir volume](#). O procedimento a seguir demonstra o uso do console.

Antes de excluir um volume, faça backup de seus dados ou obtenha um snapshot dos dados essenciais. No caso de volumes armazenados, seus discos locais não são apagados. Depois de excluir um volume, você não poderá mais obtê-lo de volta.

Para excluir um volume

1. Abra o console do Storage Gateway em <https://console.aws.amazon.com/storagegateway/home>.
2. Escolha Volumes e selecione um ou mais volumes para excluir.
3. Em Ações, escolha Excluir volume. Uma caixa de diálogo de confirmação é exibida.
4. Verifique se você deseja excluir os volumes especificados, digite a palavra excluir na caixa de confirmação e escolha Excluir.

Mover seus volumes para um gateway diferente

À medida que o volume de dados e o desempenho precisarem aumentar, será possível querer mover seus volumes para outro gateway de volumes. Para fazer isso, é possível desanexar e anexar um volume usando o console ou a API do Storage Gateway.

Ao desanexar e anexar um volume, você pode fazer o seguinte:

- Mova os volumes para plataformas host melhores ou instâncias do Amazon EC2 mais recentes.
- Atualize o hardware subjacente para seu servidor.
- Mova seus volumes entre tipos de hipervisor.

Ao desanexar um volume, seu gateway carrega e armazena os metadados e dados do volume para o serviço do Storage Gateway na AWS. Você pode facilmente anexar um volume desanexado a um gateway em qualquer plataforma de hospedagem com suporte posteriormente.

Note

Um volume desanexado é cobrado de acordo com a taxa de armazenamento de volume padrão até que você o exclua. Para obter informações sobre como reduzir sua fatura, consulte [Redução da quantidade de armazenamento faturado em um volume](#).

Note


Há algumas limitações para anexar e desanexar volumes:

- Desanexar um volume pode levar muito tempo. Quando você separa um volume, o gateway carrega todos os dados no volume para AWS antes que o volume seja desanexado. O tempo necessário para a conclusão do carregamento depende da quantidade de dados que precisam ser carregados e da conectividade de rede com a AWS.
- Se você desanexar um volume armazenado em cache, não poderá anexá-lo novamente como um volume armazenado.
- Se você desanexar um volume armazenado, não poderá anexá-lo novamente como um volume armazenado em cache.
- Um volume desanexado não pode ser usado até que seja anexado a um gateway.
- Quando você anexar um volume armazenado, ele precisará ser totalmente restaurado para que você possa anexá-lo a um gateway.
- Quando você começa a anexar ou desanexar um volume, é necessário aguardar até que a operação seja concluída para poder usar o volume.
- Atualmente, a exclusão forçada de um volume tem suporte somente na API.
- Se você excluir um gateway enquanto o volume está sendo desanexado desse gateway, isso resultará na perda de dados. Aguarde até que a operação de desanexar o volume seja concluída antes de excluir o gateway.
- Se um gateway é armazenado no estado de restauração, não é possível desanexar um volume dele.

As etapas a seguir mostram como desanexar e anexar um volume usando o console do Storage Gateway. Para obter mais informações sobre como fazer isso usando a API, consulte [DetachVolume](#) ou [AttachVolume](#) na Referência da AWS Storage Gateway API.

Para desanexar um volume de um gateway

1. Abra o console do Storage Gateway em <https://console.aws.amazon.com/storagegateway/home>.
2. Escolha Volumes e selecione um ou mais volumes para desanexar.
3. Em Actions (Ações), selecione Detach Volume (Desanexar volume). Uma caixa de diálogo de confirmação é exibida.
4. Verifique se você deseja excluir os volumes especificados, digite a palavra desanexar na caixa de confirmação e escolha Desanexar.

 Note

Se um volume que você desanexar tiver uma grande quantidade de dados, ele passará do status Attached (Anexado) para Detaching (Desanexando) até que a conclusão do carregamento de todos os dados. Em seguida, o status é alterado para Detached (Desanexado). Para pequenas quantidades de dados, talvez você não veja o status Detaching (Desanexando). Se o volume não tem dados, o status é alterado de Attached (Anexado) para Detached (Desanexado).

Agora, você pode anexar o volume a um gateway diferente.

Para anexar um volume a um gateway

1. Abra o console do Storage Gateway em <https://console.aws.amazon.com/storagegateway/home>.
2. No painel de navegação, selecione Volumes. O status de cada volume desanexado é exibido como Detached (Anexado).
3. Na lista de volumes desanexados, selecione o volume que você deseja anexar. Você pode anexar apenas um volume por vez.
4. Em Actions (Ações), selecione Attach volume (Anexar volume).
5. Na caixa de diálogo Attach Volume (Anexar volume), selecione o gateway ao qual você deseja anexar o volume e insira o destino do iSCSI ao qual você deseja conectar o volume.

Se você anexar um volume armazenado, insira o identificador de disco em Disk ID (ID do disco).

6. Selecione **Attach volume (Anexar volume)**. Se um volume que você anexar tiver uma grande quantidade de dados, ele passará de **Detached (Desanexado)** para **Attached (Anexado)** se a operação `AttachVolume` for bem-sucedida.
7. No assistente **Configurar autenticação CHAP** que é exibido, insira o **Initiator name (Nome do iniciador)**, o **Initiator secret (Segredo do iniciador)** e o **Target secret (Segredo de destino)** e selecione **Save (Salvar)**. Para obter mais informações sobre como trabalhar com a autenticação do Challenge-Handshake Authentication Protocol (CHAP), consulte [Como configurar a autenticação CHAP para destinos iSCSI](#).

Como criar um único snapshot

Além dos snapshots programados, é possível tirar snapshots únicos (ad hoc) para os gateways de volumes. Desse modo, você pode fazer backup de seu volume de armazenamento imediatamente, sem precisar esperar o próximo snapshot programado.

Para criar um único snapshot de seu volume de armazenamento

1. Abra o console do Storage Gateway em <https://console.aws.amazon.com/storagegateway/home>.
2. No painel de navegação, escolha **Volumes** em seguida o volume do qual você deseja criar o snapshot.
3. Em **Actions (Ações)**, escolha **Create snapshot (Criar snapshot)**.
4. Na caixa de diálogo **Create snapshot**, digite a descrição do snapshot e escolha **Create snapshot**.

Você pode verificar se o snapshot foi criado usando o console.

Seu snapshot é listado em **Snapshots**, na mesma linha do volume.

Como editar uma programação de snapshots

Para volumes armazenados, AWS Storage Gateway cria uma programação padrão de snapshots de uma vez por dia.

Note

Você não pode remover a programação padrão de snapshots. Os volumes armazenados exigem pelo menos uma programação de snapshots. No entanto, é possível alterar uma

programação de snapshots especificando o horário no qual o snapshot é obtido por dia ou a frequência (a cada 1, 2, 4, 8, 12 ou 24 horas), ou ambos.

Para volumes em cache, AWS Storage Gateway não cria um agendamento de instantâneos padrão. Nenhuma programação padrão é criada porque os dados são armazenados no Amazon S3, e portanto você não precisa de snapshots ou de uma programação de snapshots para fins de recuperação de desastres. No entanto, você pode configurar uma programação de snapshots a qualquer momento, se precisa. A criação de snapshots para volumes armazenados em cache é uma opção a mais para recuperar seus dados, se necessário.

Por meio das etapas a seguir, você pode editar a programação de snapshots de um volume.

Para editar o a programação de snapshots de um volume

1. Abra o console do Storage Gateway em <https://console.aws.amazon.com/storagegateway/home>.
2. No painel de navegação, escolha Volumes e em seguida o volume do qual o snapshot foi criado.
3. Em Actions (Ações), escolha Edit snapshot schedule (Editar programação de snapshots).
4. Na caixa de diálogo Edit snapshot schedule, modifique a programação e escolha Save.

Excluir um snapshot

Você pode excluir um snapshot de seu volume de armazenamento. Por exemplo, você pode fazer isso se tiver tirado muitos snapshots de um volume de armazenamento ao longo de um período e não precisar dos snapshots mais antigos. Como os snapshots são backups incrementais, se excluir um snapshot, somente os dados que não são necessários em outros snapshots são excluídos.

Tópicos

- [Como excluir snapshots com o AWS SDK para Java](#)
- [Como excluir snapshots com o AWS SDK para .NET](#)
- [Como excluir snapshots com as AWS Tools for Windows PowerShell](#)

No console do Amazon EBS, é possível excluir um snapshot por vez. Para obter informações sobre como excluir snapshots usando o console do Amazon EBS, consulte [Como excluir um snapshot no Amazon EBS](#) no Guia do usuário do Amazon EC2.

Para excluir vários instantâneos ao mesmo tempo, você pode usar um dos AWS SDKs que oferece suporte às operações do Storage Gateway. Para obter exemplo, consulte [Como excluir snapshots com o AWS SDK para Java](#), [Como excluir snapshots com o AWS SDK para .NET](#) e [Como excluir snapshots com as AWS Tools for Windows PowerShell](#).

Como excluir snapshots com o AWS SDK para Java

Para excluir vários snapshots associados a um volume, você pode usar uma abordagem programática. O exemplo a seguir demonstra como excluir snapshots usando o AWS SDK para Java. Para usar o código de exemplo, você deve estar familiarizado com a execução de aplicativos em console Java. Para obter mais informações, consulte [Conceitos básicos](#) no Guia do desenvolvedor do AWS SDK para Java. Se você precisar excluir apenas alguns snapshots, use o console tal como descrito em [Excluir um snapshot](#).

Example : Excluindo instantâneos usando o AWS SDK for Java

O exemplo de código Java a seguir mostra os snapshots de cada volume do gateway e se o horário de início do snapshot é antes ou depois de uma data específica. Ele usa a API AWS SDK for Java para Storage Gateway e Amazon EC2. A API do Amazon EC2 inclui operações para trabalhar com snapshots.

Atualize o código para fornecer o endpoint de serviço, o nome de recurso da Amazon (ARN) do gateway e o número de dias retroativos para os quais deseja salvar os snapshots. Os snapshots tirados antes desse limite são excluídos. Além disso, você precisa especificar o valor booleano `viewOnly`, que indica se deseja visualizar os snapshots a serem excluídos ou se na verdade deseja excluir os snapshots. Primeiro, execute o código apenas com a opção de visualização (isto é, com `viewOnly` definida como `true`) para ver o que o código excluirá. Para obter uma lista dos endpoints de AWS serviço que você pode usar com o Storage Gateway, consulte [AWS Storage Gateway Endpoints and Quotas](#) no. Referência geral da AWS

```
import java.io.IOException;
import java.util.ArrayList;
import java.util.Calendar;
import java.util.Collection;
import java.util.Date;
import java.util.GregorianCalendar;
import java.util.List;

import com.amazonaws.auth.PropertiesCredentials;
import com.amazonaws.services.ec2.AmazonEC2Client;
import com.amazonaws.services.ec2.model.DeleteSnapshotRequest;
```

```
import com.amazonaws.services.ec2.model.DescribeSnapshotsRequest;
import com.amazonaws.services.ec2.model.DescribeSnapshotsResult;
import com.amazonaws.services.ec2.model.Filter;
import com.amazonaws.services.ec2.model.Snapshot;
import com.amazonaws.services.storagegateway.AWSStorageGatewayClient;
import com.amazonaws.services.storagegateway.model.ListVolumesRequest;
import com.amazonaws.services.storagegateway.model.ListVolumesResult;
import com.amazonaws.services.storagegateway.model.VolumeInfo;

public class ListDeleteVolumeSnapshotsExample {

    public static AWSStorageGatewayClient sgClient;
    public static AmazonEC2Client ec2Client;
    static String serviceURLSG = "https://storagegateway.us-east-1.amazonaws.com";
    static String serviceURLEC2 = "https://ec2.us-east-1.amazonaws.com";

    // The gatewayARN
    public static String gatewayARN = "**** provide gateway ARN ****";

    // The number of days back you want to save snapshots. Snapshots before this cutoff
    are deleted
    // if viewOnly = false.
    public static int daysBack = 10;

    // true = show what will be deleted; false = actually delete snapshots that meet
    the daysBack criteria
    public static boolean viewOnly = true;

    public static void main(String[] args) throws IOException {

        // Create a Storage Gateway and amazon ec2 client
        sgClient = new AWSStorageGatewayClient(new PropertiesCredentials(
ListDeleteVolumeSnapshotsExample.class.getResourceAsStream("AwsCredentials.properties")));

        sgClient.setEndpoint(serviceURLSG);

        ec2Client = new AmazonEC2Client(new PropertiesCredentials(
ListDeleteVolumeSnapshotsExample.class.getResourceAsStream("AwsCredentials.properties")));
        ec2Client.setEndpoint(serviceURLEC2);

        List<VolumeInfo> volumes = ListVolumesForGateway();
        DeleteSnapshotsForVolumes(volumes, daysBack);
    }
}
```

```
}
public static List<VolumeInfo> ListVolumesForGateway()
{
    List<VolumeInfo> volumes = new ArrayList<VolumeInfo>();

    String marker = null;
    do {
        ListVolumesRequest request = new
ListVolumesRequest().withGatewayARN(gatewayARN);
        ListVolumesResult result = sgClient.listVolumes(request);
        marker = result.getMarker();

        for (VolumeInfo vi : result.getVolumeInfos())
        {
            volumes.add(vi);
            System.out.println(OutputVolumeInfo(vi));
        }
    } while (marker != null);

    return volumes;
}
private static void DeleteSnapshotsForVolumes(List<VolumeInfo> volumes,
        int daysBack2) {

    // Find snapshots and delete for each volume
    for (VolumeInfo vi : volumes) {

        String volumeARN = vi.getVolumeARN();
        String volumeId =
volumeARN.substring(volumeARN.lastIndexOf("/") + 1).toLowerCase();
        Collection<Filter> filters = new ArrayList<Filter>();
        Filter filter = new Filter().withName("volume-id").withValues(volumeId);
        filters.add(filter);

        DescribeSnapshotsRequest describeSnapshotsRequest =
            new DescribeSnapshotsRequest().withFilters(filters);
        DescribeSnapshotsResult describeSnapshotsResult =
            ec2Client.describeSnapshots(describeSnapshotsRequest);

        List<Snapshot> snapshots = describeSnapshotsResult.getSnapshots();
        System.out.println("volume-id = " + volumeId);
        for (Snapshot s : snapshots){
            StringBuilder sb = new StringBuilder();
```

```

        boolean meetsCriteria = !CompareDates(daysBack, s.getStartTime());
        sb.append(s.getSnapshotId() + ", " + s.getStartTime().toString());

        sb.append(", meets criteria for delete? " + meetsCriteria);
        sb.append(", deleted? ");
        if (!viewOnly & meetsCriteria) {
            sb.append("yes");
            DeleteSnapshotRequest deleteSnapshotRequest =
                new DeleteSnapshotRequest().withSnapshotId(s.getSnapshotId());
            ec2Client.deleteSnapshot(deleteSnapshotRequest);
        }
        else {
            sb.append("no");
        }
        System.out.println(sb.toString());
    }
}

private static String OutputVolumeInfo(VolumeInfo vi) {

    String volumeInfo = String.format(
        "Volume Info:\n" +
        "  ARN: %s\n" +
        "  Type: %s\n",
        vi.getVolumeARN(),
        vi.getVolumeType());
    return volumeInfo;
}

// Returns the date in two formats as a list
public static boolean CompareDates(int daysBack, Date snapshotDate) {
    Date today = new Date();
    Calendar cal = new GregorianCalendar();
    cal.setTime(today);
    cal.add(Calendar.DAY_OF_MONTH, -daysBack);
    Date cutoffDate = cal.getTime();
    return (snapshotDate.compareTo(cutoffDate) > 0) ? true : false;
}
}

```


Como excluir snapshots com o AWS SDK para .NET

Para excluir vários snapshots associados a um volume, você pode usar uma abordagem programática. O exemplo a seguir demonstra como excluir snapshots usando o AWS SDK para .NET versões 2 e 3. Para usar o código de exemplo, você deve estar familiarizado com a execução de aplicativos em console do .NET. Para obter mais informações, consulte [Conceitos básicos](#) no Guia do desenvolvedor do AWS SDK para .NET. Se você precisar excluir apenas alguns snapshots, use o console tal como descrito em [Excluir um snapshot](#).

Example : Excluindo instantâneos usando o AWS SDK para .NET

No exemplo de código C# a seguir, um AWS Identity and Access Management usuário pode listar os instantâneos de cada volume de um gateway. O usuário pode determinar se o horário de início do snapshot deve ser antes ou depois de uma determinada data (período de retenção) e excluir os snapshots que tenham passado do período de retenção. Ele usa a API do AWS SDK para .NET para o Storage Gateway e o Amazon EC2. A API do Amazon EC2 inclui operações para trabalhar com snapshots.

O exemplo de código a seguir usa o AWS SDK para .NET versões 2 e 3. Você pode migrar as versões anteriores do .NET para a versão mais recente. Para obter mais informações, consulte [Como migrar seu código para a versão mais recente do AWS SDK para .NET](#).

Atualize o código para fornecer o endpoint de serviço, o nome de recurso da Amazon (ARN) do gateway e o número de dias retroativos para os quais deseja salvar os snapshots. Os snapshots tirados antes desse limite são excluídos. Além disso, você precisa especificar o valor booleano `viewOnly`, que indica se deseja visualizar os snapshots a serem excluídos ou se na verdade deseja excluir os snapshots. Primeiro, execute o código apenas com a opção de visualização (isto é, com `viewOnly` definida como `true`) para ver o que o código excluirá. Para obter uma lista dos endpoints de AWS serviço que você pode usar com o Storage Gateway, consulte [AWS Storage Gateway Endpoints and Quotas](#) no. Referência geral da AWS

Primeiro, você cria um usuário e anexa a política mínima do IAM ao usuário. Em seguida, você pode programar snapshots automatizados para seu gateway.

O código a seguir cria a política mínima que permite que um usuário do IAM exclua snapshots. Neste exemplo, a política é denominada **sgw-delete-snapshot**.

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

```
{
  "Sid": "StmtEC2Snapshots",
  "Effect": "Allow",
  "Action": [
    "ec2:DeleteSnapshot",
    "ec2:DescribeSnapshots"
  ],
  "Resource": [
    "*"
  ]
},
{
  "Sid": "StmtSgwListVolumes",
  "Effect": "Allow",
  "Action": [
    "storagegateway:ListVolumes"
  ],
  "Resource": [
    "*"
  ]
}
]
```

O código C# a seguir localiza todos os snapshots no gateway especificado que correspondem aos volumes e ao período limite especificado, e os exclui em seguida.

```
using System;
using System.Collections.Generic;
using System.Text;
using Amazon.EC2;
using Amazon.EC2.Model;
using Amazon.StorageGateway.Model;
using Amazon.StorageGateway;

namespace DeleteStorageGatewaySnapshotNS
{
    class Program
    {
        /*
         * Replace the variables below to match your environment.
         */
    }
}
```

```
/* IAM AccessKey */
static String AwsAccessKey = "AKIA.....";

/* IAM SecretKey */
static String AwsSecretKey = "*****";

/* Account number, 12 digits, no hyphen */
static String OwnerID = "123456789012";

/* Your Gateway ARN. Use a Storage Gateway ID, sgw-XXXXXXX* */
static String GatewayARN = "arn:aws:storagegateway:ap-
southeast-2:123456789012:gateway/sgw-XXXXXXX";

/* Snapshot status: "completed", "pending", "error" */

static String SnapshotStatus = "completed";

/* Region where your gateway is activated */
static String AwsRegion = "ap-southeast-2";

/* Minimum age of snapshots before they are deleted (retention policy) */
static int daysBack = 30;

/*
 * Do not modify the four lines below.
 */
static AmazonEC2Config ec2Config;
static AmazonEC2Client ec2Client;
static AmazonStorageGatewayClient sgClient;
static AmazonStorageGatewayConfig sgConfig;

static void Main(string[] args)
{
    // Create an EC2 client.
    ec2Config = new AmazonEC2Config();
    ec2Config.ServiceURL = "https://ec2." + AwsRegion + ".amazonaws.com";
    ec2Client = new AmazonEC2Client(AwsAccessKey, AwsSecretKey, ec2Config);

    // Create a Storage Gateway client.
    sgConfig = new AmazonStorageGatewayConfig();
    sgConfig.ServiceURL = "https://storagegateway." + AwsRegion +
".amazonaws.com";
    sgClient = new AmazonStorageGatewayClient(AwsAccessKey, AwsSecretKey,
sgConfig);
}
```

```

        List<VolumeInfo> StorageGatewayVolumes = ListVolumesForGateway();
        List<Snapshot> StorageGatewaySnapshots =
ListSnapshotsForVolumes(StorageGatewayVolumes,
                                daysBack);
        DeleteSnapshots(StorageGatewaySnapshots);
    }

    /**
     * List all volumes for your gateway
     * returns: A list of VolumeInfos, or null.
     */
    private static List<VolumeInfo> ListVolumesForGateway()
    {
        ListVolumesResponse response = new ListVolumesResponse();
        try
        {
            ListVolumesRequest request = new ListVolumesRequest();
            request.GatewayARN = GatewayARN;
            response = sgClient.ListVolumes(request);

            foreach (VolumeInfo vi in response.VolumeInfos)
            {
                Console.WriteLine(OutputVolumeInfo(vi));
            }
        }
        catch (AmazonStorageGatewayException ex)
        {
            Console.WriteLine(ex.Message);
        }
        return response.VolumeInfos;
    }

    /**
     * Gets the list of snapshots that match the requested volumes
     * and cutoff period.
     */
    private static List<Snapshot> ListSnapshotsForVolumes(List<VolumeInfo> volumes,
int snapshotAge)
    {
        List<Snapshot> SelectedSnapshots = new List<Snapshot>();
        try
        {
            foreach (VolumeInfo vi in volumes)

```

```
{
    String volumeARN = vi.VolumeARN;
    String volumeID = volumeARN.Substring(volumeARN.LastIndexOf("/") +
1).ToLower();

    DescribeSnapshotsRequest describeSnapshotsRequest = new
DescribeSnapshotsRequest();

    Filter ownerFilter = new Filter();
    List<String> ownerValues = new List<String>();
    ownerValues.Add(OwnerID);
    ownerFilter.Name = "owner-id";
    ownerFilter.Values = ownerValues;
    describeSnapshotsRequest.Filters.Add(ownerFilter);

    Filter statusFilter = new Filter();
    List<String> statusValues = new List<String>();
    statusValues.Add(SnapshotStatus);
    statusFilter.Name = "status";
    statusFilter.Values = statusValues;
    describeSnapshotsRequest.Filters.Add(statusFilter);

    Filter volumeFilter = new Filter();
    List<String> volumeValues = new List<String>();
    volumeValues.Add(volumeID);
    volumeFilter.Name = "volume-id";
    volumeFilter.Values = volumeValues;
    describeSnapshotsRequest.Filters.Add(volumeFilter);

    DescribeSnapshotsResponse describeSnapshotsResponse =
    ec2Client.DescribeSnapshots(describeSnapshotsRequest);

    List<Snapshot> snapshots = describeSnapshotsResponse.Snapshots;
    Console.WriteLine("volume-id = " + volumeID);
    foreach (Snapshot s in snapshots)
    {
        if (IsSnapshotPastRetentionPeriod(snapshotAge, s.StartTime))
        {
            Console.WriteLine(s.SnapshotId + ", " + s.VolumeId + ",
                " + s.StartTime + ", " + s.Description);
            SelectedSnapshots.Add(s);
        }
    }
}
```

```
    }
    catch (AmazonEC2Exception ex)
    {
        Console.WriteLine(ex.Message);
    }
    return SelectedSnapshots;
}

/**
 * Deletes a list of snapshots.
 */
private static void DeleteSnapshots(List<Snapshot> snapshots)
{
    try
    {
        foreach (Snapshot s in snapshots)
        {
            DeleteSnapshotRequest deleteSnapshotRequest = new
DeleteSnapshotRequest(s.SnapshotId);
            DeleteSnapshotResponse response =
ec2Client.DeleteSnapshot(deleteSnapshotRequest);
            Console.WriteLine("Volume: " +
                s.VolumeId +
                " => Snapshot: " +
                s.SnapshotId +
                " Response: "
                + response.HttpStatusCode.ToString());
        }
    }
    catch (AmazonEC2Exception ex)
    {
        Console.WriteLine(ex.Message);
    }
}

/**
 * Checks if the snapshot creation date is past the retention period.
 */
private static Boolean IsSnapshotPastRetentionPeriod(int daysBack, DateTime
snapshotDate)
{
    DateTime cutoffDate = DateTime.Now.Add(new TimeSpan(-daysBack, 0, 0, 0));
    return (DateTime.Compare(snapshotDate, cutoffDate) < 0) ? true : false;
}
```

```
    }

    /*
     * Displays information related to a volume.
     */
    private static String OutputVolumeInfo(VolumeInfo vi)
    {
        String volumeInfo = String.Format(
            "Volume Info:\n" +
            "  ARN: {0}\n" +
            "  Type: {1}\n",
            vi.VolumeARN,
            vi.VolumeType);
        return volumeInfo;
    }
}
}
```

Como excluir snapshots com as AWS Tools for Windows PowerShell

Para excluir vários snapshots associados a um volume, você pode usar uma abordagem programática. O exemplo a seguir demonstra como excluir snapshots usando o AWS Tools for Windows PowerShell. Para usar o script de exemplo, você deve estar familiarizado com a execução de um PowerShell script. Para obter mais informações, consulte [Conceitos básicos](#) no AWS Tools for Windows PowerShell. Se você precisar excluir somente alguns snapshots, use o console tal como descrito em [Excluir um snapshot](#).

Example : Excluindo instantâneos usando o AWS Tools for Windows PowerShell

O exemplo de PowerShell script a seguir lista os instantâneos de cada volume de um gateway e se a hora de início do instantâneo é antes ou depois de uma data especificada. Ele usa os AWS Tools for Windows PowerShell cmdlets do Storage Gateway e do Amazon EC2. A API do Amazon EC2 inclui operações para trabalhar com snapshots.

Você precisa atualizar o script e fornecer o nome de recurso da Amazon (ARN) do gateway e o número de dias retroativos para os quais deseja salvar os snapshots. Os snapshots tirados antes desse limite são excluídos. Além disso, você precisa especificar o valor booleano `viewOnly`, que indica se deseja visualizar os snapshots a serem excluídos ou se na verdade deseja excluir os snapshots. Primeiro, execute o código apenas com a opção de visualização (isto é, com `viewOnly` definida como `true`) para ver o que o código excluirá.

```
<#
.DESCRPTION
    Delete snapshots of a specified volume that match given criteria.

.NOTES
    PREREQUISITES:
    1) AWS Tools for Windows PowerShell from https://aws.amazon.com/powershell/
    2) Credentials and AWS Region stored in session using Initialize-AWSDefault.
    For more info see, https://docs.aws.amazon.com/powershell/latest/userguide/specifying-your-aws-credentials.html

.EXAMPLE
    powershell.exe .\SG_DeleteSnapshots.ps1
#>

# Criteria to use to filter the results returned.
$daysBack = 18
$gatewayARN = "**** provide gateway ARN ****"
$viewOnly = $true;

#ListVolumes
$volumesResult = Get-SGVolume -GatewayARN $gatewayARN
$volumes = $volumesResult.VolumeInfos
Write-Output("`nVolume List")
foreach ($volumes in $volumesResult)
{ Write-Output("`nVolume Info:")
  Write-Output("ARN: " + $volumes.VolumeARN)
  write-Output("Type: " + $volumes.VolumeType)
}

Write-Output("`nWhich snapshots meet the criteria?")
foreach ($volume in $volumesResult)
{
  $volumeARN = $volume.VolumeARN

  $volumeId = ($volumeARN-split"/")[3].ToLower()

  $filter = New-Object Amazon.EC2.Model.Filter
  $filter.Name = "volume-id"
  $filter.Value.Add($volumeId)

  $snapshots = get-EC2Snapshot -Filter $filter
  Write-Output("`nFor volume-id = " + $volumeId)
```



```
foreach ($s in $snapshots)
{
    $d = ([DateTime]::Now).AddDays(-$daysBack)
    $meetsCriteria = $false
    if ([DateTime]::Compare($d, $s.StartTime) -gt 0)
    {
        $meetsCriteria = $true
    }

    $sb = $s.SnapshotId + ", " + $s.StartTime + ", meets criteria for delete? " +
    $meetsCriteria
    if (!$viewOnly -AND $meetsCriteria)
    {
        $resp = Remove-EC2Snapshot -SnapshotId $s.SnapshotId
        #Can get RequestId from response for troubleshooting.
        $sb = $sb + ", deleted? yes"
    }
    else {
        $sb = $sb + ", deleted? no"
    }
    Write-Output($sb)
}
}
```

Noções básicas sobre transições e status de volumes

Todo volume tem um status associado que indica rapidamente a integridade do volume. Na maioria das vezes, o status indica que o volume está funcionando normalmente e que nenhuma ação é necessária de sua parte. Em alguns casos, o status indica um problema com o volume que pode ou não exigir uma ação de sua parte. Você pode encontrar informações a seguir para ajudá-lo a decidir em que momento precisa agir. [Você pode ver o status do volume no console do Storage Gateway ou usando uma das operações da API do Storage Gateway, por exemplo DescribeCachediSCSIVolumes ou DescribeStorediSCSIVolumes.](#)

Tópicos

- [Noções básicas de status de volume](#)
- [Noções básicas sobre o status da associação](#)
- [Noções básicas sobre a transição de status de volumes armazenados em cache](#)
- [Noções básicas sobre a transição de status de volumes armazenados](#)

Noções básicas de status de volume

A tabela a seguir mostra o status do volume no console do Storage Gateway. O status do volume é exibido na coluna Status para cada volume de armazenamento em seu gateway. O status do volume que está funcionando normalmente é Available (Disponível).

Na tabela a seguir, você encontrará uma descrição de cada status de volume de armazenamento, e se e quando você deve agir com base em cada status. O status Available (Disponível) é o status normal de um volume. Um volume deve apresentar esse status durante todo o tempo ou na maior parte do tempo em que está em uso.

Status	Significado
Disponível	<p>O volume está disponível para uso. Esse status é o status de execução normal de um volume.</p> <p>Quando a fase de Bootstrapping for concluída, o volume retornará ao estado Available (Disponível). Ou seja, o gateway sincronizou todas as alterações feitas no volume desde que entrou pela primeira vez no status Pass Through (Passagem).</p>
Bootstrapping	<p>O gateway está sincronizando dados localmente com uma cópia dos dados armazenados em AWS. Geralmente, você não precisa executar nenhuma ação em relação a esse status, pois na maioria dos casos o volume de armazenamento vê automaticamente o status Available (Disponível).</p> <p>Veja a seguir os cenários em que um status de volume é Bootstrapping:</p> <ul style="list-style-type: none">• Um gateway foi encerrado inesperadamente.• O limite do buffer de upload de um gateway foi ultrapassado. Nesse cenário, o bootstrapping ocorre quando o volume tem o status Pass Through (Passagem) e o espaço do buffer de upload gratuito aumenta suficientemente. Você pode fornecer espaço do buffer de upload complementar para aumentar a porcentagem de espaço do buffer de upload gratuito. Neste cenário específico, o volume de armazenamento passa do status Pass Through (Passagem) para Bootstrapping e

Status	Significado
	<p>para Available (Disponível). Você pode continuar a usar esse volume durante esse período de bootstrapping. No entanto, você não pode tirar snapshots do volume nesse momento.</p> <ul style="list-style-type: none">• Você está criando um gateway de volumes armazenado e preservando os dados do disco local existente. Nesse cenário, seu gateway começa a carregar todos os dados para o. AWS O volume tem o status Bootstrapping até que todos os dados do disco local sejam copiados para. AWS Você pode a usar o volume durante esse período de bootstrapping. No entanto, você não pode tirar snapshots do volume nesse momento.
Criando	O volume está sendo criado no momento e não está pronto para ser usado. O status Creating (Criando) é transitório. Nenhuma ação é necessária.
Deleting	O volume está sendo excluído no momento. O status Deleting (Excluindo) é transitório. Nenhuma ação é necessária.
Irrecoverable (Não recuperável)	Ocorreu um erro do qual o volume não pode se recuperar. Para obter informações sobre o que fazer nessa situação, consulte Como solucionar problemas em volumes .

Status	Significado
Pass Through (Passagem)	<p>Os dados mantidos localmente estão fora de sincronia com os dados armazenados em AWS. Os dados gravados em um volume enquanto o volume encontra-se no status Pass Through (Passagem) permanecem no cache até que o status do volume seja Bootstrapping. Esses dados começam a ser carregados AWS quando o status do Bootstrapping começa.</p> <p>O status Pass Through (Passagem) pode ocorrer pelos vários motivos listados a seguir:</p> <ul style="list-style-type: none">• O status Pass Through (Passagem) ocorre se o seu gateway tiver excedido o limite do espaço do buffer de upload. Seus aplicativos podem continuar a ler e gravar dados em seus volumes de armazenamento enquanto os volumes permanecerem no status Pass Through (Passagem). No entanto, o gateway não está gravando nenhum dos dados do volume no respectivo buffer de upload nem está fazendo upload desses dados para a AWS. <p>O gateway continuará a carregar todos os dados gravados no volume antes que o volume inserido assuma o status Pass Through (Passagem). Ocorrerá uma falha em todos os snapshots pendentes ou programados de um volume de armazenamento enquanto o volume encontra-se no status Pass Through (Passagem). Para obter informações sobre o que fazer quando o volume de armazenamento estiver no status Pass Through (Passagem) porque o buffer de upload foi excedido, consulte Como solucionar problemas em volumes.</p> <p>Para retornar ao status ATIVO, o volume em Pass Through (Passagem) deve concluir a fase de Bootstrapping. Durante a inicialização, o volume restabelece a sincronização interna AWS, para que possa retomar o registro (log) das alterações no volume e ativar a funcionalidade. <code>CreateSnapshot</code> Durante o Bootstrapping, as gravações no volume são registradas no buffer de upload.</p> <ul style="list-style-type: none">•

Status	Significado
	<p>O status Pass Through (Passagem) ocorre quando mais de um volume de armazenamento realiza bootstrapping por vez. Apenas um volume de armazenamento por vez do gateway pode executar bootstrap. Por exemplo, suponha que você criou dois volumes de armazenamento e optou por preservar os dados existentes em ambos. Nesse caso, o segundo volume de armazenamento manterá o status Pass Through (Passagem) até que o primeiro volume de armazenamento conclua o bootstrapping. Neste cenário, você não precisa executar nenhuma ação. O status de cada um dos volumes de armazenamento é automaticamente alterado para Available (Disponível) assim que sua criação é concluída. Você pode ler e gravar no volume de armazenamento enquanto ele estiver no status Pass Through (Passagem) ou Bootstrapping.</p> <ul style="list-style-type: none">• O status Pass Through (Passagem) raramente pode indicar que ocorreu uma falha em um disco reservado para uso do buffer de upload. Para obter informações sobre que ação executar nesse cenário, consulte Como solucionar problemas em volumes.• O status Pass Through (Passagem) pode ocorrer quando um volume encontra-se no estado Active (Ativo) ou Bootstrapping. Nesse caso, o volume recebe uma gravação, mas o buffer de upload tem uma capacidade insuficiente para registrar (em log) essa gravação.• O status Pass Through (Passagem) ocorre quando um volume encontra-se em qualquer estado e o gateway não é desligado corretamente. Esse tipo de desligamento pode acontecer porque o software travou ou a VM foi desligada. Nesse caso, seja qual for o estado do volume, seu status será alterado para Pass Through (Passagem).

Status	Significado
Restoring (Restaurando)	<p>O volume está sendo restaurado por meio de um snapshot existente. Esse status aplica-se somente a volumes armazenados. Para ter mais informações, consulte Como funciona o gateway de volumes (arquitetura).</p> <p>Se você restaurar dois volumes de armazenamento ao mesmo tempo, ambos exibirão o status Restoring (Restaurando). O status de cada um dos volumes de armazenamento é automaticamente alterado para Available (Disponível) assim que sua criação é concluída. Você pode ler e gravar em um volume de armazenamento e criar um snapshot enquanto ele estiver no status Restoring (Restaurando).</p>
Restoring Pass Through (Restaurando passagem)	<p>O volume está sendo restaurado por meio de um snapshot existente e encontrou um problema no buffer de upload. Esse status aplica-se somente a volumes armazenados. Para ter mais informações, consulte Como funciona o gateway de volumes (arquitetura).</p> <p>Um dos motivos que determinam o status Restoring Pass Through (Restaurando passagem) é quando o gateway esgota o espaço do buffer de upload. Seus aplicativos podem continuar a ler e gravar dados nos volumes de armazenamento enquanto os volumes permanecem no status Restoring Pass Through (Restaurando passagem). No entanto, você não poderá criar snapshots de um volume de armazenamento enquanto ele estiver no status Restoring Pass Through (Restaurando passagem). Para obter informações sobre a ação a ser executada quando o volume de armazenamento estiver no status Restoring Pass Through (Restaurando passagem) em virtude de a capacidade do buffer de upload ter sido excedida, consulte Como solucionar problemas em volumes.</p> <p>O status Restoring Pass Through (Restaurando passagem) raramente pode indicar que ocorreu uma falha em um disco reservado para um buffer de upload. Para obter informações sobre que ação executar nesse cenário, consulte Como solucionar problemas em volumes.</p>

Status	Significado
Upload Buffer Not Configured (Buffer de upload não configurado)	Você não pode criar nem usar o volume porque não há nenhum buffer de upload configurado para o gateway. Para obter informações sobre como ampliar a capacidade do buffer de upload para os volumes em uma configuração de volume armazenado em cache, consulte Como determinar o tamanho do buffer de upload para alocar . Para obter informações sobre como ampliar a capacidade do buffer de upload para os volumes em uma configuração de volume armazenado, consulte Como determinar o tamanho do buffer de upload para alocar .

Noções básicas sobre o status da associação

Você pode desanexar um volume de um gateway ou anexá-lo a um gateway usando o console ou a API do Storage Gateway. A tabela a seguir mostra o status de associação do volume no console do Storage Gateway. O status da associação do volume é exibido na coluna Attachment status (Status da associação) para cada volume de armazenamento em seu gateway. Por exemplo, um volume desanexado de um gateway tem um status de Detached (Desanexado). Para obter informações sobre como desanexar e anexar um volume, consulte [Mover seus volumes para um gateway diferente](#).

Status	Significado
Attached	O volume é anexado a um gateway.
Detached	O volume é desanexado de um gateway.
Detaching (Desanexando)	O volume está sendo desanexado de um gateway. Quando você desanexa um volume, e o volume não tem dados, talvez você não veja esse status.

Noções básicas sobre a transição de status de volumes armazenados em cache

Use o seguinte diagrama de estado para entender as transições mais comuns entre os status dos volumes em gateways armazenados em cache. Você não precisa entender detalhadamente o

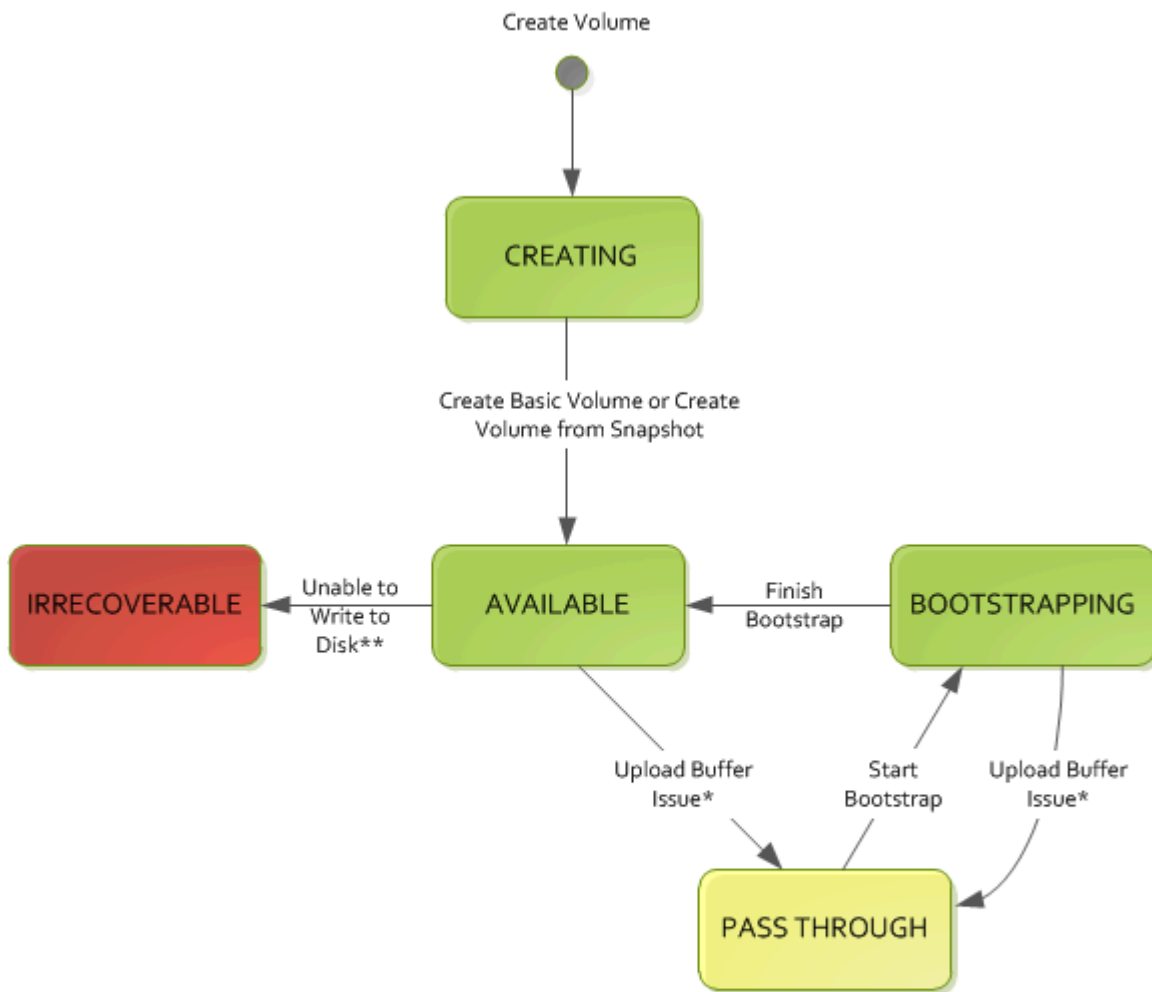
diagrama para usar seu gateway eficazmente. Na verdade, esse diagrama oferece informações detalhadas caso você tenha interesse em saber como um gateway de volumes funciona.

O diagrama não mostra o status Upload Buffer Not Configured (Buffer de upload não configurado) ou o status Deleting (Excluindo). Os estados dos volumes no diagrama são exibidos em quadrados verdes, amarelos e vermelhos. Você pode interpretar as cores como descrito a seguir.

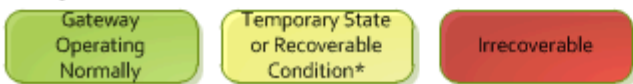
Cor	Status do volume
Verde	O gateway está funcionando normalmente. O status do volume é Available (Disponível) ou passará a ser Available (Disponível).
Amarelo	O status do volume é Pass Through (Passagem), o que indica um possível problema no volume de armazenamento. Se esse status for exibido porque o espaço do buffer de upload está cheio, em alguns casos esse espaço torna-se novamente disponível. Nesse ponto, o volume de armazenamento corrige-se automaticamente para o status Available (Disponível). Em outros casos, talvez você precise adicionar mais espaço do buffer de upload ao seu gateway para permitir que o status do volume de armazenamento passe a ser Available (Disponível). Para obter informações sobre como solucionar um caso em que o limite de capacidade do buffer de upload tenha sido ultrapassado, consulte Como solucionar problemas em volumes . Para obter informações sobre como ampliar a capacidade do buffer de upload, consulte Como determinar o tamanho do buffer de upload para alocar .
Vermelha	O status do volume de armazenamento é Irrecoverable (Irrecuperável). Nesse caso, você deve excluir o volume. Para obter informações

Cor	Status do volume
	sobre como fazer isso, consulte Para excluir um volume .

No diagrama, a transição entre dois estados é indicada por uma legenda. Por exemplo, a transição do status Creating (Criando) para o status Available (Disponível) é indicada como Criar um volume básico ou criar um volume por meio de snapshot. Esta transição representa a criação de um volume armazenado em cache. Para obter mais informações sobre a criação de volume armazenados, consulte [Como adicionar um volume](#).



Key



- * e.g. run out of upload buffer
- ** e.g. lost connectivity

Note

O status do volume Pass Through (Passagem) é exibido em amarelo no diagrama. No entanto, ele não corresponde à cor do ícone de status na caixa Status do console do Storage Gateway.

Noções básicas sobre a transição de status de volumes armazenados

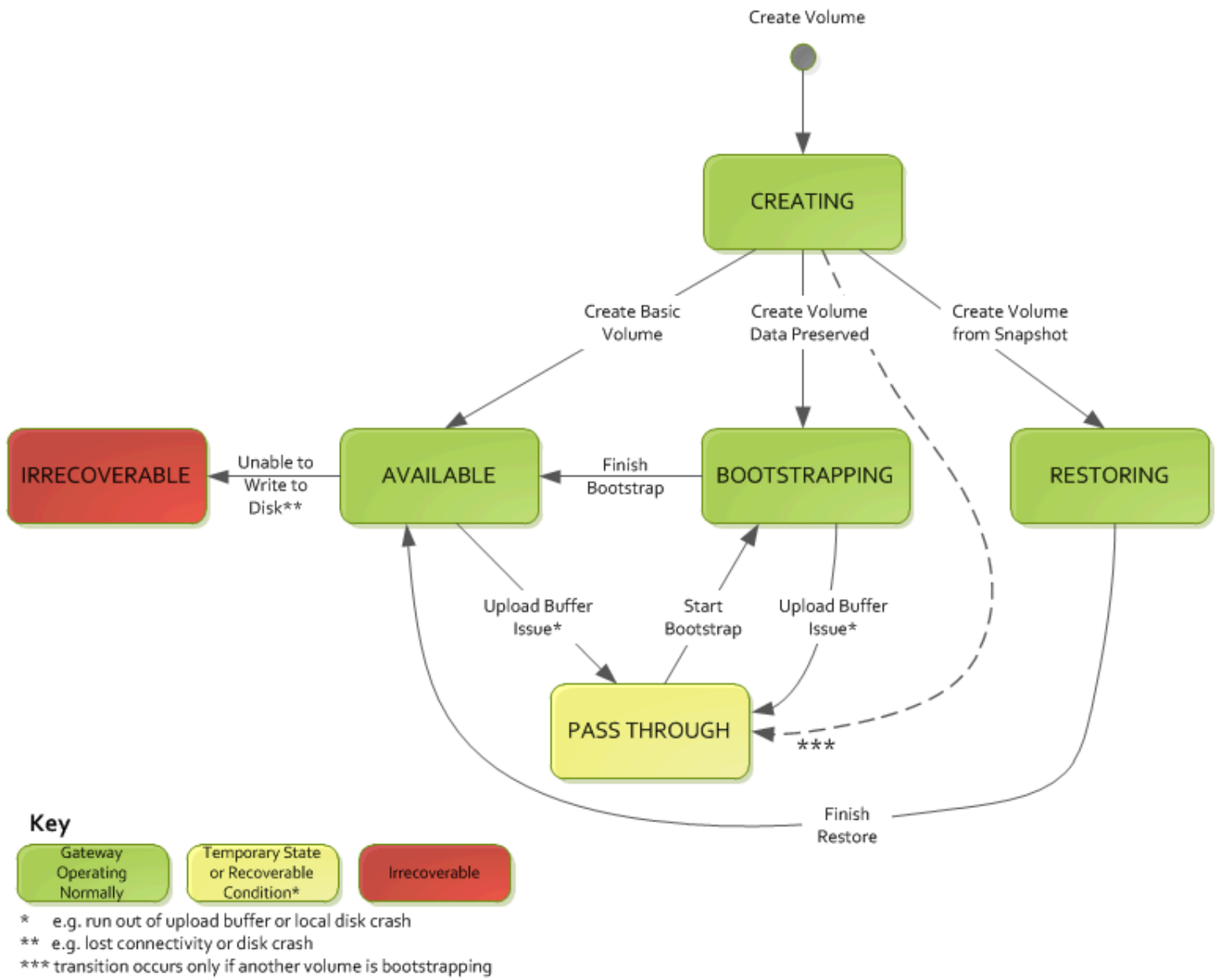
Use o seguinte diagrama de estado para entender as transições mais comuns entre os status dos volumes em um gateway armazenado. Você não precisa entender detalhadamente o diagrama para usar seu gateway eficazmente. Na verdade, esse diagrama oferece informações detalhadas caso você tenha interesse em entender melhor como os gateways de volumes funcionam.

O diagrama não mostra o status Upload Buffer Not Configured (Buffer de upload não configurado) ou o status Deleting (Excluindo). Os estados dos volumes no diagrama são exibidos em quadrados verdes, amarelos e vermelhos. Você pode interpretar as cores como descrito a seguir.

Cor	Status do volume
Verde	O gateway está funcionando normalmente. O status do volume é Available (Disponível) ou passará a ser Available (Disponível).
Amarelo	Quando você criar um volume de armazenamento e preservar dados, a transição entre o status Creating (Criando) e o status Pass Through (Passagem) ocorrerá se outro volume estiver realizando bootstrapping. Nesse caso, o volume com status Pass Through (Passagem) assumirá o status Bootstrapping e Available (Disponível) quando o primeiro volume estiver finalizando o bootstrapping. Além do cenário específico mencionado, o amarelo (status Pass Through (Passagem)) indica que provavelmente o volume de armazenamento está com algum problema, que geralmente está relacionado ao buffer de upload. Se o limite de capacidade do buffer de upload tiver sido ultrapassado, em alguns casos o espaço do buffer torna-se novamente disponível. Nesse ponto, o volume de armazenamento corrige-se automaticamente para o status Available (Disponível). Em outros casos, talvez você precise adicionar mais capacidade do buffer de upload ao seu gateway para que o

Cor	Status do volume
	volume de armazenamento volte para o status Available (Disponível). Para obter informações sobre como solucionar um caso em que o limite de capacidade do buffer de upload tenha sido ultrapassado, consulte Como solucionar problemas em volumes . Para obter informações sobre como ampliar a capacidade do buffer de upload, consulte Como determinar o tamanho do buffer de upload para alocar .
Vermelha	O status do volume de armazenamento é Irrecoverable (Irrecuperável). Nesse caso, você deve excluir o volume. Para obter informações sobre como fazer isso, consulte Exclusão de um volume .

No diagrama a seguir, a transição entre dois estados é indicada por uma legenda. Por exemplo, a transição do status Creating (Criando) para o status Available (Disponível) é indicada como Criar um volume básico. Essa transição representa a criação de um volume armazenado sem preservar dados ou criar o volume de um snapshot.



Note

O status do volume Pass Through (Passagem) é exibido em amarelo no diagrama. No entanto, ele não corresponde à cor do ícone de status na caixa Status do console do Storage Gateway.

Como mover seus dados para um novo gateway

Você pode mover dados entre gateways à medida que suas necessidades de dados e desempenho aumentam ou se você receber uma AWS notificação para migrar seu gateway. Veja os seguintes motivos para fazer isso:

- Mova os dados para plataformas host melhores ou instâncias do Amazon EC2 mais recentes.
- Atualize o hardware subjacente para seu servidor.

As etapas que você segue para mover seus dados para um novo gateway dependem do tipo de gateway que você tem.

Note

Os dados só podem ser movidos entre os mesmos tipos de gateway.

Como mover os volumes armazenados para um novo gateway de volumes armazenado

Para mover os volumes armazenados para um novo gateway de volumes armazenado

1. Interrompa qualquer aplicação que esteja gravando no antigo Gateway de Volumes armazenado.
2. Use as etapas a seguir para criar um snapshot do seu volume e aguarde a conclusão do snapshot.
 - a. Abra o console do Storage Gateway em <https://console.aws.amazon.com/storagegateway/home>.
 - b. No painel de navegação, escolha Volumes e o volume do qual você deseja criar o snapshot.
 - c. Em Actions (Ações), escolha Create snapshot (Criar snapshot).
 - d. Na caixa de diálogo Criar snapshot, digite a descrição do snapshot e escolha Criar snapshot.

Você pode verificar se o snapshot foi criado usando o console. Se os dados ainda estiverem sendo enviados para o volume, aguarde até que o upload seja concluído antes de

prosseguir para a próxima etapa. Para ver o status do snapshot e validar se nenhum está pendente, selecione os links do snapshot nos volumes.

3. Use as etapas a seguir para interromper o gateway de volumes antigo armazenado:
 - a. No painel de navegação, escolha Gateways e o gateway de volumes antigo armazenado que você deseja interromper. O status do gateway é Running.
 - b. Em Ações, escolha Interromper gateway. Verifique o ID do gateway na caixa de diálogo e, depois, escolha Interromper gateway.

Enquanto o gateway estiver interrompido, você provavelmente verá uma mensagem indicando o status do gateway. Quando o gateway é encerrado, uma mensagem e o botão Iniciar gateway aparece na guia Detalhes. Quando o gateway é encerrado, o status do gateway é Desligado.

- c. Desligue a VM usando os controles do hipervisor.

Para obter mais informações sobre como interromper um gateway, consulte [Como iniciar e interromper um gateway de volumes](#).


4. Separe os discos de armazenamento associados aos seus volumes armazenados da VM do gateway. Isto exclui o disco raiz da VM.
5. Ative um novo gateway de volumes armazenado com uma nova imagem de VM de hipervisor disponível no console do Storage Gateway em <https://console.aws.amazon.com/storagegateway/home>.
6. Conecte os discos de armazenamento físico que você desconectou da antiga VM do gateway de volumes armazenada na etapa 5.
7. Para preservar os dados existentes no disco, use as etapas a seguir para criar volumes armazenados.
 - a. No console do Storage Gateway, escolha Criar volume.
 - b. Na caixa de diálogo Criar volume, selecione o gateway de volumes armazenado que você criou na etapa 5.
 - c. Selecione um valor ID de disco na lista.
 - d. Em Conteúdo do volume, escolha Preservar dados existentes no disco.

Para obter mais informações sobre a criação de volume, consulte [Como criar um volume](#).

8. Opcional) No assistente Configurar autenticação CHAP que é exibido, insira o Nome do iniciador, o Segredo do iniciador, o Segredo de destino e selecione Salvar.


Para obter mais informações sobre como trabalhar com a autenticação do Challenge-Handshake Authentication Protocol (CHAP), consulte [Como configurar a autenticação CHAP para destinos iSCSI](#).

9. Inicie a aplicação que grava no volume armazenado.
10. Ao confirmar que seu novo gateway de volumes está funcionando corretamente, é possível excluir o antigo gateway de volumes.

 Important

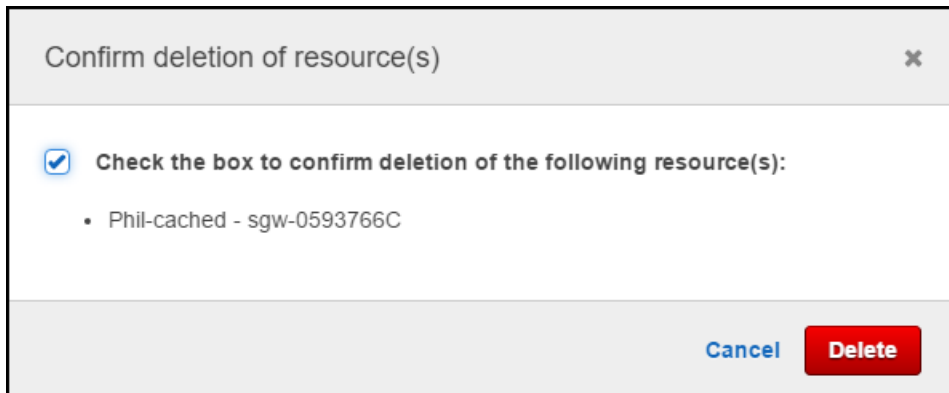
Antes de excluir um gateway, verifique se não há nenhuma aplicação gravando no momento nos volumes do gateway. Se excluir o gateway enquanto ele estiver em uso, poderá perder dados.

Use as etapas a seguir para excluir o gateway de volumes antigo armazenado:

 Warning

Não é possível recuperar um gateway excluído.

- a. No painel de navegação, escolha Gateways e o gateway de volumes antigo armazenado que você deseja excluir.
- b. Em Actions (Ações), selecione Delete gateway (Excluir gateway).
- c. Na caixa de diálogo de confirmação exibida, marque a caixa de seleção para confirmar a exclusão. Certifique-se que o ID de gateway listado especifica o gateway de volumes antigo que deseja excluir e escolha Excluir.



11. Exclua a VM antiga do gateway. Para obter informações sobre como excluir uma VM, consulte a documentação do seu hipervisor.

Como mover os volumes em cache para uma nova máquina virtual do gateway de volumes em cache

Para mover seus volumes em cache para uma nova máquina virtual (VM) do gateway de volumes em cache

1. Interrompa todas as aplicações que estão gravando no antigo Gateway de Volumes em cache.
2. Desmonte ou desconecte volumes iSCSI de qualquer cliente que esteja usando esses volumes. Isto ajuda a manter os dados nesses volumes consistentes, impedindo que os clientes alterem ou adicionem dados a esses volumes.
3. Use as etapas a seguir para criar um snapshot do seu volume e aguarde a conclusão do snapshot.
 - a. Abra o console do Storage Gateway em <https://console.aws.amazon.com/storagegateway/home>.
 - b. No painel de navegação, escolha Volumes e o volume do qual você deseja criar o snapshot.
 - c. Em Actions (Ações), escolha Create snapshot (Criar snapshot).
 - d. Na caixa de diálogo Criar snapshot, digite a descrição do snapshot e escolha Criar snapshot.

Você pode verificar se o snapshot foi criado usando o console. Se os dados ainda estiverem sendo enviados para o volume, aguarde até que o upload seja concluído antes de prosseguir para a próxima etapa. Para ver o status do snapshot e validar se nenhum está pendente, selecione os links do snapshot nos volumes.

Para obter mais informações sobre como verificar o status do volume no console do, consulte [Noções básicas sobre transições e status de volumes](#). Para obter informações sobre status de volume em cache, consulte [Noções básicas sobre a transição de status de volumes armazenados em cache](#).


4. Use as etapas a seguir para excluir o gateway de volumes antigo em cache:
 - a. No painel de navegação, escolha Gateways e o gateway de volumes antigo em cache que você deseja interromper. O status do gateway é Running.
 - b. Em Ações, escolha Interromper gateway. Verifique o ID do gateway na caixa de diálogo e, depois, escolha Interromper gateway. Anote o ID do gateway, conforme necessário em uma etapa posterior.

Enquanto o gateway antigo estiver interrompido, você provavelmente verá uma mensagem indicando o status do gateway. Quando o gateway é encerrado, uma mensagem e o botão Iniciar gateway aparecem na guia Detalhes. Quando o gateway é encerrado, o status do gateway é Desligado.

- c. Desligue a VM antiga usando os controles do hipervisor. Para obter mais informações sobre o encerramento de uma instância do Amazon EC2, consulte [Como interromper e iniciar suas](#) instâncias no Guia do usuário do Amazon EC2. Para obter mais informações sobre como desligar uma VM do KVM, VMware ou Hyper-V, consulte a documentação do hipervisor.

Para obter mais informações sobre como interromper um gateway, consulte [Como iniciar e interromper um gateway de volumes](#).

5. Separe todos os discos, incluindo o disco raiz, os discos de cache e os discos de buffer de upload, da antiga VM do gateway.


 Note

Anote a ID do volume do disco raiz, bem como a ID do gateway associada a este disco raiz. Esse disco do novo hipervisor é desanexado do novo Storage Gateway em uma etapa posterior. (Consulte a etapa 11.)

Se você estiver usando uma instância do Amazon EC2 como a VM para seu gateway de volume em cache, consulte Separar um volume do [Amazon EBS de uma instância Linux no Guia do](#)

[usuário do Amazon EC2](#). Para obter informações sobre como desanexar discos de uma VM do KVM, VMware ou Hyper-V, consulte a documentação do seu hipervisor.

6. Crie uma nova instância de VM de hipervisor do Storage Gateway, mas não a ative como gateway. Para obter mais informações sobre como criar uma nova VM com hipervisor do Storage Gateway, consulte [Configurar um gateway de volumes](#). Este novo gateway assumirá a identidade do antigo gateway.

 Note

Não adicione discos para cache ou buffer de upload na nova VM. A nova VM usará os mesmos discos de cache e carregará discos de buffer que foram usados pela VM antiga.

7. Sua nova instância de VM hipervisor do Storage Gateway deve usar a mesma configuração de rede da VM antiga. A configuração de rede padrão para o gateway é Dynamic Host Configuration Protocol (DHCP). Com o DHCP, um endereço IP é atribuído automaticamente ao seu gateway.

Se você precisar configurar manualmente um endereço IP estático para sua nova VM, consulte [Como configurar uma rede de gateway](#) para obter mais detalhes. Se seu gateway precisar usar um proxy Socket Secure versão 5 (SOCKS5) para se conectar à Internet, consulte [Como rotear seu gateway local por meio de um proxy](#) para obter mais detalhes.

8. Inicie a nova VM.
9. Conecte os discos que você desconectou da antiga VM do gateway de volumes em cache na etapa 5 ao novo gateway de volumes em cache. Anexe-os à nova VM do gateway na mesma ordem em que estão na antiga VM do gateway.

Todos os discos devem manter a transição inalterada. Não altere os tamanhos dos volumes, pois isso fará com que os metadados fiquem inconsistentes.

10. Inicie o processo de migração do gateway conectando-se à nova VM com uma URL que usa o formato a seguir.

```
http://your-VM-IP-address/migrate?gatewayId=your-gateway-ID
```

É possível reutilizar o mesmo endereço IP para a nova VM do gateway que usou para a antiga VM do gateway. O URL deve ser semelhante ao exemplo a seguir.

```
http://198.51.100.123/migrate?gatewayId=sgw-12345678
```

Use este URL de um navegador ou da linha de comando usando `curl` para iniciar o processo de migração.

Quando o processo de migração do gateway for iniciado com êxito, você receberá a seguinte mensagem:

```
Successfully imported Storage Gateway information. Please refer to
Storage Gateway documentation to perform the next steps to complete the
migration.
```

11. Separe o disco raiz do gateway antigo, cujo ID de volume você anotou na etapa 5.
12. Inicie o gateway.

Use as etapas a seguir para excluir o novo gateway de volumes em cache:

- a. Abra o console do Storage Gateway em <https://console.aws.amazon.com/storagegateway/home>.
- b. No painel de navegação, escolha Gateways e, em seguida, o gateway a ser iniciado. O status do gateway é Shutdown.
- c. Escolha Detalhes e escolha Iniciar gateway.

Para obter mais informações sobre como iniciar um gateway, consulte [Como iniciar e interromper um gateway de volumes](#).

13. Agora, seus volumes devem estar disponíveis para suas aplicações no endereço IP da nova VM do gateway.
14. Confirme se os volumes estão disponíveis e exclua a VM antiga do gateway. Para obter informações sobre como excluir uma VM, consulte a documentação do seu hipervisor.

Como monitorar o Storage Gateway

Esta seção descreve como monitorar um gateway, incluindo recursos de monitoramento associados ao gateway, usando a Amazon CloudWatch. É possível monitorar o buffer de upload e o armazenamento em cache do gateway. O console do Storage Gateway é usado para visualizar métricas e alarmes do gateway. Por exemplo, é possível visualizar o número de bytes usado em operações de leitura e gravação, o tempo gasto nas operações de leitura e gravação e o tempo necessário para recuperar dados da nuvem da Amazon Web Services. Com essas métricas, você pode acompanhar a integridade de seu gateway e definir alarmes para notificá-lo quando uma ou mais métricas afastarem-se de um limite definido.

O Storage Gateway fornece CloudWatch métricas sem custo adicional. As métricas do Storage Gateway ficam arquivadas por um período de duas semanas. Ao usar essas métricas, você pode acessar informações históricas e obter uma melhor visão do desempenho do gateway e dos volumes. O Storage Gateway também fornece CloudWatch alarmes, exceto alarmes de alta resolução, sem custo adicional. Para obter mais informações sobre CloudWatch preços, consulte [CloudWatch Preços da Amazon](#). Para obter mais informações sobre CloudWatch, consulte o [Guia CloudWatch do usuário da Amazon](#).

Tópicos


- [Noções básicas de métricas de gateway](#)
- [Dimensões das métricas do Storage Gateway](#)
- [Monitorar o buffer de upload](#)
- [Monitorar um armazenamento em cache](#)
- [Entendendo os CloudWatch alarmes](#)
- [Criação de CloudWatch alarmes recomendados para seu gateway](#)
- [Criando um CloudWatch alarme personalizado para seu gateway](#)
- [Como monitorar um gateway de volume](#)

Noções básicas de métricas de gateway

Para a discussão deste tópico, definimos as métricas de gateway como métricas dimensionadas para o gateway, isto é, elas avaliam um fator relacionado ao gateway. Como um gateway contém um ou mais volumes, uma métrica específica ao gateway representa todos os volumes presentes no

gateway. Por exemplo, a métrica `CloudBytesUploaded` é o número total de bytes que o gateway envia à nuvem durante o período de relatório. Essa métrica inclui a atividade de todos os volumes no gateway.

Ao trabalhar com dados de métricas de gateway, você especifica a identificação exclusiva do gateway cujas métricas está interessado em visualizar. Para fazer isso, você especifica os valores `GatewayId` e `GatewayName`. Quando desejar trabalhar com uma métrica para gateway, especifique a dimensão do gateway no namespace da métrica, que distingue uma métrica específica a um gateway ou específica a um volume. Para ter mais informações, consulte [Usando o Amazon CloudWatch Metrics](#).

 Note

Algumas métricas retornam pontos de dados somente quando novos dados são gerados durante o período de monitoramento mais recente.

Métrica	Descrição
<code>AvailabilityNotifications</code>	<p>Número de notificações de integridade relacionadas à disponibilidade geradas pelo gateway.</p> <p>Use essa métrica com a estatística <code>Sum</code> para observar se o gateway está enfrentando eventos relacionados à disponibilidade. Para obter detalhes sobre os eventos, verifique seu grupo de CloudWatch registros configurado.</p> <p>Unidade: número</p>
<code>CacheHitPercent</code>	Porcentagem de leituras de aplicativos feitas pelo cache.

Métrica	Descrição	
	A amostra é capturada no final do período do relatório. Unidade: percentual	
CacheUsed	O número total de bytes sendo utilizados no armazenamento em cache do gateway. A amostra é capturada no final do período do relatório. Unidade: bytes	
IoWaitPercent	Porcentagem de tempo em que o gateway está aguardando uma resposta do disco local. Unidade: percentual	
MemTotalBytes	Quantidade de RAM provisionada para a VM do gateway, em bytes. Unidade: bytes	
MemUsedBytes	Quantidade de RAM atualmente em uso pela VM do gateway, em bytes. Unidade: bytes	

Métrica	Descrição	
QueuedWrites	<p>O número de bytes aguardand o para serem gravados AWS, amostrado no final do período do relatório para todos os volumes no gateway. Esses bytes são mantidos no armazenamento de trabalho do seu gateway.</p> <p>Unidade: bytes</p>	
ReadBytes	<p>O número total de bytes lidos dos aplicativos locais no período do relatório para todos os volumes no gateway.</p> <p>Use essa métrica com a estatística Sum para medir a taxa de transferência e com a estatística Samples para medir IOPS.</p> <p>Unidade: bytes</p>	
ReadTime	<p>O número total de milissegundos gastos em operações de leitura dos aplicativos locais no período do relatório para todos os volumes no gateway.</p> <p>Use essa métrica com a estatística Average para medir a latência.</p> <p>Unidade: milissegundos</p>	

Métrica	Descrição	
TimeSinceLastRecoveryPoint	<p>O tempo desde o último ponto de recuperação disponível. Para ter mais informações, consulte O gateway armazenado em cache é inacessível e você deseja recuperar seus dados.</p> <p>Unidade: segundos</p>	
TotalCacheSize	<p>O tamanho total de cache em bytes. A amostra é capturada no final do período do relatório.</p> <p>Unidade: bytes</p>	
UploadBufferPercentageUsed	<p>Percentual de uso do buffer de upload do gateway. A amostra é capturada no final do período do relatório.</p> <p>Unidade: percentual</p>	
UploadBufferUsed	<p>O número total de bytes sendo utilizados no buffer de upload do gateway. A amostra é capturada no final do período do relatório.</p> <p>Unidade: bytes</p>	

Métrica	Descrição	
UserCpuPercent	<p>Porcentagem de tempo de CPU gasto no processamento do gateway, com média calculada em todos os núcleos.</p> <p>Unidade: percentual</p>	
WorkingStorageFree	<p>A quantidade total de espaço não utilizado no armazenamento de trabalho do gateway. A amostra é capturada no final do período do relatório.</p> <p>Unidade: bytes</p>	
WorkingStoragePercentUsed	<p>Percentual de uso do buffer de upload do gateway. A amostra é capturada no final do período do relatório.</p> <p>Unidade: percentual</p>	
WorkingStorageUsed	<p>O número total de bytes sendo utilizados no buffer de upload do gateway. A amostra é capturada no final do período do relatório.</p> <p>Unidade: bytes</p>	

Métrica	Descrição	
WriteBytes	<p>O número total de bytes gravados nos aplicativos locais no período do relatório para todos os volumes no gateway.</p> <p>Use essa métrica com a estatística Sum para medir a taxa de transferência e com a estatística Samples para medir IOPS.</p> <p>Unidade: bytes</p>	
WriteTime	<p>O número total de milissegundos gastos em operações de gravação dos aplicativos locais no período do relatório para todos os volumes no gateway.</p> <p>Use essa métrica com a estatística Average para medir a latência.</p> <p>Unidade: milissegundos</p>	

Dimensões das métricas do Storage Gateway

O CloudWatch namespace do serviço Storage Gateway é `AWS/StorageGateway`. Os dados são disponibilizados automaticamente em períodos de cinco minutos, sem custo adicional.

Dimensão	Descrição
GatewayId , GatewayName	<p>Essas dimensões filtram os dados que você solicita para métricas específicas do gateway. É possível identificar um gateway para trabalhar pelo valor de GatewayId ou de GatewayName . Se o nome do gateway for diferente para o intervalo de tempo em que você está interessado em visualizar métricas, use o GatewayId .</p> <p>Os dados de throughput e latência de um gateway são baseados em todos os volumes para o gateway em questão. Para obter informações sobre como trabalhar com métricas de gateway, consulte Medindo o desempenho entre seu gateway AWS e.</p>
VolumeId	<p>Essa dimensão filtra os dados que você solicitar para as métricas específicas ao volume. Identifique um volume de armazenamento para trabalhar por seu valor de VolumeId. Para obter informações sobre como trabalhar com métricas de volume, consulte Medir o desempenho entre o aplicativo e o gateway.</p>

Monitorar o buffer de upload

Você pode encontrar informações a seguir sobre como monitorar o buffer de upload de um gateway e como criar um alarme para obter uma notificação quando o buffer exceder um limite especificado. Ao usar essa abordagem, é possível adicionar um armazenamento em buffer a um gateway antes que ele fique completamente cheio e seu aplicativo de armazenamento pare de fazer backup para a AWS.

O buffer de upload é monitorado da mesma forma nas arquiteturas de volume armazenado em cache e gateway de fitas. Para ter mais informações, consulte [Como funciona o gateway de volumes \(arquitetura\)](#).

Note

As métricas `WorkingStoragePercentUsed`, `WorkingStorageUsed` e `WorkingStorageFree` representam o buffer de upload para os volumes armazenados somente antes do lançamento do atributo de volume armazenado em cache no Storage Gateway. Agora, use as métricas de buffer de upload equivalentes `UploadBufferPercentUsed`, `UploadBufferUsed` e `UploadBufferFree`. Essas métricas se aplicam a ambas as arquiteturas de gateway.

Item de Interesse	Como medir
Uso do buffer de upload	Use as métricas <code>UploadBufferPercentUsed</code> , <code>UploadBufferUsed</code> e <code>UploadBufferFree</code> com a estatística <code>Average</code> . Por exemplo, use <code>UploadBufferUsed</code> com a estatística <code>Average</code> para analisar o uso de armazenamento ao longo de um período.

Como medir a porcentagem do buffer de upload que é usado

1. Abra o CloudWatch console em <https://console.aws.amazon.com/cloudwatch/>.
2. Escolha a dimensão `StorageGateway: Gateway Metrics` e encontre o gateway com o qual você deseja trabalhar.
3. Escolha a métrica `UploadBufferPercentUsed`.
4. Em `Time Range`, escolha um valor.
5. Escolha a estatística `Average`.
6. Em `Period`, escolha o valor de 5 minutos para corresponder ao período de relatório padrão.

O conjunto de pontos de dados resultante, ordenado por tempo, contém a porcentagem usada do buffer de upload.

Usando o procedimento a seguir, você pode criar um alarme usando o CloudWatch console. Para saber mais sobre alarmes e limites, consulte [Criação de CloudWatch alarmes](#) no Guia do usuário da Amazon CloudWatch .

Para definir um alarme com limite superior para o buffer de upload de um gateway

1. Abra o CloudWatch console em <https://console.aws.amazon.com/cloudwatch/>.
2. Selecione Create Alarm (Criar alarme) para iniciar o assistente de criação de alarme.
3. Especifique uma métrica para o alarme.
 - a. Na página Selecionar métrica do assistente de criação de alarme, escolha a GatewayName dimensão AWS/StorageGateway:GatewayId, e localize o gateway com o qual você deseja trabalhar.
 - b. Escolha a métrica UploadBufferPercentUsed. Use a estatística Average e um período de 5 minutos.
 - c. Escolha Continuar.
4. Defina o nome do alarme, a descrição e o limite:
 - a. Na página Define Alarm (Definir alarme) do assistente de criação de alarme, identifique o alarme atribuindo um nome e uma descrição nas caixas Name (Nome) e Description (Descrição).
 - b. Defina o limite do alarme.
 - c. Escolha Continuar.
5. Configure uma ação de e-mail para o alarme:
 - a. Na página Configure Actions (Configurar ações) do assistente de criação de alarme, selecione Alarm (Alarme) para Alarm State (Estado do alarme).
 - b. Escolha Choose or create email topic para Topic.

Para criar um tópico de e-mail significa que você configurou um tópico do Amazon SNS. Para obter mais informações sobre o Amazon SNS, consulte [Configurar o Amazon SNS](#) no Guia do usuário da Amazon CloudWatch .

- c. Em Topic (Tópico), insira um nome descritivo para o tópico.
 - d. Escolha Add Action.
 - e. Escolha Continuar.
6. Revise as configurações de alarme e crie o alarme:

- a. Na página Review (Revisar) do assistente de criação de alarme, revise a definição e a métrica do alarme e as ações associadas a serem executadas (por exemplo, enviar uma notificação por e-mail).
 - b. Depois de rever o resumo do alarme, escolha Save Alarm.
7. Confirme a assinatura do tópico do alarme:
- a. Abra o e-mail do Amazon SNS que foi enviado para o endereço de e-mail especificado ao criar o tópico.

A imagem a seguir mostra uma típica notificação de e-mail.



- b. Confirme sua assinatura clicando no link no e-mail.

A confirmação de assinatura é exibida.

Monitorar um armazenamento em cache

Você pode encontrar informações a seguir sobre como monitorar o armazenamento em cache de um gateway e como criar um alarme para obter uma notificação quando os parâmetros do cache ultrapassarem os limites especificados. Ao usar esse alarme, você sabe quando adicionar armazenamento em cache a um gateway.

O armazenamento em cache é monitorado apenas na arquitetura de volumes armazenados em cache. Para ter mais informações, consulte [Como funciona o gateway de volumes \(arquitetura\)](#).

Item de Interesse	Como medir
Uso total de cache	<p>Use as métricas <code>CachePercentUsed</code> e <code>TotalCacheSize</code> com a estatística <code>Average</code>. Por exemplo, use <code>CachePercentUsed</code> com a estatística <code>Average</code> para analisar o uso de cache ao longo de um período.</p> <p>A métrica <code>TotalCacheSize</code> muda apenas quando você amplia o cache do gateway.</p>
Porcentagem de solicitações de leitura que são feitas do cache	<p>Use a métrica <code>CacheHitPercent</code> com a estatística <code>Average</code>.</p> <p>Normalmente, é desejável que <code>CacheHitPercent</code> mantenha-se alta.</p>
Porcentagem do cache que está suja, ou seja, contém conteúdo que não foi enviado para AWS	<p>Use a métrica <code>CachePercentDirty</code> com a estatística <code>Average</code>.</p> <p>Normalmente, é desejável que <code>CachePercentDirty</code> mantenha-se baixa.</p>

Como medir a porcentagem de um cache que está sujo para um gateway e todos os seus volumes

1. Abra o CloudWatch console em <https://console.aws.amazon.com/cloudwatch/>.
2. Escolha a dimensão `StorageGateway: Gateway Metrics` e encontre o gateway com o qual você deseja trabalhar.
3. Escolha a métrica `CachePercentDirty`.
4. Em `Time Range`, escolha um valor.
5. Escolha a estatística `Average`.
6. Em `Period`, escolha o valor de 5 minutos para corresponder ao período de relatório padrão.

O conjunto de pontos de dados resultante, ordenados por tempo, contém a porcentagem de cache sujo por 5 minutos.

Como medir a porcentagem do cache que está sujo para um volume

1. Abra o CloudWatch console em <https://console.aws.amazon.com/cloudwatch/>.
2. Escolha a dimensão StorageGateway: Métricas de volume e encontre o volume com o qual você deseja trabalhar.
3. Escolha a métrica CachePercentDirty.
4. Em Time Range, escolha um valor.
5. Escolha a estatística Average.
6. Em Period, escolha o valor de 5 minutos para corresponder ao período de relatório padrão.

O conjunto de pontos de dados resultante, ordenados por tempo, contém a porcentagem de cache sujo por 5 minutos.

Entendendo os CloudWatch alarmes

CloudWatch os alarmes monitoram informações sobre seu gateway com base em métricas e expressões. Você pode adicionar CloudWatch alarmes ao seu gateway e visualizar seus status no console do Storage Gateway. Para obter mais informações sobre as métricas usadas para monitorar o gateway de volumes, consulte [Como entender as métricas do gateway](#) e [Como entender as métricas de volume](#). Para cada alarme, você especifica as condições que iniciarão o estado ALARM. Os indicadores de status do alarme no console do Storage Gateway ficam vermelhos quando estão no estado ALARM, facilitando o monitoramento proativo do status. É possível configurar alarmes para invocar ações automaticamente com base em mudanças sustentadas no estado. Para obter mais informações sobre CloudWatch alarmes, consulte [Usando CloudWatch alarmes da Amazon no Guia CloudWatch](#) do usuário da Amazon.


Note

Se você não tiver permissão para visualizar CloudWatch, não poderá ver os alarmes.

Para cada gateway ativado, recomendamos que você crie os seguintes alarmes do CloudWatch:

- Espera alta de E/S: IoWaitpercent \geq 20 para 3 pontos de dados em 15 minutos
- Percentual de cache sujo: CachePercentDirty $>$ 80 para 4 pontos de dados em 20 minutos

- Notificações de integridade: `HealthNotifications >= 1` para 1 ponto de dados em cinco minutos. Ao configurar esse alarme, defina Tratamento de dados ausentes como `notBreaching`.

 Note

Você poderá definir um alarme de notificação de integridade somente se o gateway tiver uma notificação de integridade anterior no CloudWatch.

Para gateways em plataformas de host VMware com o modo HA ativado, também recomendamos este alarme adicional: CloudWatch

- Notificações de disponibilidade: `AvailabilityNotifications >= 1` para 1 ponto de dados em cinco minutos. Ao configurar esse alarme, defina Tratamento de dados ausentes como `notBreaching`.

A tabela a seguir descreve o estado de um alarme.

Estado	Descrição
OK	A métrica ou a expressão está dentro do limite definido.
Alarme	A métrica ou a expressão está fora do limite definido.
Dados insuficientes	O alarme acabou de ser acionado, a métrica não está disponível ou não há dados suficientes para a métrica determinar o estado do alarme.
Nenhum	Nenhum alarme foi criado para o gateway. Para criar um alarme, consulte Criando um CloudWatch alarme personalizado para seu gateway .

Estado	Descrição
Indisponível	O estado do alarme é desconhecido. Escolha Indisponível para visualizar informações de erro na guia Monitoramento.

Criação de CloudWatch alarmes recomendados para seu gateway

Ao criar um novo gateway usando o console do Storage Gateway, você pode optar por criar todos os CloudWatch alarmes recomendados automaticamente como parte do processo de configuração inicial. Para obter mais informações, consulte [Como configurar o gateway de volumes](#). Se você quiser adicionar ou atualizar CloudWatch os alarmes recomendados para um gateway existente, use o procedimento a seguir.

Para adicionar ou atualizar CloudWatch os alarmes recomendados para um gateway existente

Note

Esse recurso requer permissões CloudWatch de política, que não são concedidas automaticamente como parte da política de acesso total pré-configurada do Storage Gateway. Certifique-se de que sua política de segurança conceda as seguintes permissões antes de tentar criar CloudWatch alarmes recomendados:

- `cloudwatch:PutMetricAlarm`: criar alarmes
- `cloudwatch:DisableAlarmActions`: desativar as ações de alarme
- `cloudwatch:EnableAlarmActions`: ativar as ações de alarme
- `cloudwatch>DeleteAlarms`: excluir alarmes

1. Abra o console do Storage Gateway em <https://console.aws.amazon.com/storagegateway/home/>.
2. No painel de navegação, escolha Gateways e, em seguida, escolha o gateway para o qual você deseja criar os alarmes recomendados CloudWatch .
3. Na página de detalhes do gateway, selecione a guia Monitoramento.
4. Em Alarmes, escolha Criar alarmes recomendados. Os alarmes recomendados são criados automaticamente.

A seção Alarmes lista todos os CloudWatch alarmes de um gateway específico. Daqui, é possível selecionar e excluir um ou mais alarmes, ativar ou desativar as ações de alarme e criar novos alarmes.

Criando um CloudWatch alarme personalizado para seu gateway

CloudWatch usa o Amazon Simple Notification Service (Amazon SNS) para enviar notificações de alarme quando um alarme muda de estado. Um alarme observa uma única métrica ao longo de um período especificado por você e realiza uma ou mais ações com base no valor da métrica relativo a um determinado limite ao longo de vários períodos. A ação é uma notificação que é enviada para um tópico do Amazon SNS. Você pode criar um tópico do Amazon SNS ao criar um CloudWatch alarme. Para ter mais informações sobre o Amazon SNS, consulte [O que é o Amazon SNS?](#) no Guia do desenvolvedor do Amazon Simple Notification Service.

Para criar um CloudWatch alarme no console do Storage Gateway

1. Abra o console do Storage Gateway em <https://console.aws.amazon.com/storagegateway/home/>.
2. No painel de navegação, escolha Gateways e o gateway para o qual você deseja criar um alarme.
3. Na página de detalhes do gateway, selecione a guia Monitoramento.
4. Em Alarmes, escolha Criar alarme para abrir o CloudWatch console.
5. Use o CloudWatch console para criar o tipo de alarme que você deseja. É possível criar os seguintes tipos de alarmes:
 - Alarme de limite estático: um alarme baseado em um limite definido para uma métrica escolhida. O alarme passa para o estado ALARME quando a métrica atinge o limite de um número especificado de períodos de avaliação.

Para criar um alarme de limite estático, consulte [Criação de um CloudWatch alarme com base em um limite estático no Guia CloudWatch](#) do usuário da Amazon.

- Alarme de detecção de anomalias: a detecção de anomalias mina dados de métricas anteriores e cria um modelo de valores esperados. Você define um valor para o limite de detecção de anomalias e CloudWatch usa esse limite com o modelo para determinar a faixa “normal” de valores para a métrica. Um valor mais alto para o limite produz uma faixa mais larga de valores “normais”. É possível escolher se o alarme deve ser ativado quando o valor

da métrica estiver acima do segmento de valores esperados, abaixo do segmento ou acima ou abaixo do segmento.

Para criar um alarme de detecção de anomalias, consulte [Criação de um CloudWatch alarme com base na detecção de anomalias](#) no Guia CloudWatch do usuário da Amazon.

- Alarme de expressão matemática de métrica: um alarme baseado em uma ou mais métricas usadas em uma expressão matemática. Especifique a expressão, o limite e os períodos de avaliação.

Para criar um alarme de expressão matemática métrica, consulte [Criação de um CloudWatch alarme com base em uma expressão matemática métrica](#) no Guia CloudWatch do usuário da Amazon.

- Alarme composto: um alarme que determina o seu estado de alarme observando os estados de alarme de outros alarmes. Um alarme composto pode ajudar a reduzir o ruído do alarme.

Para criar um alarme composto, consulte [Criação de um alarme composto no Guia CloudWatch](#) do usuário da Amazon.

6. Depois de criar o alarme no CloudWatch console, retorne ao console do Storage Gateway. É possível visualizar o alarme fazendo o seguinte:

- No painel de navegação, escolha Gateways e o gateway para o qual você deseja visualizar os alarmes. Na guia Detalhes, em Alarmes, escolha CloudWatch Alarmes.
- No painel de navegação, escolha Gateways, escolha um gateway para o qual você deseja visualizar os alarmes e escolha a guia Monitoramento.

A seção Alarmes lista todos os CloudWatch alarmes de um gateway específico. Daqui, é possível selecionar e excluir um ou mais alarmes, ativar ou desativar as ações de alarme e criar novos alarmes.

- No painel de navegação, escolha Gateways e o estado de alarme do gateway para o qual você deseja visualizar os alarmes.

Para obter informações sobre como editar ou excluir um alarme, consulte [Editando ou excluindo um CloudWatch alarme](#).

Note

Quando você exclui um gateway usando o console do Storage Gateway, todos os CloudWatch alarmes associados ao gateway também são excluídos automaticamente.

Como monitorar um gateway de volume

Esta seção descreve como monitorar um gateway com configuração de volumes armazenados em cache ou volumes armazenados, incluindo volumes associados ao gateway e o buffer de upload. Você usa o AWS Management Console para visualizar as métricas do seu gateway. Por exemplo, é possível visualizar o número de bytes usado em operações de leitura e gravação, o tempo gasto nas operações de leitura e gravação e o tempo necessário para recuperar dados da nuvem da Amazon Web Services. Com essas métricas, você pode acompanhar a integridade de seu gateway e definir alarmes para notificá-lo quando uma ou mais métricas afastarem-se de um limite definido.

O Storage Gateway fornece CloudWatch métricas sem custo adicional. As métricas do Storage Gateway ficam arquivadas por um período de duas semanas. Ao usar essas métricas, você pode acessar informações históricas e obter uma melhor visão do desempenho do gateway e dos volumes. Para obter informações detalhadas sobre CloudWatch, consulte o [Guia CloudWatch do usuário da Amazon](#).

Tópicos

- [Obtendo registros de saúde do Volume Gateway com o Amazon CloudWatch Logs](#)
- [Usando o Amazon CloudWatch Metrics](#)
- [Como medir o desempenho entre seu aplicativo e o gateway](#)
- [Como medir o desempenho entre o gateway e a AWS](#)
- [Noções básicas de métricas de volume](#)

Obtendo registros de saúde do Volume Gateway com o Amazon CloudWatch Logs

Você pode usar o Amazon CloudWatch Logs para obter informações sobre a integridade do seu Volume Gateway e recursos relacionados. É possível usar esses logs para monitorar o gateway em busca de erros encontrados. Além disso, você pode usar filtros de CloudWatch assinatura da

Amazon para automatizar o processamento das informações de log em tempo real. Para obter mais informações, consulte [Processamento em tempo real de dados de log com assinaturas no Guia CloudWatch](#) do usuário da Amazon.

Por exemplo, suponha que o gateway seja implantado em um cluster compatível com o VMware High Availability (HA) e que você precise saber sobre todos os erros. Você pode configurar um grupo de CloudWatch registros para monitorar seu gateway e ser notificado quando o gateway encontrar um erro. É possível configurar o grupo quando estiver ativando o gateway ou depois que o gateway estiver ativado e em execução. Para obter informações sobre como configurar um grupo de CloudWatch registros ao ativar um gateway, consulte [Configure o gateway de volumes](#). Para obter informações gerais sobre grupos de CloudWatch registros, consulte Como [trabalhar com grupos de registros e fluxos](#) de registros no Guia do CloudWatch usuário da Amazon.

Para obter informações sobre como solucionar problemas e corrigir esses tipos de erros, consulte [Como solucionar problemas em volumes](#).

O procedimento a seguir mostra como configurar um grupo de CloudWatch logs após a ativação do gateway.

Para configurar um grupo de CloudWatch registros para trabalhar com seu gateway

1. Faça login AWS Management Console e abra o console do Storage Gateway em <https://console.aws.amazon.com/storagegateway/home>.
2. No painel de navegação esquerdo, escolha Gateways e, em seguida, escolha o gateway para o qual você deseja configurar o grupo de CloudWatch registros.
3. Em Ações, escolha Editar informações do gateway ou, na guia Detalhes, em Health logs e Not Enabled, escolha Configurar grupo de registros para abrir a caixa de *CustomerGatewayName* diálogo Editar.
4. Em Grupo de logs de integridade do Gateway, escolha uma das seguintes opções:
 - Desative o registro se você não quiser monitorar seu gateway usando grupos de CloudWatch registros.
 - Crie um novo grupo de registros para criar um novo grupo de CloudWatch registros.
 - Use um grupo de registros existente para usar um grupo de CloudWatch registros que já existe. Escolha um grupo de logs na Lista de grupos de logs existentes.
5. Escolha Salvar alterações.
6. Para obter os logs de integridade do gateway, faça o seguinte:

1. No painel de navegação esquerdo, escolha Gateways e, em seguida, escolha o gateway para o qual você configurou o grupo de CloudWatch registros.
2. Escolha a guia Detalhes e, em Health logs, escolha CloudWatch Logs. A página de detalhes do grupo de registros é aberta no CloudWatch console da Amazon.

Usando o Amazon CloudWatch Metrics

Você pode obter dados de monitoramento para seu gateway usando a API AWS Management Console ou a CloudWatch API. O console exibe uma série de gráficos com base nos dados brutos da CloudWatch API. Você também pode usar a CloudWatch API por meio de um dos [kits de desenvolvimento de AWS software \(SDKs\)](#) ou das ferramentas de [CloudWatch API da Amazon](#). Dependendo das necessidades, você pode preferir usar os gráficos exibidos no console ou recuperados da API.

Independentemente do método que você usar para trabalhar com métricas, deverá especificar as seguintes informações:

- A dimensão da métrica com a qual trabalhará. Uma dimensão é um par nome/valor, que ajuda a identificar com exclusividade uma métrica. As dimensões do Storage Gateway são GatewayId, GatewayName e VolumeId. No CloudWatch console, você pode usar as Volume Metrics visualizações Gateway Metrics e para selecionar facilmente as dimensões específicas do gateway e do volume. Para obter mais informações sobre dimensões, consulte [Dimensões](#) no Guia do CloudWatch usuário da Amazon.
- O nome da métrica, como ReadBytes.

A tabela a seguir resume que tipo de dados de métrica do Storage Gateway podem ser usados.

CloudWatch Namespace	Dimensão	Descrição
AWS/StorageGateway	GatewayId , GatewayName	Essas dimensões filtram dados de métrica que descrevem aspectos do gateway. Você pode identificar um gateway com o qual deve trabalhar especificando as dimensões GatewayId e GatewayName .

CloudWatch Namespace	Dimensão	Descrição
		<p>Os dados de throughput e a latência de um gateway se baseiam em todos os volumes no gateway.</p> <p>Os dados são disponibilizados automaticamente em períodos de cinco minutos, sem custo adicional.</p>
	VolumeId	<p>Essa dimensão filtra dados de métrica específicos a um volume. Identifique um volume com o qual deve trabalhar por sua dimensão VolumeId.</p> <p>Os dados são disponibilizados automaticamente em períodos de cinco minutos, sem custo adicional.</p>

Trabalhar com métricas de gateway e volume é semelhante a trabalhar com outras métricas de serviço. Você pode encontrar uma discussão sobre algumas das tarefas mais comuns relacionadas a métricas na documentação do CloudWatch listada a seguir:

- [Visualizar métricas disponíveis](#)
- [Obter estatísticas para uma métrica](#)
- [Criação de alarmes do CloudWatch](#)

Como medir o desempenho entre seu aplicativo e o gateway

A taxa de transferência de dados, a latência de dados e as operações por segundo são três medidas que podem ser usadas para saber qual o desempenho de um armazenamento de aplicativos que esteja usando o gateway. Ao usar a estatística de agregação correta, pode usar as métricas do Storage Gateway para medir esses valores.

Estatística é a agregação de uma métrica durante um espaço de tempo específico. Ao visualizar os valores de uma métrica em CloudWatch, use a Average estatística para latência de dados (milissegundos), use a Sum estatística para taxa de transferência de dados (bytes por segundo) e use a Samples estatística para operações de entrada/saída por segundo (IOPS). Para obter mais informações, consulte [Estatísticas](#) no Guia do CloudWatch usuário da Amazon.

A tabela a seguir resume as métricas e estatísticas correspondentes que você pode usar para medir taxa de transferência, latência e IOPS entre seus aplicativos e gateways.

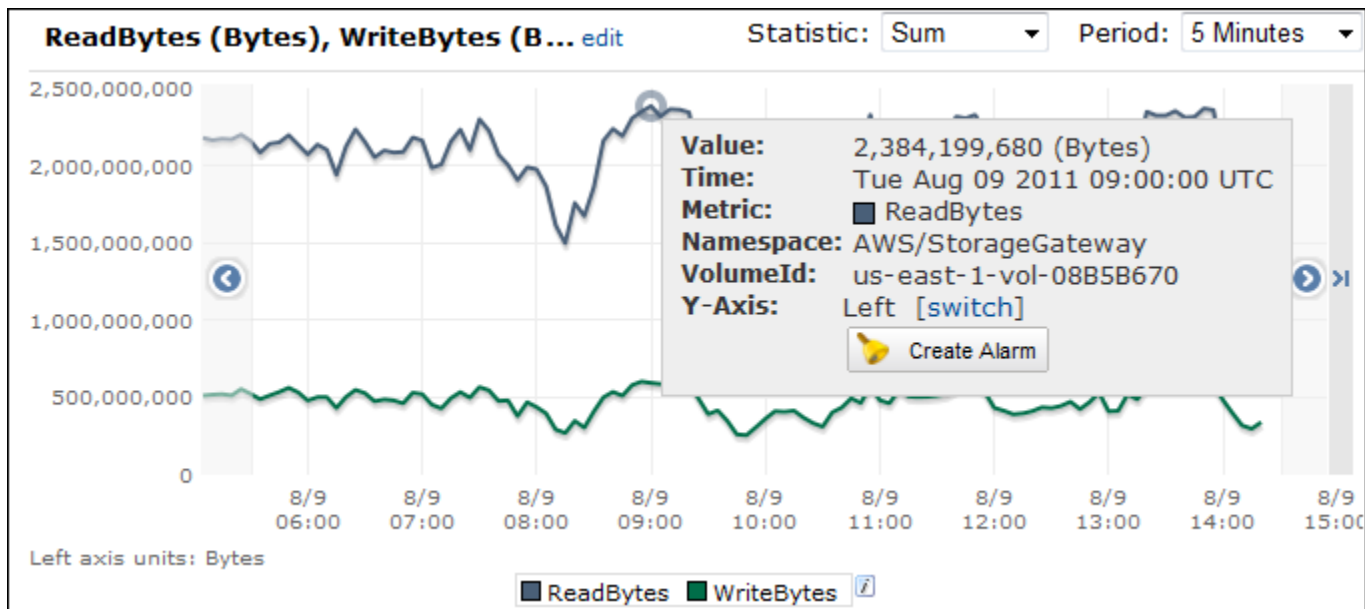
Item de Interesse	Como medir
Throughput	Use as métricas <code>ReadBytes</code> e <code>WriteBytes</code> com a estatística <code>Sum</code> <code>CloudWatch</code> . Por exemplo, o valor <code>Sum</code> da métrica <code>ReadBytes</code> em um período de amostra de 5 minutos dividido por 300 segundos fornece a taxa de transferência em bytes por segundo.
Latência	Use as métricas <code>ReadTime</code> e <code>WriteTime</code> com a estatística <code>Average</code> <code>CloudWatch</code> . Por exemplo, o valor <code>Average</code> da métrica <code>ReadTime</code> fornece a latência por operação durante o período de amostra.
IOPS	Use as métricas <code>ReadBytes</code> e <code>WriteBytes</code> com a estatística <code>Samples</code> <code>CloudWatch</code> . Por exemplo, o valor <code>Samples</code> da métrica <code>ReadBytes</code> durante um período de amostra de 5 minutos dividido por 300 segundos fornece o IOPS.

Para os gráficos de latência média e os gráficos de tamanho médio, a média é calculada em relação ao número total de operações (leitura ou gravação, a que for aplicável ao gráfico) concluídas durante o período.

Para medir a taxa de transferência de dados de um aplicativo para um volume

1. Abra o `CloudWatch` console em <https://console.aws.amazon.com/cloudwatch/>.
2. Escolha `Metrics`, escolha a guia `All metrics` e depois escolha `Storage Gateway`.
3. Escolha a dimensão `Volume metrics` e encontre o volume com o qual deseja trabalhar.
4. Escolha as métricas `ReadBytes` e `WriteBytes`.
5. Em `Time Range`, escolha um valor.
6. Escolha a estatística `Sum`.
7. Em `Period`, escolha o valor de 5 minutos ou superior.
8. Nos conjuntos de pontos de dados resultantes ordenados por tempo (um para `ReadBytes` e um para `WriteBytes`), divida cada ponto de dados pelo período (em segundos) para obter a taxa de transferência no ponto de amostra. A taxa de transferência total é a soma das taxas de transferência.

A imagem a seguir mostra as métricas ReadBytes e WriteBytes para um volume com a estatística Sum. Na imagem, o cursor sobre um ponto de dados exibe informações a respeito do ponto de dados, incluindo o valor e o número de bytes. Divida o valor de bytes pelo valor em Period (5 minutos) para obter a taxa de transferência de dados nesse ponto de amostra. Para o ponto realçado, a taxa de transferência de leitura é 2.384.199.680 bytes divididos por 300 segundos, o que resulta em 7,6 megabytes por segundo.

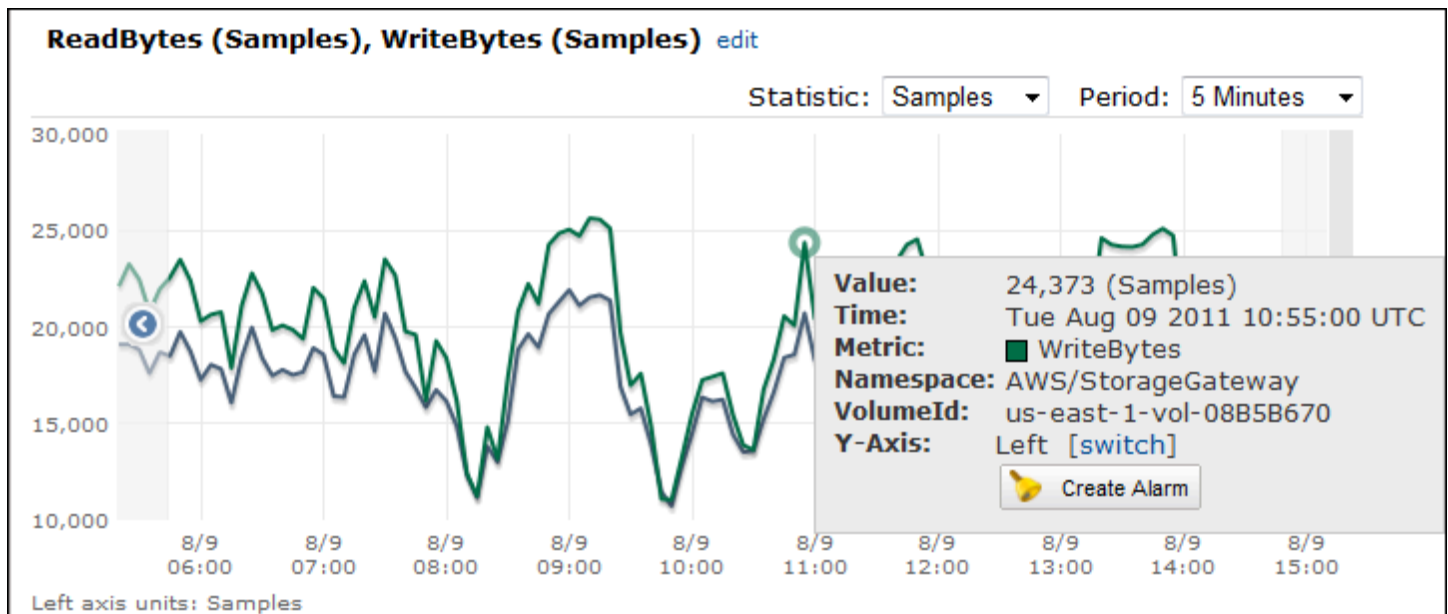


Para medir as operações de entrada/saída de dados por segundo de um aplicativo para um volume

1. Abra o CloudWatch console em <https://console.aws.amazon.com/cloudwatch/>.
2. Escolha Metrics, escolha a guia All metrics e depois escolha Storage Gateway.
3. Escolha a dimensão Volume metrics e encontre o volume com o qual deseja trabalhar.
4. Escolha as métricas ReadBytes e WriteBytes.
5. Em Time Range, escolha um valor.
6. Escolha a estatística Samples.
7. Em Period, escolha o valor de 5 minutos ou superior.
8. Nos conjuntos de pontos de dados resultantes ordenados por tempo (um para ReadBytes e um para WriteBytes), divida cada ponto de dados pelo período (em segundos) para obter o IOPS.

A imagem a seguir mostra as métricas ReadBytes e WriteBytes para um volume de armazenamento com a estatística Samples. Na imagem, o cursor sobre um ponto de dados exibe informações a respeito do ponto de dados, incluindo o valor e o número de amostras. Divida o valor

de amostras pelo valor em Period (5 minutos) para obter as operações por segundo nesse ponto de amostra. Para o ponto realçado, a taxa de transferência de leitura é 24.373 bytes divididos por 300 segundos, o que resulta em 81 operações de leitura por segundo.



Como medir o desempenho entre o gateway e a AWS

O throughput de dados, a latência de dados e as operações por segundo são três medidas que podem ser usadas para saber qual o desempenho de um armazenamento de aplicações que esteja usando o Storage Gateway. Estes três valores podem ser medidos usando as métricas do Storage Gateway que são fornecidas quando você usa a estatística de agregação correta. A tabela a seguir resume as métricas e estatísticas correspondentes a serem usadas para medir o throughput, a latência e as operações de entrada e saída por segundo (IOPS) entre o gateway e a AWS.

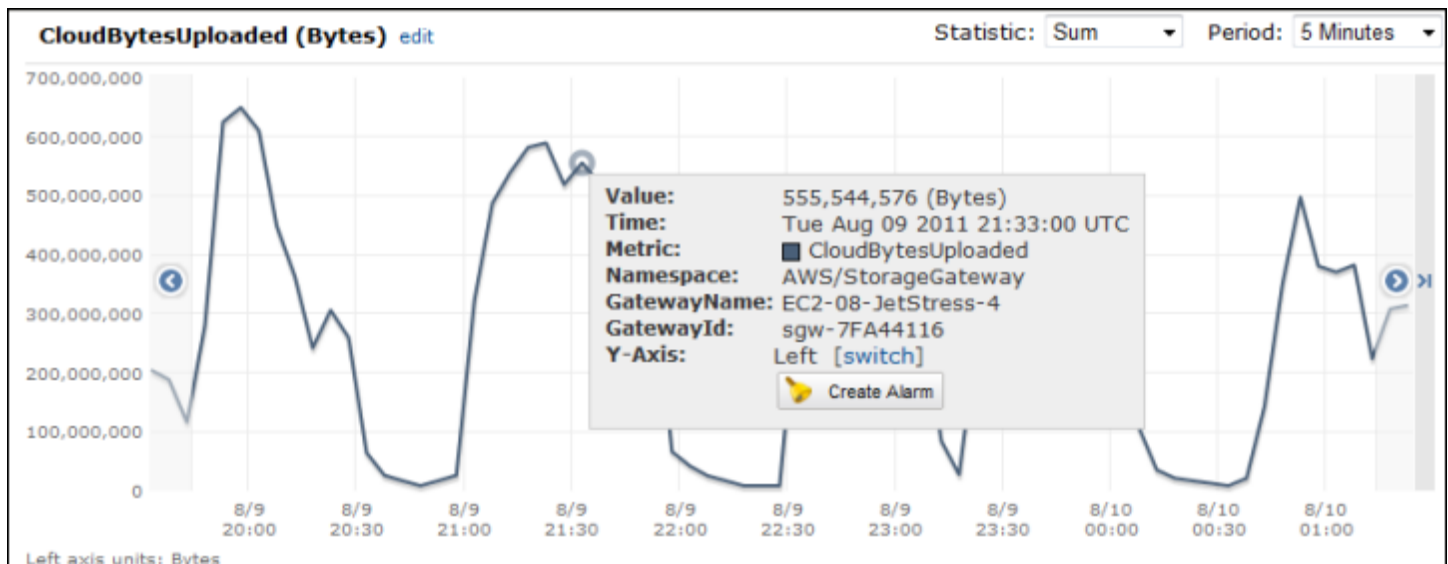
Item de Interesse	Como medir
Throughput	Use as métricas <code>ReadBytes</code> e <code>WriteBytes</code> com a estatística <code>Sum</code> <code>CloudWatch</code> . Por exemplo, o valor <code>Sum</code> da métrica <code>ReadBytes</code> em um período de amostra de 5 minutos dividido por 300 segundos fornece a taxa de transferência em bytes por segundo.
Latência	Use as métricas <code>ReadTime</code> e <code>WriteTime</code> com a estatística <code>Average</code> <code>CloudWatch</code> . Por exemplo, o valor <code>Average</code> da métrica <code>ReadTime</code> fornece a latência por operação durante o período de amostra.

Item de Interesse	Como medir
IOPS	Use as métricas <code>ReadBytes</code> e <code>WriteBytes</code> com a estatística <code>Samples</code> CloudWatch. Por exemplo, o valor <code>Samples</code> da métrica <code>ReadBytes</code> durante um período de amostra de 5 minutos dividido por 300 segundos fornece o IOPS.
Rendimento até AWS	Use as <code>CloudBytesUploaded</code> métricas <code>CloudBytesDownloaded</code> e com a <code>Sum</code> CloudWatch estatística. Por exemplo, o <code>Sum</code> valor da <code>CloudBytesDownloaded</code> métrica em um período de amostragem de 5 minutos dividido por 300 segundos fornece a taxa de transferência de AWS até o gateway em bytes por segundo.
Latência dos dados para AWS	Use a métrica <code>CloudDownloadLatency</code> com a estatística <code>Average</code> . Por exemplo, a estatística <code>Average</code> da métrica <code>CloudDownloadLatency</code> fornece a latência por operação.

Para medir a taxa de transferência de dados de upload de um gateway para AWS

1. Abra o CloudWatch console em <https://console.aws.amazon.com/cloudwatch/>.
2. Escolha Metrics, escolha a guia All metrics e depois escolha Storage Gateway.
3. Escolha a dimensão Gateway metrics e encontre o volume com o qual deseja trabalhar.
4. Escolha a métrica `CloudBytesUploaded`.
5. Em Time Range, escolha um valor.
6. Escolha a estatística `Sum`.
7. Em Period, escolha o valor de 5 minutos ou superior.
8. No conjunto de pontos de dados resultante, ordenados por tempo, divida cada ponto de dados pelo período (em segundos) para obter a taxa de transferência nesse período de amostra.

A imagem a seguir mostra as métricas `CloudBytesUploaded` para um volume de gateway com a estatística `Sum`. Na imagem, o cursor sobre um ponto de dados exibe informações a respeito do ponto de dados, incluindo o valor e os bytes carregados. Divida esse valor pelo valor em Period (5 minutos) para obter a taxa de transferência nesse ponto de amostra. Para o ponto destacado, a taxa de transferência do gateway para AWS é de 555.544.576 bytes dividida por 300 segundos, o que é 1,7 megabytes por segundo.



Para medir a latência por operação de um gateway

1. Abra o CloudWatch console em <https://console.aws.amazon.com/cloudwatch/>.
2. Escolha Metrics, escolha a guia All metrics e depois escolha Storage Gateway.
3. Escolha a dimensão Gateway metrics e encontre o volume com o qual deseja trabalhar.
4. Escolha as métricas ReadTime e WriteTime.
5. Em Time Range, escolha um valor.
6. Escolha a estatística Average.
7. Em Period, escolha o valor de 5 minutos para corresponder ao período de relatório padrão.
8. No conjunto de pontos resultante, ordenados por tempo (um para ReadTime e um para WriteTime), adicione pontos de dados e ao mesmo tempo amostra para obter a latência total em milissegundos.

Para medir a latência de dados de um gateway para AWS

1. Abra o CloudWatch console em <https://console.aws.amazon.com/cloudwatch/>.
2. Escolha Metrics, escolha a guia All metrics e depois escolha Storage Gateway.
3. Escolha a dimensão Gateway metrics e encontre o volume com o qual deseja trabalhar.
4. Escolha a métrica CloudDownloadLatency.
5. Em Time Range, escolha um valor.
6. Escolha a estatística Average.

7. Em **Period**, escolha o valor de 5 minutos para corresponder ao período de relatório padrão.

O conjunto de pontos de dados resultante, ordenados por tempo, contém a latência em milissegundos.

Para definir um alarme de limite superior para a taxa de transferência de um gateway para AWS

1. Abra o CloudWatch console em <https://console.aws.amazon.com/cloudwatch/>.
2. Escolha **Alarmes**.
3. Selecione **Create Alarm (Criar alarme)** para iniciar o assistente de criação de alarme.
4. Escolha a dimensão **Storage Gateway** e encontre o gateway com o qual deseja trabalhar.
5. Escolha a métrica **CloudBytesUploaded**.
6. Para definir o alarme, defina o estado do alarme quando a métrica **CloudBytesUploaded** for superior ou igual ao valor especificado durante o período especificado. Por exemplo, você pode definir um alarme quando a métrica **CloudBytesUploaded** mantiver-se superior a 10 MB durante 60 minutos.
7. Configure as ações a serem tomadas para o estado do alarme. Por exemplo, você pode definir o envio de notificação por e-mail.
8. Escolha **Create Alarm**.

Para definir um alarme de limite superior para leitura de dados de AWS

1. Abra o CloudWatch console em <https://console.aws.amazon.com/cloudwatch/>.
2. Selecione **Create Alarm (Criar alarme)** para iniciar o assistente de criação de alarme.
3. Escolha a dimensão **StorageGateway: Gateway Metrics** e encontre o gateway com o qual você deseja trabalhar.
4. Escolha a métrica **CloudDownloadLatency**.
5. Para definir o alarme, defina o estado do alarme quando a métrica **CloudDownloadLatency** for superior ou igual ao valor especificado durante o período especificado. Por exemplo, você pode definir um alarme quando a métrica **CloudDownloadLatency** mantiver-se superior a 60.000 milissegundos por mais de 2 horas.
6. Configure as ações a serem tomadas para o estado do alarme. Por exemplo, você pode definir o envio de notificação por e-mail.
7. Escolha **Create Alarm**.

Noções básicas de métricas de volume

É possível encontrar informações a seguir sobre as métricas do Storage Gateway que abrangem volumes de um gateway. Cada volume de um gateway tem um conjunto de métricas associado a ele.

Algumas métricas específicas do volume têm o mesmo nome que determinadas métricas específicas do gateway. Essas métricas representam medições do mesmo tipo, mas são dimensionadas para o volume, e não para o gateway. Antes de iniciar o trabalho, especifique se deseja trabalhar com uma métrica de gateway ou uma métrica de volume. Especificamente, ao trabalhar com métricas de volume, especifique o ID do volume de armazenamento do qual você deseja visualizar as métricas. Para ter mais informações, consulte [Usando o Amazon CloudWatch Metrics](#).

Note

Algumas métricas retornam pontos de dados somente quando novos dados são gerados durante o período de monitoramento mais recente.

A tabela a seguir descreve as métricas do Storage Gateway que podem ser usadas para obter informações sobre os volumes de armazenamento.

Métrica	Descrição	Volumes armazenados em cache	Volumes armazenados
AvailabilityNotification	O número de notificações de disponibilidades enviadas pelo volume. Unidade: contagem	Sim	Sim
CacheHitPercent	Porcentagem de operações de leitura do aplicativo do volume que são feitas pelo cache. A amostra é capturada	Sim	Não

Métrica	Descrição	Volumes armazenados em cache	Volumes armazenados
	<p>no final do período do relatório.</p> <p>Quando não há operações de leitura do aplicativo a partir do volume, esta métrica relata 100%.</p> <p>Unidades: percentual</p>		
CachePercentDirty	<p>A contribuição do volume para o percentual geral do cache do gateway que não persiste na AWS. A amostra é capturada no final do período do relatório.</p> <p>Use a métrica CachePercentDirty do gateway para visualizar o percentual geral do cache do gateway que não persiste na AWS. Para ter mais informações, consulte Noções básicas de métricas de gateway.</p> <p>Unidades: percentual</p>	Sim	Sim

Métrica	Descrição	Volumes armazenados em cache	Volumes armazenados
CachePercentUsed	<p>A contribuição do volume para o percentual geral de uso do armazenamento em cache do gateway. A amostra é capturada no final do período do relatório.</p> <p>Use a métrica CachePercentUsed do gateway para visualizar o percentual geral de uso do cache do gateway de armazenamento. Para ter mais informações, consulte Noções básicas de métricas de gateway.</p> <p>Unidades: percentual</p>	Sim	Não
CloudBytesDownloaded	<p>A quantidade de bytes obtidos baixados da nuvem para o volume.</p> <p>Unidades: bytes</p>	Sim	Sim
CloudBytesUploaded	<p>A quantidade de bytes carregados da nuvem para o volume.</p> <p>Unidades: bytes</p>	Sim	Sim

Métrica	Descrição	Volumes armazenados em cache	Volumes armazenados
HealthNotification	O número de notificações de integridade enviadas pelo volume. Unidade: contagem	Sim	Sim
IoWaitPercent	A porcentagem de IoWaitPercent unidades usadas atualmente pelo volume. Unidades: percentual	Sim	Sim
MemTotalBytes	A porcentagem de memória total que está sendo usada pelo volume. Unidades: percentual	Sim	Não
MemoryUsage	A porcentagem de memória que está sendo usada pelo volume. Unidades: percentual	Sim	Não

Métrica	Descrição	Volumes armazenados em cache	Volumes armazenados
ReadBytes	<p>O número total de bytes lidos dos aplicativos locais no período do relatório.</p> <p>Use essa métrica com a estatística Sum para medir a taxa de transferência e com a estatística Samples para medir IOPS.</p> <p>Unidades: bytes</p>	Sim	Sim
ReadTime	<p>O número total de milissegundos gastos em operações de leitura dos aplicativos no local durante o período do relatório.</p> <p>Use essa métrica com a estatística Average para medir a latência.</p> <p>Unidade: milissegundos</p>	Sim	Sim

Métrica	Descrição	Volumes armazenados em cache	Volumes armazenados
UserCpuPercent	<p>A porcentagem de unidades de computação da CPU alocadas que são usadas atualmente pelo volume.</p> <p>Unidades: percentual</p>	Sim	Sim
WriteBytes	<p>O número total de bytes gravados nos aplicativos locais no período do relatório.</p> <p>Use essa métrica com a estatística Sum para medir a taxa de transferência e com a estatística Samples para medir IOPS.</p> <p>Unidades: bytes</p>	Sim	Sim

Métrica	Descrição	Volumes armazenados em cache	Volumes armazenados
<code>WriteTime</code>	<p>O número total de milissegundos gastos em operações de gravação dos aplicativos no local durante o período do relatório.</p> <p>Use essa métrica com a estatística <code>Average</code> para medir a latência.</p> <p>Unidade: milissegundos</p>	Sim	Sim
<code>QueuedWrites</code>	<p>O número de bytes aguardando para serem gravados AWS, amostrado no final do período do relatório.</p> <p>Unidades: bytes</p>	Sim	Sim

Como manter seu gateway

A manutenção de seu gateway inclui tarefas como configuração de armazenamento em cache e espaço do buffer de upload e manutenção geral do desempenho de seu gateway. Essas tarefas são comuns a todos os tipos de gateway. Se você não tiver criado um gateway, consulte [Como criar um gateway](#).

Tópicos

- [Encerramento da VM do gateway](#)
- [Como gerenciar discos locais para o Storage Gateway](#)
- [Gerenciando a largura de banda do seu gateway de volumes](#)
- [Gerenciando atualizações de gateway usando o AWS Storage Gateway console](#)
- [Como executar tarefas de manutenção no console local](#)
- [Como excluir seu gateway usando o console do AWS Storage Gateway e como limpar os recursos associados](#)

Encerramento da VM do gateway

Você pode precisar encerrar ou reiniciar a VM para manutenção; por exemplo, ao aplicar um patch ao hipervisor. Antes de desligar a VM, você deve primeiro interromper o gateway. Para o gateway de arquivos, basta encerrar a VM. Embora o foco desta seção seja mostrar como o gateway é iniciado e interrompido por meio do Storage Gateway Management Console, você também pode iniciá-lo e encerrá-lo usando o console local da VM ou a API do Storage Gateway. Quando você ligar a VM, lembre-se de reiniciar o gateway.

Important

Se você estiver usando o armazenamento temporário e interromper e iniciar o gateway do Amazon EC2, o gateway ficará permanentemente off-line. Isso acontece porque o disco de armazenamento físico é substituído. Não há uma solução alternativa para esse problema. A única solução é excluir o gateway e ativar um novo em uma nova instância do EC2.

Note

Se encerrar seu gateway enquanto o software de backup estiver gravando ou lendo em uma fita, a tarefa de gravação ou leitura pode não funcionar. Para encerrar seu gateway, você deve primeiro verificar o software de backup e a programação de backup de qualquer tarefas em andamento.

- Console local da VM do gateway, consulte [Como fazer login no console local usando credenciais padrão](#).
- API Storage Gateway — consulte [ShutdownGateway](#)

Para o gateway de arquivos, simplesmente encerre a VM. Você não desliga o gateway.

Como iniciar e interromper um gateway de volumes

Para interromper um gateway de volumes

1. Abra o console do Storage Gateway em <https://console.aws.amazon.com/storagegateway/home>.
2. No painel de navegação, escolha Gateways e, em seguida, o gateway a ser interrompido. O status do gateway é Running.
3. Em Actions (Ações), escolha Stop gateway (Interromper gateway), verifique o ID do gateway na caixa de diálogo e, depois, escolha Stop gateway (Interromper gateway).

Enquanto o gateway estiver interrompido, você provavelmente verá uma mensagem indicando o status do gateway. Quando o gateway é encerrado, uma mensagem e o botão Start gateway aparecem na guia Details.

Quando interrompe seu gateway, os recursos de armazenamento ficarão inacessíveis até você iniciar seu armazenamento. Caso o gateway tenha sido interrompido enquanto fazia upload de dados, o upload será retomado quando você iniciar o gateway.

Para iniciar um gateway de volumes

1. Abra o console do Storage Gateway em <https://console.aws.amazon.com/storagegateway/home>.
2. No painel de navegação, escolha Gateways e, em seguida, o gateway a ser iniciado. O status do gateway é Shutdown.

3. Escolha Detalhes e Inicie.

Como gerenciar discos locais para o Storage Gateway

O gateway da máquina virtual (VM) usa os discos locais que você aloca no local para buffer e armazenamento. Os gateways criados em instâncias do Amazon EC2 usam volumes do Amazon EBS como discos locais.

Tópicos

- [Como determinar o volume de armazenamento do disco local](#)
- [Como determinar o tamanho do buffer de upload para alocar](#)
- [Como determinar o tamanho do armazenamento em cache para alocar](#)
- [Como configurar um buffer de upload ou armazenamento em cache](#)

Como determinar o volume de armazenamento do disco local


Você decide o número e o tamanho dos discos que deseja alocar para o gateway. Dependendo da solução de armazenamento que implantar (consulte [Planeje sua implantação do Storage Gateway](#)), o gateway exigirá o seguinte armazenamento adicional:

- Gateways de volumes:
 - Gateways armazenados exigem pelo menos um disco para usar como buffer de upload.
 - Gateways em cache exigem pelo menos dois discos. Um para uso como cache e um para uso como buffer de upload.

A tabela a seguir recomenda tamanhos para armazenamento em disco local para o gateway implantado. Você pode adicionar mais armazenamento local depois de configurar o gateway e conforme a demanda de carga de trabalho aumentar.

Armazenamento local	Descrição	
Buffer de upload	O buffer de upload fornece uma área de preparação para os dados antes de o gateway fazer upload dos dados para o Amazon S3. Seu	

Armazenamento local	Descrição	
	gateway faz upload desses dados do buffer para a AWS por meio de uma conexão Secure Sockets Layer (SSL) criptografada.	
Armazenamento em cache	O armazenamento em cache funciona como um armazenamento on-premises duradouro para dados no buffer com upload pendente para o Amazon S3. Quando seu aplicativo executa E/S em um volume ou em uma fita, o gateway economiza os dados para o armazenamento em cache para acesso de baixa latência. Quando seu aplicativo solicita dados de um volume ou de uma fita, o gateway primeiro verifica o armazenamento em cache para os dados antes de baixar os dados provenientes da AWS.	

 Note

Ao provisionar discos, é altamente recomendável não provisionar discos locais para o buffer de upload e armazenamento em cache, se eles usarem os mesmos recursos físicos (o mesmo disco). Os recursos de armazenamento físico subjacentes são representados como armazenamento de dados no VMware. Ao implantar a VM do gateway, você escolhe um armazenamento de dados para armazenar os arquivos da VM. Ao provisionar um disco local (por exemplo, para uso como armazenamento em cache ou buffer de upload), você tem a opção de armazenar o disco virtual no mesmo armazenamento de dados que a VM ou outro armazenamento de dados distinto.

Se você tiver mais de um armazenamento de dados, é altamente recomendável escolher um armazenamento de dados para o armazenamento em cache e outro para o buffer de

upload. O armazenamento de dados que conta apenas com um disco físico subjacente pode apresentar um desempenho ruim em algumas situações, quando é usado para respaldar o armazenamento em cache e o buffer de upload. Isso também é válido quando o backup é uma configuração de RAID menos eficiente, como RAID1.

Após a configuração inicial e a implantação do gateway, você pode ajustar o armazenamento local adicionando ou removendo discos para um buffer de upload. Você também pode adicionar discos para armazenamento em cache.

Como determinar o tamanho do buffer de upload para alocar

Você pode determinar o tamanho do buffer de upload para alocar usando uma fórmula para isso. É altamente recomendável alocar pelo menos 150 GiB de buffer de upload. Se a fórmula retornar um valor inferior a 150 GiB, use 150 GiB como espaço alocado no buffer de upload. Você pode configurar até 2 TiB de capacidade de buffer de upload para cada gateway.

Note

Em gateways de volumes, quando a capacidade do buffer de upload atinge a respectiva capacidade, o volume assume o status `PASS THROUGH`. Nesse status, os novos dados que seu aplicativo grava são mantidos localmente, mas não são enviados AWS imediatamente. Desse modo, você não pode tirar novos snapshots. Quando há liberação de capacidade no buffer de upload, o volume assume o status `BOOTSTRAPPING`. Nesse status, todos os novos dados que foram persistidos localmente são enviados para AWS. Por fim, o volume retorna ao status `ACTIVE`. Em seguida, o Storage Gateway retoma a sincronização normal dos dados armazenados localmente com a cópia armazenada AWS, e você pode começar a tirar novos instantâneos. Para obter mais informações sobre status de volume, consulte [Noções básicas sobre transições e status de volumes](#).

Para estimar o espaço do buffer de upload para alocar, você pode determinar as taxas de dados de entrada e saída e inseri-las na fórmula a seguir.

Taxa de dados de entrada

Essa taxa refere-se à taxa de transferência do aplicativo, aquela segundo a qual seus aplicativos locais gravam dados em seu gateway, durante um espaço de tempo específico.

Taxa de dados de saída

Essa taxa refere-se à taxa de transferência de rede, aquela segundo a qual seu gateway é capaz de fazer upload de dados para a AWS. Esta taxa depende da velocidade de sua rede, de sua utilização, e de você ter ativado o controle de utilização de largura de banda. Ela deve ser ajustada para compactação. Ao fazer o upload de dados para AWS, o gateway aplica a compactação de dados sempre que possível. Por exemplo, se os dados do aplicativo forem somente texto, você pode obter uma taxa de compactação eficaz de cerca de 2:1. No entanto, se você estiver gravando vídeos, o gateway talvez não consiga obter nenhuma compactação de dados e pode exigir um buffer de upload maior para o gateway.

É altamente recomendável que você aloque pelo menos 150 GiB de espaço de buffer de upload em uma das seguintes situações:

- Sua taxa de entrada é maior do que a taxa de saída.
- A fórmula retorna um valor menor que 150 GiB.

$$\left(\text{Application Throughput (MB/s)} - \text{Network Throughput to AWS (MB/s)} \times \text{Compression Factor} \right) \times \text{Duration of writes (s)} = \text{Upload Buffer (MB)}$$

Por exemplo, imagine que seus aplicativos de negócios gravam dados de texto no gateway a uma taxa de 40 MB por segundo durante 12 horas por dia, e a taxa de transferência de rede é de 12 MB por segundo. Supondo um fator de compressão de 2:1 para os dados de texto, você alocaria aproximadamente 690 GiB de espaço para o buffer de upload.

Example

$$((40 \text{ MB/sec}) - (12 \text{ MB/sec} * 2)) * (12 \text{ hours} * 3600 \text{ seconds/hour}) = 691200 \text{ megabytes}$$

Inicialmente, você pode usar essa estimativa para determinar o tamanho do disco que deseja alocar ao gateway como espaço do buffer de upload. Amplie o espaço do buffer de upload conforme a necessidade usando o console do Storage Gateway. Além disso, você pode usar as métricas CloudWatch operacionais da Amazon para monitorar o uso do buffer de upload e determinar requisitos adicionais de armazenamento. Para obter informações sobre métricas e configuração de alarmes, consulte [Monitorar o buffer de upload](#).

Como determinar o tamanho do armazenamento em cache para alocar

Seu gateway usa armazenamento em cache para fornecer acesso de baixa latência aos dados recém-acessados. O armazenamento em cache funciona como um armazenamento on-premises duradouro para dados no buffer com upload pendente para o Amazon S3. De modo geral, costuma-se dimensionar o armazenamento em cache com 1,1 vez o tamanho do buffer de upload. Para obter mais informações sobre como estimar o tamanho do armazenamento em cache, consulte [Como determinar o tamanho do buffer de upload para alocar](#).

A princípio, você pode usar essa estimativa para provisionar discos para armazenamento em cache. Em seguida, você pode usar as métricas CloudWatch operacionais da Amazon para monitorar o uso do armazenamento em cache e provisionar mais armazenamento conforme necessário usando o console. Para obter informações sobre como usar métricas e configurar de alarmes, consulte [Monitorar um armazenamento em cache](#).

Como configurar um buffer de upload ou armazenamento em cache

À medida que as necessidades de seu aplicativo mudarem, você poderá aumentar a capacidade de armazenamento em cache ou de buffer de upload do gateway. É possível adicionar a capacidade de armazenamento ao seu gateway sem interromper a funcionalidade ou causar tempo de inatividade. Ao adicionar mais armazenamento, você o faz com a VM do gateway ativada.


Important

Ao adicionar cache ou fazer upload de buffer para um gateway existente, você deve criar novos discos no hipervisor do host do gateway ou na instância do Amazon EC2. Não remova nem altere o tamanho dos discos existentes que já foram alocados como cache ou buffer de upload.

Para configurar um buffer de upload ou armazenamento em cache adicionais para o gateway

1. Provisione um ou mais discos novos no gateway, no host, no hipervisor ou na instância do Amazon EC2. Para obter informações sobre como provisionar um disco em um hipervisor, consulte o manual do usuário do hipervisor. Para obter informações sobre o provisionamento de volumes do Amazon EBS para uma instância do Amazon EC2, consulte [Volumes do Amazon EBS](#) no Manual do usuário para instâncias do Linux do Amazon Elastic Computer Cloud. Nas etapas a seguir, você configurará esse disco como buffer de upload ou armazenamento em cache.

2. Abra o console do Storage Gateway em <https://console.aws.amazon.com/storagegateway/home>.
3. No painel de navegação, selecione Gateways da .
4. Procure seu gateway e selecione-o na lista.
5. No menu Ações, selecione Configurar armazenamento.
6. Na seção Configurar armazenamento, identifique os discos que você provisionou. Se você não vir os discos, selecione o ícone de atualização para atualizar a lista. Para cada disco, escolha UPLOAD BUFFER (Buffer do upload) ou CACHE STORAGE (Armazenamento em cache) no menu suspenso Alocado para.

 Note

O UPLOAD BUFFER é a única opção disponível para alocar discos em gateways de volumes armazenados.

7. Escolha Salvar alterações para salvar as definições de configuração.

Gerenciando a largura de banda do seu gateway de volumes

Você pode limitar (ou limitar) a taxa de transferência de upload do gateway para AWS ou a taxa de transferência de AWS download para seu gateway. O controle de largura de banda ajuda você a controlar a largura de banda da rede usada por seu gateway. Por padrão, um gateway ativado não tem limites para taxas de upload ou download.

Você pode especificar o limite de taxa usando ou programaticamente usando a AWS Management Console API Storage Gateway (consulte [UpdateBandwidthRateLimit](#)) ou um kit de desenvolvimento de AWS software (SDK). Com o controle de utilização programático da largura de banda, é possível alterar os limites automaticamente durante o dia como, por exemplo, programando tarefas para alterar a largura de banda.

Também é possível definir o controle de utilização de largura de banda baseada em agendamento para seu gateway. Você agenda a limitação da largura de banda definindo um ou mais intervalos. `bandwidth-rate-limit` Para ter mais informações, consulte [Controle de utilização da largura de banda por meio do agendamento usando o console do Storage Gateway](#).

Definir uma única configuração para limitação de largura de banda é o equivalente funcional de definir uma programação com um único `bandwidth-rate-limit` intervalo definido para todos os dias, com uma hora de início **00:00** e uma hora de término de **23:59**

Note

As informações nesta seção são específicas para gateways de fitas e volumes. Para gerenciar a largura de banda de um gateway de arquivos do Amazon S3, consulte [Como gerenciar a largura de banda do gateway de arquivos do Amazon S3](#). Atualmente, os limites de taxa de largura de banda não são suportados pelo gateway de arquivos do Amazon FSx.

Tópicos

- [Como alterar o controle de utilização da largura de banda por meio do console do Storage Gateway](#)
- [Controle de utilização da largura de banda por meio do agendamento usando o console do Storage Gateway](#)
- [Atualizando os limites de taxa de largura de banda do gateway usando o AWS SDK for Java](#)
- [Atualizando os limites de taxa de largura de banda do gateway usando o AWS SDK for .NET](#)
- [Atualizando os limites de taxa de largura de banda do gateway usando o AWS Tools for Windows PowerShell](#)

Como alterar o controle de utilização da largura de banda por meio do console do Storage Gateway

O procedimento a seguir mostra como alterar o controle de utilização da largura de banda de um gateway por meio do console do Storage Gateway.

Para alterar o controle de largura de banda de um gateway por meio do console

1. Abra o console do Storage Gateway em <https://console.aws.amazon.com/storagegateway/home>.
2. No painel de navegação, escolha Gateways e, em seguida, o gateway que você deseja gerenciar.
3. Em Ações, escolha Editar limite da taxa de largura de banda.
4. Na caixa de diálogo Editar limites de taxa, insira os novos valores de limite e escolha Salvar. Suas alterações são exibidas na guia Details de seu gateway.

Controle de utilização da largura de banda por meio do agendamento usando o console do Storage Gateway

O procedimento a seguir mostra como alterar o controle de utilização da largura de banda de um gateway usando o console do Storage Gateway.

Para adicionar ou modificar um agendamento para controle de utilização da largura de banda do gateway

1. Abra o console do Storage Gateway em <https://console.aws.amazon.com/storagegateway/home>.
2. No painel de navegação, escolha Gateways e, em seguida, o gateway que você deseja gerenciar.
3. Em Ações, escolha Editar programação do limite da taxa de largura de banda.

A bandwidth-rate-limit programação do gateway é exibida na caixa de diálogo Editar programação de limite de taxa de largura de banda. Por padrão, uma nova bandwidth-rate-limit agenda de gateway está vazia.

4. Na caixa de diálogo Editar programação de limite de taxa de largura de banda, escolha Adicionar novo item para adicionar um novo bandwidth-rate-limit intervalo. Insira as seguintes informações para cada bandwidth-rate-limit intervalo:
 - Dias da semana — Você pode criar o bandwidth-rate-limit intervalo para os dias da semana (de segunda a sexta-feira), para fins de semana (sábado e domingo), para todos os dias da semana ou para um ou mais dias específicos da semana.
 - Hora de término: insira a hora de término para o intervalo de largura de banda no fuso horário local do gateway, usando o formato HH:MM.

Note

Seu bandwidth-rate-limit intervalo começa no início do minuto especificado aqui.

- Hora de término — Insira a hora de término do bandwidth-rate-limit intervalo no fuso horário local do gateway, usando o formato HH:MM.

Important

O bandwidth-rate-limit intervalo termina no final do minuto especificado aqui. Para agendar um intervalo que termine no final de uma hora, insira **59**.

Para programar intervalos contínuos consecutivos, fazendo a transição no início da hora, sem interrupção entre os intervalos, insira **59** para o minuto final do primeiro intervalo. Insira **00** para o minuto inicial do intervalo seguinte.


- Taxa de download: insira o limite da taxa de download, em kilobits por segundo (Kbps), ou selecione Sem limite para desativar o controle de utilização da largura de banda para download. O valor mínimo da taxa de download é 100 Kbps.
- Taxa de upload: insira o limite da taxa de upload, em Kbps, ou selecione Sem limite para desativar o controle de utilização da largura de banda para upload. O valor mínimo da taxa de upload é 50 Kbps.

Para modificar seus bandwidth-rate-limit intervalos, você pode inserir valores revisados para os parâmetros do intervalo.

Para remover seus bandwidth-rate-limit intervalos, você pode escolher Remover à direita do intervalo a ser excluído.

Quando você tiver concluído as alterações, escolha Salvar.

5. Continue adicionando bandwidth-rate-limit intervalos escolhendo Adicionar novo item e inserindo o dia, os horários de início e término e os limites da taxa de download e upload.

 Important

bandwidth-rate-limit Os intervalos B não podem se sobrepor. A hora de início de um intervalo deve ocorrer após a hora de término de um intervalo anterior e antes da hora de início de um intervalo seguinte.

6. Depois de inserir todos os bandwidth-rate-limit intervalos, escolha Salvar alterações para salvar sua bandwidth-rate-limit agenda.

Quando a bandwidth-rate-limit programação for atualizada com sucesso, você poderá ver os limites atuais da taxa de download e upload no painel Detalhes do gateway.

Atualizando os limites de taxa de largura de banda do gateway usando o AWS SDK for Java

Ao atualizar programaticamente os limites de taxa de largura de banda, é possível ajustar limites automaticamente ao longo de um período como, por exemplo, usando tarefas programadas. O exemplo a seguir demonstra como atualizar os limites de taxa de largura de banda de um gateway usando o AWS SDK for Java. Para usar o código de exemplo, você deve estar familiarizado com a execução de aplicativos em console Java. Para obter mais informações, consulte [Conceitos básicos](#) no Guia do desenvolvedor do AWS SDK for Java .

Example : Atualizando os limites de taxa de largura de banda do gateway usando o AWS SDK for Java

O exemplo de código Java a seguir atualiza os limites de taxa de largura de banda de um gateway. Você precisa atualizar o código e fornecer o endpoint de serviço, o nome do recurso da Amazon (ARN) para o gateway e os limites de upload e download. Para obter uma lista de endpoints de AWS serviço que você pode usar com o Storage Gateway, consulte [AWS Storage Gateway Endpoints and Quotas](#) no. Referência geral da AWS

```
import java.io.IOException;

import com.amazonaws.AmazonClientException;
import com.amazonaws.auth.PropertiesCredentials;
import com.amazonaws.services.storagegateway.AWSStorageGatewayClient;
import com.amazonaws.services.storagegateway.model.UpdateBandwidthRateLimitRequest;
import com.amazonaws.services.storagegateway.model.UpdateBandwidthRateLimitResult;

public class UpdateBandwidthExample {

    public static AWSStorageGatewayClient sgClient;

    // The gatewayARN
    public static String gatewayARN = "*** provide gateway ARN ***";

    // The endpoint
    static String serviceURL = "https://storagegateway.us-east-1.amazonaws.com";

    // Rates
    static long uploadRate = 51200; // Bits per second, minimum 51200
    static long downloadRate = 102400; // Bits per second, minimum 102400
```

```
public static void main(String[] args) throws IOException {

    // Create a Storage Gateway client
    sgClient = new AWSStorageGatewayClient(new PropertiesCredentials(
UpdateBandwidthExample.class.getResourceAsStream("AwsCredentials.properties")));
    sgClient.setEndpoint(serviceURL);

    UpdateBandwidth(gatewayARN, uploadRate, downloadRate);

}

private static void UpdateBandwidth(String gatewayARN2, long uploadRate2,
    long downloadRate2) {
    try
    {
        UpdateBandwidthRateLimitRequest updateBandwidthRateLimitRequest =
            new UpdateBandwidthRateLimitRequest()
                .withGatewayARN(gatewayARN)
                .withAverageDownloadRateLimitInBitsPerSec(downloadRate)
                .withAverageUploadRateLimitInBitsPerSec(uploadRate);

        UpdateBandwidthRateLimitResult updateBandwidthRateLimitResult =
sgClient.updateBandwidthRateLimit(updateBandwidthRateLimitRequest);
        String returnGatewayARN = updateBandwidthRateLimitResult.getGatewayARN();
        System.out.println("Updated the bandwidth rate limits of " +
returnGatewayARN);
        System.out.println("Upload bandwidth limit = " + uploadRate + " bits per
second");
        System.out.println("Download bandwidth limit = " + downloadRate + " bits
per second");
    }
    catch (AmazonClientException ex)
    {
        System.err.println("Error updating gateway bandwidth.\n" + ex.toString());
    }
}
}
```

Atualizando os limites de taxa de largura de banda do gateway usando o AWS SDK for .NET

Ao atualizar programaticamente os limites de taxa de largura de banda, é possível ajustar limites automaticamente ao longo de um período como, por exemplo, usando tarefas programadas. O exemplo a seguir demonstra como atualizar os limites de taxa de largura de banda de um gateway por meio do AWS SDK for .NET. Para usar o código de exemplo, você deve estar familiarizado com a execução de aplicativos em console do .NET. Para obter mais informações, consulte [Conceitos básicos](#) no Guia do desenvolvedor do AWS SDK for .NET .

Example : Atualizando os limites de taxa de largura de banda do gateway usando o AWS SDK for .NET

O exemplo de código C# a seguir atualiza os limites de taxa de largura de banda de um gateway. Você precisa atualizar o código e fornecer o endpoint de serviço, o nome do recurso da Amazon (ARN) para o gateway e os limites de upload e download. Para obter uma lista de endpoints de AWS serviço que você pode usar com o Storage Gateway, consulte [AWS Storage Gateway Endpoints and Quotas](#) no. Referência geral da AWS

```
using System;
using System.Collections.Generic;
using System.Linq;
using System.Text;
using Amazon.StorageGateway;
using Amazon.StorageGateway.Model;

namespace AWSStorageGateway
{
    class UpdateBandwidthExample
    {
        static AmazonStorageGatewayClient sgClient;
        static AmazonStorageGatewayConfig sgConfig;

        // The gatewayARN
        public static String gatewayARN = "**** provide gateway ARN ****";

        // The endpoint
        static String serviceURL = "https://storagegateway.us-east-1.amazonaws.com";

        // Rates
        static long uploadRate = 51200; // Bits per second, minimum 51200
    }
}
```

```
static long downloadRate = 102400; // Bits per second, minimum 102400

public static void Main(string[] args)
{
    // Create a Storage Gateway client
    sgConfig = new AmazonStorageGatewayConfig();
    sgConfig.ServiceURL = serviceURL;
    sgClient = new AmazonStorageGatewayClient(sgConfig);

    UpdateBandwidth(gatewayARN, uploadRate, downloadRate);

    Console.WriteLine("\nTo continue, press Enter.");
    Console.Read();
}

public static void UpdateBandwidth(string gatewayARN, long uploadRate, long
downloadRate)
{
    try
    {
        UpdateBandwidthRateLimitRequest updateBandwidthRateLimitRequest =
            new UpdateBandwidthRateLimitRequest()
                .WithGatewayARN(gatewayARN)
                .WithAverageDownloadRateLimitInBitsPerSec(downloadRate)
                .WithAverageUploadRateLimitInBitsPerSec(uploadRate);

        UpdateBandwidthRateLimitResponse updateBandwidthRateLimitResponse =
sgClient.UpdateBandwidthRateLimit(updateBandwidthRateLimitRequest);
        String returnGatewayARN =
updateBandwidthRateLimitResponse.UpdateBandwidthRateLimitResult.GatewayARN;
        Console.WriteLine("Updated the bandwidth rate limits of " +
returnGatewayARN);
        Console.WriteLine("Upload bandwidth limit = " + uploadRate + " bits per
second");
        Console.WriteLine("Download bandwidth limit = " + downloadRate + " bits
per second");
    }
    catch (AmazonStorageGatewayException ex)
    {
        Console.WriteLine("Error updating gateway bandwidth.\n" +
ex.ToString());
    }
}
}
```

}

Atualizando os limites de taxa de largura de banda do gateway usando o AWS Tools for Windows PowerShell

Ao atualizar programaticamente os limites de taxa de largura de banda, é possível ajustar limites automaticamente ao longo de um período como, por exemplo, usando tarefas programadas. O exemplo a seguir demonstra como atualizar os limites de taxa de largura de banda de um gateway usando o AWS Tools for Windows PowerShell. Para usar o código de exemplo, você deve estar familiarizado com a execução de um PowerShell script. Para obter mais informações, consulte [Conceitos básicos](#) no Guia do usuário do AWS Tools for Windows PowerShell .

Example : Atualizando os limites de taxa de largura de banda do gateway usando o AWS Tools for Windows PowerShell

O exemplo de PowerShell script a seguir atualiza os limites da taxa de largura de banda de um gateway. Você precisa atualizar este script de exemplo e fornecer o nome do recurso da Amazon (ARN) para o gateway e os limites de upload e download.

```
<#
.DESCRIPTION
    Update Gateway bandwidth limits.

.NOTES
    PREREQUISITES:
    1) AWS Tools for PowerShell from https://aws.amazon.com/powershell/
    2) Credentials and region stored in session using Initialize-AWSDefault.
    For more info, see https://docs.aws.amazon.com/powershell/latest/userguide/
    specifying-your-aws-credentials.html

.EXAMPLE
    powershell.exe .\SG_UpdateBandwidth.ps1
#>

$UploadBandwidthRate = 51200
$DownloadBandwidthRate = 102400
$gatewayARN = "*** provide gateway ARN ***"

#Update Bandwidth Rate Limits
Update-SGBandwidthRateLimit -GatewayARN $gatewayARN `
```

```
-AverageUploadRateLimitInBitsPerSec $UploadBandwidthRate `
-AverageDownloadRateLimitInBitsPerSec
$DownloadBandwidthRate

$limits = Get-SGBandwidthRateLimit -GatewayARN $gatewayARN

Write-Output("`nGateway: " + $gatewayARN);
Write-Output("`nNew Upload Rate: " + $limits.AverageUploadRateLimitInBitsPerSec)
Write-Output("`nNew Download Rate: " + $limits.AverageDownloadRateLimitInBitsPerSec)
```

Gerenciando atualizações de gateway usando o AWS Storage Gateway console

O Storage Gateway consiste em um componente de serviços de nuvem gerenciados e um componente de dispositivo de gateway que você implanta localmente ou em uma instância do Amazon EC2 na nuvem. AWS atualiza o componente de serviços em nuvem conforme necessário, sem causar interrupções nos gateways implantados.

Seus dispositivos de gateway implantados também exigem atualizações periódicas. As atualizações podem incluir atualizações de sistema operacional e software, correções para tratar de estabilidade, desempenho e segurança, além de acesso a novos recursos. Todas as atualizações são cumulativas e atualizam os gateways para a versão atual quando aplicadas.


Os dispositivos de gateway recebem atualizações de forma recorrente, e a aplicação dessas atualizações pode causar uma breve interrupção do serviço. O host da VM do gateway não precisa ser reinicializado durante as atualizações, mas o gateway ficará indisponível por um curto período enquanto o dispositivo de software for atualizado e reiniciado.

Important

Trate o dispositivo Storage Gateway como uma máquina virtual gerenciada e não tente acessar ou modificar a instalação do dispositivo. A tentativa de instalar ou atualizar qualquer pacote de software usando métodos diferentes do mecanismo normal de atualização do gateway (por exemplo, ferramentas SSM ou hipervisor) pode causar um mau funcionamento do gateway.

Você pode configurar seus gateways para aplicar atualizações de manutenção automaticamente durante as janelas de manutenção programadas ou esperar até iniciá-las manualmente. Quando

você implanta e ativa seu gateway, um cronograma padrão de janela de manutenção semanal é definido. Você pode modificar o cronograma da janela de manutenção a qualquer momento. Quando as atualizações estão disponíveis, a guia Detalhes do gateway exibe uma mensagem de manutenção. Você também pode ver a data e a hora em que a última atualização bem-sucedida foi aplicada na guia Detalhes.

 Note

Algumas atualizações importantes às vezes serão aplicadas de acordo com o cronograma da janela de manutenção, mesmo que as atualizações de manutenção regulares estejam desativadas.

Antes que qualquer atualização seja aplicada ao seu gateway, AWS notifica você com uma mensagem no console do Storage Gateway e no seu AWS Health Dashboard. Para ter mais informações, consulte [AWS Health Dashboard](#). Para modificar o endereço de e-mail para o qual as notificações de atualização de software são enviadas, acesse a página [Gerenciando uma AWS conta](#) e atualize o contato alternativo para “operações”.

Os procedimentos nas seções a seguir descrevem como gerenciar as atualizações do gateway usando o console do Storage Gateway. Para gerenciar essas configurações de forma programática usando a API, consulte [UpdateMaintenanceStartTime](#) na Referência da API do Storage Gateway.

Ativar ou desativar as atualizações de manutenção

Quando as atualizações de manutenção são ativadas, seu gateway aplica automaticamente essas atualizações de acordo com a programação da janela de manutenção configurada. Para obter mais informações, consulte [da janela de manutenção do gateway](#).

Se as atualizações de manutenção estiverem desativadas, o gateway não aplicará essas atualizações automaticamente, mas você ainda poderá aplicá-las manualmente usando o console, a API ou a CLI do Storage Gateway. Algumas atualizações importantes às vezes serão aplicadas durante a janela de manutenção configurada, independentemente dessa configuração.

Para ativar ou desativar as atualizações de manutenção para um gateway específico:

1. Abra o console do Storage Gateway em <https://console.aws.amazon.com/storagegateway/home>.
2. No painel de navegação, escolha Gateways e, em seguida, escolha o gateway para o qual você deseja configurar as atualizações de manutenção.

3. Escolha Ações e, em seguida, escolha Editar configurações de manutenção.
4. Para atualizações de manutenção, selecione Ativado ou Desativado.
5. Escolha Salvar alterações ao terminar.

Você pode verificar a configuração atualizada na guia Detalhes do gateway selecionado no console do Storage Gateway.

Modificar o cronograma da janela de manutenção do gateway

Se as atualizações de manutenção estiverem ativadas, seu gateway aplicará automaticamente novas atualizações de software de acordo com o cronograma da janela de manutenção. Algumas atualizações importantes às vezes serão aplicadas durante a janela de manutenção configurada, independentemente da configuração das atualizações de manutenção.

Para modificar a programação da janela de manutenção de um gateway específico:

1. Abra o console do Storage Gateway em <https://console.aws.amazon.com/storagegateway/home>.
2. No painel de navegação, escolha Gateways e, em seguida, escolha o gateway para o qual você deseja configurar as atualizações de manutenção.
3. Escolha Ações e, em seguida, escolha Editar configurações de manutenção.
4. Em Hora de início da janela de manutenção, faça o seguinte:
 - a. Em Programação, escolha Semanal ou Mensal para definir a cadência da janela de manutenção.
 - b. Se você escolher Semanal, modifique os valores para Dia da semana e Hora para definir o ponto específico durante cada semana em que a janela de manutenção começará.

Se você escolher Mensal, modifique os valores para Dia do mês e Hora para definir o ponto específico durante cada mês em que a janela de manutenção começará.

Note

O valor máximo que pode ser definido para o dia do mês é 28. Não é possível definir o cronograma de manutenção para começar nos dias 29 a 31.

Se você receber um erro ao definir essa configuração, isso pode significar que o software do gateway está desatualizado. Considere primeiro atualizar seu gateway

manualmente e depois tentar configurar o cronograma da janela de manutenção novamente.

5. Escolha Salvar alterações ao terminar.

Você pode verificar as configurações atualizadas na guia Detalhes do gateway selecionado no console do Storage Gateway.

Como executar tarefas de manutenção no console local

Você pode realizar as seguintes tarefas de manutenção usando o console local do host. As tarefas do console local podem ser realizadas no host da VM ou na instância do Amazon EC2. Muitas das tarefas são comuns entre os hosts diferentes, mas também há algumas diferenças.

Realizar tarefas no console local da VM do

Para um gateway implantado localmente, você pode executar as seguintes tarefas de manutenção usando o console local do host da VM. Essas tarefas são comuns aos hosts VMware, Hyper-V e Linux Kernel-based Virtual Machine (KVM).

Tópicos

- [Como fazer login no console local usando credenciais padrão](#)
- [Como definir a senha do console local no console do Storage Gateway](#)
- [Como rotear seu gateway local por meio de um proxy](#)
- [Como configurar uma rede de gateway](#)
- [Como testar a conexão de seu gateway com a Internet](#)
- [Como sincronizar o horário da VM do gateway](#)
- [Como executar comandos do Storage Gateway no console local](#)
- [Como exibir o status de recursos de sistema do gateway](#)
- [Como configurar adaptadores de rede para seu gateway](#)

Como fazer login no console local usando credenciais padrão

Quando a VM está pronta para o login, a tela de login é exibida. Se for a primeira vez que você faz login no console local, faça login com as credenciais padrão. Estas credenciais de login padrão

concedem acesso aos menus onde é possível definir configurações de rede do gateway e alterar a senha no console local. O Storage Gateway permite que você defina sua própria senha no AWS Storage Gateway console em vez de alterá-la no console local. Você não precisa saber qual é a senha padrão para definir uma nova senha. Para ter mais informações, consulte [Como definir a senha do console local no console do Storage Gateway](#).

Para fazer login no console local do gateway

1. Se for a primeira vez que você faz login no console local, faça login na VM com as credenciais padrão. O nome de usuário padrão é `admin` e a senha é `password`.

Do contrário, use suas credenciais para fazer login.

Note

É recomendável alterar a senha padrão digitando o número correspondente para o console do Gateway no menu principal Ativação do AWS equipamento: Configuração e, em seguida, executando o `passwd` comando. Para obter informações sobre como executar o comando, consulte [Como executar comandos do Storage Gateway no console local](#). Você também pode definir sua própria senha no AWS Storage Gateway console. Para ter mais informações, consulte [Como definir a senha do console local no console do Storage Gateway](#).

Important

Para versões mais antigas do volume ou do gateway de fitas, o nome de usuário é `sguser` e a senha é `sgpassword`. Se você redefinir a senha e o gateway for atualizado para uma versão mais recente, o nome de usuário será alterado para `admin`, mas a senha será mantida.

2. Depois de fazer login, será possível ver o menu principal de Configuração do AWS Storage Gateway: configuração, onde você pode executar várias tarefas.

Para saber mais sobre esta tarefa	Consulte este tópico
Configurar um proxy SOCKS para seu gateway	Como rotear seu gateway local por meio de um proxy.
Configurar sua rede	Como configurar uma rede de gateway.
Testar a conectividade de rede	Como testar a conexão de seu gateway com a Internet.
Gerenciar o tempo da VM	Como sincronizar o horário da VM do gateway.
Executar comandos do console do Storage Gateway	Como executar comandos do Storage Gateway no console local.
Exibir uma verificação de recursos do sistema	Como exibir o status de recursos de sistema do gateway.

Para encerrar o gateway, digite **0**.

Para sair da sessão de configuração, insira **X**.


Como definir a senha do console local no console do Storage Gateway

Ao fazer login pela primeira vez no console local, você faz login na VM com as credenciais padrão: o nome de usuário é `admin` e a senha é `password`. Recomendamos que você sempre defina uma nova senha imediatamente após criar o novo gateway. Se quiser, você pode definir essa senha no console do AWS Storage Gateway, e não no console local. Você não precisa saber qual é a senha padrão para definir uma nova senha.

Para definir a senha do console local no console do Storage Gateway

1. Abra o console do Storage Gateway em <https://console.aws.amazon.com/storagegateway/home>.
2. No painel de navegação, selecione Gateways e escolha o gateway para o qual você deseja definir uma nova senha.
3. Em Actions (Ações), escolha Set Local Console Password (Definir senha do console local).


4. Na caixa de diálogo Set Local Console Password, digite uma nova senha, confirme a senha e escolha Save. A nova senha substitui a senha padrão. O Storage Gateway não salva a senha, mas a transmite com segurança para a VM.

 Note

A senha pode conter qualquer caractere do teclado e ter de 1 a 512 caracteres de extensão.

Como rotear seu gateway local por meio de um proxy

Os gateways de volumes e os gateways de fitas comportam a configuração de um proxy do Secure Socket versão 5 (SOCKS5) entre o gateway on-premises e a AWS.

 Note

A única configuração de proxy compatível é SOCKS5.

Se o gateway tiver de usar um servidor de proxy para se comunicar com a Internet, será necessário definir as configurações de proxy SOCKS para o gateway. Para fazer isso, especifique um endereço IP e um número de porta para o host que executa o proxy. Após fazer isso, o Storage Gateway roteia todos os tráfegos por meio do servidor de proxy. Para obter informações sobre os requisitos de rede para seu gateway, consulte [Requisitos de rede e firewall](#).

O procedimento a seguir mostra como configurar o proxy SOCKS para gateway de volumes e gateway de fitas.

Para configurar um proxy SOCKS5 para gateways de volumes e de fitas

1. Faça login no console local do gateway.
 - VMware ESXi: para obter mais informações, consulte [Acesso ao console local do gateway com o VMware ESXi](#).
 - Microsoft Hyper-V: para obter mais informações, consulte [Acessar o console local do gateway com o Microsoft Hyper-V](#).
 - KVM: para obter mais informações, consulte [Acessar o console local do gateway com o Linux KVM](#).

2. No menu principal AWS Storage Gateway: configuração, insira o número correspondente para selecionar Configuração do proxy SOCKS.
3. No menu Configuração do proxy SOCKS do AWS Storage Gateway, insira o número correspondente para realizar uma das seguintes tarefas:

Para executar esta tarefa	Faça o seguinte
Configurar um proxy SOCKS	<p>Insira o número correspondente para selecionar Configurar proxy de SOCKS.</p> <p>Você precisará fornecer um nome de host e a porta para concluir a configuração.</p>
Visualizar a configuração de proxy SOCKS atual	<p>Insira o número correspondente para selecionar Visualizar configuração atual do proxy de SOCKS.</p> <p>Se não houver nenhum proxy SOCKS configurado, a mensagem SOCKS Proxy not configured é exibida. Se houver um proxy SOCKS configurado, o nome do host e a porta do proxy serão exibidos.</p>
Remover a configuração de proxy SOCKS	<p>Insira o número correspondente para selecionar Remover proxy de SOCKS.</p> <p>A mensagem SOCKS Proxy Configuration Removed é exibida.</p>

4. Reinicie a VM para aplicar a configuração de HTTP.

Como configurar uma rede de gateway

A configuração de rede padrão para o gateway é Dynamic Host Configuration Protocol (DHCP). Com o DHCP, um endereço IP é atribuído automaticamente ao seu gateway. Em alguns casos, pode ser

necessário atribuir manualmente o IP do gateway como endereço IP estático, tal como descrito a seguir.

Para configurar seu gateway para usar endereços IP estáticos


1. Faça login no console local do gateway.
 - VMware ESXi: para obter mais informações, consulte [Acesso ao console local do gateway com o VMware ESXi](#).
 - Microsoft Hyper-V: para obter mais informações, consulte [Acessar o console local do gateway com o Microsoft Hyper-V](#).
 - KVM: para obter mais informações, consulte [Acessar o console local do gateway com o Linux KVM](#).
2. No menu principal AWS Storage Gateway: configuração, insira o número correspondente para selecionar Testar conectividade de rede.
3. No menu Configuração de rede do AWS Storage Gateway, execute uma das seguintes tarefas:


Para executar esta tarefa	Faça o seguinte
Descrever o adaptador de rede	<p>Insira o número correspondente para selecionar Descrever adaptador.</p> <p>Uma lista de nomes de adaptadores é exibida e você é solicitado a digitar um nome de adaptador como, por exemplo, eth0. Se o adaptador especificado estiver em uso, serão exibidas as seguintes informações sobre o adaptador:</p> <ul style="list-style-type: none">• O endereço de controle de acesso de mídia (MAC)• Endereço IP• Máscara de rede•

Para executar esta tarefa	Faça o seguinte
	<p>Endereço IP do gateway</p> <ul style="list-style-type: none">• Status de DHCP ativado <p>Os nomes dos adaptadores listados aqui são usados ao configurar um endereço IP estático ou definir o adaptador padrão do seu gateway.</p>
Configurar o DHCP	<p>Insira o número correspondente para selecionar Configurar DHCP.</p> <p>Você será solicitado a configurar a interface de rede para usar o DHCP.</p>

Para executar esta tarefa	Faça o seguinte
Configurar um endereço IP estático para gateway	<p data-bbox="829 260 1500 338">Insira o número correspondente para selecionar Configurar IP estático.</p> <p data-bbox="829 388 1463 512">Você será solicitado a digitar as seguintes informações para configurar um endereço IP estático:</p> <ul data-bbox="829 569 1425 1073" style="list-style-type: none">• Nome do adaptador de rede• Endereço IP• Máscara de rede• Endereço de gateway padrão• Endereço Domain Name Service (DNS)• Endereço DNS secundário <div data-bbox="829 1209 1508 1619" style="border: 1px solid #f08080; border-radius: 10px; padding: 10px;"><p data-bbox="862 1251 1045 1283">⚠ Important</p><p data-bbox="907 1308 1471 1577">Se o gateway já tiver sido ativado, você deverá encerrá-lo e reiniciá-lo por meio do console do Storage Gateway para que as configurações sejam aplicadas. Para ter mais informações, consulte Encerramento da VM do gateway.</p></div> <p data-bbox="829 1724 1495 1801">Se seu gateway usar mais de uma interface de rede, você deverá definir todas as interfaces</p>

Para executar esta tarefa	Faça o seguinte
	<p>habilitadas para usar DHCP ou endereços IP estáticos.</p> <p>Por exemplo, suponha que a VM do gateway use duas interfaces configuradas como DHCP. Se você definir posteriormente uma interface para um endereço IP estático, a outra interface será desativada. Para ativar a interface, nesse caso, você deve configurá-la para um IP estático.</p> <p>Se as duas interfaces forem definidas inicialmente para usar endereços IP estáticos e depois você configurar o gateway para usar DHCP, ambas as interfaces usarão DHCP.</p>

Para executar esta tarefa	Faça o seguinte
Configure um nome de host para seu gateway	<p data-bbox="824 226 1502 310">Insira o número correspondente para selecionar Configurar nome do host.</p> <p data-bbox="824 352 1502 531">Você será solicitado a escolher se o gateway usará um nome de host estático especificado por você ou adquirirá um automaticamente por meio do DHCP ou rDNS.</p> <p data-bbox="824 573 1502 762">Se você selecionar Estático, você será solicitado a fornecer um nome de host estático, como. <code>testgateway.example.com</code> Entre y para aplicar a configuração.</p> <div data-bbox="829 800 1507 1304" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px;"><p data-bbox="857 835 982 877"> Note</p><p data-bbox="906 892 1474 1266">Se você configurar um nome de host estático para seu gateway, certifique-se de que o nome de host fornecido esteja no domínio ao qual o gateway está associado. Você também deve criar um registro A em seu sistema DNS que aponte o endereço IP do gateway para seu nome de host estático.</p></div>

Para executar esta tarefa	Faça o seguinte
Redefinir todas as configurações de rede do gateway para DHCP	<p data-bbox="829 260 1500 338">Insira o número correspondente para selecionar Redefinir tudo para DHCP.</p> <p data-bbox="829 388 1500 466">Todas as interfaces de rede são definidas para usar DHCP.</p> <div data-bbox="829 541 1500 951" style="border: 1px solid #f08080; border-radius: 10px; padding: 10px;"><p data-bbox="862 583 1045 615"> Important</p><p data-bbox="907 638 1471 909">Se o gateway já tiver sido ativado, você deverá encerrá-lo e reiniciá-lo por meio do console do Storage Gateway para que as configurações sejam aplicadas . Para ter mais informações, consulte Encerramento da VM do gateway.</p></div>
Configurar o adaptador de rota padrão do gateway	<p data-bbox="829 1089 1500 1167">Insira o número correspondente para selecionar Configurar adaptador padrão.</p> <p data-bbox="829 1218 1500 1341">Os adaptadores disponíveis para seu gateway são mostrados e você é solicitado a selecionar um dos adaptadores como, por exemplo, eth0.</p>
Visualizar a configuração de DNS do gateway	<p data-bbox="829 1421 1500 1499">Insira o número correspondente para selecionar Visualizar configuração atual do DNS.</p> <p data-bbox="829 1549 1500 1627">Os endereços IP dos servidores de nome DNS primário e secundário são exibidos.</p>

Para executar esta tarefa	Faça o seguinte
Visualizar tabelas de roteamento	<p>Insira o número correspondente para selecionar Visualizar rotas.</p> <p>A rota padrão de seu gateway é exibida.</p>

Como testar a conexão de seu gateway com a Internet

Você pode usar o console local do seu gateway para testar a conexão à internet. Este teste pode ser útil quando estiver solucionando problemas de rede em seu gateway.

Para testar a conexão de seu gateway à internet

1. Faça login no console local do gateway.
 - VMware ESXi: para obter mais informações, consulte [Acesso ao console local do gateway com o VMware ESXi](#).
 - Microsoft Hyper-V: para obter mais informações, consulte [Acessar o console local do gateway com o Microsoft Hyper-V](#).
 - KVM: para obter mais informações, consulte [Acessar o console local do gateway com o Linux KVM](#).
2. No menu principal AWS Storage Gateway: configuração, insira o número correspondente para selecionar Testar conectividade de rede.

Se o gateway já tiver sido ativado, o teste de conectividade começará imediatamente. Para gateways que ainda não foram ativados, você deve especificar o tipo de endpoint e Região da AWS conforme descrito nas etapas a seguir.

3. Se o gateway ainda não estiver ativado, insira o número correspondente para selecionar o tipo de endpoint do gateway.
4. Se você selecionou o tipo de endpoint público, insira o número correspondente para selecionar o Região da AWS que você deseja testar. Para obter suporte Regiões da AWS e uma lista dos endpoints de AWS serviço que você pode usar com o Storage Gateway, consulte [AWS Storage Gateway endpoints e cotas](#) no. Referência geral da AWS

Conforme o teste progride, cada endpoint exibe [PASSED] ou [FAILED], indicando o status da conexão da seguinte forma:

Message	Descrição
[PASSED]	O Storage Gateway tem conectividade de rede.
[FAILED]	O Storage Gateway não tem conectividade de rede.

Como sincronizar o horário da VM do gateway

Assim que seu gateway estiver implantado e em execução, em algumas situações o horário da VM do gateway pode apresentar desvios. Por exemplo, se houver alguma interrupção prolongada na rede e o host do hipervisor e o gateway não receberem atualizações de horário, o horário da VM do gateway será diferente do horário real. Quando há um desvio de horário, ocorre uma discrepância entre os horários declarados de operações como snapshots e os horários reais em que essas operações ocorreram.

Para um gateway implantado no VMware ESXi, configurar o horário do host do hipervisor e sincronizar o horário da VM com o host é suficiente para evitar desvios de horário. Para ter mais informações, consulte [Como sincronizar o tempo da VM com o tempo do host](#).

Para um gateway implantado no Microsoft Hyper-V, você deve verificar periodicamente o tempo da sua VM. Para ter mais informações, consulte [Como sincronizar o horário da VM do gateway](#).

Como executar comandos do Storage Gateway no console local

O console local da VM no Storage Gateway ajuda a oferecer um ambiente seguro para a configuração e o diagnóstico de problemas em seu gateway. Usando os comandos do console local, você pode realizar tarefas de manutenção, como salvar tabelas de roteamento, conectar-se a AWS Support, etc.



Para executar um comando de configuração ou diagnóstico

1. Faça login no console local do seu gateway:

- Para obter mais informações sobre o registro em log no console local do VMware ESXi, consulte [Acesso ao console local do gateway com o VMware ESXi](#).

- Para obter mais informações sobre o registro em log no console local do Microsoft Hyper-V, consulte [Acessar o console local do gateway com o Microsoft Hyper-V](#).
 - Para obter mais informações sobre o registro em log no console local da KVM, consulte [Acessar o console local do gateway com o Linux KVM](#).
2. No menu principal Ativação do equipamento da AWS : configuração, insira o número correspondente para selecionar Console do gateway.
 3. No prompt de comando do console do gateway, insira **h**.

O console exibe o menu COMANDOS DISPONÍVEIS, que lista os comandos disponíveis:

Comando	Função
dig	Colete a saída do dig para solucionar problemas de DNS.
exit	Retorne ao menu Configuração.
h	Exibir a lista de comandos disponível.
ifconfig	Visualize ou configure interfaces de rede. <div data-bbox="834 1119 1507 1528" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Note</p> <p>É recomendável definir as configurações de rede ou IP usando o console do Storage Gateway ou a opção de menu do console local dedicado. Para obter instruções, consulte Como configurar a rede de gateway.</p> </div>
ip	Mostra/manipule roteamentos, dispositivos e túneis. <div data-bbox="834 1692 1507 1873" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Note</p> <p>É recomendável definir as configurações de rede ou IP usando o console</p> </div>

Comando	Função
	do Storage Gateway ou a opção de menu do console local dedicado. Para obter instruções, consulte Como configurar a rede de gateway .
iptables	Ferramenta de administração para filtragem de pacotes IPv4 e NAT.
ncport	Teste a conectividade com uma porta TCP específica em uma rede.
nping	Colete a saída do nping para solucionar problemas de rede.
open-support-channel	Connect to AWS Support.
passwd	Atualize os tokens de autenticação.
save-iptables	Mantenha as tabelas IP.
save-routing-table	Salve a entrada da tabela de rotas recém-adicionada.
tcptracert	Colete a saída de traceroute no tráfego TCP para um destino.

- No prompt de comando do console do gateway, digite o comando correspondente para a função que você deseja usar e siga as instruções.

Para obter informações a respeito de um comando, insira **man** e o *nome do comando* no prompt do comando.

Como exibir o status de recursos de sistema do gateway

Quando o seu gateway é iniciado, ele verifica os núcleos da CPU virtual, o tamanho do volume raiz e a RAM. Ele determina se esses recursos do sistema são suficientes para seu gateway funcionar corretamente. Você pode visualizar os resultados dessa verificação no console local do gateway.

Para visualizar o status de uma verificação de recursos do sistema

1. Faça login no console local do seu gateway:
 - Para obter mais informações sobre o registro em log no console do VMware ESXi, consulte [Acesso ao console local do gateway com o VMware ESXi](#).
 - Para obter mais informações sobre o registro em log no console local do Microsoft Hyper-V, consulte [Acessar o console local do gateway com o Microsoft Hyper-V](#).
 - Para obter mais informações sobre o registro em log no console local da KVM, consulte [Acessar o console local do gateway com o Linux KVM](#).
2. No menu principal Ativação do equipamento da AWS : configuração, insira o número correspondente para selecionar Visualizar verificação de recursos do sistema.

Cada recurso exibe [OK], [AVISO] ou [FALHA], indicando o status do recurso da seguinte forma:

Message	Descrição
[OK]	O recurso passou na verificação de recursos do sistema.
[WARNING]	O recurso não atende aos requisitos recomendados, mas seu gateway vai continuar funcionando. O Storage Gateway exibe uma mensagem que descreve os resultados da verificação de recursos.
[FAIL]	O recurso não atende aos requisitos mínimos. Talvez o gateway não funcione corretamente. O Storage Gateway exibe uma mensagem que descreve os resultados da verificação de recursos.

O console também exibe o número de erros e avisos ao lado da opção de menu de verificação de recursos.

Como configurar adaptadores de rede para seu gateway

Por padrão, o Storage Gateway é configurado para usar o tipo de adaptador de rede E1000, mas é possível reconfigurar seu gateway para usar o adaptador de rede VMXNET3 (10 GbE). É possível configurar o Storage Gateway para que ele possa ser acessado por mais de um endereço IP. Isso é feito ao configurar o gateway para usar mais de um adaptador de rede.

Tópicos

- [Como configurar o gateway para usar o adaptador de rede VMXNET3](#)
- [Como configurar seu gateway para vários NICs](#)

Como configurar o gateway para usar o adaptador de rede VMXNET3

O Storage Gateway é compatível com o tipo de adaptador de rede E1000 nos hosts VMware ESXi e Microsoft Hyper-V Hypervisor. Entretanto, o adaptador de rede VMXNET3 (10 GbE) é compatível apenas com o hipervisor VMware ESXi. Se seu gateway estiver hospedado em um hipervisor VMware ESXi, você poderá reconfigurá-lo para usar o tipo de adaptador VMXNET3 (10 GbE). Para obter mais informações sobre esses adaptadores, consulte [Escolha de um adaptador de rede para sua máquina virtual](#) no site da Broadcom (VMware).

Important

Para selecionar o VMXNET3, o tipo do sistema operacional convidado deve ser Other Linux64.

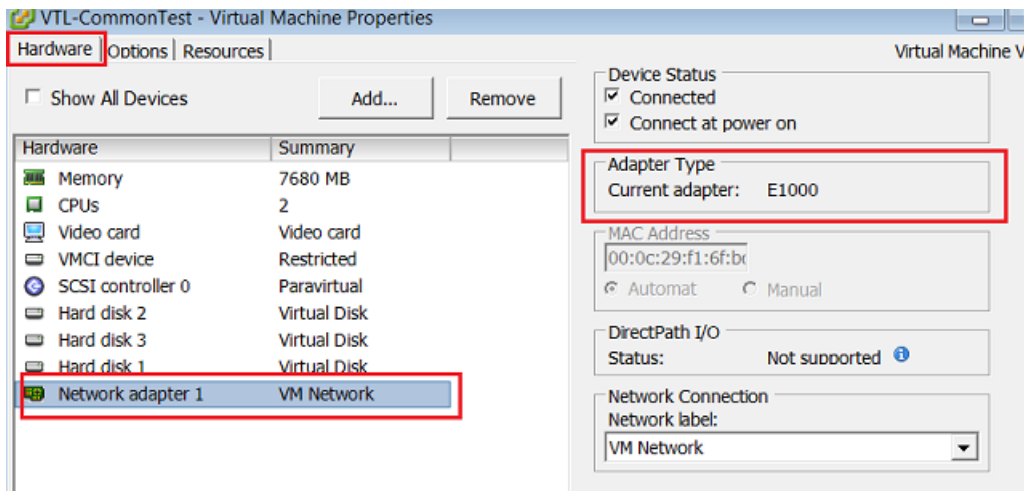
Veja a seguir as etapas executadas para configurar seu gateway para usar o adaptador VMXNET3:

1. Elimine o adaptador padrão E1000.
2. Adicione o adaptador VMXNET3.
3. Reinicie o gateway.
4. Configure o adaptador para a rede.

A seguir são apresentados detalhes sobre como executar cada etapa.

Para remover o adaptador padrão E1000 e configurar seu gateway para usar o adaptador VMXNET3

1. No VMware, abra o menu de contexto (clique com o botão direito do mouse) do gateway e escolha Edit Settings.
2. Na janela Virtual Machine Properties, escolha a guia Hardware.
3. Em Hardware, escolha Network adapter. Observe que o adaptador atual é E1000 na seção Adapter Type. Você substituirá esse adaptador pelo adaptador VMXNET3.



4. Escolha o adaptador de rede E1000 e em seguida Remover. Nesse exemplo, o adaptador de rede E1000 é Network adapter 1.

Note

Embora você possa usar simultaneamente os adaptadores de rede E1000 e VMXNET3 em seu gateway, isso não é recomendável porque pode provocar problemas de rede.

5. Escolha Add para abrir o assistente Add Hardware.
6. Escolha Ethernet Adapter e em seguida Next.
7. No assistente Network Type, selecione **VMXNET3** para Adapter Type (Tipo de adaptador) e escolha Próximo.
8. No assistente Virtual Machine Properties, verifique se na seção Adapter Type o campo Current adapter está definido como VMXNET3 e escolha OK.
9. No cliente VMware vSphere, encerre seu gateway.
10. No cliente VMware vSphere, reinicie seu gateway.

Assim que seu gateway reiniciar, reconfigure o adaptador que acabou de adicionar para ter certeza de que a conectividade de rede à internet foi estabelecida.

Para configurar o adaptador para a rede

1. No cliente VSphere, escolha a guia Console para iniciar o console local. Utilize as credenciais de login padrão para fazer login no console local do gateway para essa tarefa de configuração. Para obter informações sobre como fazer login usando as credenciais padrão, consulte [Como fazer login no console local usando credenciais padrão](#).
2. No prompt, insira o número correspondente para selecionar Configuração de rede.
3. No prompt, digite o número correspondente para selecionar Redefinir tudo para DHCP e digite **y** (para "sim") no prompt para redefinir todos os adaptadores para usar o Protocolo de Configuração Dinâmica de Host (DHCP). Todos os adaptadores disponíveis são configurados para usar DHCP.

Se o gateway já estiver ativado, você deve encerrá-lo e reiniciá-lo no Storage Gateway Management Console. Assim que o gateway reiniciar, você deve testar a conectividade de rede à internet. Para obter informações sobre como testar a conectividade de rede, consulte [Como testar sua conexão de gateway com a Internet](#).

Como configurar seu gateway para vários NICs

Se você configurar seu gateway para usar vários adaptadores de rede (NICs), ele poderá ser acessado por mais de um endereço IP. Talvez você queira fazer isso nas seguintes situações:

- Maximização da taxa de transferência – Você pode maximizar a taxa de transferência de um gateway quando os adaptadores de rede forem um gargalo.
- Separação de aplicações: talvez seja necessário distinguir o modo como suas aplicações gravam nos volumes de um gateway. Por exemplo, você pode determinar que um aplicativo de armazenamento essencial use exclusivamente um adaptador específico definido para o gateway.
- Restrições de rede – Seu ambiente de aplicativos pode exigir que você mantenha seus destinos iSCSI e os iniciadores que se conectam a eles em uma rede separada, diferente daquela por meio da qual o gateway se comunica com a AWS.

Em um caso de uso típico de vários adaptadores, um adaptador é configurado como a rota pela qual o gateway se comunica AWS (ou seja, como o gateway padrão). Exceto para esse adaptador

específico, os iniciadores devem estar na mesma sub-rede que o adaptador que contém os destinos iSCSI com os quais eles se conectam. Do contrário, a comunicação com os destinos pode não ser possível. Se um destino estiver configurado no mesmo adaptador usado para comunicação com AWS, o tráfego iSCSI desse destino e o AWS tráfego fluirão pelo mesmo adaptador.

Ao configurar um adaptador para se conectar ao console do Storage Gateway e em seguida adicionar um segundo adaptador, o Storage Gateway configura automaticamente a tabela de rotas para usar o segundo adaptador como rota preferencial. Para obter instruções sobre como configurar vários adaptadores, consulte as seções a seguir.

- [Configuração do Gateway para várias NICs em um host do VMware ESXi](#)
- [Configuração do Gateway para várias NICs em um host do Microsoft Hyper-V](#)

Como realizar tarefas no console local do Amazon EC2

Algumas tarefas de manutenção exigem que você faça login no console local ao executar um gateway implantado em uma instância do Amazon EC2. Esta seção descreve como fazer login no console local e realizar tarefas de manutenção.

Tópicos

- [Como fazer login no console local do gateway do Amazon EC2](#)
- [Como rotear um gateway implantado no EC2 por meio de um proxy HTTP](#)
- [Como testar a conectividade de rede do gateway](#)
- [Como visualizar o status de recursos de sistema do gateway](#)
- [Como executar comandos do Storage Gateway no console local](#)

Como fazer login no console local do gateway do Amazon EC2

É possível se conectar à sua instância do Amazon EC2 usando um cliente Secure Shell (SSH). Para obter informações detalhadas, consulte [Conectar-se à sua instância](#) no Guia do usuário do Amazon EC2. Para se conectar dessa forma, você precisará do par de chaves SSH que você especificou ao executar a instância. Para obter informações sobre pares de chaves do Amazon EC2, consulte [Pares de chave do Amazon EC2](#) no Guia do usuário do Amazon EC2.

Para fazer login no console local do gateway

1. Faça login no console local. Se você estiver se conectando à instância do EC2 em um computador Windows, faça login como administrador.
2. Depois de fazer login, será possível ver o menu principal de AWS Storage Gateway: configuração, onde você pode executar várias tarefas.

Para saber mais sobre esta tarefa	Consulte este tópico
Configurar um proxy SOCKS para seu gateway	Como rotear um gateway implantado no EC2 por meio de um proxy HTTP
Testar a conectividade de rede	Como testar a conectividade de rede do gateway
Executar comandos do console do Storage Gateway	Como executar comandos do Storage Gateway no console local
Exibir uma verificação de recursos do sistema	Como visualizar o status de recursos de sistema do gateway.

Para encerrar o gateway, digite **0**.

Para sair da sessão de configuração, insira **X**.

Como rotear um gateway implantado no EC2 por meio de um proxy HTTP

O Storage Gateway suporta a configuração de um proxy Secure Socket versão 5 (SOCKS5) entre o gateway implantado no Amazon EC2 e na AWS.

Se seu gateway precisar usar um servidor de proxy para se comunicar com a internet, será preciso definir as configurações de proxy HTTP para esse gateway. Para fazer isso, especifique um endereço IP e um número de porta para o host que executa o proxy. Depois de fazer isso, o Storage Gateway roteia todo o tráfego AWS do endpoint por meio do seu servidor proxy. As comunicações entre o gateway e os endpoints são criptografadas, mesmo quando se usa o proxy HTTP.

Para rotear o tráfego de internet de seu gateway por meio de um servidor de proxy local

1. Faça login no console local do gateway. Para obter instruções, consulte [Como fazer login no console local do gateway do Amazon EC2](#).
2. No menu principal Ativação do equipamento da AWS : configuração, insira o número correspondente para selecionar Configurar proxy HTTP.
3. No menu Configuração do proxy HTTP de ativação do equipamento da AWS , insira o número correspondente para a tarefa que você deseja realizar:
 - Configurar proxy de HTTP: você precisará fornecer um nome de host e a porta para concluir a configuração.
 - Visualizar a configuração atual do proxy HTTP: se nenhum proxy HTTP estiver configurado, a mensagem HTTP Proxy not configured será exibida. Se houver um proxy HTTP configurado, o nome do host e a porta do proxy serão exibidos.
 - Remover uma configuração de proxy de HTTP: a mensagem HTTP Proxy Configuration Removed será exibida.

Como testar a conectividade de rede do gateway

É possível usar o console local de seu gateway para testar a sua conexão com a Internet. Este teste pode ser útil quando estiver solucionando problemas de rede em seu gateway.

Para testar a conectividade do gateway

1. Faça login no console local do gateway. Para obter instruções, consulte [Como fazer login no console local do gateway do Amazon EC2](#).
2. No menu principal Ativação do equipamento da AWS : configuração, insira o número correspondente para selecionar Testar conectividade de rede.

Se o gateway já tiver sido ativado, o teste de conectividade começará imediatamente. Para gateways que ainda não foram ativados, você deve especificar o tipo de endpoint e Região da AWS conforme descrito nas etapas a seguir.

3. Se o gateway ainda não estiver ativado, insira o número correspondente para selecionar o tipo de endpoint do gateway.
4. Se você selecionou o tipo de endpoint público, insira o número correspondente para selecionar o Região da AWS que você deseja testar. Para obter suporte Regiões da AWS e uma lista dos

endpoints de AWS serviço que você pode usar com o Storage Gateway, consulte [AWS Storage Gateway endpoints e cotas](#) no. Referência geral da AWS

Conforme o teste progride, cada endpoint exibe [PASSED] ou [FAILED], indicando o status da conexão da seguinte forma:

Message	Descrição
[PASSED]	O Storage Gateway tem conectividade de rede.
[FAILED]	O Storage Gateway não tem conectividade de rede.

Como visualizar o status de recursos de sistema do gateway

Quando o seu gateway é iniciado, ele verifica os núcleos da CPU virtual, o tamanho do volume raiz e a RAM. Ele determina se esses recursos do sistema são suficientes para seu gateway funcionar corretamente. Você pode visualizar os resultados dessa verificação no console local do gateway.

Para visualizar o status de uma verificação de recursos do sistema

1. Faça login no console local do gateway. Para obter instruções, consulte [Como fazer login no console local do gateway do Amazon EC2](#).
2. No menu principal Ativação do equipamento da AWS : configuração, insira o número correspondente para selecionar Visualizar verificação de recursos do sistema.

Cada recurso exibe [OK], [AVISO] ou [FALHA], indicando o status do recurso da seguinte forma:

Message	Descrição
[OK]	O recurso passou na verificação de recursos do sistema.
[WARNING]	O recurso não atende aos requisitos recomendados, mas seu gateway vai continuar funcionando. O Storage Gateway exibe uma

Message	Descrição
	mensagem que descreve os resultados da verificação de recursos.
[FAIL]	O recurso não atende aos requisitos mínimos. Talvez o gateway não funcione corretamente. O Storage Gateway exibe uma mensagem que descreve os resultados da verificação de recursos.

O console também exibe o número de erros e avisos ao lado da opção de menu de verificação de recursos.

Como executar comandos do Storage Gateway no console local



O AWS Storage Gateway console ajuda a fornecer um ambiente seguro para configurar e diagnosticar problemas com seu gateway. Usando os comandos do console, você pode realizar tarefas de manutenção, como salvar tabelas de roteamento ou conectar-se a AWS Support

Para executar um comando de configuração ou diagnóstico

1. Faça login no console local do gateway. Para obter instruções, consulte [Como fazer login no console local do gateway do Amazon EC2](#).
2. No menu principal Ativação do equipamento da AWS : configuração, insira o número correspondente para selecionar Console do gateway.
3. No prompt de comando do console do gateway, insira h.

O console exibe o menu AVAILABLE COMMANDS (Comandos disponíveis), que lista os comandos disponíveis:

Command	Função
dig	Colete a saída do dig para solucionar problemas de DNS.
exit	Retorne ao menu Configuração.

Command	Função
h	Exibir a lista de comandos disponível.
ifconfig	Visualize ou configure interfaces de rede. <div data-bbox="836 388 1507 699"><p> Note</p><p>É recomendável definir as configurações de rede ou IP usando o console do Storage Gateway ou a opção de menu do console local dedicado.</p></div>
ip	Mostra/manipule roteamentos, dispositivos e túneis. <div data-bbox="836 861 1507 1171"><p> Note</p><p>É recomendável definir as configurações de rede ou IP usando o console do Storage Gateway ou a opção de menu do console local dedicado.</p></div>
iptables	Ferramenta de administração para filtragem de pacotes IPv4 e NAT.
ncport	Teste a conectividade com uma porta TCP específica em uma rede.
nping	Colete a saída do nping para solucionar problemas de rede.
open-support-channel	Connect to AWS Support.
save-iptables	Mantenha as tabelas IP.
save-routing-table	Salve a entrada da tabela de rotas recém-adicionada.

Command	Função
sslcheck	Verifique a validade de SSL para solucionar problemas de rede.
tcptraceroute	Colete a saída de traceroute no tráfego TCP para um destino.

4. No prompt de comando do console do gateway, digite o comando correspondente para a função que você deseja usar e siga as instruções.

Para saber mais sobre um comando, insira o nome do comando seguido pela opção `-h`, por exemplo: `sslcheck -h`.

Acessar o console local do gateway

O modo como você acessa o console local da VM depende do tipo do hipervisor no qual você implantou a VM do gateway. Nesta seção, é possível encontrar informações sobre como acessar o console local da VM usando a Linux Kernel-based Virtual Machine (KVM), VMware ESXi e Microsoft Hyper-V Manager.

Tópicos

- [Acessar o console local do gateway com o Linux KVM](#)
- [Acesso ao console local do gateway com o VMware ESXi](#)
- [Acessar o console local do gateway com o Microsoft Hyper-V](#)

Acessar o console local do gateway com o Linux KVM

Existem diferentes maneiras de configurar máquinas virtuais em execução na KVM, dependendo da distribuição do Linux que estiver sendo usada. Siga as instruções para acessar as opções de configuração da KVM na linha de comando. As instruções podem variar dependendo da sua implementação da KVM.

Como acessar o console local do gateway com a KVM

1. Use o comando a seguir para listar as VMs que estão atualmente disponíveis na KVM.

```
# virsh list
```

É possível escolher VMs disponíveis por Id.

```
[root@localhost vms]# virsh list
 Id   Name           State
-----
  7   SGW_KVM        running

[root@localhost vms]# virsh console 7
```

2. Use o comando a seguir para acessar o console local.

```
# virsh console VM_Id
```

```
[[root@localhost vms]# virsh console 7
Connected to domain SGW_KVM
Escape character is ^]

AWS Appliance

Login to change your network configuration and other settings.
localhost login: _
```

3. Para obter credenciais padrão para fazer login no console local, consulte [Como fazer login no console local usando credenciais padrão](#).
4. Depois de fazer login, é possível ativar e configurar o gateway.

```
AWS Appliance Activation - Configuration

#####
## Currently connected network adapters:
##
## eth0: 10.0.3.32
#####

1: HTTP/SOCKS Proxy Configuration
2: Network Configuration
3: Test Network Connectivity
4: View System Resource Check (0 Errors)
5: System Time Management
6: License Information
7: Command Prompt

0: Get activation key

Press "x" to exit session

Enter command: _
```

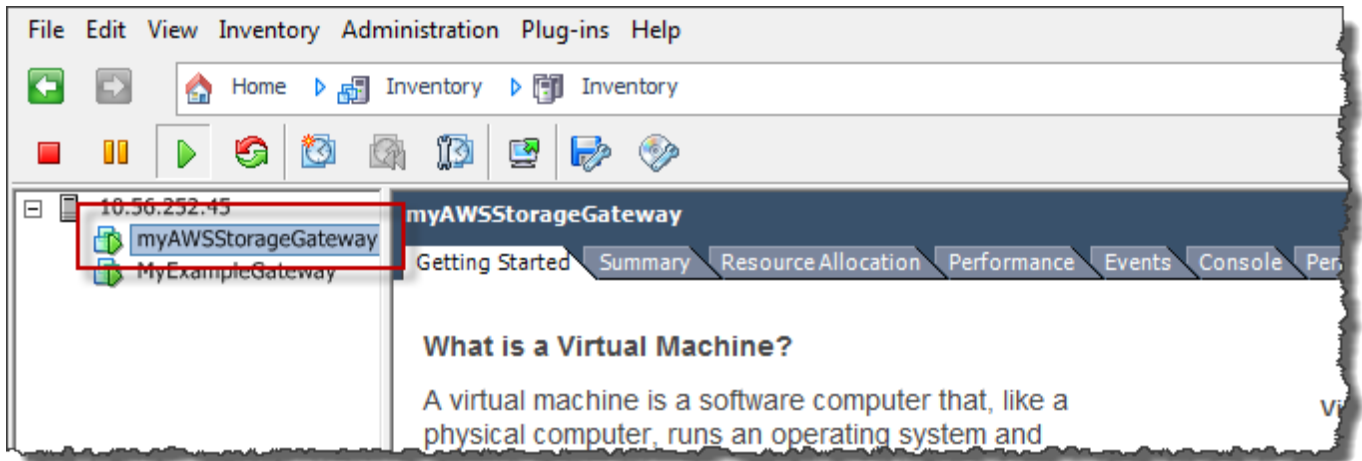
Acesso ao console local do gateway com o VMware ESXi

Para acessar o console local de seu gateway com VMware ESXi

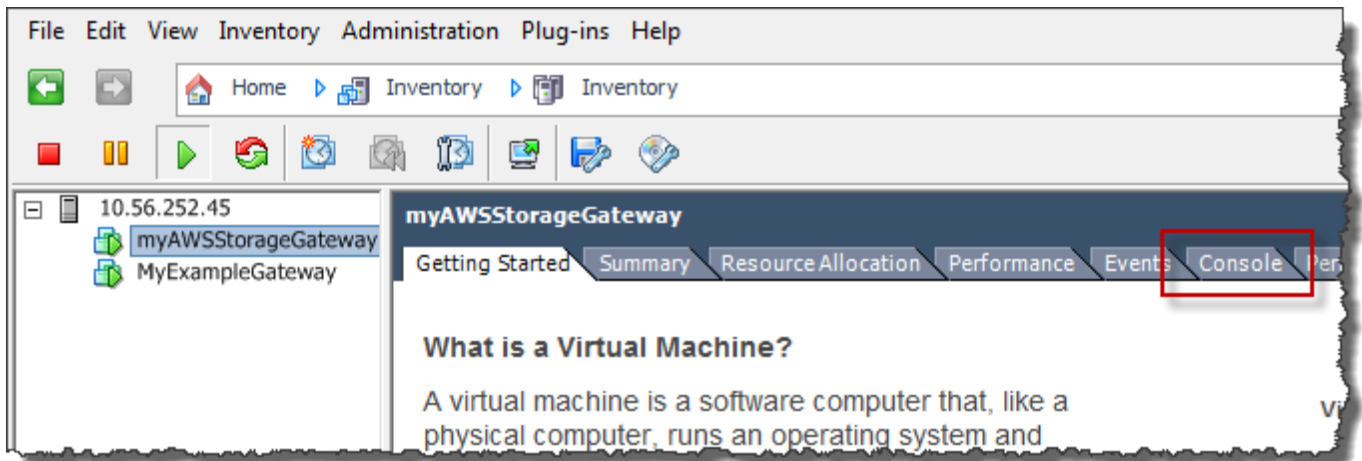
1. No cliente VMware vSphere, selecione a VM de seu gateway.
2. Verifique se o gateway está ativado.

Note

Se a VM do gateway estiver ativada, será exibido um ícone de seta verde com o ícone da VM, conforme mostrado na captura de tela a seguir. Se a VM do gateway não estiver ativada, você poderá ativá-la escolhendo o ícone verde Ligar no menu da Barra de ferramentas.



3. Escolha a guia Console.



Depois de alguns instantes, a VM estará pronta para você fazer login.

Note

Para liberar o cursor da janela do console, pressione Ctrl+Alt.

```
AWS Storage Gateway

Login to change your network configuration and other gateway settings.

For more information, please see:
https://docs.aws.amazon.com/console/storagegateway/LocalConsole

localhost login: _
```

4. Para fazer login usando as credenciais padrão, vá para o procedimento [Como fazer login no console local usando credenciais padrão](#).

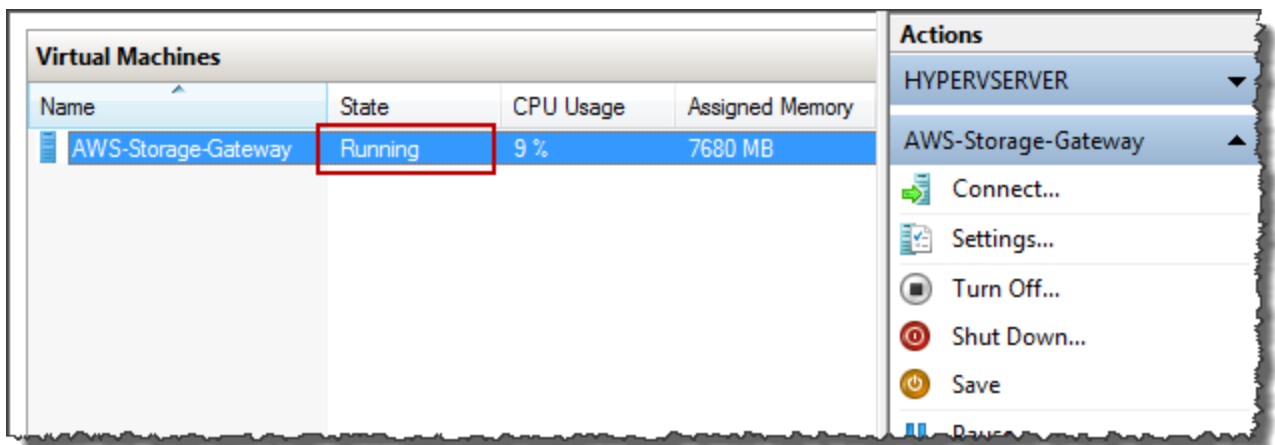
Acessar o console local do gateway com o Microsoft Hyper-V

Para acessar o console local do gateway (Microsoft Hyper-V)

1. Na lista Virtual Machines do Microsoft Hyper-V Manager, selecione a VM de seu gateway.
2. Verifique se o gateway está ativado.

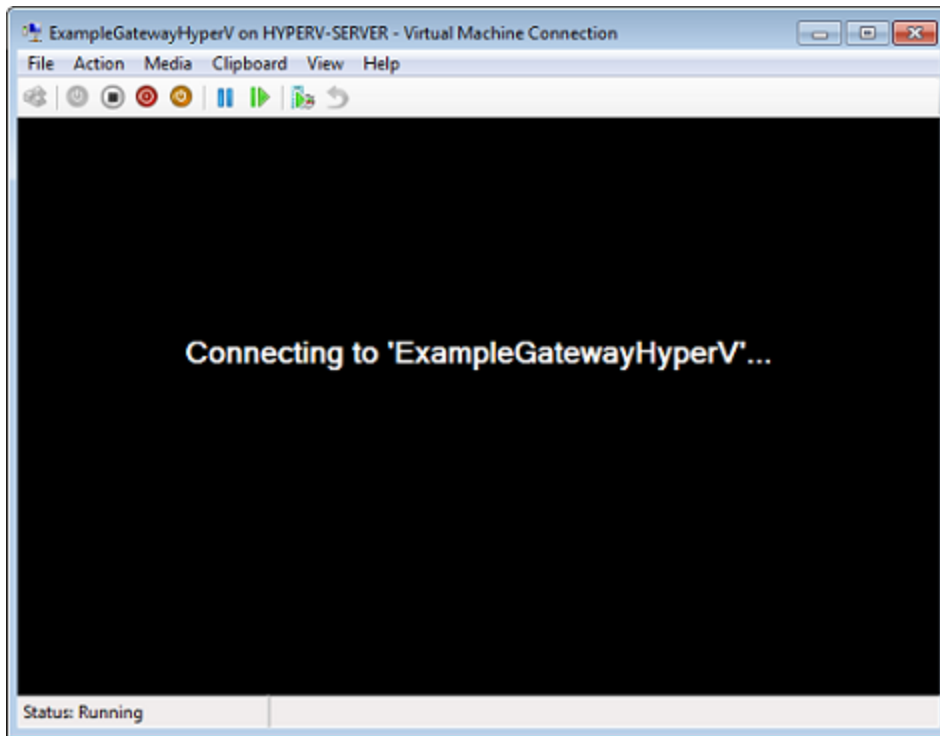
Note

Se a VM do gateway estiver ativada, o estado Running da VM é exibido em State, tal como mostrado na captura de tela a seguir. Se a VM do gateway não estiver ativada, você pode ativá-la escolhendo Start no painel Actions.



3. No painel Actions, escolha Connect.

A janela Virtual Machine Connection é exibida. Se uma janela de autenticação for exibida, digite as credenciais fornecidas pelo administrador do hipervisor.



Depois de alguns instantes, a VM estará pronta para você fazer login.

```
AWS Storage Gateway

Login to change your network configuration and other gateway settings.

For more information, please see:
https://docs.aws.amazon.com/console/storagegateway/LocalConsole

localhost login: _
```

4. Para fazer login usando as credenciais padrão, vá para o procedimento [Como fazer login no console local usando credenciais padrão](#).

Como configurar adaptadores de rede para seu gateway

Nesta seção, você pode encontrar informações sobre como configurar vários adaptadores de rede para seu gateway.

Tópicos

- [Configuração do Gateway para várias NICs em um host do VMware ESXi](#)
- [Configuração do Gateway para várias NICs em um host do Microsoft Hyper-V](#)

Configuração do Gateway para várias NICs em um host do VMware ESXi

O procedimento a seguir pressupõe que a VM do gateway já tem um adaptador de rede definido e que você está adicionando um segundo adaptador.

Para configurar um adaptador de rede adicional no host do VMware ESXi para seu gateway

1. Encerre o gateway.
2. No cliente VMware vSphere, selecione a VM de seu gateway.

A VM pode permanecer ativada para esse procedimento.

3. No cliente, abra o menu de contexto (clique com o botão direito do mouse) da VM do gateway e escolha Editar COnfigurações.
4. Na guia Hardware da caixa de diálogo Propriedades da Máquina Virtual, escolha Adicionar para adicionar um dispositivo.
5. Siga o assistente Add Hardware para adicionar um adaptador de rede.
 - a. No painel Tipo de Dispositivo, escolha Adaptador Ethernet para adicionar um adaptador e em seguida Seguinte.
 - b. No painel Tipo de Rede, confirme se Connect at power on está selecionada para Tipo e escolha Seguinte.

É recomendável usar o adaptador de rede VMXNET3 com o Storage Gateway. Para obter mais informações sobre o tipo de adaptador que pode ser exibido na lista de adaptadores, consulte Network Adapter Types em [ESXi and vCenter Server Documentation](#).

- c. No painel Pronto para Completar, reveja as informações e escolha Terminar.
6. Escolha a guia Resumo da VM e escolha Visualizar tudo, ao lado da caixa Endereço IP. A janela Endereços IP da máquina virtual exibe todos os endereços IP que podem ser usados para acessar o gateway. Confirme se um segundo endereço IP é listado para o gateway.

Note

Pode demorar vários minutos para as alterações do adaptador entrarem em vigor e as informações resumidas da VM atualizarem.

7. No console do Storage Gateway, ative o gateway.
8. No painel Navegação do console do Storage Gateway, escolha Gateways e o gateway ao qual você adicionou o adaptador. Confirme se o segundo endereço IP está listado na guia Details.

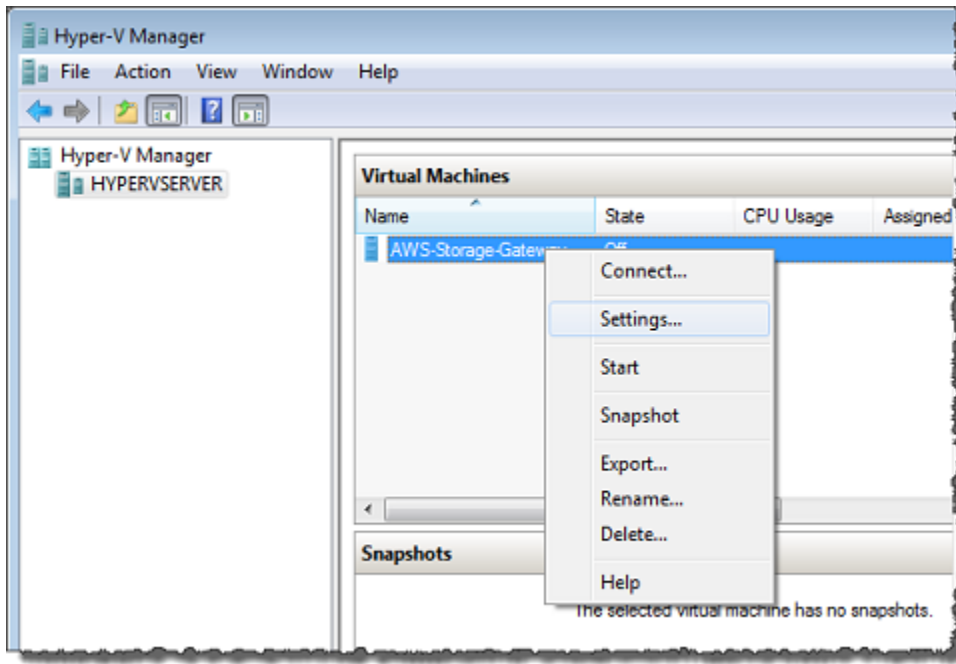
Para obter informações sobre as tarefas do console local comuns ao host do VMware, do Hyper-V e da KVM, consulte [Realizar tarefas no console local da VM do](#)

Configuração do Gateway para várias NICs em um host do Microsoft Hyper-V

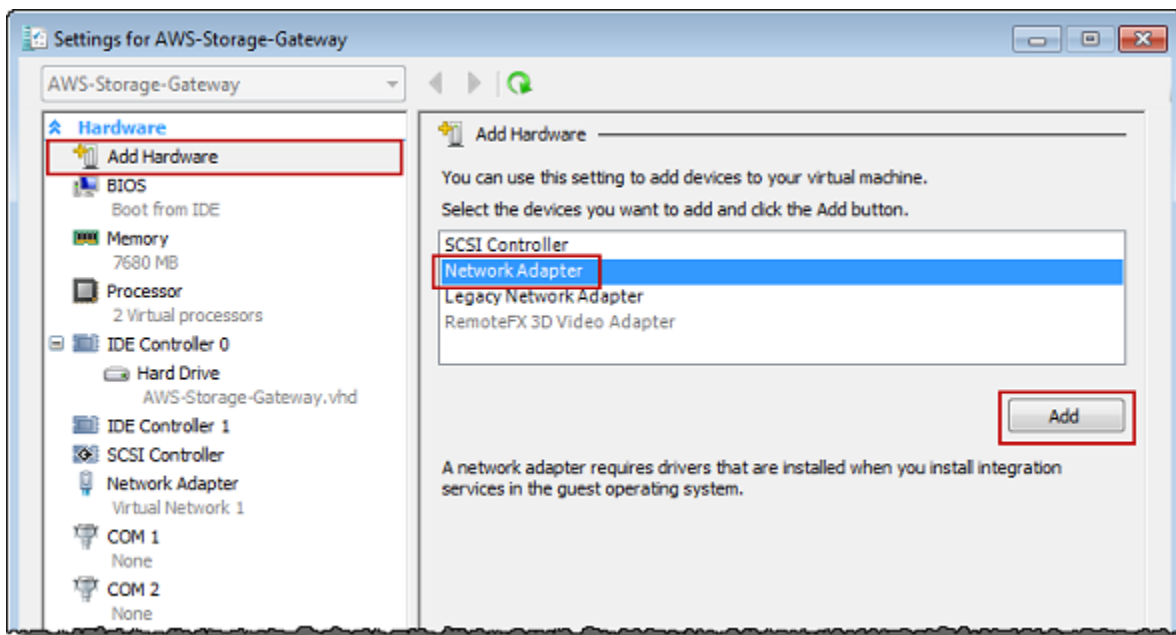
O procedimento a seguir pressupõe que a VM do gateway já tem um adaptador de rede definido e que você está adicionando um segundo adaptador. Este procedimento mostra como adicionar um adaptador para um host do Microsoft Hyper-V.

Para configurar um adaptador de rede adicional em um host do Microsoft Hyper-V para seu gateway

1. No console do Storage Gateway, desative o gateway. Para obter instruções, consulte [Para interromper um gateway de volumes](#).
2. No Microsoft Hyper-V Manager, selecione a VM do gateway.
3. Se a VM ainda não estiver desativada, abra o menu de contexto (clique com o botão direito do mouse) do gateway e escolha Turn Off.
4. No cliente, abra o menu de contexto da VM do gateway e escolha Settings.

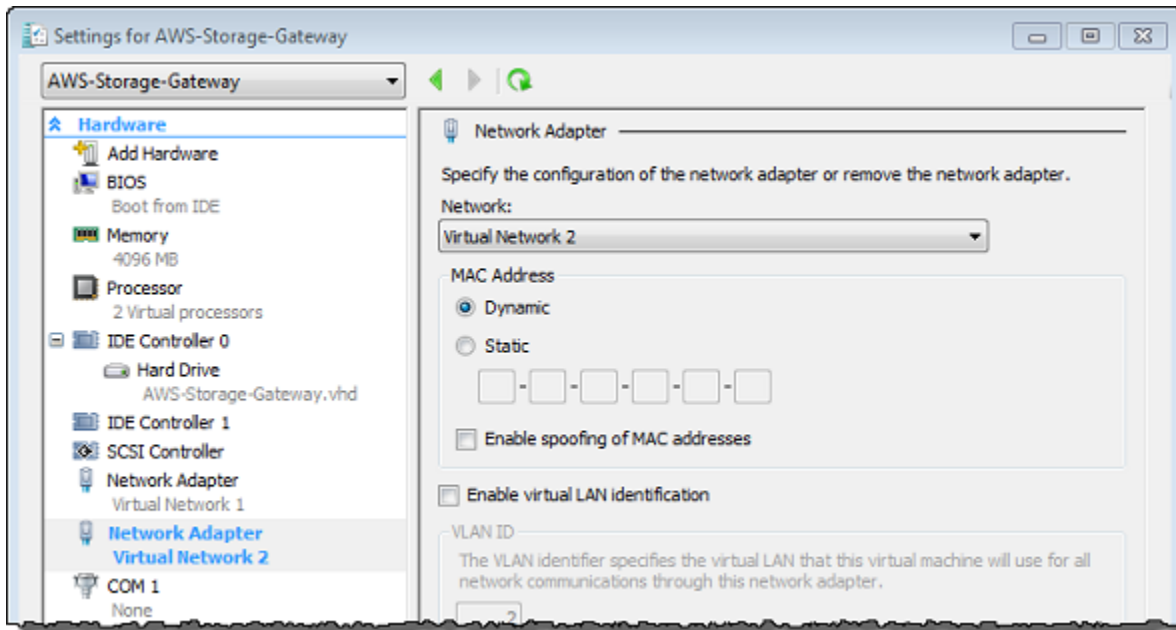


5. Na caixa de diálogo Settings da VM, para Hardware, escolha Add Hardware.
6. No painel Add Hardware, escolha Network Adapter e em seguida Add para adicionar um dispositivo.



7. Configure o adaptador de rede e escolha Apply para aplicar as configurações.

No exemplo a seguir, Virtual Network 2 está selecionada para o novo adaptador.



8. Na caixa de diálogo Settings, para Hardware, confirme se o segundo adaptador foi adicionado e escolha OK.
9. No console do Storage Gateway, ative o gateway. Para obter instruções, consulte [Para iniciar um gateway de volumes](#).
10. No painel Navigation, escolha Gateways e selecione o gateway ao qual você adicionou o adaptador. Confirme se o segundo endereço IP está listado na guia Details.

Note

Os exemplos de comandos de montagem fornecidos na página de informações de um compartilhamento de arquivos no console do Storage Gateway sempre incluirão o endereço IP do adaptador de rede que foi adicionado mais recentemente ao gateway associado ao compartilhamento de arquivos.

Para obter informações sobre as tarefas do console local comuns ao host do VMware, do Hyper-V e da KVM, consulte [Realizar tarefas no console local da VM do](#)

Como excluir seu gateway usando o console do AWS Storage Gateway e como limpar os recursos associados

Se você não pretende continuar usando seu gateway, pense na possibilidade de excluir o gateway e os recursos a ele associados. A remoção de recursos pode ajudá-lo a evitar cobranças por recursos que você não pretende continuar a usar e a reduzir sua fatura mensal.

Quando você exclui um gateway, ele não aparece mais no console AWS Storage Gateway de gerenciamento e sua conexão iSCSI com o iniciador é fechada. O procedimento para excluir um gateway é o mesmo para todos os tipos de gateway; no entanto, dependendo do tipo de gateway que você deseja excluir e do host no qual ele está implantado, siga as instruções específicas para remover recursos associados.

É possível excluir um gateway usando o console do Storage Gateway ou de forma programática. É possível encontrar informações a seguir sobre como excluir um gateway usando o console do Storage Gateway. Se você deseja excluir seu gateway de forma programática, consulte [Referência de API do AWS Storage Gateway](#).

Tópicos

- [Como excluir um gateway usando o console do Storage Gateway](#)
- [Como remover recursos de um gateway implantado no local](#)
- [Como remover recursos de um gateway implantado em uma instância do Amazon EC2](#)

Como excluir um gateway usando o console do Storage Gateway

O procedimento para excluir um gateway é o mesmo para todos os tipos de gateway. No entanto, dependendo do tipo de gateway que você deseja excluir e do host no qual está implantado, talvez você precise executar outras tarefas para remover recursos associados ao gateway. A remoção desses recursos ajuda-o a evitar despesas com recursos que você não pretende usar.

Note


Para os gateways implantados em uma instância do Amazon EC2, a instância continua a existir até que você a exclua.

Para gateways implantados em uma máquina virtual (VM), depois que você exclui seu gateway, a VM do gateway continua presente em seu ambiente de virtualização. Para

remover a VM, use o cliente VMware vSphere, o Microsoft Hyper-V Manager ou o cliente de Linux Kernel-based Virtual Machine (KVM) para se conectar ao host e remover a VM. Observe que você não pode reutilizar a VM do gateway excluído para ativar um novo gateway.


Para excluir um gateway

1. Abra o console do Storage Gateway em <https://console.aws.amazon.com/storagegateway/home>.
2. Escolha Gateways e selecione um ou mais gateways para excluir.
3. Em Actions (Ações), selecione Delete gateway (Excluir gateway). Uma caixa de diálogo de confirmação é exibida.

 Warning

Antes de executar esta etapa, verifique se não há nenhuma aplicação gravando no momento nos volumes do gateway. Se excluir o gateway enquanto ele estiver em uso, poderá perder dados. Não é possível recuperar um gateway excluído.

4. Verifique se você deseja excluir os gateways especificados, digite a palavra excluir na caixa de confirmação e escolha Excluir.
5. (Opcional) Se você quiser fornecer feedback sobre o gateway excluído, preencha a caixa de diálogo de comentários e escolha Enviar. Caso contrário, selecione Interromper.

 Important

Ao excluir um gateway, você não deixa de pagar as despesas de software, mas recursos, como fitas virtuais, snapshots do Amazon Elastic Block Store (Amazon EBS) e instâncias do Amazon EC2 se mantêm. Você continuará a ser cobrado por esses recursos. É possível optar por remover instâncias do Amazon EC2 e snapshots do Amazon EBS ao cancelar sua assinatura do Amazon EC2. Se deseja manter sua assinatura do Amazon EC2, é possível excluir seus snapshots do Amazon EBS usando o console do Amazon EC2.

Como remover recursos de um gateway implantado no local

Você pode usar as instruções a seguir para remover recursos de um gateway implantado no local.

Como remover recursos de um gateway de volume implantado em uma VM

Se o gateway que você deseja excluir estiver implantado em uma máquina virtual (VM), é recomendável realizar as ações a seguir para limpar recursos:

- Exclua o gateway. Para obter instruções, consulte [Como excluir um gateway usando o console do Storage Gateway](#).
- Exclua todos os snapshots do Amazon EBS que você não necessita. Para obter instruções, consulte [Excluir um snapshot do Amazon EBS](#) no Guia do usuário do Amazon EC2.

Como remover recursos de um gateway implantado em uma instância do Amazon EC2

Se você quiser excluir um gateway que você implantou em uma instância do Amazon EC2, recomendamos que você limpe os recursos que foram usados com AWS o gateway, especificamente a instância do Amazon EC2, todos os volumes do Amazon EBS e também as fitas se você implantou um gateway de fita. Isso ajuda a evitar despesas de uso não intencionais.

Como remover recursos em seus volumes armazenados em cache implantados no Amazon EC2

Se você implantou um gateway com volumes armazenados no EC2, é recomendável executar as ações a seguir para excluir o gateway e limpar os respectivos recursos:

1. No console do Storage Gateway, exclua o gateway, conforme mostrado em [Como excluir um gateway usando o console do Storage Gateway](#).
2. No console do Amazon EC2, interrompa a sua instância do EC2 se tiver a intenção de usá-la novamente. Do contrário, encerre-a. Se tiver intenção de excluir volumes, tome nota dos dispositivos de bloco anexados à instância e dos identificadores de dispositivos antes de encerrar a instância. Você precisará dessas anotações para identificar os volumes que deseja excluir.
3. No console do Amazon EC2, remova todos os volumes do Amazon EBS que estão anexados à instância se não tiver a intenção de usá-los novamente. Para obter mais informações, consulte [Limpe sua instância e volume](#) no Guia do usuário do Amazon EC2.

Performance

Esta seção descreve o desempenho do Storage Gateway.

Tópicos

- [Como otimizar o desempenho de um gateway](#)
- [Como usar o VMware vSphere High Availability com o Storage Gateway](#)

Como otimizar o desempenho de um gateway

Configuração recomendada do servidor do gateway

Para obter o melhor desempenho do seu gateway, o Storage Gateway recomenda a seguinte configuração de gateway para o servidor host do gateway:

- Pelo menos 24 núcleos de CPU físicos dedicados
- Para o gateway de volumes, seu hardware deve dedicar as seguintes quantidades de RAM:
 - Pelo menos 16 GiB de RAM é reservada para os gateways com tamanho de cache de até 16 TiB
 - Pelo menos 32 GiB de RAM é reservada para os gateways com tamanho de cache de 16 TiB a 32 TiB
 - Pelo menos 48 GiB de RAM é reservada para os gateways com tamanho de cache de 32 TiB a 64 TiB
- Disco 1, para ser usado como cache do gateway da seguinte forma:
 - SSD com um controlador NVMe.
- Disco 2, para ser usado como buffer de upload do gateway da seguinte forma:
 - SSD com um controlador NVMe.
- Disco 3, para ser usado como buffer de upload do gateway da seguinte forma:
 - SSD com um controlador NVMe.
- Adaptador de rede 1 configurado na rede 1 da VM:
 - Use a rede 1 da VM e adicione o VMXnet3 (10 Gbps) para ser usado para ingestão.
- Adaptador de rede 2 configurado na rede 2 da VM:
 - Use a rede 2 da VM e adicione o VMXnet3 (10 Gbps) para ser usado conexão com a AWS.

Como adicionar recursos ao seu gateway

Os gargalos a seguir podem reduzir o desempenho do seu abaixo da taxa de transferência máxima sustentada teórica (sua largura de banda para a nuvem): AWS

- Contagem de núcleos de CPU
- Throughput do disco de buffer de cache/upload
- Quantidade total de RAM
- Largura de banda de rede até AWS
- Largura de banda da rede do iniciador ao gateway

Esta seção contém as etapas que podem ser seguidas para otimizar o desempenho do gateway. Esta orientação é baseada na adição de recursos ao gateway ou ao servidor de aplicações.

Você pode otimizar o desempenho do gateway adicionando recursos ao seu gateway em uma ou mais das seguintes maneiras.

Use discos de desempenho superior

O throughput do disco de cache e buffer de upload pode limitar o desempenho de upload e download do gateway. Se o gateway estiver exibindo um desempenho significativamente abaixo do esperado, considere melhorar o throughput do cache e do disco do buffer de upload da seguinte forma:

- Usando um RAID distribuído, como o RAID 10, para melhorar o throughput do disco, de preferência com um controlador RAID de hardware.


Note

O RAID (matriz redundante de discos independentes) ou, especificamente, configurações de RAID com distribuição de disco, como o RAID 10, é o processo de dividir um corpo de dados em blocos e distribuir os blocos de dados em vários dispositivos de armazenamento. O nível de RAID usado afeta a velocidade exata e a tolerância a falhas que é possível alcançar. Ao distribuir as workloads de E/S em vários discos, o throughput do dispositivo RAID é muito maior do que o de qualquer disco de membro único.

- Como usar discos de alto desempenho que são conectados diretamente

Para otimizar o desempenho do gateway, você pode adicionar discos de alto desempenho, como unidades de estado sólido (SSDs) e um controlador NVMe. Você pode também anexar discos virtuais diretamente à sua VM em uma rede de área de armazenamento (SAN), e não no NTFS do Microsoft Hyper-V. Um disco com melhor desempenho geralmente contribui para uma taxa de transferência mais alta e mais operações de entrada/saída por segundo (IOPS).

Para medir a produtividade, use as `WriteBytes` métricas `ReadBytes` e com a `CloudWatch` estatística da `Samples Amazon`. Por exemplo, a estatística `Samples` da métrica `ReadBytes` durante um período de amostra de 5 minutos divididos por 300 segundos fornece o IOPS. Como regra geral, ao analisar essas métricas para um gateway, procure taxas de transferência baixas e IOPS com baixas tendências para indicar gargalos relacionados ao disco. .

 Note

`CloudWatch` as métricas não estão disponíveis para todos os gateways. Para obter informações sobre métricas de gateway, consulte [Como monitorar o Storage Gateway](#).

Adicionar mais discos de buffer de upload

Para ter um throughput de gravação maior, adicione pelo menos dois discos de buffer de upload. Quando os dados são gravados no gateway, eles são gravados e armazenados localmente nos discos de buffer de upload. Depois disso, os dados locais armazenados são lidos de forma assíncrona dos discos a serem processados e carregados na AWS. Adicionar mais discos de buffer de upload pode reduzir a quantidade de operações simultâneas de E/S realizadas em cada disco individual. Isso pode resultar em um throughput maior de gravação no gateway.

Respalde os discos virtuais com discos físicos separados.

Ao provisionar discos de gateway, é altamente recomendável não provisionar discos locais para o buffer de upload e o armazenamento em cache que usam os mesmos recursos subjacentes de armazenamento físico. Por exemplo, para VMware ESXi, os recursos subjacentes de armazenamento físico são representados como armazenamento de dados. Ao implantar a VM do gateway, você escolhe um armazenamento de dados para armazenar os arquivos da VM. Ao provisionar um disco virtual (por exemplo, como buffer de upload), você pode armazenar o disco virtual no mesmo armazenamento de dados que a VM ou em outro armazenamento de dados distinto.

Se você tiver mais de um armazenamento de dados, é altamente recomendável escolher um armazenamento de dados para cada tipo de armazenamento local que você estiver criando. O

armazenamento de dados que conta apenas com um disco físico subjacente pode apresentar um desempenho ruim. Um exemplo é quando você usa um disco para apoiar o armazenamento em cache e o buffer de upload em uma configuração de gateway. Da mesma forma, um armazenamento de dados que conta uma configuração de RAID de desempenho mais baixo, como RAID 1 ou RAID 6, pode apresentar um desempenho ruim.

Adicione recursos de CPU ao host de seu gateway

O requisito mínimo para o servidor de host do gateway é quatro processadores virtuais. Para otimizar o desempenho do gateway, confirme se cada processador virtual atribuídos à VM do gateway contam com o suporte de um núcleo dedicado. Além disso, confirme se você não está comprometendo exageradamente as CPUs do servidor de host.

Ao adicionar mais CPUs ao servidor de host do gateway, você pode aumentar a capacidade de processamento do gateway. Isso permite que seu gateway lide paralelamente com o armazenamento de dados de sua aplicação no armazenamento local e o upload desses dados para o Amazon S3. As CPUs adicionais também ajudam a garantir que seu gateway tenha recursos de CPU suficientes quando o host for compartilhado com outras VMs. Ao fornecer recursos suficientes de CPU, o resultado de modo geral é a melhoria da taxa de transferência.

Aumente a largura de banda entre o gateway e a nuvem da AWS

Aumentar sua largura de banda de ida e AWS volta aumentará a taxa máxima de entrada de dados em seu gateway e saída para a nuvem. AWS Isso pode melhorar o desempenho do gateway se a velocidade da rede for o fator limitante na configuração do gateway, em vez de outros fatores, como discos lentos ou baixa largura de banda da conexão do iniciador do gateway.

Note

O desempenho observado do gateway provavelmente será menor do que a largura de banda da rede devido a outros fatores limitantes listados aqui, como o throughput do disco do buffer de cache/upload, a contagem de núcleos da CPU, a quantidade total de RAM ou a largura de banda entre o iniciador e o gateway. Além disso, a operação normal do gateway envolve muitas ações tomadas para proteger seus dados, o que pode fazer com que o desempenho observado seja menor que a largura de banda da rede.

Altere a configuração de volumes

Em gateways de volume, se você perceber que a adição de mais volumes a um gateway reduz o throughput para o gateway, pense na possibilidade de adicionar volumes a um gateway diferente. Mais especificamente, se um volume for usado por um aplicativo com alta taxa de transferência, pense na possibilidade de criar um gateway diferente para o aplicativo com alta taxa de transferência. No entanto, de modo geral, você não deve usar um único gateway para todos os aplicativos com alta taxa de transferência e outro gateway para todos os aplicativos com baixa taxa de transferência. Para medir a taxa de transferência do volume, use as métricas `ReadBytes` e `WriteBytes`.

Para ter mais informações sobre essas métricas, consulte [Como medir o desempenho entre seu aplicativo e o gateway](#).

Otimizar as configurações iSCSI

É possível otimizar as configurações iSCSI no iniciador iSCSI para obter maior desempenho de E/S. Recomendamos escolher 256 KiB para `MaxReceiveDataSegmentLength` e `FirstBurstLength` e 1 MiB para `MaxBurstLength`. Para obter mais informações sobre como definir configurações iSCSI, consulte [Como personalizar as configurações iSCSI](#).

Note

Estas configurações recomendadas podem facilitar um melhor desempenho geral. No entanto, as configurações iSCSI específicas que são necessárias para otimizar o desempenho variam dependendo do software de backup usado. Para obter detalhes, consulte a documentação do software de backup.

Como adicionar recursos ao seu ambiente de aplicativos

Aumente a largura de banda entre o servidor de aplicativos e o gateway

A conexão entre o iniciador iSCSI e o gateway pode limitar o desempenho de upload e download. Se o gateway estiver apresentando desempenho significativamente pior do que o esperado e você já tiver melhorado a contagem de núcleos de CPU e o throughput de disco, considere:

- Como atualizar os cabos de rede para ter uma maior largura de banda entre o iniciador e o gateway.

Para otimizar o desempenho do gateway, confirme se a largura de banda da rede entre o aplicativo e o gateway pode atender às necessidades de seu aplicativo. É possível usar as métricas `ReadBytes` e `WriteBytes` do gateway para medir o total de throughput de dados..

Para seu aplicativo, compare a taxa de transferência medidas com a taxa de transferência desejada. Se a taxa de transferência medida for inferior à taxa de transferência desejada, a ampliação da largura de banda entre o aplicativo e o gateway pode melhorar o desempenho se a rede for o gargalo. Da mesma forma, você pode aumentar a largura de banda entre a VM e os discos locais, se eles não estiverem diretamente vinculados.

Adicione recursos de CPU ao seu ambiente de aplicativos

Se seu aplicativo puder usar outros recursos de CPU, adicionar mais CPUs pode ajudar seu aplicativo a dimensionar a respectiva carga de E/S.

Como usar o VMware vSphere High Availability com o Storage Gateway

O Storage Gateway fornece uma alta disponibilidade no VMware por meio de um conjunto de verificações de integridade no nível da aplicação integradas à Alta Disponibilidade do VMware vSphere (VMware HA). Essa abordagem ajuda a proteger as cargas de trabalho de armazenamento contra falhas de hardware, de hipervisor ou de rede. Ela também ajuda a proteger contra erros de software, como tempos limite de conexão e compartilhamento de arquivos ou indisponibilidade de volume.

O vSphere HA funciona agrupando máquinas virtuais e os hosts em que elas residem em um cluster para redundância. Os hosts no cluster são monitorados e, em caso de falha, as máquinas virtuais em um host com falha são reiniciadas em hosts alternativos. Geralmente, essa recuperação acontece rapidamente e sem perda de dados. Para obter mais informações sobre o vSphere HA, consulte Como o [vSphere HA funciona na documentação da VMware](#).

Note

O tempo necessário para reiniciar uma máquina virtual com falha e restabelecer a conexão iSCSI em um novo host depende de muitos fatores, como o sistema operacional e a carga de recursos do host, a velocidade do disco, a conexão de rede e a infraestrutura de SAN/armazenamento.

Para usar o VMware HA com o Storage Gateway, siga as etapas listadas a seguir.

Tópicos

- [Configurar o cluster do vSphere VMware HA](#)
- [Baixe a imagem .ova do console do Storage Gateway](#)
- [Implantar o gateway](#)
- [\(Opcional\) Adicionar opções de substituição para outras VMs no cluster](#)
- [Ativar o gateway.](#)
- [Teste a configuração do VMware High Availability](#)

Configurar o cluster do vSphere VMware HA

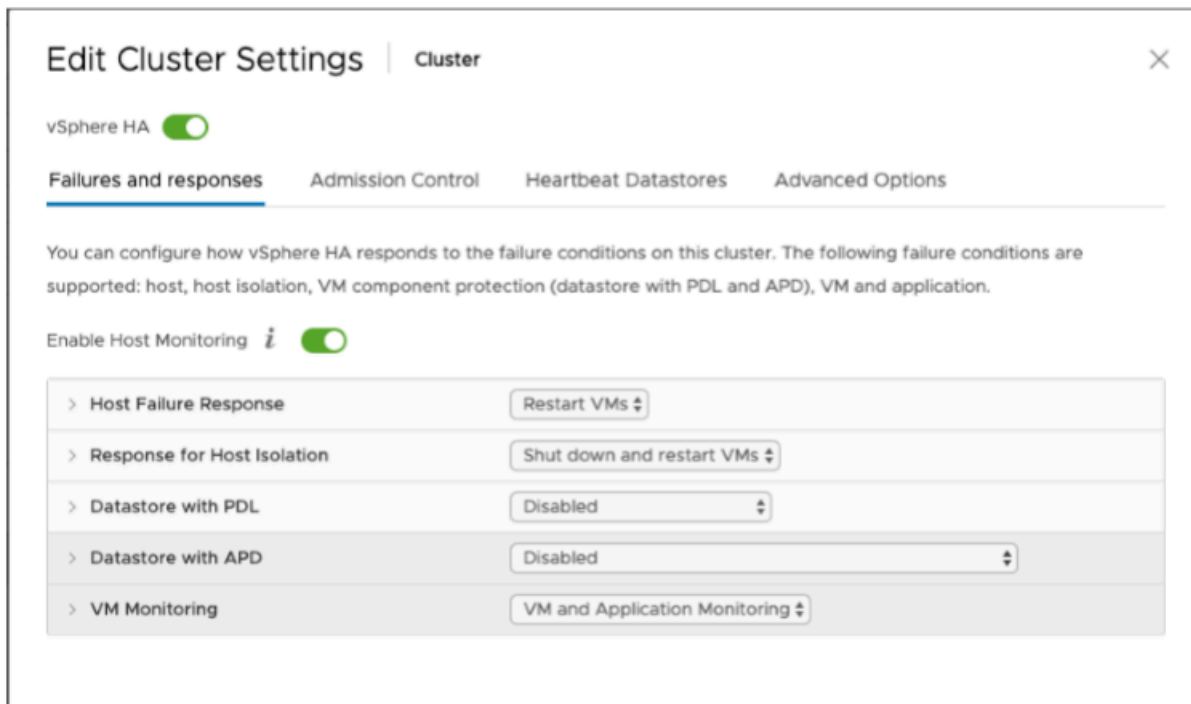
Primeiro, se você ainda não tiver criado um cluster do VMware, crie um. Para obter informações sobre como criar um cluster do VMware, consulte [Create a vSphere HA Cluster](#) na documentação do VMware.

Depois, configure o cluster do VMware para trabalhar com o Storage Gateway.

Como configurar o cluster do VMware

1. Na página Edit Cluster Settings (Editar configurações do cluster) no VMware vSphere, verifique se o monitoramento da VM está configurado para monitoramento de VM e aplicativos. Para fazer isso, defina as seguintes opções conforme indicado:
 - Host Failure Response (Resposta à falha do host): Restart VMs (Reiniciar VMs)
 - Response for Host Isolation (Resposta ao isolamento do host): Shut down and restart VMs (Desligar e reiniciar VMs)
 - Datastore with PDL (Armazenamento de dados com PDL): Disabled (Desativado)
 - Datastore with APD (Armazenamento de dados com APD): Disabled (Desativado)
 - VM Monitoring (Monitoramento de VM): VM and Application Monitoring (Monitoramento de VM e aplicativos)

Para obter um exemplo, consulte as capturas de tela a seguir.



2. Ajuste a sensibilidade do cluster ajustando os seguintes valores:

- Intervalo de falha: após esse intervalo, a VM será reiniciada se uma pulsação da VM não for recebida.
- Tempo mínimo de atividade: o cluster aguarda esse tempo depois que uma VM começa a monitorar as pulsações das ferramentas de VM.
- Redefinições máximas por VM: define o máximo de vezes que o cluster reinicia a VM durante a janela temporal para o máximo de redefinições.
- Janela de tempo de redefinições máximas: a janela de tempo na qual ocorre a contagem de redefinições máximas por VM.

Se você não tiver certeza de quais valores definir, use estas configurações de exemplo:

- Failure interval (Intervalo de falha): **30** segundos
- Minimum uptime (Tempo mínimo de atividade): **120** segundos
- Maximum per-VM resets (Máximo de redefinições por VM): **3**
- Maximum resets time window (Janela temporal para o máximo de redefinições): **1** hora

Se você tiver outras VMs em execução no cluster, talvez você queira definir esses valores especificamente para sua VM. Não é possível fazer isso até implantar a VM a partir do .ova. Para

obter mais informações sobre como definir esses valores, consulte [\(Opcional\) Adicionar opções de substituição para outras VMs no cluster](#).

Baixe a imagem .ova do console do Storage Gateway

Para baixar a imagem .ova para o gateway

- Na página Configurar gateway no console do Storage Gateway, selecione o tipo de gateway e a plataforma do host e use o link fornecido no console para baixar o .ova, conforme descrito em [Configurar um gateway de volumes](#).

Implantar o gateway

No cluster configurado, implante a imagem .ova em um dos hosts do cluster.

Como implantar a imagem .ova do gateway

1. Implante a imagem .ova em um dos hosts no cluster.
2. Verifique se os armazenamentos de dados escolhidos para o disco raiz e o cache estão disponíveis para todos os hosts no cluster. Ao implantar o arquivo .ova do Storage Gateway em um ambiente VMware ou local, os discos são descritos como discos SCSI paravirtualizados. Paravirtualização é um modo no qual a VM do gateway funciona com o sistema operacional do host para que o console possa identificar os discos virtuais que você adiciona à sua VM.

Para configurar sua VM para usar controladores paravirtualizados

1. No cliente VMware vSphere, abra o menu de contexto (clique com o botão direito) da VM do gateway e escolha Edit Settings.
2. Na caixa de diálogo Virtual Machine Properties, escolha a guia Hardware, selecione SCSI controller 0 e escolha Change Type.
3. Na caixa de diálogo Change SCSI Controller Type, selecione o tipo de controlador SCSI VMware Paravirtual e escolha OK.

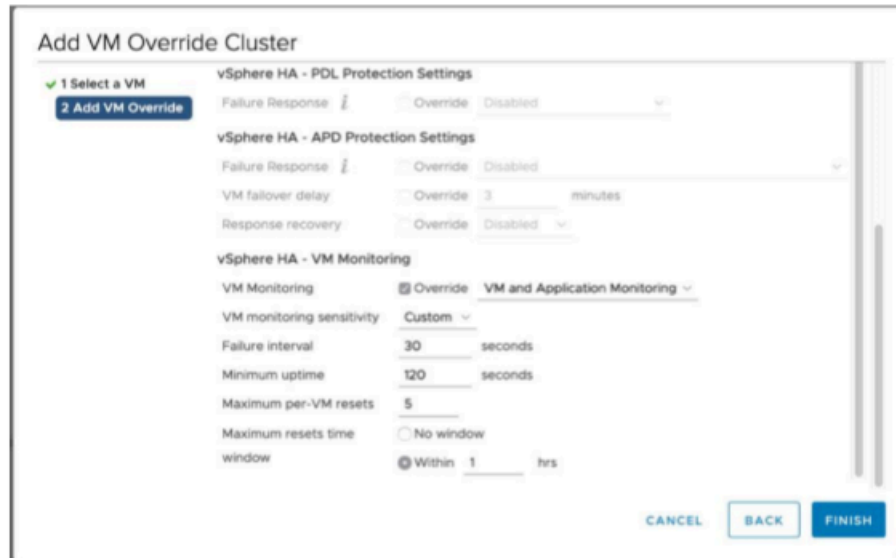
(Opcional) Adicionar opções de substituição para outras VMs no cluster

Se tiver outras VMs em execução no cluster, talvez você queira definir os valores do cluster especificamente para cada VM.

Como adicionar opções de substituição para outras VMs no cluster

1. Na página Summary (Resumo) do VMware vSphere, escolha o cluster para abrir a página do cluster e selecione Configure (Configurar).
2. Selecione a guia Configuration (Configuração) e selecione VM Overrides (Substituições de VM).
3. Adicione uma nova opção de substituição de VM para alterar cada valor.

Para opções de substituição, consulte a captura de tela a seguir.



Ativar o gateway.

Depois que o .ova do gateway for implantado, ative o gateway. As instruções de como fazer isso são diferentes para cada tipo de gateway.

Para ativar seu gateway

- Siga os procedimentos descritos nos seguintes tópicos:
 - a. [Conecte seu Volume Gateway a AWS](#)
 - b. [Analisar as configurações e ativar o gateway de volumes](#)
 - c. [Configure o gateway de volumes](#)

Teste a configuração do VMware High Availability

Depois de ativar o gateway, teste a configuração.

Como testar a configuração do VMware HA

1. Abra o console do Storage Gateway em <https://console.aws.amazon.com/storagegateway/home>.
2. No painel de navegação, selecione Gateways e escolha o gateway que você deseja testar para o VMware HA.
3. Em Actions (Ações), selecione Verify VMware HA (Verificar VMware HA).
4. Na caixa Verify VMware High Availability Configuration (Verificar configuração do VMware High Availability) exibida, selecione OK.

Note

Testar a configuração do VMware HA reinicializa a VM do gateway e interrompe a conectividade com o gateway. O teste pode levar alguns minutos para ser concluído.

Se o teste for bem-sucedido, o status Verified (Verificado) será exibido na guia de detalhes do gateway no console.

5. Selecione Exit (Sair).

Você pode encontrar informações sobre eventos do VMware HA nos grupos de CloudWatch log da Amazon. Para obter mais informações, consulte [Obter registros de integridade do gateway de volume com CloudWatch grupos de registros](#).

Segurança no AWS Storage Gateway

A segurança na nuvem AWS é a maior prioridade. Como AWS cliente, você se beneficia de uma arquitetura de data center e rede criada para atender aos requisitos das organizações mais sensíveis à segurança.

A segurança é uma responsabilidade compartilhada entre você AWS e você. O modelo de [responsabilidade compartilhada](#) descreve isso como a segurança da nuvem e segurança na nuvem:

- **Segurança da nuvem** — AWS é responsável por proteger a infraestrutura que executa AWS serviços na Amazon Web Services Cloud. AWS também fornece serviços que você pode usar com segurança. Auditores terceirizados testam e verificam regularmente a eficácia de nossa segurança como parte dos Programas de Conformidade Programas de [AWS](#) de . Para saber mais sobre os programas de conformidade que se aplicam ao AWS Storage Gateway, consulte [AWS Serviços no escopo do programa de conformidade AWS](#) .
- **Segurança na nuvem** — Sua responsabilidade é determinada pelo AWS serviço que você usa. Você também é responsável por outros fatores, incluindo a confidencialidade de seus dados, os requisitos da empresa e as leis e regulamentos aplicáveis.

Esta documentação ajuda você a entender como aplicar o modelo de responsabilidade compartilhada ao usar o Storage Gateway. Os tópicos a seguir mostram como configurar o Storage Gateway para atender aos seus objetivos de segurança e de conformidade. Você também aprenderá a usar outros AWS serviços que ajudam a monitorar e proteger seus recursos do Storage Gateway.

Tópicos

- [Proteção de dados no AWS Storage Gateway](#)
- [Identity and Access Management para AWS Storage Gateway](#)
- [Registro e monitoramento em AWS Storage Gateway](#)
- [Validação de conformidade do AWS Storage Gateway](#)
- [Resiliência no AWS Storage Gateway](#)
- [Segurança da infraestrutura no AWS Storage Gateway](#)
- [AWS Melhores práticas de segurança](#)

Proteção de dados no AWS Storage Gateway

O modelo de [responsabilidade AWS compartilhada O modelo](#) se aplica à proteção de dados no AWS Storage Gateway. Conforme descrito neste modelo, AWS é responsável por proteger a infraestrutura global que executa todos os Nuvem AWS. Você é responsável por manter o controle sobre seu conteúdo hospedado nessa infraestrutura. Você também é responsável pelas tarefas de configuração e gerenciamento de segurança dos Serviços da AWS que usa. Para obter mais informações sobre a privacidade de dados, consulte as [Perguntas frequentes sobre privacidade de dados](#). Para mais informações sobre a proteção de dados na Europa, consulte o artigo [AWS Shared Responsibility Model and GDPR](#) no Blog de segurança da AWS .

Para fins de proteção de dados, recomendamos que você proteja Conta da AWS as credenciais e configure usuários individuais com AWS IAM Identity Center 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. AWS Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Configure a API e o registro de atividades do usuário com AWS CloudTrail.
- Use soluções de AWS criptografia, juntamente com todos os controles de segurança padrão Serviços da AWS.
- Use serviços gerenciados de segurança avançada, como o Amazon Macie, que ajuda a localizar e proteger dados sigilosos armazenados no Amazon S3.
- Se você precisar de módulos criptográficos validados pelo FIPS 140-2 ao acessar AWS por meio de uma interface de linha de comando ou de uma API, use um endpoint FIPS. Para ter mais informações sobre endpoints do FIPS, consulte [Federal Information Processing Standard \(FIPS\) 140-2](#).

É altamente recomendável que nunca sejam colocadas informações de identificação confidenciais, como endereços de e-mail dos seus clientes, em marcações ou campos de formato livre, como um campo Nome. Isso inclui quando você trabalha com o Storage Gateway ou outro Serviços da AWS usando o console, a API ou AWS os SDKs. AWS CLI Quaisquer dados inseridos em tags ou 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, recomendamos fortemente que não sejam incluídas informações de credenciais no URL para validar a solicitação a esse servidor.

Criptografia de dados usando AWS KMS

O Storage Gateway usa SSL/TLS (Secure Socket Layers/Transport Layer Security) para criptografar dados que são transferidos entre o dispositivo de gateway e o armazenamento. AWS Por padrão, o Storage Gateway usa chaves de criptografia gerenciadas do Amazon S3 (SSE-S3) do lado do servidor para criptografar todos os dados armazenados no Amazon S3. Você tem a opção de usar a API Storage Gateway para configurar seu gateway para criptografar dados armazenados na nuvem usando criptografia do lado do servidor com chaves AWS Key Management Service (SSE-KMS).

Important

Ao usar uma AWS KMS chave para criptografia do lado do servidor, você deve escolher uma chave simétrica. O Storage Gateway não é compatível com chaves assimétricas. Para obter mais informações, consulte [Como usar chaves simétricas e assimétricas](#) no AWS Key Management Service Guia do desenvolvedor.

Como criptografar um compartilhamento de arquivos

Para um compartilhamento de arquivos, é possível configurar seu gateway para criptografar seus objetos com chaves gerenciadas pelo AWS KMS usando o SSE-KMS. Para obter informações sobre como usar a API Storage Gateway para criptografar dados gravados em um compartilhamento de arquivos, consulte [CreateNFS FileShare na Referência](#) da AWS Storage Gateway API.

Como criptografar um volume

Para volumes em cache e armazenados, você pode configurar seu gateway para criptografar dados de volume armazenados na nuvem com chaves AWS KMS gerenciadas usando a API Storage Gateway. É possível especificar uma das chaves mestras de cliente como a chave do KMS. A chave que você usa para criptografar o volume não pode ser alterada depois que o volume for criado. [Para obter informações sobre como usar a API Storage Gateway para criptografar dados gravados em um volume armazenado ou em cache, consulte CreateCachediscsiVolume ou scsiVolume na Referência CreateStorédi da API.AWS Storage Gateway](#)

Como criptografar uma fita

Para uma fita virtual, você pode configurar seu gateway para criptografar dados de fita armazenados na nuvem com chaves AWS KMS gerenciadas usando a API Storage Gateway. É possível especificar uma das chaves mestras de cliente como a chave do KMS. A chave que você usa para criptografar os dados da fita não pode ser alterada depois que a fita for criada. Para obter informações sobre como usar a API Storage Gateway para criptografar dados gravados [CreateTapes](#) em uma fita virtual, consulte a Referência da AWS Storage Gateway API.

Ao usar AWS KMS para criptografar seus dados, tenha em mente o seguinte:

- Seus dados estão criptografados em repouso na nuvem. Ou seja, os dados são criptografados no Amazon S3.
- Os usuários do IAM devem ter as permissões necessárias para chamar as operações AWS KMS da API. Para obter mais informações, consulte [Como usar políticas do IAM com o AWS KMS](#) no Guia do desenvolvedor do AWS Key Management Service .
- Se você excluir ou desativar sua AWS KMS chave ou revogar o token de concessão, não poderá acessar os dados no volume ou na fita. Para obter mais informações, consulte [Como excluir chaves do KMS](#) no Guia do desenvolvedor do AWS Key Management Service .
- Se você criar um snapshot de um volume criptografado pelo KMS, o snapshot será criptografado. O snapshot herdar a chave do KMS do volume.
- Se você criar um novo volume de um snapshot criptografado pelo KMS, o volume será criptografado. Você poderá especificar outra chave do KMS para o novo volume.

Note

O Storage Gateway não é compatível com a criação de um volume não criptografado de um ponto de recuperação de um volume criptografado pelo KMS ou snapshot criptografado pelo KMS.

Para obter mais informações sobre AWS KMS, consulte [O que é AWS Key Management Service?](#)

Como configurar a autenticação CHAP para os volumes

No Storage Gateway, os iniciadores iSCSI se conectam aos seus volumes como destinos iSCSI. O Storage Gateway usa o Challenge-Handshake Authentication Protocol (CHAP) para autenticar o iSCSI e as conexões de iniciadores. O CHAP oferece proteção contra ataques de playback exigindo autenticação para acessar os destinos de volumes de armazenamento. Para cada volume de

destino, é possível definir uma ou mais credenciais de CHAP. Você pode visualizar e editar essas credenciais para os diferentes iniciadores na caixa de diálogo de configuração de credenciais do CHAP.

Para configurar as credenciais do CHAP

1. No console do Storage Gateway, escolha Volumes e selecione o volume para o qual você deseja configurar as credenciais CHAP.
2. Em Actions (Ações), escolha Configure CHAP authentication (Configurar autenticação do CHAP).
3. Em Initiator name, digite o nome do iniciador. O nome deve ter pelo menos 1 caractere e no máximo 255 caracteres.
4. Em Segredo do iniciador, insira a frase secreta que você deseja usar para autenticar o iniciador iSCSI. A frase secreta do iniciador deve ter pelo menos 12 caracteres e no máximo 16 caracteres.
5. Em Target secret, insira a frase secreta que você deseja usar para autenticar o destino do CHAP mútuo. A frase secreta do destino deve ter pelo menos 12 caracteres e no máximo 16 caracteres.
6. Escolha Save para salvar as entradas.

Para visualizar ou atualizar as credenciais do CHAP, você precisa ter as permissões necessárias de perfil do IAM para executar essa operação.

Como visualizar e editar as credenciais CHAP

Você pode adicionar, remover ou atualizar as credenciais do CHAP para cada usuário. Para visualizar ou editar as credenciais do CHAP, você deve ter as permissões necessárias de perfil do IAM para executar essa operação, e o gateway ao qual o destino do iniciador está conectado deve ser um gateway em funcionamento.

Initiator name	Initiator secret ⓘ	Target secret ⓘ
initiator2	*****	***** ⓘ
initiator1	*****	***** ⓘ
Add an initiator name.	Add an initiator secret value.	Add a target secret value. ⓘ

This volume accepts only connections from authenticated iSCSI initiators. [Learn more](#)

Cancel Save

Para adicionar credenciais do CHAP

1. No console do Storage Gateway, escolha Volumes e selecione o volume para o qual você deseja adicionar as credenciais CHAP.
2. Em Actions (Ações), escolha Configure CHAP authentication (Configurar autenticação do CHAP).
3. Na página de configuração do CHAPS, insira o Initiator name, o Initiator secret e o Target secret em suas respectivas caixas e, em seguida, selecione Save.

Para remover as credenciais do CHAP

1. No console do Storage Gateway, escolha Volumes e selecione o volume para o qual você deseja remover as credenciais CHAP.
2. Em Actions (Ações), escolha Configure CHAP authentication (Configurar autenticação do CHAP).
3. Clique no X próximo às credenciais que você deseja remover e escolha Salvar.

Para atualizar as credenciais do CHAP

1. No console do Storage Gateway, escolha Volumes e selecione o volume para o qual você deseja atualizar as credenciais CHAP.
2. Em Actions (Ações), escolha Configure CHAP authentication (Configurar autenticação do CHAP).

3. Na página de configuração das credenciais do CHAP, altere as entradas das credenciais que você deseja atualizar.
4. Escolha Salvar.

Identity and Access Management para AWS Storage Gateway

AWS Identity and Access Management (IAM) é uma ferramenta AWS service (Serviço da AWS) que ajuda o administrador a controlar com segurança o acesso aos AWS recursos. Os administradores do IAM controlam quem pode ser autenticado (conectado) e autorizado (tem permissões) para usar os recursos do AWS SGW. O IAM é um AWS service (Serviço da AWS) que você pode usar sem custo adicional.

Tópicos

- [Público](#)
- [Autenticando com identidades](#)
- [Gerenciando acesso usando políticas](#)
- [Como o AWS Storage Gateway funciona com o IAM](#)
- [Exemplos de políticas baseadas em identidade para o AWS Storage Gateway](#)
- [Solução de problemas AWS de identidade e acesso ao Storage Gateway](#)

Público

A forma como você usa AWS Identity and Access Management (IAM) difere, dependendo do trabalho que você faz no AWS SGW.

Usuário do serviço — Se você usar o serviço AWS SGW para fazer seu trabalho, seu administrador fornecerá as credenciais e as permissões de que você precisa. À medida que você usa mais recursos do AWS SGW para fazer seu trabalho, talvez precise de permissões adicionais.

Entender como o acesso é gerenciado pode ajudar você a solicitar as permissões corretas ao seu administrador. Se não for possível acessar um atributo no AWS Storage Gateway, consulte [Solução de problemas AWS de identidade e acesso ao Storage Gateway](#).

Administrador de serviços — Se você é responsável pelos recursos do AWS SGW em sua empresa, provavelmente tem acesso total ao AWS SGW. É seu trabalho determinar quais recursos e recursos

do AWS SGW seus usuários do serviço devem acessar. Assim, você deve enviar solicitações ao administrador do IAM para alterar as permissões dos usuários de seu serviço. Revise as informações nesta página para entender os Introdução ao IAM. Para saber mais sobre como sua empresa pode usar o IAM com o AWS SGW, consulte [Como o AWS Storage Gateway funciona com o IAM](#).

Administrador do IAM — Se você for administrador do IAM, talvez queira saber detalhes sobre como criar políticas para gerenciar o acesso ao AWS SGW. Para ver exemplos de políticas baseadas em identidade AWS SGW que você pode usar no IAM, consulte. [Exemplos de políticas baseadas em identidade para o AWS Storage Gateway](#)

Autenticando com identidades

A autenticação é como você faz login AWS usando suas credenciais de identidade. Você deve estar autenticado (conectado AWS) como o Usuário raiz da conta da AWS, como usuário do IAM ou assumindo uma função do IAM.

Você pode entrar AWS como uma identidade federada usando credenciais fornecidas por meio de uma fonte de identidade. AWS IAM Identity Center Usuários (IAM Identity Center), a autenticação de login único da sua empresa e suas credenciais do Google ou do Facebook são exemplos de identidades federadas. Quando você faz login como identidade federada, o administrador já configurou anteriormente a federação de identidades usando perfis do IAM. Ao acessar AWS usando a federação, você está assumindo indiretamente uma função.

Dependendo do tipo de usuário que você é, você pode entrar no AWS Management Console ou no portal de AWS acesso. Para obter mais informações sobre como fazer login AWS, consulte [Como fazer login Conta da AWS no](#) Guia do Início de Sessão da AWS usuário.

Se você acessar AWS programaticamente, AWS fornece um kit de desenvolvimento de software (SDK) e uma interface de linha de comando (CLI) para assinar criptograficamente suas solicitações usando suas credenciais. Se você não usa AWS ferramentas, você mesmo deve assinar as solicitações. Para obter mais informações sobre como usar o método recomendado para assinar solicitações por conta própria, consulte [Assinatura de solicitações de AWS API](#) no Guia do usuário do IAM.

Independente do método de autenticação usado, também pode ser exigido que você forneça informações adicionais de segurança. Por exemplo, AWS recomenda que você use a autenticação multifator (MFA) para aumentar a segurança da sua conta. Para saber mais, consulte [Autenticação Multifator](#) no Guia do Usuário do AWS IAM Identity Center . [Usar a autenticação multifator \(MFA\) na AWS](#) no Guia do Usuário do IAM.

Conta da AWS usuário root

Ao criar uma Conta da AWS, você começa com uma identidade de login que tem acesso completo a todos Serviços da AWS os recursos da conta. Essa identidade é chamada de usuário Conta da AWS raiz e é acessada fazendo login com o endereço de e-mail e a senha que você usou para criar a conta. É altamente recomendável não usar o usuário raiz para tarefas diárias. Proteja as credenciais do usuário raiz e use-as para executar as tarefas que somente ele puder executar. Para obter a lista completa das tarefas que exigem login como usuário raiz, consulte [Tarefas que exigem credenciais de usuário raiz](#) no Guia do Usuário do IAM.

Identidade federada

Como prática recomendada, exija que usuários humanos, incluindo usuários que precisam de acesso de administrador, usem a federação com um provedor de identidade para acessar Serviços da AWS usando credenciais temporárias.

Uma identidade federada é um usuário do seu diretório de usuários corporativo, de um provedor de identidade da web AWS Directory Service, do diretório do Identity Center ou de qualquer usuário que acesse usando credenciais fornecidas Serviços da AWS por meio de uma fonte de identidade. Quando as identidades federadas são acessadas Contas da AWS, elas assumem funções, e as funções fornecem credenciais temporárias.

Para o gerenciamento de acesso centralizado, recomendamos usar o AWS IAM Identity Center. Você pode criar usuários e grupos no IAM Identity Center ou pode se conectar e sincronizar com um conjunto de usuários e grupos em sua própria fonte de identidade para uso em todos os seus Contas da AWS aplicativos. Para obter mais informações sobre o Centro de Identidade do IAM, consulte [O que é o Centro de Identidade do IAM?](#) no Manual do Usuário do AWS IAM Identity Center .

Usuários e grupos do IAM

Um [usuário do IAM](#) é uma identidade dentro da sua Conta da AWS que tem permissões específicas para uma única pessoa ou aplicativo. Sempre que possível, recomendamos contar com credenciais temporárias em vez de criar usuários do IAM com credenciais de longo prazo, como senhas e chaves de acesso. No entanto, se você tiver casos de uso específicos que exijam credenciais de longo prazo com usuários do IAM, recomendamos alternar as chaves de acesso. Para obter mais informações, consulte [Altere as chaves de acesso regularmente para casos de uso que exijam credenciais de longo prazo](#) no Guia do Usuário do IAM.

Um [grupo do IAM](#) é uma identidade que especifica uma coleção de usuários do IAM. Não é possível fazer login como um grupo. É possível usar grupos para especificar permissões para vários usuários

de uma vez. Os grupos facilitam o gerenciamento de permissões para grandes conjuntos de usuários. Por exemplo, você pode ter um grupo chamado IAMAdmins e conceder a esse grupo permissões para administrar recursos do IAM.

Usuários são diferentes de perfis. Um usuário é exclusivamente associado a uma pessoa ou a uma aplicação, mas um perfil pode ser assumido por qualquer pessoa que precisar dele. Os usuários têm credenciais permanentes de longo prazo, mas os perfis fornecem credenciais temporárias. Para saber mais, consulte [Quando criar um usuário do IAM \(em vez de um perfil\)](#) no Guia do usuário do IAM.

Perfis do IAM

Uma [função do IAM](#) é uma identidade dentro da sua Conta da AWS que tem permissões específicas. Ele é semelhante a um usuário do IAM, mas não está associado a uma pessoa específica. Você pode assumir temporariamente uma função do IAM no AWS Management Console [trocando de funções](#). Você pode assumir uma função chamando uma operação de AWS API AWS CLI ou usando uma URL personalizada. Para obter mais informações sobre métodos para o uso de perfis, consulte [Utilizar perfis do IAM](#) no Guia do usuário do IAM.

Funções do IAM com credenciais temporárias são úteis nas seguintes situações:

- **Acesso de usuário federado:** para atribuir permissões a identidades federadas, você pode criar um perfil e definir permissões para ele. Quando uma identidade federada é autenticada, essa identidade é associada ao perfil e recebe as permissões definidas pelo mesmo. Para obter mais informações sobre perfis para federação, consulte [Criar um perfil para um provedor de identidades de terceiros](#) no Guia do Usuário do IAM. Se você usar o Centro de identidade do IAM, configure um conjunto de permissões. Para controlar o que suas identidades podem acessar após a autenticação, o Centro de identidade do IAM correlaciona o conjunto de permissões a um perfil no IAM. Para obter informações sobre conjuntos de permissões, consulte [Conjuntos de Permissões](#) no Manual do Usuário do AWS IAM Identity Center .
- **Permissões temporárias para usuários do IAM** — um usuário ou um perfil do IAM pode presumir um perfil do IAM para obter temporariamente permissões diferentes para uma tarefa específica.
- **Acesso entre contas** — é possível usar um perfil do IAM para permitir que alguém (uma entidade principal confiável) em outra conta acesse recursos em sua conta. Os perfis são a principal forma de conceder acesso entre contas. No entanto, com alguns Serviços da AWS, você pode anexar uma política diretamente a um recurso (em vez de usar uma função como proxy). Para saber a diferença entre perfis e políticas baseadas em recurso para acesso entre contas, consulte [Acesso a recursos entre contas no IAM](#) no Guia do usuário do IAM.

- **Acesso entre serviços** — Alguns Serviços da AWS usam recursos em outros Serviços da AWS. Por exemplo, quando você faz uma chamada em um serviço, é comum que esse serviço execute aplicativos no Amazon EC2 ou armazene objetos no Amazon S3. Um serviço pode fazer isso usando as permissões do principal de chamada, usando um perfil de serviço ou um perfil vinculado a serviço.
- **Sessões de acesso direto (FAS)** — Quando você usa um usuário ou uma função do IAM para realizar ações AWS, você é considerado principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O FAS usa as permissões do diretor chamando um AWS service (Serviço da AWS), combinadas com a solicitação AWS service (Serviço da AWS) para fazer solicitações aos serviços posteriores. As solicitações do FAS são feitas somente quando um serviço recebe uma solicitação que requer interações com outros Serviços da AWS ou com recursos para ser concluída. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte [Encaminhar sessões de acesso](#).
- **Função de serviço**: um perfil de serviço é um [perfil do IAM](#) que um serviço assume para realizar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para obter mais informações, consulte [Criar um perfil para delegar permissões a um AWS service \(Serviço da AWS\)](#) no Guia do Usuário do IAM.
- **Função vinculada ao serviço** — Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um AWS service (Serviço da AWS). O serviço pode presumir a função de executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não editar as permissões para funções vinculadas ao serviço.
- **Aplicativos em execução no Amazon EC2** — Você pode usar uma função do IAM para gerenciar credenciais temporárias para aplicativos que estão sendo executados em uma instância do EC2 e fazendo AWS CLI solicitações de API. É preferível fazer isso e armazenar chaves de acesso na instância do EC2. Para atribuir uma AWS função a uma instância do EC2 e disponibilizá-la para todos os seus aplicativos, você cria um perfil de instância anexado à instância. Um perfil de instância contém o perfil e permite que os programas em execução na instância do EC2 obtenham credenciais temporárias. Para mais informações, consulte [Utilizar um perfil do IAM para conceder permissões a aplicações em execução nas instâncias do Amazon EC2](#) no Guia do usuário do IAM.

Para saber se deseja usar perfis do IAM, consulte [Quando criar um perfil do IAM \(em vez de um usuário\)](#) no Guia do usuário do IAM.

Gerenciando acesso usando políticas

Você controla o acesso AWS criando políticas e anexando-as a AWS identidades ou recursos. Uma política é um objeto AWS que, quando associada a uma identidade ou recurso, define suas permissões. AWS avalia essas políticas quando um principal (usuário, usuário raiz ou sessão de função) faz uma solicitação. As permissões nas políticas determinam se a solicitação será permitida ou negada. A maioria das políticas é armazenada AWS como documentos JSON. Para obter mais informações sobre a estrutura e o conteúdo de documentos de políticas JSON, consulte [Visão geral das políticas JSON](#) no Guia do Usuário do IAM.

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

Por padrão, usuários e funções não têm permissões. Para conceder aos usuários permissões para executar ações nos recursos que eles precisam, um administrador do IAM pode criar políticas do IAM. O administrador pode então adicionar as políticas do IAM aos perfis e os usuários podem presumir os perfis.

As políticas do IAM definem permissões para uma ação independente do método usado para executar a operação. Por exemplo, suponha que você tenha uma política que permite a ação `iam:GetRole`. Um usuário com essa política pode obter informações de função da AWS Management Console AWS CLI, da ou da AWS API.

Políticas baseadas em identidade

As políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como usuário do IAM, grupo de usuários ou perfil. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte [Criando políticas do IAM](#) no Guia do Usuário do IAM.

As políticas baseadas em identidade podem ser categorizadas ainda adicionalmente como políticas em linha ou políticas gerenciadas. As políticas em linha são anexadas diretamente a um único usuário, grupo ou perfil. As políticas gerenciadas são políticas autônomas que você pode associar a vários usuários, grupos e funções em seu Conta da AWS. As políticas AWS gerenciadas incluem políticas gerenciadas e políticas gerenciadas pelo cliente. Para saber como escolher entre uma política gerenciada ou uma política em linha, consulte [Escolher entre políticas gerenciadas e políticas em linha](#) no Guia do Usuário do IAM.

Políticas baseadas em recursos

Políticas baseadas em recursos são documentos de políticas JSON que você anexa a um recurso. São exemplos de políticas baseadas em recursos as políticas de confiança de perfil do IAM e as políticas de bucket do Amazon S3. Em serviços que suportem políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o recurso ao qual a política está anexada, a política define quais ações um principal especificado pode executar nesse recurso e em que condições. Você deve [especificar uma entidade principal](#) em uma política baseada em recursos. Os diretores podem incluir contas, usuários, funções, usuários federados ou. Serviços da AWS

Políticas baseadas em recursos são políticas em linha localizadas nesse serviço. Você não pode usar políticas AWS gerenciadas do IAM em uma política baseada em recursos.

Listas de controle de acesso (ACLs)

As listas de controle de acesso (ACLs) controlam quais entidades principais (membros, usuários ou perfis da conta) têm permissões para acessar um recurso. As ACLs são semelhantes as políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

O Amazon S3 e o Amazon VPC são exemplos de serviços que oferecem suporte a ACLs. AWS WAF Para saber mais sobre ACLs, consulte [Visão geral da lista de controle de acesso \(ACL\)](#) no Guia do Desenvolvedor do Amazon Simple Storage Service.

Outros tipos de política

AWS oferece suporte a tipos de políticas adicionais menos comuns. Esses tipos de política podem definir o máximo de permissões concedidas a você pelos tipos de política mais comuns.

- **Limites de permissões:** um limite de permissões é um atributo avançado no qual você define o máximo de permissões que uma política baseada em identidade pode conceder a uma entidade do IAM (usuário ou perfil do IAM). É possível definir um limite de permissões para uma entidade. As permissões resultantes são a interseção das políticas baseadas em identidade de uma entidade com seus limites de permissões. As políticas baseadas em recurso que especificam o usuário ou o perfil no campo `Principal` não são limitadas pelo limite de permissões. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações sobre limites de permissões, consulte [Limites de permissões para identidades do IAM](#) no Guia do Usuário do IAM.

- Políticas de controle de serviço (SCPs) — SCPs são políticas JSON que especificam as permissões máximas para uma organização ou unidade organizacional (OU) em AWS Organizations. AWS Organizations é um serviço para agrupar e gerenciar centralmente várias Contas da AWS que sua empresa possui. Se você habilitar todos os atributos em uma organização, poderá aplicar políticas de controle de serviço (SCPs) a qualquer uma ou a todas as contas. O SCP limita as permissões para entidades nas contas dos membros, incluindo cada uma Usuário raiz da conta da AWS. Para obter mais informações sobre as Organizações e SCPs, consulte [Como os SCPs Funcionam](#) no Manual do Usuário do AWS Organizations .
- Políticas de sessão: são políticas avançadas que você transmite como um parâmetro quando cria de forma programática uma sessão temporária para um perfil ou um usuário federado. As permissões da sessão resultante são a interseção das políticas baseadas em identidade do usuário ou do perfil e das políticas de sessão. As permissões também podem ser provenientes de uma política baseada em atributo. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações, consulte [Políticas de sessão](#) no Guia do Usuário do IAM.

Vários tipos de política

Quando vários tipos de política são aplicáveis a uma solicitação, é mais complicado compreender as permissões resultantes. Para saber como AWS determina se uma solicitação deve ser permitida quando vários tipos de políticas estão envolvidos, consulte [Lógica de avaliação de políticas](#) no Guia do usuário do IAM.

Como o AWS Storage Gateway funciona com o IAM

Antes de usar o IAM para gerenciar o acesso ao AWS SGW, saiba quais recursos do IAM estão disponíveis para uso com o AWS SGW.

Recursos do IAM que você pode usar com o AWS Storage Gateway

Atributo do IAM	AWS Suporte SGW
Políticas baseadas em identidade	Sim
Políticas baseadas em recursos	Não
Ações das políticas	Sim

Atributo do IAM	AWS Suporte SGW
Atributos de políticas	Sim
Chaves de condição de política (específicas do serviço)	Sim
ACLs	Não
ABAC (tags em políticas)	Parcial
Credenciais temporárias	Sim
Sessões de acesso direto (FAS)	Sim
Perfis de serviço	Sim
Funções vinculadas a serviço	Sim

Para ter uma visão de alto nível de como o AWS SGW e outros AWS serviços funcionam com a maioria dos recursos do IAM, consulte [AWS os serviços que funcionam com o IAM no Guia do usuário do IAM](#).

Políticas baseadas em identidade para SGW AWS

Suporta políticas baseadas em identidade	Sim
--	-----

As políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como usuário, grupo de usuários ou perfil do IAM. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte [Criando políticas do IAM](#) no Guia do Usuário do IAM.

Com as políticas baseadas em identidade do IAM, é possível especificar ações ou recursos permitidos ou negados, assim como as condições sob as quais as ações são permitidas ou negadas. Você não pode especificar a entidade principal em uma política baseada em identidade porque ela se aplica ao usuário ou perfil ao qual ela está anexada. Para saber mais sobre todos os elementos

que podem ser usados em uma política JSON, consulte [Referência de elementos da política JSON do IAM](#) no Guia do Usuário do IAM.

Exemplos de políticas baseadas em identidade para SGW AWS

Para ver exemplos de políticas baseadas em identidade do AWS SGW, consulte. [Exemplos de políticas baseadas em identidade para o AWS Storage Gateway](#)

Políticas baseadas em recursos no SGW AWS

Oferece compatibilidade com políticas baseadas em recursos	Não
--	-----

Políticas baseadas em recursos são documentos de políticas JSON que você anexa a um recurso. São exemplos de políticas baseadas em recursos as políticas de confiança de perfil do IAM e as políticas de bucket do Amazon S3. Em serviços que suportem políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o recurso ao qual a política está anexada, a política define quais ações um principal especificado pode executar nesse recurso e em que condições. Você deve [especificar uma entidade principal](#) em uma política baseada em recursos. Os diretores podem incluir contas, usuários, funções, usuários federados ou. Serviços da AWS

Para permitir o acesso entre contas, você pode especificar uma conta inteira ou as entidades do IAM em outra conta como a entidade principal em uma política baseada em atributo. Adicionar uma entidade principal entre contas à política baseada em recurso é apenas metade da tarefa de estabelecimento da relação de confiança. Quando o principal e o recurso são diferentes Contas da AWS, um administrador do IAM na conta confiável também deve conceder permissão à entidade principal (usuário ou função) para acessar o recurso. Eles concedem permissão ao anexar uma política baseada em identidade para a entidade. No entanto, se uma política baseada em recurso conceder acesso a uma entidade principal na mesma conta, nenhuma política baseada em identidade adicional será necessária. Consulte mais informações em [Acesso a recursos entre contas no IAM](#) no Guia do usuário do IAM.

Ações políticas para a AWS SGW

Oferece compatibilidade com ações de políticas	Sim
--	-----

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos, e em que condições.

O elemento `Action` de uma política JSON descreve as ações que você pode usar para permitir ou negar acesso em uma política. As ações de política geralmente têm o mesmo nome da operação de AWS API associada. Existem algumas exceções, como ações somente de permissão, que não têm uma operação de API correspondente. Algumas operações também exigem várias ações em uma política. Essas ações adicionais são chamadas de ações dependentes.

Incluem ações em uma política para conceder permissões para executar a operação associada.

Para ver uma lista de ações do AWS SGW, consulte [Ações definidas pelo AWS Storage Gateway](#) na Referência de Autorização de Serviço.

As ações de política no AWS SGW usam o seguinte prefixo antes da ação:

```
sgw
```

Para especificar várias ações em uma única instrução, separe-as com vírgulas.

```
"Action": [  
  "sgw:action1",  
  "sgw:action2"  
]
```

Para ver exemplos de políticas baseadas em identidade do AWS SGW, consulte [Exemplos de políticas baseadas em identidade para o AWS Storage Gateway](#)

Recursos de política para AWS SGW

Oferece compatibilidade com recursos de políticas	Sim
---	-----

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos, e em que condições.

O elemento de política JSON `Resource` especifica o objeto ou os objetos aos quais a ação se aplica. As instruções devem incluir um elemento `Resource` ou `NotResource`. Como prática

recomendada, especifique um recurso usando seu [nome do recurso da Amazon \(ARN\)](#). Isso pode ser feito para ações que oferecem compatibilidade com um tipo de recurso específico, conhecido como permissões em nível de recurso.

Para ações que não oferecem compatibilidade com permissões em nível de recurso, como operações de listagem, use um curinga (*) para indicar que a instrução se aplica a todos os recursos.

```
"Resource": "*" 
```

Para ver uma lista dos tipos de recursos do AWS SGW e seus ARNs, consulte [Resources Defined by AWS Storage Gateway na Referência de Autorização de Serviço](#). Para saber com quais ações você pode especificar o ARN de cada recurso, consulte [Ações definidas pelo AWS Storage Gateway](#).

Para ver exemplos de políticas baseadas em identidade do AWS SGW, consulte. [Exemplos de políticas baseadas em identidade para o AWS Storage Gateway](#)

Chaves de condição de política para AWS SGW

Suporta chaves de condição de política específicas de serviço	Sim
---	-----

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos, e em que condições.

O elemento `Condition` (ou bloco `Condition`) permite que você especifique condições nas quais uma instrução estiver em vigor. O elemento `Condition` é opcional. É possível criar expressões condicionais que usem [agentes de condição](#), como “igual a” ou “menor que”, para fazer a condição da política corresponder aos valores na solicitação.

Se você especificar vários elementos `Condition` em uma instrução ou várias chaves em um único `Condition` elemento, a AWS os avaliará usando uma operação lógica AND. Se você especificar vários valores para uma única chave de condição, AWS avalia a condição usando uma OR operação lógica. Todas as condições devem ser atendidas antes que as permissões da instrução sejam concedidas.

Você também pode usar variáveis de espaço reservado ao especificar condições. Por exemplo, é possível conceder a um usuário do IAM permissão para acessar um atributo somente se ele estiver

marcado com seu nome de usuário do IAM. Para obter mais informações, consulte [Elementos da política do IAM: variáveis e tags](#) no Guia do usuário do IAM.

AWS suporta chaves de condição globais e chaves de condição específicas do serviço. Para ver todas as chaves de condição AWS globais, consulte as [chaves de contexto de condição AWS global](#) no Guia do usuário do IAM.

Para ver uma lista das chaves de condição do AWS SGW, consulte [Chaves de condição do AWS Storage Gateway](#) na Referência de Autorização de Serviço. Para saber com quais ações e recursos você pode usar uma chave de condição, consulte [Actions Defined by AWS Storage Gateway](#).

Para ver exemplos de políticas baseadas em identidade do AWS SGW, consulte [Exemplos de políticas baseadas em identidade para o AWS Storage Gateway](#)

ACLs em SGW AWS

Oferece compatibilidade com ACLs	Não
----------------------------------	-----

As listas de controle de acesso (ACLs) controlam quais entidades principais (membros, usuários ou perfis da conta) têm permissões para acessar um recurso. As ACLs são semelhantes as políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

ABAC com AWS SGW

Oferece compatibilidade com ABAC (tags em políticas)	Parcial
--	---------

O controle de acesso baseado em recurso (ABAC) é uma estratégia de autorização que define permissões com base em recursos. Em AWS, esses atributos são chamados de tags. Você pode anexar tags a entidades do IAM (usuários ou funções) e a vários AWS recursos. A marcação de entidades e atributos é a primeira etapa do ABAC. Em seguida, você cria políticas de ABAC para permitir operações quando a tag da entidade principal corresponder à tag do recurso que ela estiver tentando acessar.

O ABAC é útil em ambientes que estão crescendo rapidamente e ajuda em situações onde o gerenciamento de políticas se torna um problema.

Para controlar o acesso baseado em tags, forneça informações sobre as tags no [elemento de condição](#) de uma política usando as `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` ou chaves de condição `aws:TagKeys`.

Se um serviço oferecer suporte às três chaves de condição para cada tipo de recurso, o valor será Sim para o serviço. Se um serviço oferecer suporte às três chaves de condição somente para alguns tipos de recursos, o valor será Parcial

Para obter mais informações sobre o ABAC, consulte [O que é ABAC?](#) no Guia do Usuário do IAM. Para visualizar um tutorial com etapas para configurar o ABAC, consulte [Utilizar controle de acesso baseado em atributos \(ABAC\)](#) no Guia do usuário do IAM.

Usando credenciais temporárias com AWS o SGW

Oferece compatibilidade com credenciais temporárias	Sim
---	-----

Alguns Serviços da AWS não funcionam quando você faz login usando credenciais temporárias. Para obter informações adicionais, incluindo quais Serviços da AWS funcionam com credenciais temporárias, consulte Serviços da AWS [“Trabalhe com o IAM”](#) no Guia do usuário do IAM.

Você está usando credenciais temporárias se fizer login AWS Management Console usando qualquer método, exceto um nome de usuário e senha. Por exemplo, quando você acessa AWS usando o link de login único (SSO) da sua empresa, esse processo cria automaticamente credenciais temporárias. Você também cria automaticamente credenciais temporárias quando faz login no console como usuário e, em seguida, alterna perfis. Para obter mais informações sobre como alternar funções, consulte [Alternar para um perfil \(console\)](#) no Guia do usuário do IAM.

Você pode criar manualmente credenciais temporárias usando a AWS API AWS CLI ou. Em seguida, você pode usar essas credenciais temporárias para acessar AWS. AWS recomenda que você gere credenciais temporárias dinamicamente em vez de usar chaves de acesso de longo prazo. Para mais informações, consulte [Credenciais de segurança temporárias no IAM](#).

Sessões de acesso direto para AWS SGW

Suporte para o recurso Encaminhamento de sessões de acesso (FAS)	Sim
--	-----

Quando você usa um usuário ou uma função do IAM para realizar ações AWS, você é considerado um principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O FAS usa as permissões do diretor chamando um AWS service (Serviço da AWS), combinadas com a solicitação AWS service (Serviço da AWS) para fazer solicitações aos serviços posteriores. As solicitações do FAS são feitas somente quando um serviço recebe uma solicitação que requer interações com outros Serviços da AWS ou com recursos para ser concluída. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte [Encaminhar sessões de acesso](#).

Perfis de serviço do AWS Storage Gateway

Oferece compatibilidade com funções de serviço	Sim
--	-----

O perfil de serviço é um [perfil do IAM](#) que um serviço assume para realizar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para obter mais informações, consulte [Criar um perfil para delegar permissões a um AWS service \(Serviço da AWS\)](#) no Guia do Usuário do IAM.

Warning

Alterar as permissões de uma função de serviço pode interromper a funcionalidade do AWS SGW. Edite as funções de serviço somente quando o AWS SGW fornecer orientação para fazer isso.

Funções vinculadas a serviços para SGW AWS

Oferece suporte a perfis vinculados ao serviço	Sim
--	-----

Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. AWS service (Serviço da AWS) O serviço pode presumir a função de executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não pode editar as permissões para perfis vinculados ao serviço.

Para obter detalhes sobre como criar ou gerenciar perfis vinculados a serviços, consulte [Serviços da AWS que funcionam com o IAM](#). Encontre um serviço na tabela que inclua um Yes na coluna Função vinculada ao serviço. Escolha o link Sim para visualizar a documentação do perfil vinculado a esse serviço.

Exemplos de políticas baseadas em identidade para o AWS Storage Gateway

Por padrão, usuários e funções não têm permissão para criar ou modificar recursos do AWS SGW. Eles também não podem realizar tarefas usando a AWS API AWS Management Console, AWS Command Line Interface (AWS CLI) ou. Para conceder aos usuários permissões para executar ações nos recursos de que eles precisam, um administrador do IAM pode criar políticas do IAM. O administrador pode então adicionar as políticas do IAM aos perfis, e os usuários podem assumir os perfis.

Para saber como criar uma política baseada em identidade do IAM usando esses exemplos de documento de política JSON, consulte [Criação de políticas do IAM](#) no Guia do Usuário do IAM.

Para obter detalhes sobre ações e tipos de recursos definidos pelo AWS SGW, incluindo o formato dos ARNs para cada um dos tipos de recursos, consulte [Actions, Resources, and Condition Keys for AWS Storage Gateway na Referência](#) de Autorização de Serviço.

Tópicos

- [Práticas recomendadas de políticas](#)
- [Usando o console AWS SGW](#)
- [Permitir que os usuários visualizem suas próprias permissões](#)

Práticas recomendadas de políticas

As políticas baseadas em identidade determinam se alguém pode criar, acessar ou excluir recursos AWS SGW em sua conta. Essas ações podem incorrer em custos para a Conta da AWS. Ao criar ou editar políticas baseadas em identidade, siga estas diretrizes e recomendações:

- Comece com as políticas AWS gerenciadas e avance para as permissões de privilégios mínimos — Para começar a conceder permissões aos seus usuários e cargas de trabalho, use as políticas AWS gerenciadas que concedem permissões para muitos casos de uso comuns. Eles estão disponíveis no seu Conta da AWS. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo AWS cliente que sejam específicas para seus casos de uso.

Para obter mais informações, consulte [Políticas gerenciadas pela AWS](#) ou [Políticas gerenciadas pela AWS para perfis de trabalho](#) no Guia do usuário do IAM.

- Aplique permissões de privilégio mínimo: ao definir permissões com as políticas do IAM, conceda apenas as permissões necessárias para executar uma tarefa. Você faz isso definindo as ações que podem ser executadas em recursos específicos sob condições específicas, também conhecidas como permissões de privilégio mínimo. Para obter mais informações sobre como usar o IAM para aplicar permissões, consulte [Políticas e permissões no IAM](#) no Guia do usuário do IAM.
- Use condições nas políticas do IAM para restringir ainda mais o acesso: você pode adicionar uma condição às políticas para limitar o acesso a ações e recursos. Por exemplo, você pode escrever uma condição de política para especificar que todas as solicitações devem ser enviadas usando SSL. Você também pode usar condições para conceder acesso às ações de serviço se elas forem usadas por meio de uma ação específica AWS service (Serviço da AWS), como AWS CloudFormation. Para obter mais informações, consulte [Elementos de política JSON do IAM: condição](#) no Guia do usuário do IAM.
- Use o IAM Access Analyzer para validar suas políticas do IAM a fim de garantir permissões seguras e funcionais: o IAM Access Analyzer valida as políticas novas e existentes para que elas sigam a linguagem de política do IAM (JSON) e as práticas recomendadas do IAM. O IAM Access Analyzer oferece mais de 100 verificações de política e recomendações acionáveis para ajudar você a criar políticas seguras e funcionais. Para obter mais informações, consulte [Validação de políticas do IAM Access Analyzer](#) no Guia do usuário do IAM.
- Exigir autenticação multifator (MFA) — Se você tiver um cenário que exija usuários do IAM ou um usuário root, ative Conta da AWS a MFA para obter segurança adicional. Para exigir a MFA quando as operações de API forem chamadas, adicione condições de MFA às suas políticas. Para obter mais informações, consulte [Configuração de acesso à API protegido por MFA](#) no Guia do usuário do IAM.

Para obter mais informações sobre as práticas recomendadas do IAM, consulte [Práticas recomendadas de segurança no IAM](#) no Guia do usuário do IAM.

Usando o console AWS SGW

Para acessar o console do AWS Storage Gateway, você deve ter um conjunto mínimo de permissões. Essas permissões devem permitir que você liste e visualize detalhes sobre os recursos do AWS SGW em seu Conta da AWS. Se você criar uma política baseada em identidade que seja mais restritiva do que as permissões mínimas necessárias, o console não funcionará como pretendido para entidades (usuários ou perfis) com essa política.

Você não precisa permitir permissões mínimas do console para usuários que estão fazendo chamadas somente para a API AWS CLI ou para a AWS API. Em vez disso, permita o acesso somente a ações que correspondam a operação de API que estiverem tentando executar.

Para garantir que usuários e funções ainda possam usar o console do AWS SGW, anexe também o AWS SGW *ConsoleAccess* ou a política *ReadOnly* AWS gerenciada às entidades. Para obter mais informações, consulte [Adicionando Permissões a um Usuário](#) no Guia do Usuário do IAM.

Permitir que os usuários visualizem suas próprias permissões

Este exemplo mostra como você pode criar uma política que permite que os usuários do IAM visualizem as políticas gerenciadas e em linha anexadas a sua identidade de usuário. Essa política inclui permissões para concluir essa ação no console ou programaticamente usando a API AWS CLI ou AWS .

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ViewOwnUserInfo",
      "Effect": "Allow",
      "Action": [
        "iam:GetUserPolicy",
        "iam:ListGroupForUser",
        "iam:ListAttachedUserPolicies",
        "iam:ListUserPolicies",
        "iam:GetUser"
      ],
      "Resource": ["arn:aws:iam::*:user/${aws:username}"]
    },
    {
      "Sid": "NavigateInConsole",
      "Effect": "Allow",
      "Action": [
        "iam:GetGroupPolicy",
        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam:ListAttachedGroupPolicies",
        "iam:ListGroupPolicies",
        "iam:ListPolicyVersions",
        "iam:ListPolicies",
        "iam:ListUsers"
      ]
    }
  ]
}
```

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

Solução de problemas AWS de identidade e acesso ao Storage Gateway

Use as informações a seguir para ajudá-lo a diagnosticar e corrigir problemas comuns que você pode encontrar ao trabalhar com o AWS SGW e o IAM.

Tópicos

- [Não estou autorizado a realizar uma ação no AWS SGW](#)
- [Não estou autorizado a realizar iam: PassRole](#)
- [Quero permitir que pessoas fora da minha acessem meus Conta da AWS recursos do AWS SGW](#)

Não estou autorizado a realizar uma ação no AWS SGW

Se você receber uma mensagem de erro informando que não tem autorização para executar uma ação, suas políticas deverão ser atualizadas para permitir que você realize a ação.

O erro do exemplo a seguir ocorre quando o usuário do IAM mateojackson tenta usar o console para visualizar detalhes sobre um atributo *my-example-widget* fictício, mas não tem as permissões *sgw:GetWidget* fictícias.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:  
sgw:GetWidget on resource: my-example-widget
```

Nesse caso, a política do usuário mateojackson deve ser atualizada para permitir o acesso ao recurso *my-example-widget* usando a ação *sgw:GetWidget*.

Se precisar de ajuda, entre em contato com seu AWS administrador. Seu administrador é a pessoa que forneceu suas credenciais de login.

Não estou autorizado a realizar iam: PassRole

Se você receber um erro informando que não está autorizado a realizar a *iam:PassRole* ação, suas políticas devem ser atualizadas para permitir que você passe uma função para o AWS SGW.

Alguns Serviços da AWS permitem que você passe uma função existente para esse serviço em vez de criar uma nova função de serviço ou uma função vinculada ao serviço. Para fazer isso, é preciso ter permissões para passar o perfil para o serviço.

O erro de exemplo a seguir ocorre quando uma usuária do IAM chamada `marymajor` tenta usar o console para executar uma ação no AWS Storage Gateway. No entanto, a ação exige que o serviço tenha permissões concedidas por um perfil de serviço. Mary não tem permissões para passar o perfil para o serviço.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
iam:PassRole
```

Nesse caso, as políticas de Mary devem ser atualizadas para permitir que ela realize a ação `iam:PassRole`.

Se precisar de ajuda, entre em contato com seu AWS administrador. Seu administrador é a pessoa que forneceu suas credenciais de login.

Quero permitir que pessoas fora da minha acessem meus Conta da AWS recursos do AWS SGW

Você pode criar um perfil que os usuários de outras contas ou pessoas fora da sua organização podem usar para acessar seus recursos. Você pode especificar quem é confiável para assumir o perfil. Para serviços que oferecem compatibilidade com políticas baseadas em recursos ou listas de controle de acesso (ACLs), você pode usar essas políticas para conceder às pessoas acesso aos seus recursos.

Para saber mais, consulte:

- Para saber se o AWS SGW oferece suporte a esses recursos, consulte [Como o AWS Storage Gateway funciona com o IAM](#).
- Para saber como fornecer acesso aos seus recursos em todos os Contas da AWS que você possui, consulte [Como fornecer acesso a um usuário do IAM em outro Conta da AWS que você possui](#) no Guia do usuário do IAM.
- Para saber como fornecer acesso aos seus recursos a terceiros Contas da AWS, consulte [Como fornecer acesso Contas da AWS a terceiros](#) no Guia do usuário do IAM.
- Para saber como conceder acesso por meio da federação de identidades, consulte [Conceder acesso a usuários autenticados externamente \(federação de identidades\)](#) no Guia do usuário do IAM.

- Para saber a diferença entre o uso de perfis e políticas baseadas em recurso para acesso entre contas, consulte [Acesso a recursos entre contas no IAM](#) no Guia do usuário do IAM.

Registro e monitoramento em AWS Storage Gateway

O Storage Gateway é integrado com AWS CloudTrail um serviço que fornece um registro das ações realizadas por um usuário, função ou AWS serviço no Storage Gateway. CloudTrail captura todas as chamadas de API para o Storage Gateway como eventos. As chamadas capturadas incluem as chamadas do console do Storage Gateway e as chamadas de código para as operações de API do Storage Gateway. Se você criar uma trilha, poderá ativar a entrega contínua de CloudTrail eventos para um bucket do Amazon S3, incluindo eventos para o Storage Gateway. Se você não configurar uma trilha, ainda poderá ver os eventos mais recentes no CloudTrail console no Histórico de eventos. Usando as informações coletadas por CloudTrail, você pode determinar a solicitação que foi feita ao Storage Gateway, o endereço IP do qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita e detalhes adicionais.

Para saber mais CloudTrail, consulte o [Guia AWS CloudTrail do usuário](#).

Informações do Storage Gateway em CloudTrail

CloudTrail é ativado na sua conta da Amazon Web Services quando você cria a conta. Quando a atividade ocorre no Storage Gateway, essa atividade é registrada em um CloudTrail evento junto com outros eventos AWS de serviço no histórico de eventos. Você pode visualizar, pesquisar e baixar os eventos recentes em sua conta da Amazon Web Services. Para obter mais informações, consulte [Visualização de eventos com histórico de CloudTrail eventos](#).

Para obter um registro contínuo dos eventos na conta da Amazon Web Services, incluindo os eventos do Storage Gateway, crie uma trilha. Uma trilha permite CloudTrail entregar arquivos de log para um bucket do Amazon S3. Por padrão, quando você cria uma trilha no console, a trilha se aplica a todas as AWS regiões. A trilha registra eventos de todas as regiões na AWS partição e entrega os arquivos de log ao bucket do Amazon S3 que você especificar. Além disso, você pode configurar outros AWS serviços para analisar e agir com base nos dados de eventos coletados nos CloudTrail registros. Para mais informações, consulte:

- [Visão Geral para Criar uma Trilha](#)
- [CloudTrail Serviços e integrações compatíveis](#)
- [Configurando notificações do Amazon SNS para CloudTrail](#)

- [Recebendo arquivos de CloudTrail log de várias regiões](#) e [recebendo arquivos de CloudTrail log de várias contas](#)

Todas as ações do Storage Gateway são registradas em log e documentadas no tópico [Ações](#). Por exemplo, chamadas para as ShutdownGateway ações ActivateGatewayListGateways, e geram entradas nos arquivos de CloudTrail log.

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 root ou 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 AWS serviço.

Para obter mais informações, consulte [Elemento userIdentity do CloudTrail](#).

Como entender as entradas dos arquivos de log do Storage Gateway

Uma trilha é uma configuração que permite a entrega de eventos como arquivos de log para um bucket do Amazon S3 que você especificar. CloudTrail os arquivos de log contêm uma ou mais entradas de log. Um evento representa uma única solicitação de qualquer fonte e inclui informações sobre a ação solicitada, a data e a hora da ação, os parâmetros da solicitação e assim por diante. CloudTrail os arquivos de log não são um rastreamento de pilha ordenado das chamadas públicas de API, portanto, eles não aparecem em nenhuma ordem específica.

O exemplo a seguir mostra uma entrada de CloudTrail registro que demonstra a ação.

```
{ "Records": [{
    "eventVersion": "1.02",
    "userIdentity": {
      "type": "IAMUser",
      "principalId": "AIDAI15AUEPBH2M7JTNVC",
      "arn": "arn:aws:iam::111122223333:user/StorageGateway-team/JohnDoe",
      "accountId": "111122223333",
      "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
      "userName": "JohnDoe"
    }
  ],
```

```

    "eventTime": "2014-12-04T16:19:00Z",
    "eventSource": "storagegateway.amazonaws.com",
    "eventName": "ActivateGateway",
    "awsRegion": "us-east-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "aws-cli/1.6.2 Python/2.7.6 Linux/2.6.18-164.el5",
    "requestParameters": {
        "gatewayTimezone": "GMT-5:00",
        "gatewayName": "cloudtrailgatewayv1",
        "gatewayRegion": "us-east-2",
        "activationKey": "EHFBX-1NDD0-P0IVU-PI259-
DHK88",
        "gatewayType": "VTL"
    },
    "responseElements": {
        "gatewayARN":
"arn:aws:storagegateway:us-east-2:111122223333:gateway/cloudtrailgatewayv1"
    },
    "requestID":
"54BTFGNQI71987UJD2IHTCT8NF1Q8GLLE1QEU3KPGG6F0KSTAUU0",
    "eventID": "635f2ea2-7e42-45f0-
bed1-8b17d7b74265",
    "eventType": "AwsApiCall",
    "apiVersion": "20130630",
    "recipientAccountId": "444455556666"
    ]}
}

```

O exemplo a seguir mostra uma entrada de CloudTrail registro que demonstra a ListGateways ação.

```

{
  "Records": [{
    "eventVersion": "1.02",
    "userIdentity": {
      "type": "IAMUser",
      "principalId": "AIDAI5AUPEBH2M7JTNVC",
      "arn": "arn:aws:iam::111122223333:user/StorageGateway-
team/JohnDoe",
      "accountId": "111122223333", "accessKeyId": "
AKIAIOSFODNN7EXAMPLE",
      "userName": "JohnDoe"
    },

```

```

" eventTime ":" 2014 - 12 - 03T19: 41: 53Z ",
" eventSource ":" storagegateway.amazonaws.com ",
" eventName ":" ListGateways ",
" awsRegion ":" us-east-2 ",
" sourceIPAddress ":" 192.0.2.0 ",
" userAgent ":" aws - cli / 1.6.2 Python / 2.7.6
Linux / 2.6.18 - 164.el5 ",
" requestParameters ":null,
" responseElements ":null,
"requestID ":"
6U2N42CU37KA08BG6V1I23FRSJ1Q8GLLE1QEU3KPGG6F0KSTAUU0 ",
" eventID ":" f76e5919 - 9362 - 48ff - a7c4 -
d203a189ec8d ",
" eventType ":" AwsApiCall ",
" apiVersion ":" 20130630 ",
" recipientAccountId ":" 444455556666"
    ]]
}

```

Validação de conformidade do AWS Storage Gateway

Audidores terceirizados avaliam a segurança e a conformidade do AWS Storage Gateway como parte de vários programas de AWS conformidade. Eles incluem SOC, PCI, ISO, FedRAMP, HIPAA, MTSC, C5, K-ISMS, ENS High, OSPAR e HITRUST CSF.

Para obter uma lista de AWS serviços no escopo de programas de conformidade específicos, consulte [AWS Serviços no escopo do programa de conformidade AWS](#) . Para obter informações gerais, consulte Programas de [AWS conformidade Programas AWS](#) de .

Você pode baixar relatórios de auditoria de terceiros usando AWS Artifact. Para obter mais informações, consulte [Baixar relatórios em AWS Artifact](#) .

Sua responsabilidade com relação à conformidade ao usar o Storage Gateway é determinada pela confidencialidade dos dados, pelos objetivos de conformidade da empresa e pelos regulamentos e leis aplicáveis. A AWS fornece os seguintes recursos para ajudar com a conformidade:

- [Guias de início rápido](#) sobre sobre segurança e conformidade — Esses guias de implantação discutem considerações arquitetônicas e fornecem etapas para a implantação de ambientes básicos com foco em segurança e conformidade em AWS

- Documento técnico [sobre arquitetura para segurança e conformidade com a HIPAA — Este whitepaper](#) descreve como as empresas podem usar para criar aplicativos compatíveis com a HIPAA. AWS
- AWS Recursos de <https://aws.amazon.com/compliance/resources/> de conformidade — Essa coleção de pastas de trabalho e guias pode ser aplicada ao seu setor e local.
- [Avaliação de recursos com as regras](#) do Guia do AWS Config Desenvolvedor — O AWS Config serviço avalia se suas configurações de recursos estão em conformidade com as práticas internas, as diretrizes e os regulamentos do setor.
- [AWS Security Hub](#)— Esse AWS serviço fornece uma visão abrangente do seu estado de segurança interno, AWS que ajuda você a verificar sua conformidade com os padrões e as melhores práticas do setor de segurança.

Resiliência no AWS Storage Gateway

A infraestrutura AWS global é construída em torno de AWS regiões e zonas de disponibilidade. AWS As regiões fornecem várias zonas de disponibilidade fisicamente separadas e isoladas, conectadas a redes de baixa latência, alta taxa de transferência e alta redundância. 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 datacenter tradicionais.

Para obter mais informações sobre AWS regiões e zonas de disponibilidade, consulte [Infraestrutura AWS global](#).

Além da infraestrutura AWS global, o Storage Gateway oferece vários recursos para ajudar a suportar suas necessidades de resiliência de dados e backup:

- Use o VMware vSphere High Availability (VMware HA) para ajudar a proteger as cargas de trabalho de armazenamento contra falhas de hardware, hipervisor ou rede. Para ter mais informações, consulte [Como usar o VMware vSphere High Availability com o Storage Gateway](#).
- Use AWS Backup para fazer backup de seus volumes. Para ter mais informações, consulte [Fazer backup de seus volumes](#).
- Clone seu volume a partir de um ponto de recuperação. Para ter mais informações, consulte [Como clonar um volume](#).

Segurança da infraestrutura no AWS Storage Gateway

Como um serviço gerenciado, o AWS Storage Gateway é protegido pelos procedimentos AWS globais de segurança de rede descritos no whitepaper [Amazon Web Services: Overview of Security Processes](#).

Você usa chamadas de API AWS publicadas para acessar o Storage Gateway pela rede. Os clientes devem ser compatíveis com o Transport Layer Security (TLS) 1.2. Os clientes também devem ter suporte a conjuntos de criptografia com perfect forward secrecy (PFS) como Ephemeral Diffie-Hellman (DHE) ou Ephemeral Elliptic Curve Diffie-Hellman (ECDHE). A maioria dos sistemas modernos como Java 7 e versões posteriores oferece suporte a esses modos.

Além disso, as solicitações devem ser assinadas utilizando um ID da chave de acesso e uma chave de acesso secreta associada a uma entidade principal do IAM. Ou você pode usar o [AWS Security Token Service](#) (AWS STS) para gerar credenciais de segurança temporárias para assinar solicitações.

AWS Melhores práticas de segurança

AWS fornece vários recursos de segurança a serem considerados ao desenvolver e implementar suas próprias políticas de segurança. Essas melhores práticas são diretrizes gerais e não representam uma solução completa de segurança. Como essas práticas recomendadas podem não ser adequadas ou suficientes no ambiente, trate-as como considerações úteis em vez de requisitos. Para obter mais informações, consulte [Práticas recomendadas de segurança da AWS](#).

Solução de problemas em seu gateway

A seguir, você pode encontrar informações sobre solução de problemas relacionados a gateways, compartilhamentos de arquivos, volumes, fitas virtuais e snapshots. As informações sobre solução de problemas em gateways locais abrangem gateways implantados em clientes VMware ESXi e Microsoft Hyper-V. As informações de solução de problemas para compartilhamentos de arquivos se aplicam ao tipo de gateway de arquivos. As informações sobre solução de problemas em volumes aplicam-se ao tipo de gateway de volumes. As informações sobre solução de problemas em fitas aplicam-se ao tipo de gateway de fitas. As informações de solução de problemas de gateway se aplicam ao uso de CloudWatch métricas. As informações de solução de problemas de alta disponibilidade abrangem gateways executados na plataforma VMware vSphere High Availability (HA).

Tópicos

- [Solução de problemas: o status do gateway é exibido offline no AWS Storage Gateway console](#)
- [Solução de problemas: erro interno recebido durante a ativação do Storage Gateway](#)
- [Como solucionar questões on-premises de solução de problemas no gateway](#)
- [Como solucionar problemas de configuração no Microsoft Hyper-V](#)
- [Como solucionar problemas de gateway do Amazon EC2](#)
- [Como solucionar problemas do dispositivo de hardware](#)
- [Como solucionar problemas em volumes](#)
- [Como solucionar problemas de alta disponibilidade](#)
- [Práticas recomendadas para a recuperação de dados](#)

Solução de problemas: o status do gateway é exibido offline no AWS Storage Gateway console

Use as informações de solução de problemas a seguir para determinar o que fazer se o AWS Storage Gateway console mostrar que seu gateway está off-line.

Seu gateway pode estar sendo exibido como off-line por um ou mais dos seguintes motivos:

- O gateway não consegue alcançar os endpoints do serviço Storage Gateway.
- O gateway foi desligado inesperadamente.

- Um disco de cache associado ao gateway foi desconectado, modificado ou falhou.

Para colocar seu gateway novamente on-line, identifique e resolva o problema que fez com que seu gateway ficasse off-line.

Verifique o firewall ou proxy associado

Se você configurou seu gateway para usar um proxy ou colocou o gateway atrás de um firewall, revise as regras de acesso do proxy ou do firewall. O proxy ou firewall deve permitir o tráfego de e para as portas de rede e os endpoints de serviço exigidos pelo Storage Gateway. Para obter mais informações, consulte Requisitos de de de de de [rede e firewall](#).

Verifique se há uma inspeção contínua de SSL ou pacotes profundos do tráfego do seu gateway

Se uma inspeção SSL ou profunda de pacotes estiver sendo executada atualmente no tráfego de rede entre seu gateway e AWS, talvez seu gateway não consiga se comunicar com os endpoints de serviço necessários. Para colocar seu gateway novamente on-line, você deve desativar a inspeção.

Verifique se há uma queda de energia ou falha de hardware no host do hipervisor

Uma queda de energia ou falha de hardware no host do hipervisor do seu gateway pode fazer com que o gateway seja desligado inesperadamente e fique inacessível. Depois de restaurar a energia e a conectividade de rede, seu gateway ficará acessível novamente.

Depois que seu gateway estiver online novamente, certifique-se de tomar medidas para recuperar seus dados. Para obter mais informações, consulte [Melhores práticas para recuperar](#) seus dados.

Verifique se há problemas com um disco de cache associado

Seu gateway pode ficar off-line se pelo menos um dos discos de cache associados ao gateway tiver sido removido, alterado ou redimensionado, ou se estiver corrompido.

Se um disco de cache funcional foi removido do host do hipervisor:

1. Encerre o gateway.
2. Adicione novamente o disco.

Note

Certifique-se de adicionar o disco ao mesmo nó de disco.

3. Reinicie o gateway.

Se um disco de cache estiver corrompido, tiver sido substituído ou redimensionado:

1. Encerre o gateway.
2. Redefina o disco de cache.
3. Reconfigure o disco para armazenamento em cache.
4. Reinicie o gateway.

Solução de problemas: erro interno recebido durante a ativação do Storage Gateway

As solicitações de ativação do Storage Gateway atravessam dois caminhos de rede. As solicitações de ativação recebidas enviadas por um cliente se conectam à máquina virtual (VM) do gateway ou à instância do Amazon Elastic Compute Cloud (Amazon EC2) pela porta 80. Se o gateway receber com êxito a solicitação de ativação, ele se comunicará com os endpoints do Storage Gateway para receber uma chave de ativação. Se o gateway não conseguir alcançar os endpoints do Storage Gateway, ele responderá ao cliente com uma mensagem de erro interna.

Use as informações de solução de problemas a seguir para determinar o que fazer se você receber uma mensagem de erro interna ao tentar ativar seu AWS Storage Gateway.

Note

- Certifique-se de implantar novos gateways usando o arquivo de imagem de máquina virtual mais recente ou a versão da Amazon Machine Image (AMI). Você receberá um erro interno se tentar ativar um gateway que usa uma AMI desatualizada.
- Certifique-se de selecionar o tipo de gateway correto que você pretende implantar antes de baixar a AMI. Os arquivos.ova e as AMIs para cada tipo de gateway são diferentes e não são intercambiáveis.

Resolva erros ao ativar seu gateway usando um endpoint público

Para resolver erros de ativação ao ativar seu gateway usando um endpoint público, execute as seguintes verificações e configurações.

Verifique as portas necessárias

Para gateways implantados localmente, verifique se as portas estão abertas no firewall local. Para gateways implantados em uma instância do Amazon EC2, verifique se as portas estão abertas no grupo de segurança da instância. Para confirmar se as portas estão abertas, execute um comando telnet no endpoint público a partir de um servidor. Esse servidor deve estar na mesma sub-rede do gateway. Por exemplo, os comandos telnet a seguir testam a conexão com a porta 443:

```
telnet d4kdq0yaxexbo.cloudfront.net 443
telnet storagegateway.region.amazonaws.com 443
telnet dp-1.storagegateway.region.amazonaws.com 443
telnet proxy-app.storagegateway.region.amazonaws.com 443
telnet client-cp.storagegateway.region.amazonaws.com 443
telnet anon-cp.storagegateway.region.amazonaws.com 443
```

Para confirmar que o próprio gateway pode alcançar o endpoint, acesse o console de VM local do gateway (para gateways implantados localmente). Ou você pode usar SSH para a instância do gateway (para gateways implantados no Amazon EC2). Em seguida, execute um teste de conectividade de rede. Confirme se o teste retorna [PASSED]. Para obter mais informações, gateway

[Testando a conexão do gateway com a Internet.](#)

Note

O nome de usuário de login padrão para o console do gateway é `admin`, e a senha padrão é `password`.

Certifique-se de que a segurança do firewall não modifique os pacotes enviados do gateway para os endpoints públicos

Inspeções SSL, inspeções profundas de pacotes ou outras formas de segurança de firewall podem interferir nos pacotes enviados do gateway. O handshake SSL falhará se o certificado SSL for modificado de acordo com o que o endpoint de ativação espera. Para confirmar que não há

nenhuma inspeção de SSL em andamento, execute um comando OpenSSL no endpoint `anon-cp.storagegateway.region.amazonaws.com` de ativação principal () na porta 443. Você deve executar esse comando em uma máquina que esteja na mesma sub-rede do gateway:

```
$ openssl s_client -connect anon-cp.storagegateway.region.amazonaws.com:443 -
servername anon-cp.storagegateway.region.amazonaws.com
```

Note

Substitua a *região* pela sua Região da AWS.

Se não houver nenhuma inspeção SSL em andamento, o comando retornará uma resposta semelhante à seguinte:

```
$ openssl s_client -connect anon-cp.storagegateway.us-east-2.amazonaws.com:443 -
servername anon-cp.storagegateway.us-east-2.amazonaws.com
CONNECTED(00000003)
depth=2 C = US, 0 = Amazon, CN = Amazon Root CA 1
verify return:1
depth=1 C = US, 0 = Amazon, OU = Server CA 1B, CN = Amazon
verify return:1
depth=0 CN = anon-cp.storagegateway.us-east-2.amazonaws.com
verify return:1
---
Certificate chain
 0 s:/CN=anon-cp.storagegateway.us-east-2.amazonaws.com
  i:/C=US/O=Amazon/OU=Server CA 1B/CN=Amazon
 1 s:/C=US/O=Amazon/OU=Server CA 1B/CN=Amazon
  i:/C=US/O=Amazon/CN=Amazon Root CA 1
 2 s:/C=US/O=Amazon/CN=Amazon Root CA 1
  i:/C=US/ST=Arizona/L=Scottsdale/O=Starfield Technologies, Inc./CN=Starfield Services
  Root Certificate Authority - G2
 3 s:/C=US/ST=Arizona/L=Scottsdale/O=Starfield Technologies, Inc./CN=Starfield Services
  Root Certificate Authority - G2
  i:/C=US/O=Starfield Technologies, Inc./OU=Starfield Class 2 Certification Authority
---
```

Se houver uma inspeção SSL em andamento, a resposta mostrará uma cadeia de certificados alterada, semelhante à seguinte:

```
$ openssl s_client -connect anon-cp.storagegateway.ap-southeast-1.amazonaws.com:443 -
servername anon-cp.storagegateway.ap-southeast-1.amazonaws.com
CONNECTED(00000003)
depth=0 DC = com, DC = amazonaws, OU = AWS, CN = anon-cp.storagegateway.ap-
southeast-1.amazonaws.com
verify error:num=20:unable to get local issuer certificate
verify return:1
depth=0 DC = com, DC = amazonaws, OU = AWS, CN = anon-cp.storagegateway.ap-
southeast-1.amazonaws.com
verify error:num=21:unable to verify the first certificate
verify return:1
---
Certificate chain
 0 s:/DC=com/DC=amazonaws/OU=AWS/CN=anon-cp.storagegateway.ap-southeast-1.amazonaws.com
  i:/C=IN/O=Company/CN=Admin/ST=KA/L=New town/OU=SGW/emailAddress=admin@company.com
---
```

O endpoint de ativação aceita handshakes SSL somente se reconhecer o certificado SSL. Isso significa que o tráfego de saída do gateway para os endpoints deve estar isento das inspeções realizadas por firewalls em sua rede. Essas inspeções podem ser uma inspeção SSL ou uma inspeção profunda de pacotes.

Verifique a sincronização de horário do gateway

Distorções de tempo excessivas podem causar erros de handshake de SSL. Para gateways locais, você pode usar o console de VM local do gateway para verificar a sincronização de horário do gateway. A diferença de tempo não deve ser maior que 60 segundos. [Para obter mais informações, consulte do do gateway](#).

A opção System Time Management não está disponível em gateways hospedados em instâncias do Amazon EC2. Para garantir que os gateways do Amazon EC2 possam sincronizar adequadamente o horário, confirme se a instância do Amazon EC2 pode se conectar à seguinte lista de pools de servidores NTP pelas portas UDP e TCP 123:

- 0.amazon.pool.ntp.org
- 1.amazon.pool.ntp.org
- 2.amazon.pool.ntp.org
- 3.amazon.pool.ntp.org

Resolva erros ao ativar seu gateway usando um endpoint Amazon VPC

Para resolver erros de ativação ao ativar seu gateway usando um endpoint da Amazon Virtual Private Cloud (Amazon VPC), execute as seguintes verificações e configurações.

Verifique as portas necessárias

Certifique-se de que as portas necessárias em seu firewall local (para gateways implantados no local) ou grupo de segurança (para gateways implantados no Amazon EC2) estejam abertas. As portas necessárias para conectar um gateway a um endpoint VPC do Storage Gateway são diferentes das necessárias para conectar um gateway a endpoints públicos. As portas a seguir são necessárias para se conectar a um endpoint VPC do Storage Gateway:

- TCP 443
- TCP 1026
- TCP 1027
- TCP 1028
- TCP 1031
- TCP 2222

[Para obter mais informações, consulte .](#)

Além disso, verifique o grupo de segurança que está conectado ao seu endpoint VPC do Storage Gateway. O grupo de segurança padrão conectado ao endpoint pode não permitir as portas necessárias. Crie um novo grupo de segurança que permita o tráfego do intervalo de endereços IP do seu gateway pelas portas necessárias. Em seguida, anexe esse grupo de segurança ao VPC endpoint.

Note

Use o [console da Amazon VPC](#) para verificar o grupo de segurança que está conectado ao endpoint da VPC. Visualize seu endpoint VPC do Storage Gateway no console e escolha a guia Security Groups.

Para confirmar se as portas necessárias estão abertas, você pode executar comandos telnet no VPC Endpoint do Storage Gateway VPC. Você deve executar esses comandos

em um servidor que esteja na mesma sub-rede do gateway. Você pode executar os testes no primeiro nome DNS que não especifica uma zona de disponibilidade. Por exemplo, os comandos telnet a seguir testam as conexões de porta necessárias usando o nome DNS `vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com`:

```
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 443
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 1026
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 1027
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 1028
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 1031
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 2222
```

Certifique-se de que a segurança do firewall não modifique os pacotes enviados do gateway para seu endpoint Amazon VPC do Storage Gateway

Inspeções SSL, inspeções profundas de pacotes ou outras formas de segurança de firewall podem interferir nos pacotes enviados do gateway. O handshake SSL falhará se o certificado SSL for modificado de acordo com o que o endpoint de ativação espera. Para confirmar que não há nenhuma inspeção de SSL em andamento, execute um comando OpenSSL no seu endpoint VPC do Storage Gateway. Você deve executar esse comando em uma máquina que esteja na mesma sub-rede do gateway. Execute o comando para cada porta necessária:

```
$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com:443 -servername
vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com:1026 -servername
vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com:1027 -servername
vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com:1028 -servername
vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com:1031 -servername
vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com
```

```
$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:2222 -servername
vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com
```

Se não houver nenhuma inspeção SSL em andamento, o comando retornará uma resposta semelhante à seguinte:

```
openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1027 -servername
vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com
CONNECTED(00000005)
depth=2 C = US, O = Amazon, CN = Amazon Root CA 1
verify return:1
depth=1 C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
verify return:1
depth=0 CN = anon-cp.storagegateway.us-east-1.amazonaws.com
verify return:1
---
Certificate chain
 0 s:CN = anon-cp.storagegateway.us-east-1.amazonaws.com
  i:C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
 1 s:C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
  i:C = US, O = Amazon, CN = Amazon Root CA 1
 2 s:C = US, O = Amazon, CN = Amazon Root CA 1
  i:C = US, ST = Arizona, L = Scottsdale, O = "Starfield Technologies, Inc.", CN =
Starfield Services Root Certificate Authority - G2
 3 s:C = US, ST = Arizona, L = Scottsdale, O = "Starfield Technologies, Inc.", CN =
Starfield Services Root Certificate Authority - G2
  i:C = US, O = "Starfield Technologies, Inc.", OU = Starfield Class 2 Certification
Authority
---
```

Se houver uma inspeção SSL em andamento, a resposta mostrará uma cadeia de certificados alterada, semelhante à seguinte:

```
openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1027 -servername
vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com
CONNECTED(00000005)
depth=2 C = US, O = Amazon, CN = Amazon Root CA 1
verify return:1
```

```
depth=1 C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
verify return:1
depth=0 DC = com, DC = amazonaws, OU = AWS, CN = anon-cp.storagegateway.us-
east-1.amazonaws.com
verify error:num=21:unable to verify the first certificate
verify return:1
---
Certificate chain
 0 s:/DC=com/DC=amazonaws/OU=AWS/CN=anon-cp.storagegateway.us-east-1.amazonaws.com
  i:/C=IN/O=Company/CN=Admin/ST=KA/L=New town/OU=SGW/emailAddress=admin@company.com
---
```

O endpoint de ativação aceita handshakes SSL somente se reconhecer o certificado SSL. Isso significa que o tráfego de saída do gateway para seu VPC endpoint pelas portas necessárias está isento das inspeções realizadas pelos firewalls de sua rede. Essas inspeções podem ser inspeções SSL ou inspeções profundas de pacotes.

Verifique a sincronização de horário do gateway

Distorções de tempo excessivas podem causar erros de handshake de SSL. Para gateways locais, você pode usar o console de VM local do gateway para verificar a sincronização de horário do gateway. A diferença de tempo não deve ser maior que 60 segundos. [Para obter mais informações, consulte do do gateway .](#)

A opção System Time Management não está disponível em gateways hospedados em instâncias do Amazon EC2. Para garantir que os gateways do Amazon EC2 possam sincronizar adequadamente o horário, confirme se a instância do Amazon EC2 pode se conectar à seguinte lista de pools de servidores NTP pelas portas UDP e TCP 123:

- 0.amazon.pool.ntp.org
- 1.amazon.pool.ntp.org
- 2.amazon.pool.ntp.org
- 3.amazon.pool.ntp.org

Verifique se há um proxy HTTP e confirme as configurações do grupo de segurança associado

Antes da ativação, verifique se você tem um proxy HTTP no Amazon EC2 configurado na VM do gateway local como um proxy Squid na porta 3128. Nesse caso, confirme o seguinte:

- O grupo de segurança anexado ao proxy HTTP no Amazon EC2 deve ter uma regra de entrada. Essa regra de entrada deve permitir o tráfego do proxy Squid na porta 3128 a partir do endereço IP da VM do gateway.
- O grupo de segurança anexado ao endpoint VPC do Amazon EC2 deve ter regras de entrada. Essas regras de entrada devem permitir o tráfego nas portas 1026-1028, 1031, 2222 e 443 a partir do endereço IP do proxy HTTP no Amazon EC2.

Resolva erros ao ativar seu gateway usando um endpoint público, e há um endpoint VPC do Storage Gateway na mesma VPC

Para resolver erros ao ativar seu gateway usando um endpoint público quando há um endpoint da Amazon Virtual Private Cloud (Amazon VPC) na mesma VPC, execute as seguintes verificações e configurações.

Confirme se a configuração Enable Private DNS Name não está habilitada em seu endpoint VPC do Storage Gateway

Se a opção Ativar nome DNS privado estiver ativada, você não poderá ativar nenhum gateway dessa VPC para o endpoint público.

Para desativar a opção de nome DNS privado:

1. Abra o [console da Amazon VPC](#).
2. No painel de navegação, escolha Endpoints.
3. Escolha seu endpoint VPC do Storage Gateway.
4. Escolha Ações.
5. Escolha Gerenciar nomes DNS privados.
6. Em Ativar nome DNS privado, desmarque Habilitar para este endpoint.
7. Escolha Modificar nomes DNS privados para salvar a configuração.

Como solucionar questões on-premises de solução de problemas no gateway

Você pode encontrar informações a seguir sobre problemas típicos que você pode encontrar ao trabalhar com seus gateways locais e como AWS Support ativá-los para ajudar a solucionar problemas com seu gateway.

A tabela a seguir lista problemas comuns que você pode encontrar ao trabalhar com gateways locais.

Problema	Medida a ser tomada
Não é possível encontrar o endereço IP de seu gateway.	<p>Use o cliente do hipervisor para se conectar ao host e encontrar o endereço IP do gateway.</p> <ul style="list-style-type: none">• No caso do VMware ESXi, o endereço IP da VM pode ser encontrado no cliente vSphere na guia Summary.• No caso do Microsoft Hyper-V, para encontrar o endereço IP da VM, faça login no console local. <p>Se você ainda estiver tendo dificuldade para encontrar o endereço IP do gateway:</p> <ul style="list-style-type: none">• Verifique se a VM está ativada. Seu endereço IP é atribuído a seu gateway somente quando a VM é ativada.• Aguarde a VM para finalizar a inicialização. Se tiver acabado de ativar sua VM, pode demorar alguns minutos para o gateway concluir a sequência de inicialização.
Você está tendo problemas de rede ou firewall.	<ul style="list-style-type: none">• Conceda permissão às portas apropriadas para seu gateway.• A validação/inspeção do certificado SSL não deve ser ativada. O Storage Gateway utiliza a autenticação TLS mútua, que falharia se alguma aplicação de terceiros tentasse interceptar/assinar um dos certificados.• Se usar um firewall ou roteador para filtrar ou limitar o tráfego de rede, você deverá configurar o firewall e o roteador para permitir a comunicação externa com a AWS nesses endpoints de serviço.

Problema	Medida a ser tomada
	Para obter mais informações sobre requisitos de rede e firewall, consulte Requisitos de rede e firewall .
A ativação do gateway falha quando você clica no botão Prosseguir para a ativação no Storage Gateway Management Console.	<ul style="list-style-type: none">• Verifique se a VM do gateway pode ser acessada executando ping na VM do cliente.• Verifique se a VM tem conectividade de rede com a Internet. Do contrário, você precisará configurar um proxy SOCKS. Para obter mais informações para fazer isso, consulte Como rotear seu gateway local por meio de um proxy.• Verifique se o horário do host está correto, se o host está configurado para sincronizar seu horário automaticamente com um servidor Network Time Protocol (NTP) e se o horário da VM do gateway está correto. Para obter informações sobre sincronização de horário de hosts e VMs de hipervisor, consulte Como sincronizar o horário da VM do gateway.• Depois que executar essas etapas, poderá realizar novamente a implantação de gateway usando o console do Storage Gateway e o assistente Definir e ativar gateway.• A validação/inspeção do certificado SSL não deve ser ativada. O Storage Gateway utiliza a autenticação TLS mútua, que falharia se alguma aplicação de terceiros tentasse interceptar/assinar um dos certificados.• Verifique se a VM tem pelo menos 7,5 GB de RAM. A alocação do gateway falhará se houver menos de 7,5 GB de RAM. Para ter mais informações, consulte Requisitos.

Problema	Medida a ser tomada
<p>Você precisa remover um disco reservado como espaço do buffer de upload. Por exemplo, talvez queira reduzir o espaço do buffer de upload de um gateway ou talvez necessite substituir um disco usado como buffer de upload que falhou.</p>	<p>Para obter instruções sobre como remover um disco reservado como espaço do buffer de upload, consulte Como remover discos de seu gateway.</p>
<p>É necessário melhorar a largura de banda entre o gateway e a AWS.</p>	<p>Você pode melhorar a largura de banda do seu gateway AWS configurando sua conexão com a Internet AWS em um adaptador de rede (NIC) separado daquele que conecta seus aplicativos e a VM do gateway. Essa abordagem é útil se você tiver uma conexão de alta largura de banda AWS e quiser evitar a contenção de largura de banda, especialmente durante a restauração de um instantâneo. Em caso de necessidades de workloads com alto throughput, é possível usar o AWS Direct Connect para estabelecer uma conexão de rede exclusiva entre o gateway on-premises e a AWS. Para medir a largura de banda da conexão do seu gateway para AWS, use as <code>CloudBytesUploaded</code> e <code>CloudBytesDownloaded</code> métricas do gateway. Para saber mais sobre esse assunto, consulte Como medir o desempenho entre o gateway e a AWS. Ao melhorar a conectividade com a Internet, você ajuda a evitar que o buffer de upload se esgote.</p>

Problema	Medida a ser tomada
A taxa de transferência de ou para seu gateway cai para zero.	<ul style="list-style-type: none">• Na guia Gateway do console do Storage Gateway, verifique se os endereços IP para a VM do gateway são os mesmos que você está vendo. Para isso, use o software cliente do hipervisor (isto é, o cliente VMware vSphere ou o Microsoft Hyper-V Manager). Se você encontrar alguma incompatibilidade, reinicie seu gateway no console do Storage Gateway, conforme mostrado em Encerramento da VM do gateway. Após a reinicialização, os endereços na lista Endereços IP, na guia Gateway do console do Storage Gateway, devem corresponder aos endereços IP de seu gateway, que são determinados no cliente do hipervisor.• No caso do VMware ESXi, o endereço IP da VM pode ser encontrado no cliente vSphere na guia Summary.• No caso do Microsoft Hyper-V, para encontrar o endereço IP da VM, faça login no console local.• Verifique a conectividade do seu gateway AWS conforme descrito em Como testar a conexão de seu gateway com a Internet.• Verifique a configuração do adaptador de rede do gateway e confirme se todas as interfaces que você queria que estivessem habilitadas para o gateway estão habilitadas. Para visualizar a configuração do adaptador de rede de seu gateway, siga as instruções em Como configurar uma rede de gateway e selecione a opção para visualizar a configuração de rede do gateway. <p>Você pode visualizar a taxa de transferência de e para seu gateway no CloudWatch console da Amazon. Para obter mais informações sobre como medir a taxa de transferência de e para seu gateway AWS, consulte Como medir o desempenho entre o gateway e a AWS.</p>

Problema	Medida a ser tomada
Você está tendo problemas para importar (implantar) o Storage Gateway no Microsoft Hyper-V.	Consulte Como solucionar problemas de configuração no Microsoft Hyper-V , que examina alguns dos problemas comuns na implantação de um gateway no Microsoft Hyper-V.
É exibida uma mensagem que diz: "Os dados que foram gravados no volume do seu gateway não estão armazenados com segurança na AWS".	Você receberá essa mensagem se a VM do gateway foi criada a partir de um clone ou snapshot de outra VM do gateway. Se este não for o caso, entre em contato com o AWS Support.


Permitindo AWS Support ajudar a solucionar problemas em seu gateway hospedado localmente

O Storage Gateway fornece um console local que você pode usar para realizar várias tarefas de manutenção, incluindo AWS Support a ativação para acessar seu gateway para ajudá-lo a solucionar problemas do gateway. Por padrão, o AWS Support acesso ao seu gateway está desativado. Esse acesso é ativado por meio do console local do host. Para dar AWS Support acesso ao seu gateway, primeiro faça login no console local do host, navegue até o console do Storage Gateway e, em seguida, conecte-se ao servidor de suporte.

Para permitir AWS Support o acesso ao seu gateway

1. Faça login no console local do host.
 - VMware ESXi: para obter mais informações, consulte [Acesso ao console local do gateway com o VMware ESXi](#).
 - Microsoft Hyper-V: para obter mais informações, consulte [Acessar o console local do gateway com o Microsoft Hyper-V](#).
2. No prompt, insira o numeral correspondente para selecionar Console do gateway.
3. Insira **h** para abrir a lista de comandos disponíveis.
4. Execute um destes procedimentos:

- Se o gateway estiver usando um endpoint público, na janela AVAILABLE COMMANDS (Comandos disponíveis), insira **open-support-channel** para se conectar ao suporte ao cliente do Storage Gateway. Permita a porta TCP 22 para que você possa abrir um canal de suporte para a AWS. Quando se conectar ao suporte ao cliente, o Storage Gateway atribuirá a você um número de suporte. Anote seu número de suporte.
- Se o gateway estiver usando um VPC endpoint, na janela AVAILABLE COMMANDS (Comandos disponíveis) insira **open-support-channel**. Se o gateway não estiver ativado, forneça o endpoint da VPC ou o endereço IP para o qual se conectar ao suporte ao cliente do Storage Gateway. Permita a porta TCP 22 para que você possa abrir um canal de suporte para a AWS. Quando se conectar ao suporte ao cliente, o Storage Gateway atribuirá a você um número de suporte. Anote seu número de suporte.

 Note

O número do canal não é um número de porta de Transmission Control Protocol/User Datagram Protocol (TCP/UDP). Na verdade, o gateway faz uma conexão Secure Shell (SSH) (TCP 22) com os servidores do Storage Gateway e providencia o canal de suporte para a conexão.

5. Depois que o canal de suporte for estabelecido, forneça seu número de serviço de suporte para AWS Support que AWS Support possa fornecer assistência na solução de problemas.
6. Quando a sessão de suporte for concluída, insira **q** para finalizá-la. Não feche a sessão até que o Suporte da Amazon Web Services notifique você que a sessão de suporte foi concluída.
7. Insira **exit** para encerrar a sessão do console do gateway.
8. Siga as instruções para sair do console local.

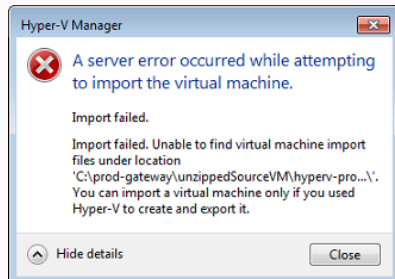
Como solucionar problemas de configuração no Microsoft Hyper-V

A tabela a seguir lista problemas comuns que podem ser encontrados ao implantar o Storage Gateway na plataforma Microsoft Hyper-V.

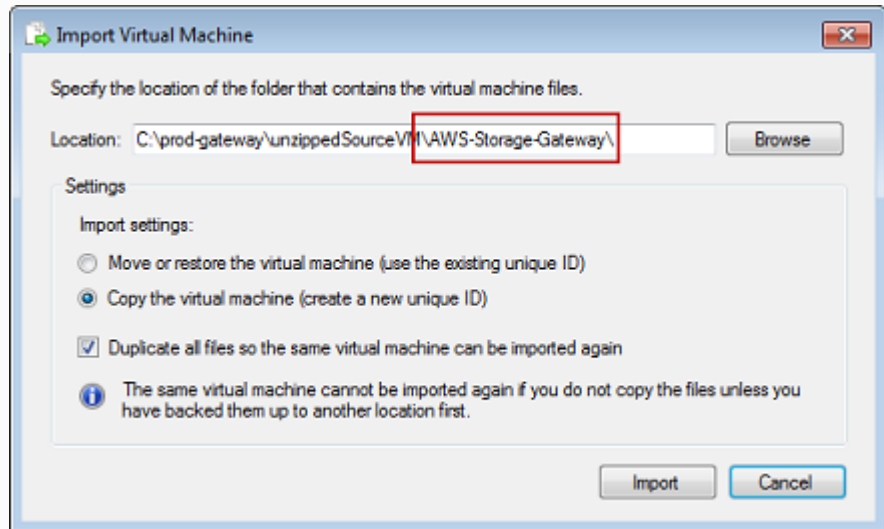
Problema	Medida a ser tomada
Você tenta importar um gateway e recebe a	Esse erro pode ocorrer pelos seguintes motivos:

Problema

mensagem de erro: "Import failed. Unable to find virtual machine import file under location..."

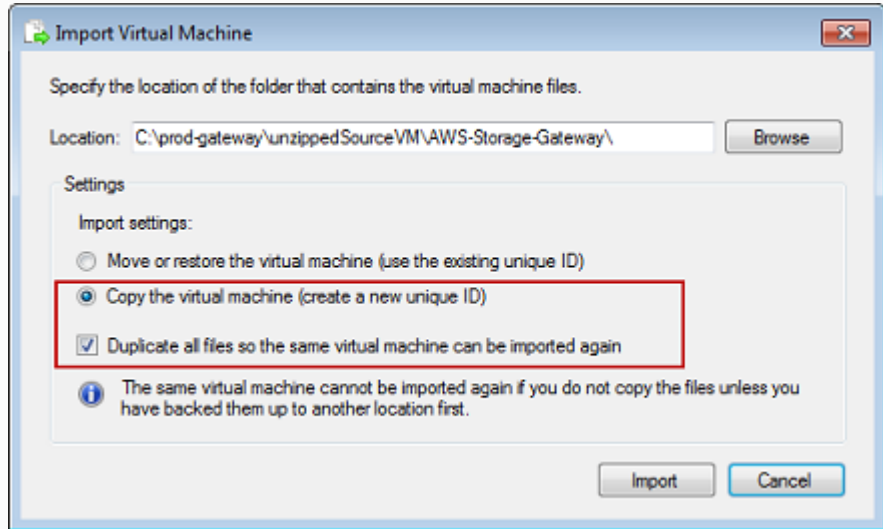
**Medida a ser tomada**

- Se você não estiver direcionado para a raiz dos arquivos de origem descompactados do gateway. A última parte do local especificado na caixa de diálogo Import Virtual Machine deve ser AWS-Storage-Gateway , tal como mostrado no exemplo a seguir:

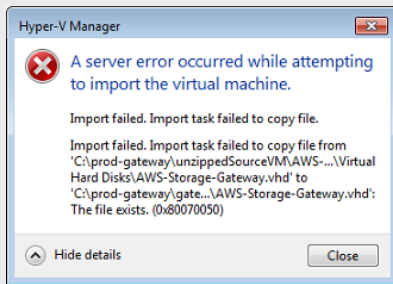


- Se já tiver implantado um gateway e não tiver selecionado a opção Copy the virtual machine e marcado a opção Duplicate all files na caixa de diálogo Import Virtual Machine, isso quer dizer que a VM foi criada no local em que se encontram os arquivos descompactados do gateway e você não pode importar desse local novamente. Para corrigir esse problema, obtenha uma cópia atualizada dos arquivos de origem descompactados do gateway e copie para um novo local. Use o novo local como origem da importação. O exemplo a seguir mostra as opções que você deve verificar se tiver intenção de criar vários gateways em um único local de arquivos de origem descompactados.

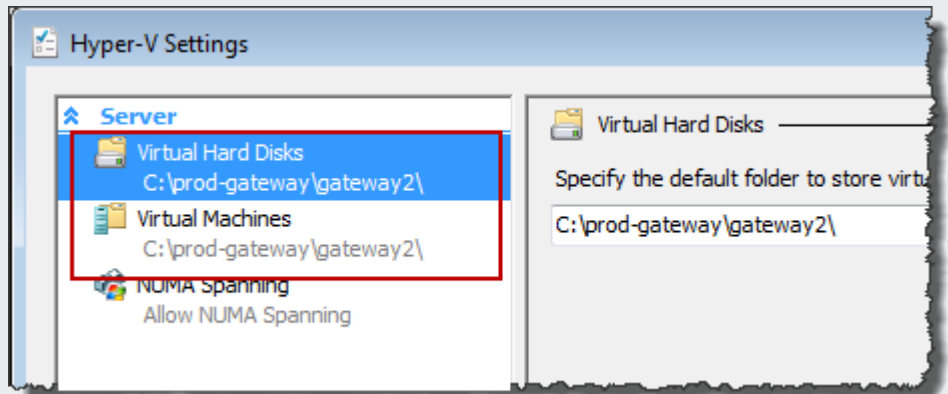
Problema	Medida a ser tomada
----------	---------------------

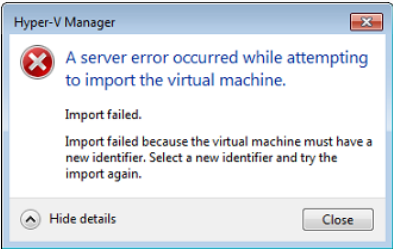
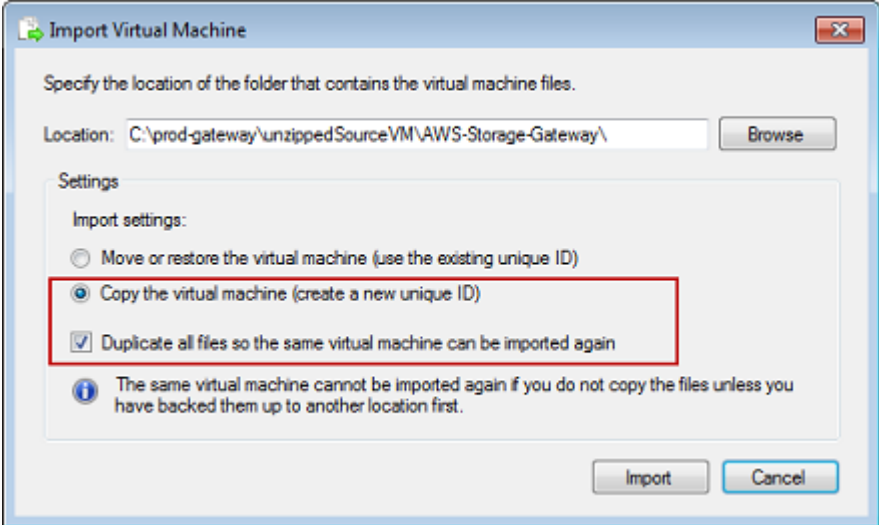


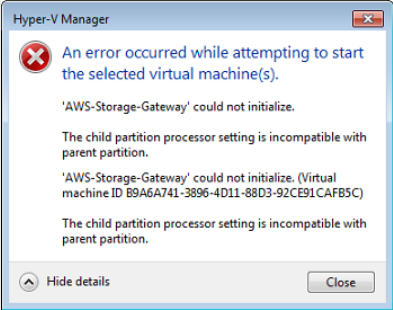
Você tenta importar um gateway e recebe a mensagem de erro: "Import failed. Tarefa de importação não copiou o arquivo".

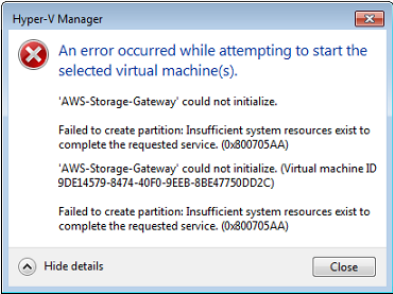


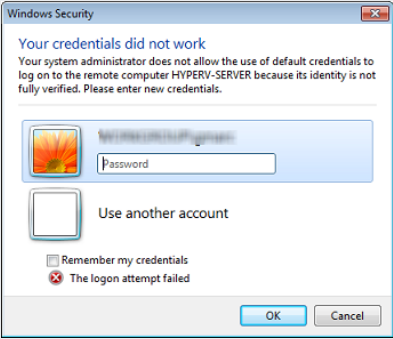
Se já tiver implantado um gateway e tentar reutilizar as pastas padrão que armazenam os arquivos do disco rígido virtual e os arquivos de configuração da máquina virtual, ocorrerá esse erro. Para corrigir esse problema, especifique novos locais na caixa de diálogo Hyper-V Settings.



Problema	Medida a ser tomada
<p>Você tenta importar um gateway e recebe uma mensagem de erro: "Import failed. Import failed because the virtual machine must have a new identifier. Select a new identifier and try the import again".</p> 	<p>Ao importar o gateway, lembre-se de selecionar a opção Copy the virtual machine e de marcar a opção Duplicate all files na caixa de diálogo Import Virtual Machine para criar um novo ID exclusivo para a VM. O exemplo a seguir mostra as opções na caixa de diálogo Import Virtual Machine que você deve usar.</p> 

<p>Você tenta iniciar uma VM do gateway e recebe a mensagem de erro "The child partition processor setting is incompatible with parent partition".</p> 	<p>Esse erro provavelmente é provocado por uma discrepância de CPU, entre as CPUs necessárias ao gateway e as CPUs disponíveis no host. Confirme se o hipervisor subjacente comporta a contagem de CPU da VM.</p> <p>Para obter mais informações sobre os requisitos do Storage Gateway, consulte Requisitos.</p>
--	---

Problema	Medida a ser tomada
<p>Você tenta iniciar uma VM do gateway e recebe a mensagem de erro "Failed to create partition: Insufficient resources exist to complete the requested service".</p> 	<p>Esse erro provavelmente é provocado por uma discrepância de RAM, entre a RAM necessária ao gateway e a RAM disponível no host.</p> <p>Para obter mais informações sobre os requisitos do Storage Gateway, consulte Requisitos.</p>
<p>Os snapshots e as atualizações de software do gateway estão ocorrendo em momentos levemente diferentes do que o previsto.</p>	<p>O relógio da VM do gateway pode estar se desviando do tempo real, o que é conhecido como desvio de relógio. Verifique e corrija o tempo da VM usando a opção de sincronização de tempo do console do gateway local. Para ter mais informações, consulte Como sincronizar o horário da VM do gateway.</p>
<p>É necessário colocar os arquivos descompactados do Storage Gateway para o Microsoft Hyper-V no sistema de arquivos do host.</p>	<p>Acesse o host do mesmo modo que faz para acessar um servidor Microsoft Windows comum. Por exemplo, se o nome do host do hipervisor for <code>hyperv-server</code>, você poderá usar o seguinte caminho UNC <code>\\hyperv-server\c\$</code>, que pressupõe que o nome <code>hyperv-server</code> pode ser resolvido ou é definido em seu arquivo de hosts locais.</p>

Problema	Medida a ser tomada
<p>Você será solicitado a fornecer credenciais ao se conectar ao hipervisor.</p> 	<p>Adicione suas credenciais de usuário como administrador local para o host do hipervisor usando a ferramenta Sconfig.cmd.</p>
<p>É possível notar um desempenho de rede ruim se ativar a fila de máquinas virtuais (VMQ) em um host Hyper-V que esteja usando um adaptador de rede Broadcom.</p>	<p>Para obter informações sobre uma solução alternativa, consulte a documentação da Microsoft, consulte Baixo desempenho de rede em máquinas virtuais em um host Hyper-V do Windows Server 2012 se o VMQ estiver ativado.</p>

Como solucionar problemas de gateway do Amazon EC2

Nas seções a seguir, você encontrará problemas comuns que podem ocorrer ao trabalhar com um gateway implantado no Amazon EC2. Para obter mais informações sobre a diferença entre um gateway on-premises e um gateway implantado no Amazon EC2, consulte [Como implantar uma instância do Amazon EC2 para hospedar seu gateway de volumes](#).

Tópicos

- [A ativação do gateway não aconteceu após alguns minutos](#)
- [Não é possível encontrar a instância do gateway do EC2 na lista de instâncias](#)
- [Um volume do Amazon EBS, mas não é possível anexá-lo à instância do gateway do EC2](#)
- [Não é possível conseguir anexar um iniciador a um destino de volume do gateway do EC2](#)
- [É exibida uma mensagem informando que não há discos disponíveis quando você tenta adicionar volumes de armazenamento](#)

- [É preciso remover um disco alocado como espaço de buffer de upload para reduzir o espaço do buffer de upload](#)
- [O throughput de ou para o gateway do EC2 cai para zero](#)
- [Você quer ajudar AWS Support a solucionar problemas do seu gateway EC2](#)
- [Você deseja se conectar à instância do gateway usando o Console de Série do Amazon EC2](#)

A ativação do gateway não aconteceu após alguns minutos

Verifique o seguinte no console do Amazon EC2:

- A porta 80 está ativada no grupo de segurança associado à instância. Para obter mais informações sobre como adicionar uma regra de grupo de segurança, consulte [Adicionar uma regra de grupo de segurança](#) no Guia do usuário do Amazon EC2.
- A instância do gateway está marcada como em execução. No console do Amazon EC2, o valor do Estado para a instância deve ser EXECUTANDO.
- Certifique-se de que o tipo de instância do Amazon EC2 atende aos requisitos mínimos, conforme descrito em [Requisitos de armazenamento](#).

Depois de corrigir o problema, tente ativar o gateway novamente. Para fazer isso, abra o console do Storage Gateway, selecione Implantar um novo gateway no Amazon EC2 e insira novamente o endereço IP da instância.

Não é possível encontrar a instância do gateway do EC2 na lista de instâncias

Se você não tiver atribuído uma tag de recurso à sua instância e tiver muitas instâncias em execução, talvez seja difícil saber em qual instância executou. Nesse caso, você pode executar as ações a seguir para encontrar a instância do gateway:

- Verifique o nome da imagem de máquina da Amazon (AMI) na guia Description (Descrição) da instância. Uma instância baseada na AMI do Storage Gateway deve iniciar com as palavras **aws-storage-gateway-ami**.
- Se tiver várias instâncias baseadas na AMI do Storage Gateway, verifique o horário de execução da instância para localizar a instância correta.

Um volume do Amazon EBS, mas não é possível anexá-lo à instância do gateway do EC2

Verifique se o volume do Amazon EBS em questão está na mesma zona de disponibilidade da instância do gateway. Se houver discrepância nas zonas de disponibilidade, crie um novo volume do Amazon EBS na mesma zona de disponibilidade que sua instância.

Não é possível conseguir anexar um iniciador a um destino de volume do gateway do EC2

Verifique se o security group com o qual você executou a instância inclui uma regra que concede à porta que você está usando o acesso ao iSCSI. A porta geralmente é definida como 3260. Para obter mais informações sobre como se conectar a volumes, consulte [Como conectar volumes a um cliente Windows](#).

É exibida uma mensagem informando que não há discos disponíveis quando você tenta adicionar volumes de armazenamento

No caso de um gateway recém-ativado, não há nenhum armazenamento de volume definido. Para poder definir o armazenamento de volume, você precisará reservar discos locais para o gateway para usar como buffer de upload e armazenamento em cache. No caso de um gateway implantado para o Amazon EC2, os discos locais são volumes do Amazon EBS anexados à instância. Esta mensagem de erro provavelmente ocorre porque não há nenhum volume do Amazon EBS definido para a instância.

Examine os dispositivos de blocos definidos para a instância que está executando o gateway. Se houver apenas dois dispositivos de blocos (os dispositivos padrão que vêm com a AMI), você deverá ampliar o armazenamento. Para obter mais informações para fazer isso, consulte [Como implantar uma instância do Amazon EC2 para hospedar seu gateway de volumes](#). Assim que anexar dois ou mais volumes do Amazon EBS, tente criar um armazenamento de volume no gateway.

É preciso remover um disco alocado como espaço de buffer de upload para reduzir o espaço do buffer de upload

Siga as etapas em [Como determinar o tamanho do buffer de upload para alocar](#).

O throughput de ou para o gateway do EC2 cai para zero

Verifique se a instância do gateway está em execução. Se a instância estiver iniciando em virtude de uma reinicialização, por exemplo, aguarde até que ela reinicie.

Verifique também se o IP do gateway não foi alterado. Se a instância tiver sido interrompida e, em seguida, reiniciada, o endereço IP da instância pode ter alterado. Nesse caso, você precisa ativar um novo gateway.

Você pode visualizar a taxa de transferência de e para seu gateway no CloudWatch console da Amazon. Para obter mais informações sobre como medir a taxa de transferência de e para seu gateway AWS, consulte [Como medir o desempenho entre o gateway e a AWS](#).

Você quer ajudar AWS Support a solucionar problemas do seu gateway EC2

O Storage Gateway fornece um console local que você pode usar para realizar várias tarefas de manutenção, incluindo AWS Support a ativação para acessar seu gateway para ajudá-lo a solucionar problemas do gateway. Por padrão, o AWS Support acesso ao seu gateway está desativado. Esse acesso é fornecido por meio do console local do EC2. O login no console local do Amazon EC2 é feito por meio do Secure Shell (SSH). Para conseguir fazer login por meio do SSH, o security group da instância deve ter uma regra que abre a porta TCP 22.

Note

Se você adicionar uma nova regra a um security group existente, essa nova regra será aplicada a todas as instâncias que usam esse security group. Para obter mais informações sobre grupos de segurança e como adicionar regras a eles, consulte [Grupos de segurança do Amazon EC2](#) no Guia do usuário do Amazon EC2.


Para permitir a AWS Support conexão com seu gateway, primeiro faça login no console local da instância do Amazon EC2, navegue até o console do Storage Gateway e, em seguida, forneça o acesso.

Para ativar o AWS Support acesso a um gateway implantado em uma instância do Amazon EC2

1. Faça login no console local da instância do Amazon EC2. Para obter instruções, consulte [Conectar-se à instância](#) no Guia do usuário do Amazon EC2.

Você pode usar o comando a seguir para fazer login no console local da Instância EC2.


```
ssh -i PRIVATE-KEY admin@INSTANCE-PUBLIC-DNS-NAME
```

 Note

O *PRIVATE-KEY* é o arquivo .pem que contém o certificado privado do par de chaves do EC2 que você usou para executar a instância do Amazon EC2. Para obter mais informações, consulte [Recuperar a chave pública para seu par de chaves](#) no Guia do usuário do Amazon EC2.

INSTANCE-PUBLIC-DNS-NAME é o nome do sistema de nomes de domínio (DNS) público da instância do Amazon EC2 na qual seu gateway está em execução. Para obter esse nome DNS público, selecione a instância do Amazon EC2 no console do EC2 e clique na guia Descrição.

2. No prompt, insira **6 - Command Prompt** para abrir o console do canal do AWS Support .
3. Insira **h** para abrir a janela COMANDOS DISPONÍVEIS.
4. Execute um destes procedimentos:
 - Se o gateway estiver usando um endpoint público, na janela COMANDO DISPONÍVEIS, insira **open-support-channel** para se conectar ao suporte ao cliente do Storage Gateway. Permita a porta TCP 22 para que você possa abrir um canal de suporte para a AWS. Quando se conectar ao suporte ao cliente, o Storage Gateway atribuirá a você um número de suporte. Anote seu número de suporte.
 - Se o gateway estiver usando um VPC endpoint, na janela AVAILABLE COMMANDS (Comandos disponíveis) insira **open-support-channel**. Se o gateway não estiver ativado, forneça o endpoint da VPC ou o endereço IP para o qual se conectar ao suporte ao cliente do Storage Gateway. Permita a porta TCP 22 para que você possa abrir um canal de suporte para a AWS. Quando se conectar ao suporte ao cliente, o Storage Gateway atribuirá a você um número de suporte. Anote seu número de suporte.

 Note

O número do canal não é um número de porta de Transmission Control Protocol/User Datagram Protocol (TCP/UDP). Na verdade, o gateway faz uma conexão Secure Shell

(SSH) (TCP 22) com os servidores do Storage Gateway e providencia o canal de suporte para a conexão.

5. Depois que o canal de suporte for estabelecido, forneça seu número de serviço de suporte para AWS Support que AWS Support possa fornecer assistência na solução de problemas.
6. Quando a sessão de suporte for concluída, insira **q** para finalizá-la. Não feche a sessão até AWS Support notificá-lo de que a sessão de suporte foi concluída.
7. Digite **exit** para sair do console do Storage Gateway.
8. Siga os menus do console para encerrar a sessão na instância do Storage Gateway.

Você deseja se conectar à instância do gateway usando o Console de Série do Amazon EC2

É possível usar o Console de Série do Amazon EC2 para solucionar a inicialização, a configuração de rede e outros problemas. Consulte as instruções e dicas de solução de problemas em [Amazon EC2 Serial Console](#) no Guia do usuário do Amazon Elastic Compute Cloud.

Como solucionar problemas do dispositivo de hardware

Os tópicos a seguir discutem os problemas que podem acontecer com o Storage Gateway Hardware Appliance e trazem sugestões sobre como solucioná-los.

Não é possível determinar o endereço IP do serviço

Ao tentar se conectar ao serviço, verifique se você está usando o endereço IP do serviço, e não o do host. Configure o endereço IP do serviço no console de serviço e o do host, no console de hardware. Você verá o console de hardware quando iniciar o dispositivo de hardware. Para acessar o console de serviço do console de hardware, escolha Open Service Console (Abrir console de serviço).

Como executar uma redefinição de fábrica?

Se precisar executar uma redefinição de fábrica no dispositivo, entre em contato com a equipe de suporte do Storage Gateway Hardware Appliance, como descrito na seção sobre suporte a seguir.

Como executar uma reinicialização remota?

Se precisar reiniciar remotamente seu equipamento, é possível fazer isso usando a interface de gerenciamento do Dell iDRAC. Para obter mais informações, consulte [Ciclo de alimentação virtual iDRAC9: reinicialize remotamente os PowerEdge servidores Dell EMC no site da Dell Technologies InfoHub](#)

Onde encontrar suporte para o Dell iDRAC?

O servidor Dell PowerEdge R640 vem com a interface de gerenciamento Dell iDRAC.

Recomendamos o seguinte:

- Se você usar a interface de gerenciamento do iDRAC, deverá alterar a senha padrão. Para obter mais informações sobre as credenciais do iDRAC, [consulte PowerEdge Dell - Quais são as credenciais de login padrão do iDRAC?](#) .
- Certifique-se de que o firmware evite violações de segurança. up-to-date
- Mover a interface de rede do iDRAC para uma porta normal (em) poderá causar problemas de performance ou impedir o funcionamento normal do dispositivo.

Não é possível encontrar o número de série do dispositivo de hardware

Para encontrar o número de série do dispositivo de hardware, acesse a página Visão geral do dispositivo de hardware no console do Storage Gateway, conforme mostrado a seguir.

Aba de hardware do console Storage Gateway com o dispositivo selecionado e os detalhes mostrados.

Storage Gateway

Gateways

File shares

Volumes

Tapes

Hardware

Successfully launched File Gateway on praksuji-bh

Order appliance Quotes and orders Activate appliance Actions

Filter by hardware appliance name, ID or launched gateway type.

	Hardware Appliance Name	Hardware Appliance ID	Model	Launched Gateway
<input checked="" type="checkbox"/>	praksuji-bh	v15loueix9yotyn5	Dell PowerEdge R640	File Gateway
<input type="checkbox"/>	praksuji-hw-pdx	wlyd0dgh6j7kg4no	Dell PowerEdge R640	File Gateway

Details

Name	praksuji-bh	Vendor	Dell
ID	v15loueix9yotyn5	Model	Dell PowerEdge R640
Time Zone	GMT	Serial Number	5Q8Y0M2
		RAID Volume Manager	ZFS

Aba de hardware do console Storage Gateway com o dispositivo selecionado e os detalhes mostrados.

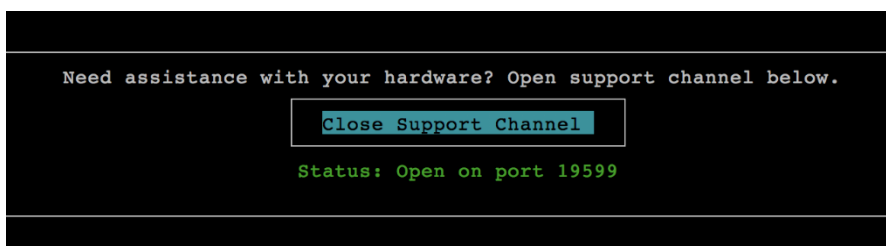
Onde obter suporte para o dispositivo de hardware

Para entrar em contato com o suporte do Storage Gateway Hardware Appliance, consulte [AWS Support](#).

A AWS Support equipe pode pedir que você ative o canal de suporte para solucionar seus problemas de gateway remotamente. Você não precisa dessa porta aberta para a operação normal do gateway, mas ela é necessária para a solução de problemas. Você pode ativar o canal de suporte no console de hardware, conforme mostrado no procedimento a seguir.

Para abrir um canal de suporte para AWS

1. Abra o console de hardware.
2. Escolha Open Support Channel (Abrir canal de suporte), como mostrado a seguir. console do dispositivo de hardware com o status do canal de suporte exibido.



console do dispositivo de hardware com o status do canal de suporte exibido.

Se não houver problemas de conectividade de rede ou firewall, o número da porta atribuída será exibido em até 30 segundos.

3. Anote o número da porta e forneça-o para AWS Support.

Como solucionar problemas em volumes

Você pode encontrar informações sobre os problemas mais comuns com os quais você pode se deparar ao trabalhar com volumes e ações sugeridas para corrigi-los.

Tópicos

- [O console informa que seu volume não está configurado](#)
- [O console informa que seu volume é irrecuperável](#)
- [O gateway armazenado em cache é inacessível e você deseja recuperar seus dados](#)
- [O console informa que o status de seu volume é PASS THROUGH](#)
- [Você deseja verificar a integridade do volume e corrigir possíveis erros](#)
- [Seu volume de destino iSCSI não aparece no Console de Gerenciamento de Disco do Windows](#)
- [Você deseja alterar o nome do destino iSCSI do volume](#)
- [O snapshot de volume programado não ocorreu](#)
- [Você precisa remover ou substituir um disco que apresentou falha](#)
- [A taxa de transferência de seu aplicativo para um volume caiu para zero](#)
- [Um disco de cache no gateway depara-se com uma falha](#)
- [O snapshot de um volume mantém-se no status PENDING por mais tempo que o esperado](#)
- [Notificações de integridade de alta disponibilidade](#)

O console informa que seu volume não está configurado

Se o console do Storage Gateway indicar que o status de seu volume é UPLOAD BUFFER NOT CONFIGURED (Buffer de upload não configurado), amplie a capacidade do buffer de upload do gateway. Você não poderá usar um gateway para armazenar dados de aplicativo se o buffer de upload do gateway não estiver configurado. Para ter mais informações, consulte [Para configurar um buffer de upload ou armazenamento em cache adicionais para o gateway](#).

O console informa que seu volume é irrecuperável

No caso de volumes armazenados, se o console do Storage Gateway indicar que o status do volume é IRRECOVERABLE (Irrecuperável), não será mais possível usar esse volume. É possível tentar excluir o volume no console do Storage Gateway. Se houver dados no volume, você poderá recuperar os dados ao criar um novo volume com base no disco local da VM que foi usado inicialmente para criar o volume. Ao criar o novo volume, selecione Preserve existing data. Lembre-se de excluir os snapshots pendentes do volume antes de excluir o volume. Para ter mais informações, consulte [Excluir um snapshot](#). Se a exclusão do volume no console do Storage Gateway não funcionar, é provável que o disco alocado ao volume tenha sido removido incorretamente da VM e não seja possível removê-lo do dispositivo.

No caso de volumes armazenados em cache, se o console do Storage Gateway indicar que o status do volume é IRRECOVERABLE, não será mais possível usar esse volume. Se houver dados no volume, você pode criar um snapshot do volume e recuperar os dados por meio do snapshot ou clonar o volume a partir do último ponto de recuperação. Você pode excluir o volume depois que tiver recuperado seus dados. Para ter mais informações, consulte [O gateway armazenado em cache é inacessível e você deseja recuperar seus dados](#).

Para volumes armazenados, você pode criar um novo volume por meio do disco que foi usado para criar o volume irrecuperável. Para ter mais informações, consulte [Como criar um volume](#). Para obter informações sobre status de volume, consulte [Noções básicas sobre transições e status de volumes](#).

O gateway armazenado em cache é inacessível e você deseja recuperar seus dados

Quando seu gateway fica inacessível (por exemplo, quando é desligado), você tem a opção de criar um snapshot em um ponto de recuperação de volume e usar esse snapshot ou de clonar um novo volume com base no último ponto de recuperação para um volume existente. Clonar com base em um ponto de recuperação de volume é mais rápido e mais econômico do que criar um snapshot. Para obter mais informações sobre clonagem de volume, consulte [Como clonar um volume](#).

O Storage Gateway fornece pontos de recuperação para cada volume em uma arquitetura de gateway de volumes armazenados em cache. Um ponto de recuperação de volume é um momento específico em que todos os dados do volume estão consistentes e no qual você pode criar um snapshot ou clonar um volume.

O console informa que o status de seu volume é PASS THROUGH

Em alguns casos, o console do Storage Gateway pode indicar que o status do volume é PASSTHROUGH (Passagem). Um volume pode ter o status PASSTHROUGH por vários motivos. Alguns motivos exigem alguma ação e outros não.

Um exemplo de situação em que você deve agir se o status do volume for PASS THROUGH é quando o gateway fica sem espaço do buffer de upload. Para verificar se seu buffer de upload foi excedido no passado, você pode visualizar a `UploadBufferPercentUsed` métrica no CloudWatch console da Amazon; para obter mais informações, consulte [Monitorar o buffer de upload](#). Se o gateway tiver o status PASS THROUGH (Passagem) porque ficou sem espaço no buffer de upload, mais espaço no buffer de upload para o gateway deverá ser alocado. Adicionar mais espaço no buffer fará com que seu volume faça a transição automática de PASS THROUGH (Passagem) para BOOTSTRAPPING e AVAILABLE (Disponível). Embora o status do volume seja BOOTSTRAPPING, o gateway lê os dados do disco do volume, faz upload desses dados no Amazon S3 e se ajusta de acordo com a necessidade. Depois que o gateway se ajusta e salva o volume de dados no Amazon S3, o status volume passa a ser AVAILABLE (Disponível) e os snapshots podem ser iniciados novamente. Observe que, quando o status do volume é PASS THROUGH ou BOOTSTRAPPING, você pode continuar a ler e gravar dados no disco do volume. Para obter mais informações sobre como ampliar o espaço do buffer de upload, consulte [Como determinar o tamanho do buffer de upload para alocar](#).

Para agir antes de o limite do buffer de upload ser ultrapassado, você pode definir um alarme de limite em um buffer de upload do gateway. Para ter mais informações, consulte [Para definir um alarme com limite superior para o buffer de upload de um gateway](#).

Em contraposição, um exemplo em que não é preciso agir com relação ao status de volume PASS THROUGH é quando o volume está aguardando o bootstrapping porque outro volume está em fase de bootstrapping. O gateway realiza bootstrap em um volume de cada vez.

O status PASS THROUGH raramente pode indicar que um disco reservado para um buffer de upload falhou. Nesse caso, você deve remover o disco. Para ter mais informações, consulte [Gateway de volumes](#). Para obter informações sobre status de volume, consulte [Noções básicas sobre transições e status de volumes](#).

Você deseja verificar a integridade do volume e corrigir possíveis erros

Se desejar verificar a integridade de volume e corrigir possíveis erros e seu gateway usa iniciadores do Microsoft Windows para se conectar aos volumes, poderá usar o utilitário Windows CHKDSK para

verificar a integridade dos volumes e corrigir quaisquer erros nos volumes. Quando é detectada uma corrupção no volume, o Windows pode executar automaticamente a ferramenta CHKDSK ou então você mesmo executá-la.

Seu volume de destino iSCSI não aparece no Console de Gerenciamento de Disco do Windows

Se seu o destino iSCSI do volume não aparecer no Console de Gerenciamento de Disco do Windows, verifique se você configurou o buffer de upload para o gateway. Para ter mais informações, consulte [Para configurar um buffer de upload ou armazenamento em cache adicionais para o gateway](#).

Você deseja alterar o nome do destino iSCSI do volume

Se desejar alterar o nome do destino iSCSI do volume, deverá excluir o volume e adicioná-lo novamente com um novo nome de destino. Se fizer isso, poderá preservar os dados no volume.

O snapshot de volume programado não ocorreu

Se o snapshot programado de um volume não tiver ocorrido, verifique se o status do volume é PASSTHROUGH ou se o buffer de upload do gateway atingiu seu limite antes do horário programado de snapshot. Você pode verificar a `UploadBufferPercentUsed` métrica do gateway no CloudWatch console da Amazon e criar um alarme para essa métrica. Para ter mais informações, consulte [Monitorar o buffer de upload](#) e [Para definir um alarme com limite superior para o buffer de upload de um gateway](#).

Você precisa remover ou substituir um disco que apresentou falha

Se precisar substituir um disco de um volume que falhou ou substituir um volume porque ele não é necessário, deverá remover o volume primeiro usando o console do Storage Gateway. Para ter mais informações, consulte [Para excluir um volume](#). Em seguida, use o cliente do hipervisor para remover o armazenamento de apoio:

- No caso do VMware ESXi, remova o armazenamento de apoio, tal como descrito em [Exclusão de um volume](#).
- Para o Microsoft Hyper-V, remova o armazenamento de apoio.

A taxa de transferência de seu aplicativo para um volume caiu para zero

Se a taxa de transferência de seu aplicativo para um volume tiver caído para zero, tente o seguinte:

- Se você estiver usando o cliente VMware vSphere, verifique se o endereço Host IP do volume corresponde a um dos endereços que aparecem no cliente vSphere, na guia Summary. É possível encontrar o endereço IP do host de um volume de armazenamento no console do Storage Gateway, na guia Detalhes do volume. Uma haver discrepância no endereço IP; por exemplo, ao atribuir um novo endereço IP estático ao gateway. Se houver alguma discrepância, reinicie seu gateway no console do Storage Gateway, conforme mostrado em [Encerramento da VM do gateway](#). Após a reinicialização, o endereço Host IP na guia iSCSI Target Info de um volume de armazenamento deve corresponder ao endereço IP mostrado no cliente vSphere na guia Summary do gateway.
- Se não houver um endereço IP na caixa Host IP do volume e o gateway estiver on-line. Por exemplo, isso pode ocorrer se você criar um volume associado a um endereço IP de um adaptador de rede de um gateway que tem dois ou mais adaptadores de rede. Ao remover ou desabilitar o adaptador de rede ao qual o volume está associado, o endereço IP pode não aparecer na caixa IP do host. Para resolver esse problema, exclua o volume e volte a criá-lo preservando os dados existentes.
- Verifique se o iniciador iSCSI usado por seu aplicativo está mapeado corretamente para o destino iSCSI do volume de armazenamento. Para obter mais informações sobre como conectar volumes de armazenamento, consulte [Como conectar volumes a um cliente Windows](#).

Você pode visualizar a taxa de transferência dos volumes e criar alarmes no console da Amazon CloudWatch. Para obter mais informações sobre como medir a taxa de transferência entre um aplicativo e um volume, consulte [Como medir o desempenho entre seu aplicativo e o gateway](#).

Um disco de cache no gateway depara-se com uma falha

Se um ou mais discos de cache tiverem um erro, o gateway impedirá as operações de leitura e gravação em fitas e volumes virtuais. Para retomar a funcionalidade normal, reconfigure seu gateway conforme a seguinte descrição:

- Se o disco de cache estiver inacessível ou inutilizável, exclua o disco da configuração do gateway.
- Se o disco de cache ainda estiver acessível e utilizável, reconecte-o ao seu gateway.

Note

Se um disco de cache for excluído, fitas ou volumes que tiverem dados limpos (ou seja, para os quais os dados no disco de cache e no Amazon S3 são sincronizados) continuarão disponíveis quando o gateway retomar a funcionalidade normal. Por exemplo, se o gateway tiver três discos de cache e dois forem excluídos, as fitas ou os volumes limpos terão o status AVAILABLE (Disponível). Outras fitas e volumes terão o status IRRECOVERABLE (Irrecuperável).

Se você usar discos efêmeros como discos de cache para seu gateway ou montar seus discos de cache em uma unidade efêmera, seus discos de cache serão perdidos quando você desligar o gateway. Desligar o gateway quando seu disco de cache e o Amazon S3 não estão sincronizados pode resultar em perda de dados. Como resultado, não recomendamos o uso de unidades ou discos temporários.

O snapshot de um volume mantém-se no status PENDING por mais tempo que o esperado

Se o snapshot de um volume permanecer no estado PENDING por mais tempo que o esperado, isso significa que a VM do gateway pode ter falhado inesperadamente ou o status de um volume pode ter mudado para PASS THROUGH ou IRRECOVERABLE. Se uma dessas situações ocorrer, o snapshot permanecerá no status PENDING e não será concluído com êxito. Nesses casos, recomendamos que você exclua o snapshot. Para ter mais informações, consulte [Excluir um snapshot](#).

Quando o volume retornar para o status AVAILABLE, crie um novo snapshot do volume. Para obter informações sobre status de volume, consulte [Noções básicas sobre transições e status de volumes](#).

Notificações de integridade de alta disponibilidade

Ao executar o gateway na plataforma do VMware vSphere High Availability (HA), você pode receber notificações de integridade. Para obter mais informações sobre notificações de integridade, consulte [Como solucionar problemas de alta disponibilidade](#).

Como solucionar problemas de alta disponibilidade

Você pode encontrar informações a seguir sobre as ações que deverão ser executadas se tiver problemas de disponibilidade.

Tópicos

- [Notificações de integridade](#)
- [Indicadores](#)

Notificações de integridade

Quando você executa seu gateway no VMware vSphere HA, todos os gateways produzem as seguintes notificações de saúde para seu grupo de log configurado da Amazon. CloudWatch Essas notificações entram em um fluxo de log chamado AvailabilityMonitor.

Tópicos

- [Notificação: Reinicializar](#)
- [Notificação: HardReboot](#)
- [Notificação: HealthCheckFailure](#)
- [Notificação: AvailabilityMonitorTest](#)

Notificação: Reinicializar

É possível obter uma notificação de reinicialização quando a VM do gateway é reiniciada. É possível reiniciar a VM de um gateway usando o console VM Hypervisor Management ou o console do Storage Gateway. Também é possível reiniciar usando o software de gateway durante o ciclo de manutenção do gateway.

Medida a ser tomada

Se a hora da reinicialização estiver dentro de 10 minutos da [hora de início da manutenção](#) configurada do gateway, isso provavelmente será uma ocorrência normal e não um sinal de algum problema. Se a reinicialização ocorreu significativamente fora da janela de manutenção, verifique se o gateway foi reiniciado manualmente.

Notificação: HardReboot

Você pode receber uma notificação HardReboot quando a VM do gateway é reiniciada inesperadamente. Essa reinicialização pode ocorrer devido à falta de energia, à uma falha de hardware ou a outro evento. Para gateways do VMware, uma reinicialização pelo High Availability Application Monitoring do vSphere pode acionar esse evento.

Medida a ser tomada

Quando o gateway for executado nesse ambiente, verifique a presença da notificação `HealthCheckFailure` e consulte o log de eventos do VMware da VM.

Notificação: `HealthCheckFailure`

Para um gateway no VMware vSphere HA, você pode receber uma notificação `HealthCheckFailure` quando uma verificação de integridade falha e uma reinicialização da VM é solicitada. Esse evento também ocorre durante um teste para monitorar a disponibilidade, indicado por uma notificação `AvailabilityMonitorTest`. Nesse caso, a notificação `HealthCheckFailure` é esperada.

Note

Esta notificação é apenas para gateways do VMware.

Medida a ser tomada

Se esse evento ocorrer repetidamente sem uma notificação `AvailabilityMonitorTest`, verifique se a infraestrutura da VM está com problemas (armazenamento, memória e assim por diante). Se precisar de assistência adicional, entre em contato AWS Support.

Notificação: `AvailabilityMonitorTest`

Para um gateway no VMware vSphere HA, é possível receber uma notificação de `AvailabilityMonitorTest` ao [executar um teste](#) do sistema de [Disponibilidade e monitoramento de aplicações](#) no VMware.

Indicadores

A métrica `AvailabilityNotifications` está disponível em todos os gateways. Essa métrica é uma contagem do número de notificações de integridade relacionadas à disponibilidade geradas pelo gateway. Use a estatística Sum para observar se o gateway está enfrentando eventos relacionados à disponibilidade. Consulte seu grupo de CloudWatch registros configurado para obter detalhes sobre os eventos.

Práticas recomendadas para a recuperação de dados

Ainda que isso seja raro, o gateway pode enfrentar uma falha irreversível. Essa falha pode ocorrer em sua máquina virtual (VM), no gateway em si, no armazenamento local ou em outro lugar. Se

ocorrer uma falha, é recomendável seguir as instruções apropriadas na seção adiante para recuperar seus dados.

Important

O Storage Gateway não consegue recuperar uma VM do gateway por meio de um snapshot criado pelo hipervisor ou de uma imagem de máquina da Amazon (AMI) do Amazon EC2. Se a VM do gateway apresentar problemas, ative um novo gateway e recupere seus dados para esse gateway usando as instruções a seguir.

Tópicos

- [Como se recuperar de um caso de encerramento inesperado da máquina virtual](#)
- [Como recuperar seus dados de um gateway ou uma VM com falha](#)
- [Como recuperar seus dados de um volume irrecuperável](#)
- [Como recuperar seus dados de um disco de cache com falha](#)
- [Como recuperar seus dados de um sistema de arquivos corrompido](#)
- [Como recuperar seus dados de um datacenter inacessível](#)

Como se recuperar de um caso de encerramento inesperado da máquina virtual

Se sua VM encerrar-se inesperadamente – por exemplo, durante uma queda de energia –, seu gateway ficará inacessível. Quando a energia e a conectividade de rede são restauradas, o gateway fica novamente acessível e começa a funcionar normalmente. Veja a seguir algumas medidas que você pode tomar em momentos como esse para ajudar a recuperar os dados:

- Se uma interrupção provocar problemas de conectividade de rede, é possível solucionar esse problema. Para obter informações sobre como testar a conectividade de rede, consulte [Como testar a conexão de seu gateway com a Internet](#).
- Para configurações de volumes ou , quando seu gateway fica acessível, os volumes ou as entram no status BOOTSTRAPPING. Essa funcionalidade garante que seus dados armazenados localmente continuem a ser sincronizados com AWS. Para obter mais informações sobre esse status, consulte [Noções básicas sobre transições e status de volumes](#).

- Se seu gateway apresentar problemas, e esses problemas ocorrerem com volumes ou fitas em consequência de encerramento inesperado, você poderá recuperar seus dados. Para obter informações sobre como recuperar seus dados, consulte as seções a seguir que se aplicam à sua situação.

Como recuperar seus dados de um gateway ou uma VM com falha

Se o gateway ou a máquina virtual não funcionarem corretamente, você poderá recuperar dados que foram carregados AWS e armazenados em um volume no Amazon S3. Para gateways de volumes armazenados em cache, os dados são recuperados por meio de um snapshot de recuperação. Para gateways de volumes armazenados, é possível recuperar os dados por meio do snapshot do Amazon EBS mais recente do volume. Em gateway de fitas, uma ou mais fitas podem ser recuperadas a partir de um ponto de recuperação para um novo gateway de fitas.

Caso seu gateway de volumes armazenados em cache fique inacessível, você poderá usar as seguintes etapas para recuperar seus dados por meio de um snapshot de recuperação:

1. Em AWS Management Console, escolha o gateway com defeito, escolha o volume que você deseja recuperar e, em seguida, crie um instantâneo de recuperação a partir dele.
2. Implante e ative um novo gateway de volumes. Ou, se você já tiver um gateway de volumes em funcionamento, poderá usar esse gateway para recuperar os dados do volume.
3. Encontre o snapshot que você criou e restaure-o em um novo volume no gateway com falha.
4. Monte o novo volume como um dispositivo iSCSI no servidor de aplicativos local.

Para obter informações detalhadas sobre como recuperar dados de volumes armazenados em cache por meio de um snapshot de recuperação, consulte [O gateway armazenado em cache é inacessível e você deseja recuperar seus dados](#).

Como recuperar seus dados de um volume irrecuperável

Se o status de um volume for IRRECOVERABLE, você não poderá mais usar esse volume.

Para volumes armazenados, é possível recuperar os dados do volume irrecuperável para um novo volume usando as seguintes etapas:

1. Crie um novo volume com o disco que foi usado para criar o volume irrecuperável.
2. Preserve os dados existentes ao criar o novo volume.

3. Exclua todos as tarefas pendentes de snapshot referentes ao volume irrecuperável.
4. Exclua o volume irrecuperável do gateway.

Para volumes armazenados em cache, é recomendável usar o último ponto de recuperação para clonar um novo volume.

Para obter informações detalhadas sobre como recuperar os dados de um volume irrecuperável para um novo volume, consulte [O console informa que seu volume é irrecuperável](#).

Como recuperar seus dados de um disco de cache com falha

Se seu disco de cache encontrar uma falha, é recomendável usar as etapas a seguir para recuperar seus dados, de acordo com sua situação:

- Se a falha ocorreu porque um disco de cache foi removido do host, desligue o gateway, adicione novamente o disco e reinicie o gateway.
- Se o disco de cache estiver corrompido ou inacessível, desligue o gateway, restaure o disco de cache, reconfigure o disco para armazenamento em cache e reinicie o gateway.

Como recuperar seus dados de um sistema de arquivos corrompido

Se o sistema de arquivos for corrompido, você poderá usar o comando **fsck** para buscar erros nele e repará-los. Se conseguir corrigir o sistema de arquivos, você poderá recuperar os dados que se encontram nos volumes do sistema de arquivos, como descrito a seguir:

1. Desligue a máquina virtual e use o Storage Gateway Management Console para criar um snapshot de recuperação. Esse instantâneo representa os dados mais atuais armazenados em AWS.

Note

Você pode usar esse snapshot como fallback se o sistema de arquivos não puder ser reparado ou se o processo de criação de snapshot não puder ser concluído com êxito.

Para obter informações sobre como criar um snapshot de recuperação, consulte [O gateway armazenado em cache é inacessível e você deseja recuperar seus dados](#).

2. Use o comando **fsck** para buscar erros no sistema de arquivos e tentar repará-los.
3. Reinicie a VM do gateway.
4. Quando o host do hipervisor começar a inicializar, pressione e mantenha a tecla Shift pressionada para entrar no menu de inicialização do Grub.
5. No menu, pressione **e** para editar.
6. Escolha a linha do kernel (a segunda linha) e pressione **e** para editar.
7. Anexe a seguinte opção à linha de comando do kernel: **init=/bin/bash**. Use um espaço para separar a opção anterior da opção recém-anexada.
8. Exclua as duas linhas do `console=`, certificando-se de excluir todos os valores após o símbolo `=`, incluindo aqueles separados por vírgulas.
9. Pressione **Return** para salvar as alterações.
10. Pressione **b** para inicializar o computador com a opção de kernel modificado. O computador inicializará para um prompt `bash#`.
11. Insira **`/sbin/fsck -f /dev/sda1`** para executar este comando manualmente no prompt e verificar e reparar seu sistema de arquivos. Se o comando não funcionar com o caminho `/dev/sda1`, será possível usar **`lsblk`** para determinar o dispositivo do sistema de arquivos raiz para `/` e, em vez disso, usar esse caminho.
12. Quando o processo de verificação e reparo do sistema de arquivos se encerrar, reinicie a instância. As configurações do Grub serão revertidas para os valores originais e o gateway inicializará normalmente.
13. Aguarde a conclusão dos snapshots em andamento no gateway original e valide os dados no snapshot.

Você pode continuar a usar o volume original no estado em que se encontra ou pode criar um novo gateway com um novo volume por meio do snapshot de recuperação ou do snapshot concluído. Outra opção é criar um novo volume de qualquer um de seus snapshots concluídos desse volume.

Como recuperar seus dados de um datacenter inacessível

Se o gateway ou datacenter ficar inacessível por algum motivo, é possível recuperar seus dados em um outro gateway em outro datacenter ou recuperar um gateway hospedado em uma instância do Amazon EC2. Se você não tiver acesso a outro datacenter, recomendamos criar o gateway em uma instância do Amazon EC2. As etapas que você segue dependem do tipo de gateway cujos dados você está cobrindo.

Para recuperar dados de um gateway de volumes em um datacenter inacessível

1. Crie e ative um novo gateway de volumes em um host do Amazon EC2. Para ter mais informações, consulte [Como implantar uma instância do Amazon EC2 para hospedar seu gateway de volumes](#).

Note

Os volumes armazenados em gateway não podem ser hospedados na instância Amazon EC2.

2. Crie um novo volume e escolha o gateway do EC2 como gateway de destino. Para ter mais informações, consulte [Como criar um volume](#).

Crie o novo volume baseado em um snapshot ou clone do Amazon EBS do último ponto de recuperação do volume que você deseja recuperar.

Se um volume basear-se em um snapshot, forneça o ID desse snapshot.

Se estiver clonando um volume a partir de um ponto de recuperação, escolha o volume de origem.

Recursos adicionais do Storage Gateway

Esta seção descreve softwares, ferramentas AWS e recursos de terceiros que podem ajudá-lo a configurar ou gerenciar seu gateway, bem como as cotas do Storage Gateway.

Tópicos

- [Configuração do host](#)
- [Gateway de volumes](#)
- [Como obter a chave de ativação para o gateway](#)
- [Como conectar iniciadores iSCSI](#)
- [Usando AWS Direct Connect com o Storage Gateway](#)
- [Requisitos de porta](#)
- [Como conectar seu gateway](#)
- [Como entender os recursos e IDs de recursos do Storage Gateway](#)
- [Como atribuir tags a recursos do Storage Gateway](#)
- [Como trabalhar com componentes de código aberto para o AWS Storage Gateway](#)
- [AWS Storage Gateway cotas](#)

Configuração do host

Tópicos

- [Configurando o VMware para o Storage Gateway](#)
- [Como sincronizar o horário da VM do gateway](#)
- [Como implantar uma instância do Amazon EC2 para hospedar seu gateway de volumes](#)
- [Implantar um Amazon EC2 com configurações padrão](#)
- [Modifique as opções de metadados da instância do Amazon EC2](#)

Configurando o VMware para o Storage Gateway

Ao configurar o VMware para o Storage Gateway, é preciso sincronizar seu tempo de VM com o tempo do host, configurar a VM para usar os controladores de disco paravirtualizados ao provisionar

armazenamento e fornecer proteção contra falhas na camada de infraestrutura subjacente a uma VM do gateway.

Tópicos

- [Como sincronizar o tempo da VM com o tempo do host](#)
- [Configurando a AWS Storage Gateway VM para usar controladores de disco paravirtualizados](#)
- [Como usar o Storage Gateway com o VMware High Availability](#)

Como sincronizar o tempo da VM com o tempo do host

Para conseguir ativar seu gateway, o tempo da VM deve estar sincronizado com tempo do host, que, por sua vez, deve ser definido corretamente. Nesta seção, você primeiro sincronizará o tempo na VM com o tempo do host. Em seguida, verificará o tempo do host e, se necessário, definirá esse tempo e configurará o host para sincronizar seu tempo automaticamente com um servidor Network Time Protocol (NTP).

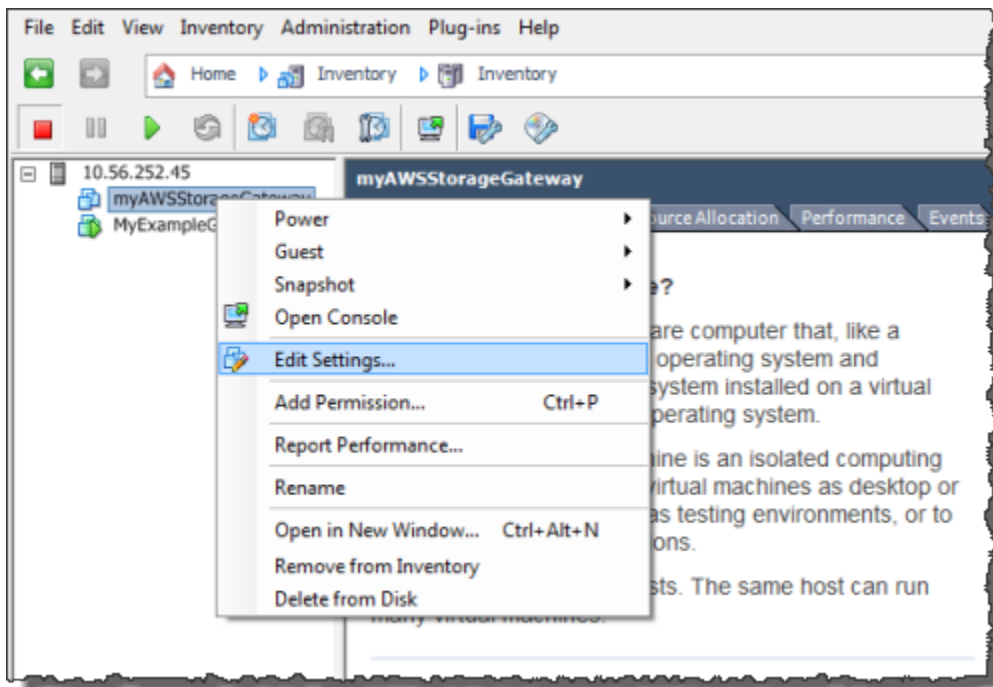
Important

É necessário sincronizar o tempo da VM com o tempo do host para conseguir ativar o gateway.

Para sincronizar o tempo da VM com o tempo do host

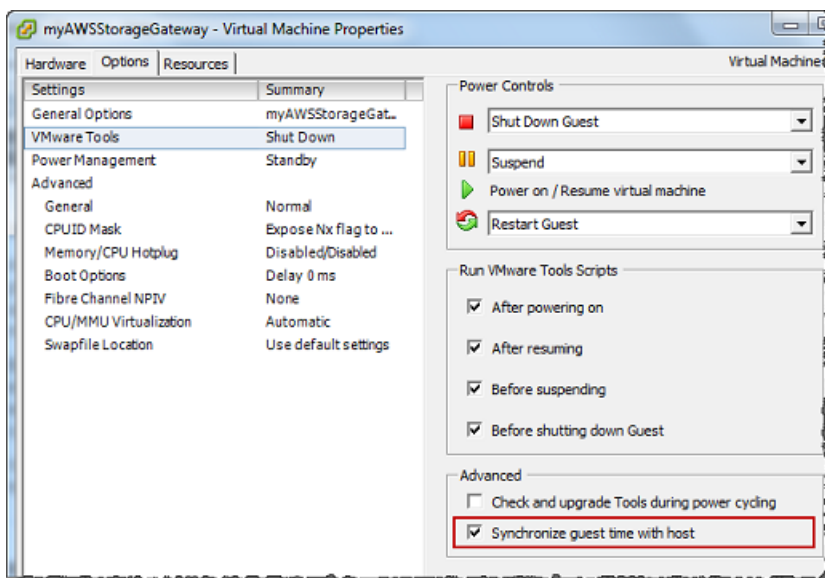
1. Configure o tempo da VM.
 - a. No cliente vSphere, abra o menu de contexto (clique com o botão direito) da VM do gateway e escolha Edit Settings.

A caixa de diálogo Virtual Machine Properties é aberta.



- b. Escolha a guia Options e, em seguida, VMware Tools na lista de opções.
- c. Marque a opção Synchronize guest time with host e escolha OK.

A VM sincroniza seu tempo com o host.

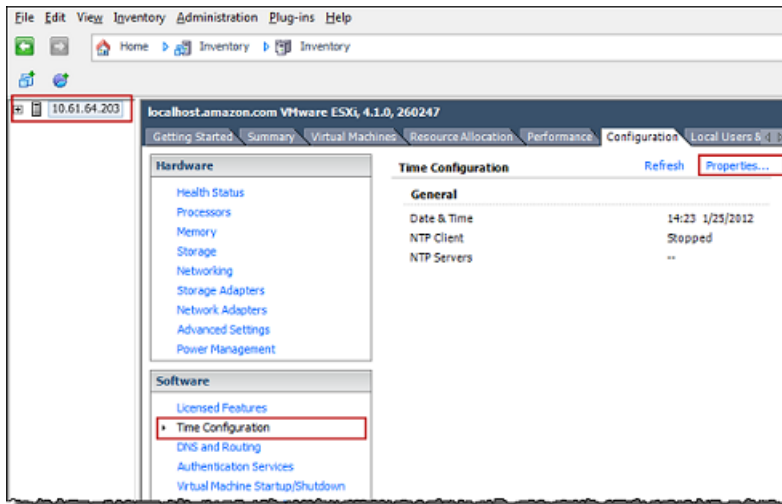


2. Configure o tempo do host.

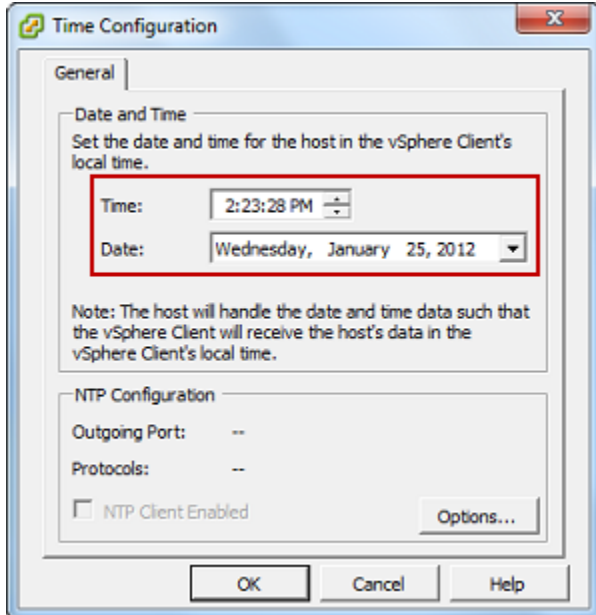
É fundamental definir corretamente o horário do relógio do host. Se você não tiver configurado o relógio do host, execute as etapas a seguir para definir e sincronizá-lo com um servidor NTP.

- a. No cliente VMware vSphere, selecione o nó do host vSphere no painel esquerdo e escolha a guia Configuration.
- b. Selecione Time Configuration no painel Software e escolha o link Properties.

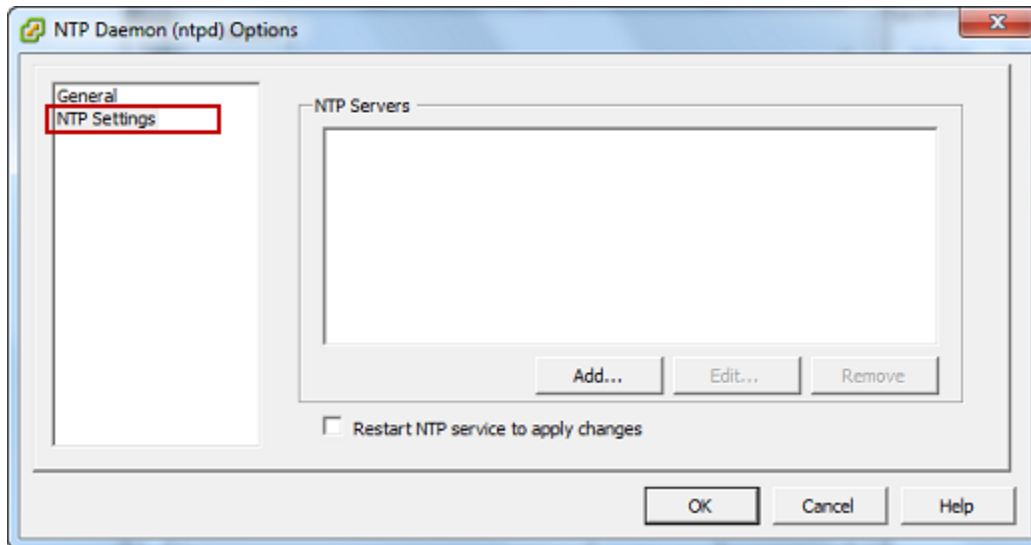
A caixa de diálogo Time Configuration é exibida.



- c. No painel Date and Time, defina a data e hora.

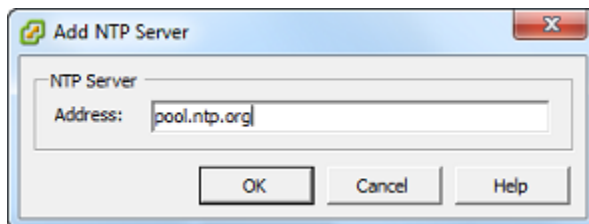


- d. Configure o host para sincronizar seu tempo automaticamente com um servidor NTP.
 - i. Escolha Options na caixa de diálogo Time Configuration e, na caixa de diálogo NTP Daemon (ntpd) Options, escolha NTP Settings, no painel esquerdo.



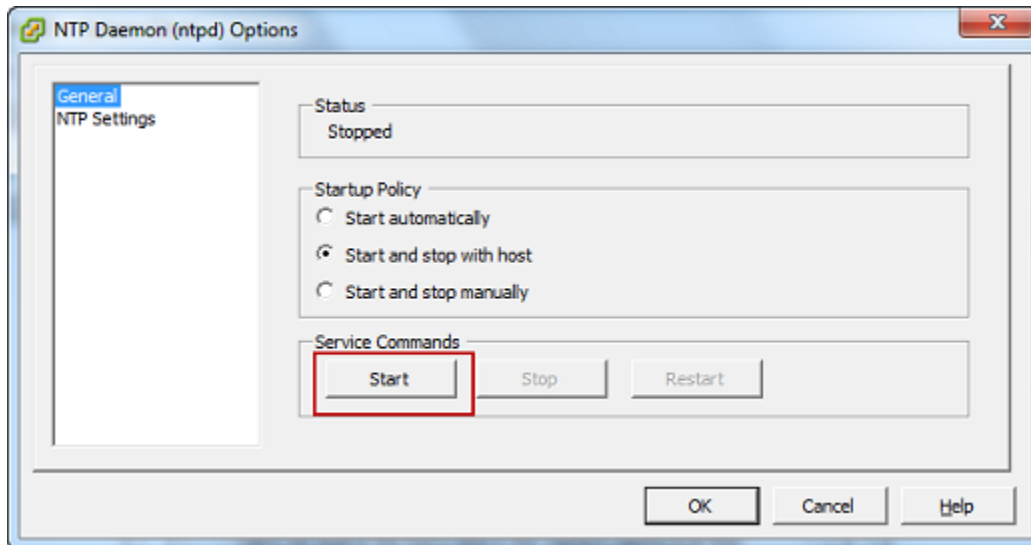
- ii. Escolha Add para adicionar um novo servidor NTP.
- iii. Na caixa de diálogo Add NTP Server, digite o endereço IP ou o nome de domínio completo de um servidor NTP e escolha OK.

Você pode usar `pool.ntp.org`, conforme mostrado no exemplo a seguir.



- iv. Na caixa de diálogo NTP Daemon (ntpd) Options, escolha General, no painel esquerdo.
- v. No painel Service Commands, escolha Start para iniciar o serviço.

Observe que, se alterar essa referência ou adicionar outro servidor NTP posteriormente, precisará reiniciar o serviço para usar o novo servidor.



- e. Escolha OK para fechar a caixa de diálogo NTP Daemon (ntpd) Options.
- f. Escolha OK para fechar a caixa de diálogo Time Configuration.

Configurando a AWS Storage Gateway VM para usar controladores de disco paravirtualizados

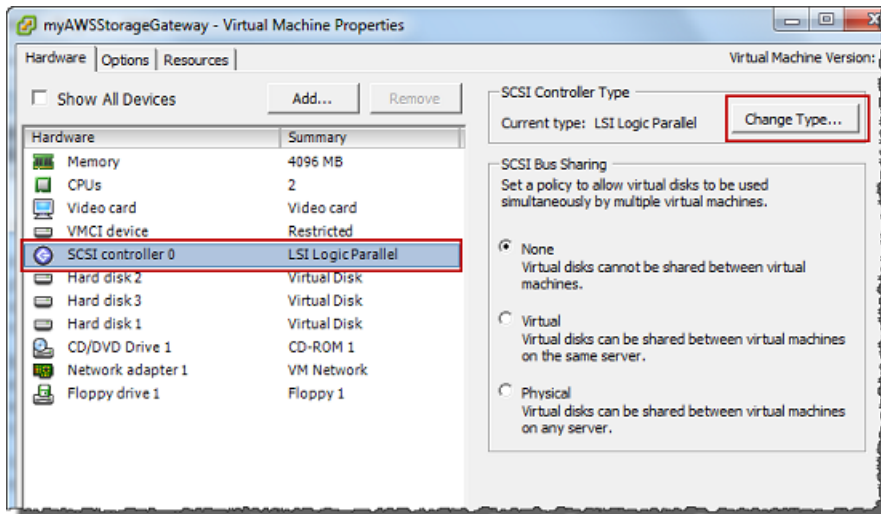
Nessa tarefa, você definirá o controlador iSCSI para que a VM use paravirtualização. Paravirtualização é um modo no qual a VM do gateway funciona com o sistema operacional do host para que o console possa identificar os discos virtuais que você adiciona à sua VM.

Note

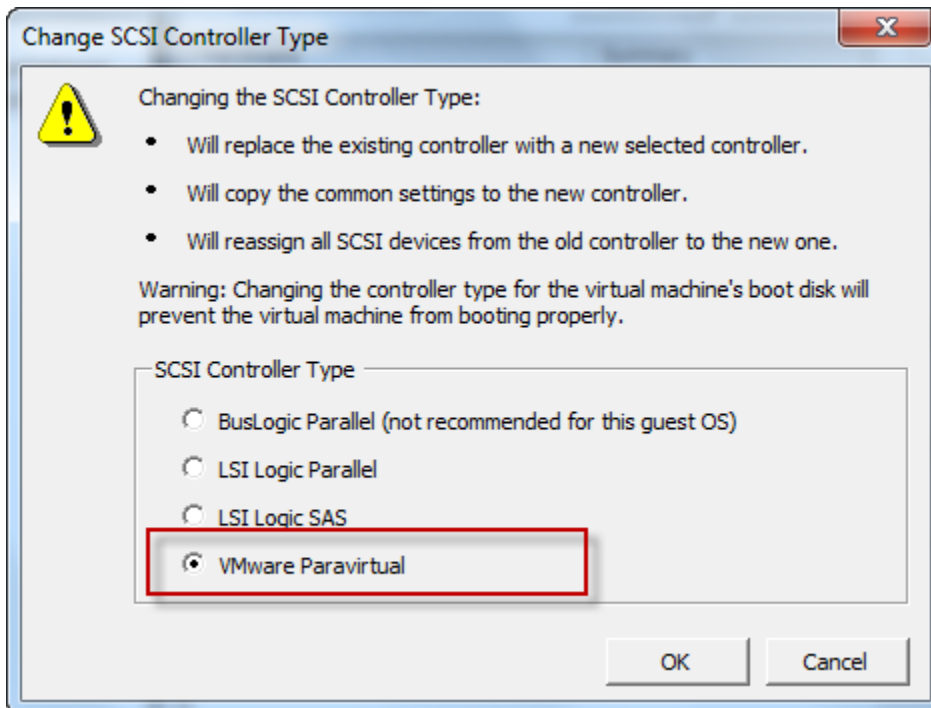
Você deve concluir esta etapa para evitar problemas na identificação desses discos ao configurá-los no console do gateway.

Para configurar sua VM para usar controladores paravirtualizados

1. No cliente VMware vSphere, abra o menu de contexto (clique com o botão direito) da VM do gateway e escolha Edit Settings.
2. Na caixa de diálogo Virtual Machine Properties, escolha a guia Hardware, selecione SCSI controller 0 e escolha Change Type.



3. Na caixa de diálogo Change SCSI Controller Type, selecione o tipo de controlador SCSI VMware Paravirtual e escolha OK.



Como usar o Storage Gateway com o VMware High Availability

O VMware High Availability (HA) é um componente do vSphere que pode fornecer proteção contra falhas na layer de infraestrutura que comporta a máquina virtual do gateway. Para isso, o VMware HA usa vários hosts configurados como cluster. Isso porque, se houver falha em um host que está executando uma VM do gateway, será possível reiniciar automaticamente a VM em outro host dentro

do cluster. Para obter mais informações sobre o VMware HA, consulte [VMware HA: Concepts and Best Practices](#) no site da VMware.

Para usar o Storage Gateway com o VMware HA, é recomendável fazer o seguinte:

- Implante o pacote .ova do VMware ESX, disponível para download, que contém a VM do Storage Gateway em apenas um host em um cluster.
- Ao implantar o pacote .ova, selecione um armazenamento de dados que não seja local em um host. Em vez disso, use um armazenamento de dados acessível a todos os hosts no cluster. Se você selecionar um armazenamento de dados local para um host e o host falhar, a fonte de dados pode ficar inacessível para outros hosts no cluster e o failover para outro host pode não ocorrer.
- Para evitar que o iniciador desconecte-se dos destinos do volume de armazenamento durante o failover, siga as configurações iSCSI recomendadas para seu sistema operacional. Em um evento de failover, a inicialização de uma máquina virtual do gateway em um novo host no cluster de failover pode demorar de alguns segundos a vários minutos. Os limites de tempo iSCSI recomendados para ambos os clientes, Windows e Linux, são superiores ao tempo usualmente necessário para o failover ocorrer. Para obter mais informações sobre como personalizar as configurações de tempo limite de clientes Windows, consulte [Como personalizar as configurações iSCSI do Windows](#). Para obter mais informações sobre como personalizar as configurações de tempo limite de clientes Linux, consulte [Como personalizar suas configurações iSCSI Linux](#).
- Com o processo de clustering, se implantar o pacote .ova para o cluster, selecione um host quando for solicitado a fazê-lo. Outra opção é implantá-lo diretamente no host de um cluster.

Como sincronizar o horário da VM do gateway

Para um gateway implantado no VMware ESXi, configurar o horário do host do hipervisor e sincronizar o horário da VM com o host é suficiente para evitar desvios de horário. Para ter mais informações, consulte [Como sincronizar o tempo da VM com o tempo do host](#). Para um gateway implantado no Microsoft Hyper-V, você deve verificar periodicamente o horário das VMs utilizando o procedimento descrito a seguir.

Como visualizar e sincronizar o horário de uma VM de gateway de hipervisor com um servidor de protocolo de tempo de rede (NTP)

1. Faça login no console local do seu gateway:

- Para obter mais informações sobre o registro em log no console local do VMware ESXi, consulte [Acesso ao console local do gateway com o VMware ESXi](#).
 - Para obter mais informações sobre o registro em log no console local do Microsoft Hyper-V, consulte [Acessar o console local do gateway com o Microsoft Hyper-V](#).
 - Para obter mais informações sobre como fazer login no console local da Linux Kernel-based Virtual Machine (KVM), consulte [Acessar o console local do gateway com o Linux KVM](#).
2. No menu principal Configuração do Storage Gateway), insira **4** para Gestão do horário do sistema.

```
AWS Storage Gateway Configuration
#####
## Currently connected network adapters:
##
## eth0: 10.0.0.45
#####

1: SOCKS Proxy Configuration
2: Network Configuration
3: Test Network Connectivity
4: System Time Management
5: Gateway Console
6: View System Resource Check (0 Errors)

0: Stop AWS Storage Gateway

Press "x" to exit session

Enter command: _
```

3. No menu System Time Management (Gestão do horário do sistema), digite **1** para View and Synchronize System Time (Exibir e sincronizar o horário do sistema).

```
System Time Management

1: View and Synchronize System Time

Press "x" to exit

Enter command: _
```

4. Se o resultado indicar que você deve sincronizar o horário de suas VMs com o horário do NTP, digite **y**. Caso contrário, digite **n**.

Se você digitar **y** para sincronizar, a sincronização poderá durar alguns minutos.

A captura de tela a seguir mostra uma VM que não requer sincronização de horário.

```
System Time Management
1: View and Synchronize System Time
Press "x" to exit
Enter command: 1
Current System Time: Sat Aug 22 00:33:41 UTC 2015
Determining current NTP time (this may take a few seconds ...)
Your Storage Gateway VM system time differs from NTP time
by 0.217617 seconds
A sync is recommended if the time differs by more than 60 seconds
Do you want to sync Storage Gateway VM system time with
NTP time? [y/n]: _
```

A captura de tela a seguir mostra uma VM que requer sincronização de horário.

```
System Time Management
1: View and Synchronize System Time
Press "x" to exit
Enter command: 1
Current System Time: Sat Aug 22 00:33:41 UTC 2015
Determining current NTP time (this may take a few seconds ...)
Your Storage Gateway VM system time differs from NTP time
by 61.217617 seconds
A sync is recommended if the time differs by more than 60 seconds
Do you want to sync Storage Gateway VM system time with
NTP time? [y/n]: _
```

Como implantar uma instância do Amazon EC2 para hospedar seu gateway de volumes

É possível implantar e ativar um e gateway de volumes em uma instância do Amazon Elastic Compute Cloud (Amazon EC2). A Imagem de máquina da Amazon (AMI) do AWS Storage Gateway está disponível como uma AMI de comunidade.

Note

As AMIs de comunidade do Storage Gateway são publicadas e totalmente apoiadas pela AWS. Você pode ver que o editor é AWS um provedor verificado.

As AMIs do Volume Gateway usam a seguinte convenção de nomenclatura. O número da versão anexado ao nome da AMI muda a cada lançamento da versão.

`aws-storage-gateway-CLASSIC-2.9.0`

Para implantar uma instância do Amazon EC2 para hospedar seu gateway de volumes

1. Comece a conectar um novo gateway de fitas usando o console do Storage Gateway. Para obter instruções, consulte [Configurar um gateway de volumes](#). Ao chegar à seção de Opções de plataforma, escolha o Amazon EC2 como a Plataforma host e use as etapas a seguir para iniciar a instância do Amazon EC2 que hospedará o gateway de volumes.

Note

A plataforma host do Amazon EC2 é compatível somente com Volumes em cache. Os gateways de volumes armazenados não podem ser implantados em instâncias do EC2.

2. Escolha Launch instance para abrir o modelo de AWS Storage Gateway AMI no console do Amazon EC2, onde você pode definir configurações adicionais.

Use o Quicklaunch para iniciar a instância do Amazon EC2 com as configurações padrão. Para obter mais informações sobre as especificações padrão do Amazon EC2 Quicklaunch, consulte [Especificações de configuração do Quicklaunch para o Amazon EC2](#).

3. Em Nome, insira um nome para a instância do Amazon EC2. Depois que a instância for implantada, será possível pesquisar esse nome para encontrar sua instância nas páginas de lista no console do Amazon EC2.
4. Em Tipo de instância, na lista Tipo de instância, escolha a configuração de hardware para a instância. A configuração do hardware deve atender a determinados requisitos mínimos para ser compatível com o gateway. É recomendável começar com o tipo de instância m5.xlarge, que atende aos requisitos mínimos de hardware para o gateway funcionar corretamente. Para ter mais informações, consulte [Requisitos para tipos de instância do Amazon EC2](#).

Você pode redimensionar sua instância depois de executá-la, se necessário. Para obter mais informações, consulte [Redimensionar sua instância](#) no Guia do usuário do Amazon EC2.

Note

Alguns tipos de instância, particularmente de i3 do EC2, usam discos SSD NVMe. Isso pode gerar problemas ao iniciar ou interromper um gateway de volumes; por exemplo, dados do cache podem ser perdidos. Monitore a CloudWatch métrica da `CachePercentDirty` Amazon e inicie ou pare seu sistema somente quando esse parâmetro for 0. Para saber mais sobre as métricas de monitoramento do seu gateway, consulte as [métricas e dimensões do Storage Gateway](#) na CloudWatch documentação.

5. Na seção Par de chaves (login), em Nome do par de chaves - obrigatório, selecione o par de chaves que você deseja usar para se conectar à sua instância com segurança. Se necessário, é possível criar um novo par de chaves. Para ter mais informações, consulte [Criar um par de chaves](#) no Guia do usuário do Amazon Elastic Compute Cloud para instâncias do Linux.
6. Na seção Configurações de rede, revise as configurações pré-definidas e escolha Editar para fazer alterações nos seguintes campos:
 - a. Em VPC - obrigatório, escolha a VPC em que você deseja iniciar sua instância do Amazon EC2. Para receber mais informações, consulte [Como funciona a Amazon VPC](#) no Guia do usuário do Amazon Virtual Private Cloud.
 - b. (Opcional) Em Sub-rede, escolha a sub-rede em que você deseja iniciar sua instância do Amazon EC2.
 - c. Para Auto-assign Public IP (Atribuir IP público automaticamente), selecione Permitir.
7. Na subseção Firewall (grupos de segurança), revise as configurações pré-definidas. É possível alterar o nome padrão e a descrição do novo grupo de segurança a ser criado para sua instância do Amazon EC2, se quiser, ou optar por aplicar regras de firewall de um grupo de segurança existente.
8. Na subseção Regras de grupos de segurança de entrada, adicione regras de firewall para abrir as portas que os clientes usarão para se conectar à sua instância. Para obter mais informações sobre as portas necessárias para o gateway de volumes, consulte [Requisitos de porta](#). Para obter mais informações sobre regras de firewall, consulte [Regras de grupo de segurança](#) no Guia do usuário do Amazon Elastic Compute Cloud para instâncias do Linux.

Note

O gateway de volumes exige que a porta TCP 80 esteja aberta para tráfego de entrada e para o acesso HTTP único durante a ativação do gateway. Após a ativação, será possível fechar essa porta.

Além disso, você deve abrir a porta TCP 3260 para acesso ao iSCSI.

9. Na subseção Configuração de rede avançada, revise as configurações pré-definidas e faça alterações, se necessário.
10. Na seção Configurar armazenamento, escolha Adicionar novo volume para adicionar armazenamento à instância do gateway.

Important

Deve ser adicionado pelo menos um volume do Amazon EBS com pelo menos 165 GiB de capacidade para o armazenamento em cache e pelo menos um volume do Amazon EBS com pelo menos 150 GiB de capacidade para buffer de upload, além do volume raiz pré-configurado. Para aumentar o desempenho, recomendamos alocar vários volumes do EBS para armazenamento em cache com pelo menos 150 GiB cada.

11. Na seção Detalhes avançados, revise as configurações pré-definidas e faça alterações, se necessário.
12. Escolha Iniciar instância para iniciar a nova instância de gateway do Amazon EC2 com as configurações definidas.
13. Para verificar se sua nova instância foi executada com sucesso, navegue até a página Instâncias no console do Amazon EC2 e pesquise a nova instância pelo nome. Certifique-se de que o estado da instância exiba Executando com uma marca de seleção verde e que a verificação de status esteja concluída e mostre uma marca de seleção verde.
14. Selecione sua instância na página de detalhes. Copie o endereço IPv4 público da seção Resumo da instância e retorne à página Configurar gateway no console do Storage Gateway para continuar a configuração do gateway de volumes.

Você pode determinar o AMI ID a ser usado para iniciar um Gateway usando o console do Storage Gateway ou consultando o repositório de AWS Systems Manager parâmetros.

Para determinar o ID da AMI, execute uma das seguintes ações:

- Comece a conectar um novo gateway de fitas usando o console do Storage Gateway. Para obter instruções, consulte [Configurar um gateway de volumes](#). Ao chegar à seção Opções de plataforma, escolha Amazon EC2 como plataforma Host e, em seguida, escolha Launch instance para abrir o modelo de AWS Storage Gateway AMI no console do Amazon EC2.

Você é redirecionado para a página da AMI da comunidade EC2, onde pode ver o ID da AMI AWS da sua região na URL.

- Consulte o repositório de parâmetros do Systems Manager. Você pode usar a API AWS CLI ou Storage Gateway para consultar o parâmetro público do Systems Manager no namespace `/aws/service/storagegateway/ami/CACHED/latest` para gateways de volume em cache ou `/aws/service/storagegateway/ami/STORED/latest` para gateways de volume armazenados. Por exemplo, o uso do comando CLI a seguir retorna o ID da AMI atual no Região da AWS que você especificar.

```
aws --region us-east-2 ssm get-parameter --name /aws/service/storagegateway/ami/STORED/latest
```

O comando da CLI retorna uma saída semelhante à seguinte:

```
{
  "Parameter": {
    "Type": "String",
    "LastModifiedDate": 1561054105.083,
    "Version": 4,
    "ARN": "arn:aws:ssm:us-east-2::parameter/aws/service/storagegateway/ami/STORED/latest",
    "Name": "/aws/service/storagegateway/ami/STORED/latest",
    "Value": "ami-123c45dd67d891000"
  }
}
```

Implantar um Amazon EC2 com configurações padrão

Este tópico lista as etapas para implantar um host Amazon EC2 usando as especificações padrão.

É possível implantar e ativar um e gateway de volumes em uma instância do Amazon Elastic Compute Cloud (Amazon EC2). A imagem de máquina da Amazon (AMI) do AWS Storage Gateway está disponível como uma AMI de comunidade.

Note

As AMIs de comunidade do Storage Gateway são publicadas e totalmente apoiadas pela AWS. Você pode ver que o editor é AWS um provedor verificado.

1. Para configurar a instância do Amazon EC2, escolha Amazon EC2 como a plataforma Host na seção Opções de plataforma do fluxo de trabalho. Para obter instruções sobre como configurar a instância do Amazon EC2, consulte [Como implantar uma instância do Amazon EC2 para hospedar seu gateway de volumes](#).
2. Selecione Launch instance para abrir o modelo de AMI do AWS Storage Gateway no console do Amazon EC2 e personalizar configurações adicionais, como tipos de instância, configurações de rede e Configurar armazenamento.
3. Opcionalmente, é possível selecionar Usar configurações padrão no console do Storage Gateway para implantar uma instância do Amazon EC2 com a configuração padrão.

A instância do Amazon EC2 criada por Usar configurações padrão tem as seguintes especificações padrão:

- Tipo de instância: m5.xlarge
- Configurações de rede
 - Em VPC, selecione a VPC na qual você deseja que sua instância do EC2 seja executada.
 - Em Sub-rede, especifique a sub-rede na qual sua instância do EC2 deve ser executada.

Note

As sub-redes da VPC aparecerão no menu suspenso somente se tiverem a configuração de atribuição automática de endereço IPv4 público ativada no console de gerenciamento da VPC.

- Atribuição automática de IP público: ativada

Um grupo de segurança do EC2 é criado e associado à instância do EC2. O grupo de segurança tem as seguintes regras de porta de entrada:

Note

Será preciso ter a porta 80 aberta durante a ativação do gateway. A porta é fechada imediatamente após a ativação. Depois disso, sua instância do EC2 só pode ser acessada pelas outras portas da VPC selecionada.

Os destinos iSCSI em seu gateway só podem ser acessados a partir dos hosts na mesma VPC do gateway. Se os destinos iSCSI precisarem ser acessados de hosts fora da VPC, você deverá atualizar as regras de grupo de segurança adequadas. É possível editar grupos de segurança a qualquer momento navegando até a página de detalhes da instância do Amazon EC2, selecionando Segurança, navegando até Detalhes do grupo de segurança e escolhendo o ID do grupo de segurança.

Porta	Protocolo	Protocolo do sistema de arquivos				
80	TCP	Acesso HTTP para ativação				
3260	TCP	iSCSI				

- Configurar armazenamento

Configurações padrão	Volume do dispositivo raiz da AMI	Cache do volume 2	Cache do volume 2			
Nome do dispositivo		'/dev/sdb'	'/dev/sdc'			

Configurações padrão	Volume do dispositivo raiz da AMI	Cache do volume 2	Cache do volume 2			
Tamanho	80 GiB	165 GiB	150 GiB			
Tipo de volume	gp3	gp3	gp3			
IOPS	3000	3000	3000			
Excluir no encerramento	Sim	Sim	Sim			
Criptografado	Não	Não	Não			
Throughput	125	125	125			

Modifique as opções de metadados da instância do Amazon EC2

O serviço de metadados da instância (IMDS) é um componente na instância que fornece acesso seguro aos metadados da instância do Amazon EC2. Uma instância pode ser configurada para aceitar solicitações de metadados recebidas que usam o IMDS versão 1 (IMDSv1) ou exigir que todas as solicitações de metadados usem o IMDS versão 2 (IMDSv2). O IMDSv2 usa solicitações orientadas para sessão e mitiga vários tipos de vulnerabilidades que podem ser usadas para tentar acessar o IMDS. Para obter informações sobre o IMDSv2, consulte [Como funciona o Instance Metadata Service versão 2 no Guia do usuário do Amazon Elastic Compute Cloud](#).

Recomendamos que você exija o IMDSv2 para todas as instâncias do Amazon EC2 que hospedam o Storage Gateway. O IMDSv2 é exigido por padrão em todas as instâncias de gateway recém-lançadas. Se você tem instâncias existentes que ainda estão configuradas para aceitar solicitações de metadados do IMDSv1, consulte [Exigir o uso do IMDSv2 no Guia do usuário do Amazon Elastic Compute Cloud para obter instruções sobre como modificar as opções de metadados da sua](#)

[instância para exigir](#) o uso do IMDSv2. A aplicação dessa alteração não exige a reinicialização da instância.

Gateway de volumes

Tópicos

- [Como remover discos de seu gateway](#)
- [Como adicionar e remover volumes do Amazon EBS para um gateway hospedado no Amazon EC2.](#)

Como remover discos de seu gateway

Embora não seja recomendável remover discos subjacentes de seu gateway, você pode remover um disco de seu gateway, por exemplo, se tiver uma falha de disco.

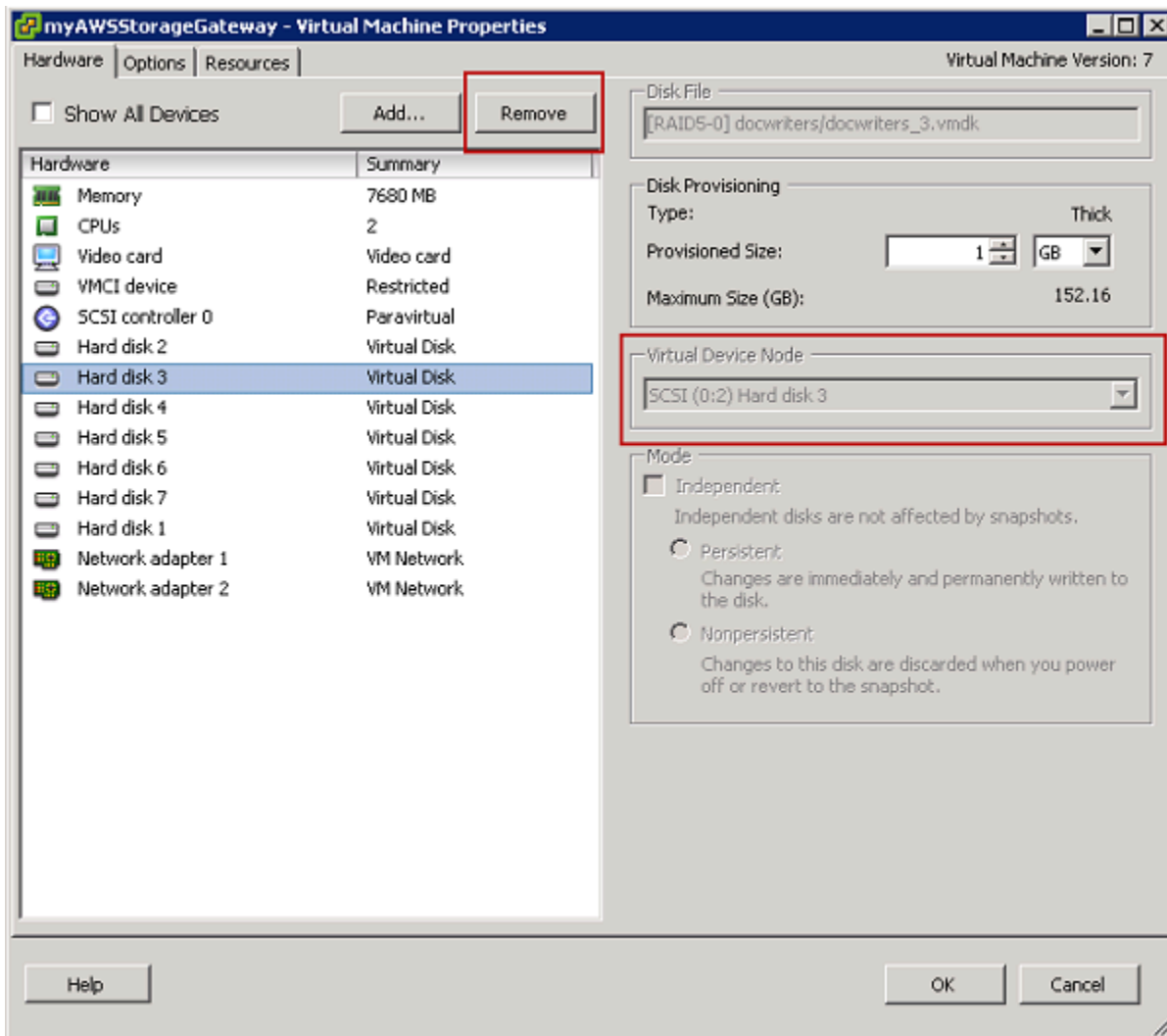
Como remover um disco de um gateway hospedado no VMware ESXi

Você pode usar o procedimento a seguir para remover um disco de seu gateway hospedado no hipervisor VMware.

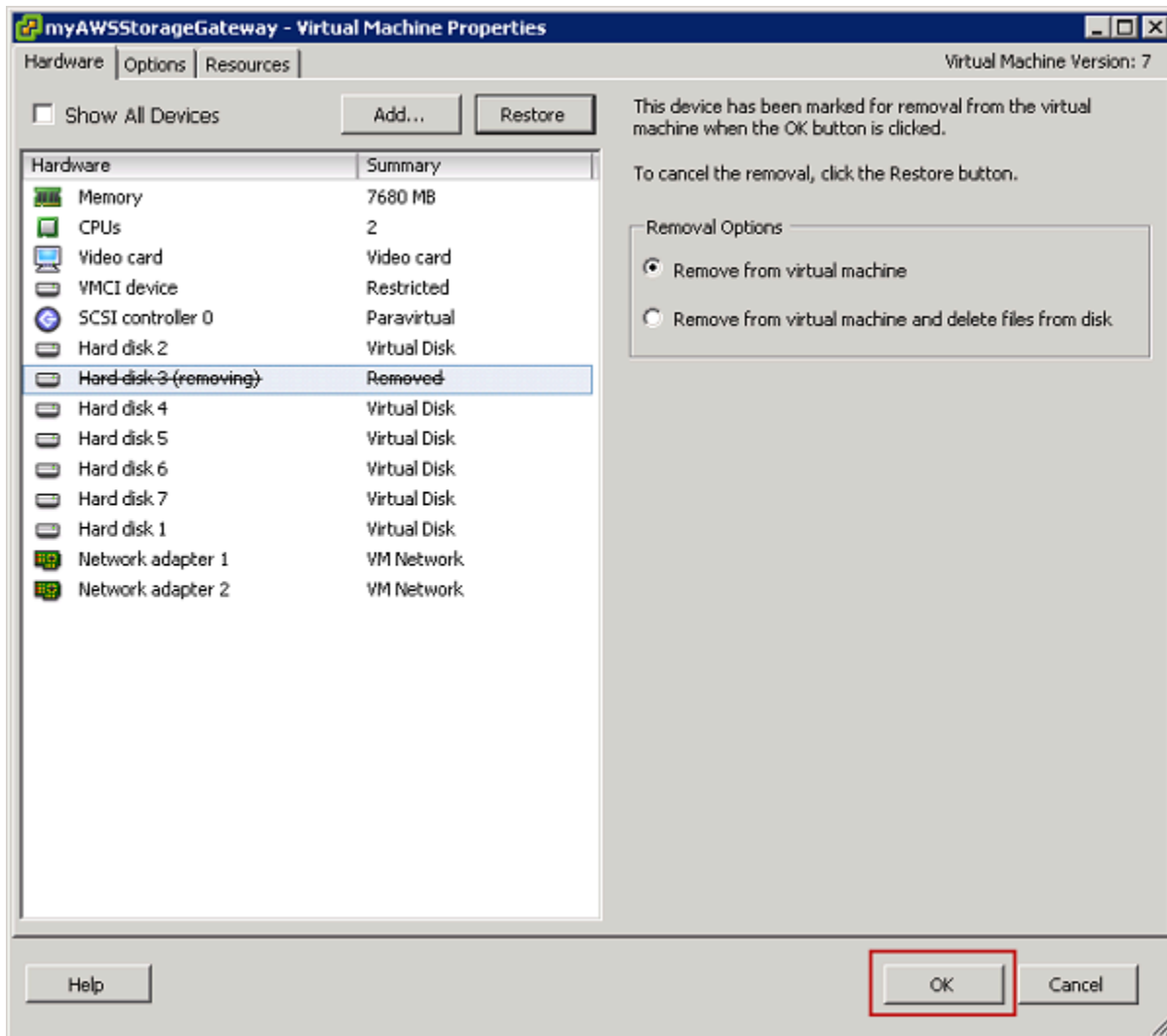
Para remover um disco alocado ao upload de buffer (VMware ESXi)

1. No cliente vSphere, abra o menu de contexto (clique com o botão direito do mouse) e escolha o nome da VM do gateway e em seguida Edit Settings.
2. Na guia Hardware da caixa de diálogo Virtual Machine Properties, selecione o disco reservado como espaço do buffer de upload e escolha Remove.

Verifique se o valor Virtual Device Node na caixa de diálogo Virtual Machine Properties é igual ao valor que você anotou anteriormente. Isso ajuda a garantir a remoção do disco correto.



3. Escolha uma opção no painel Removal Options e escolha OK para concluir o processo de remoção do disco.



Como remover um disco de um gateway hospedado no Microsoft Hyper-V

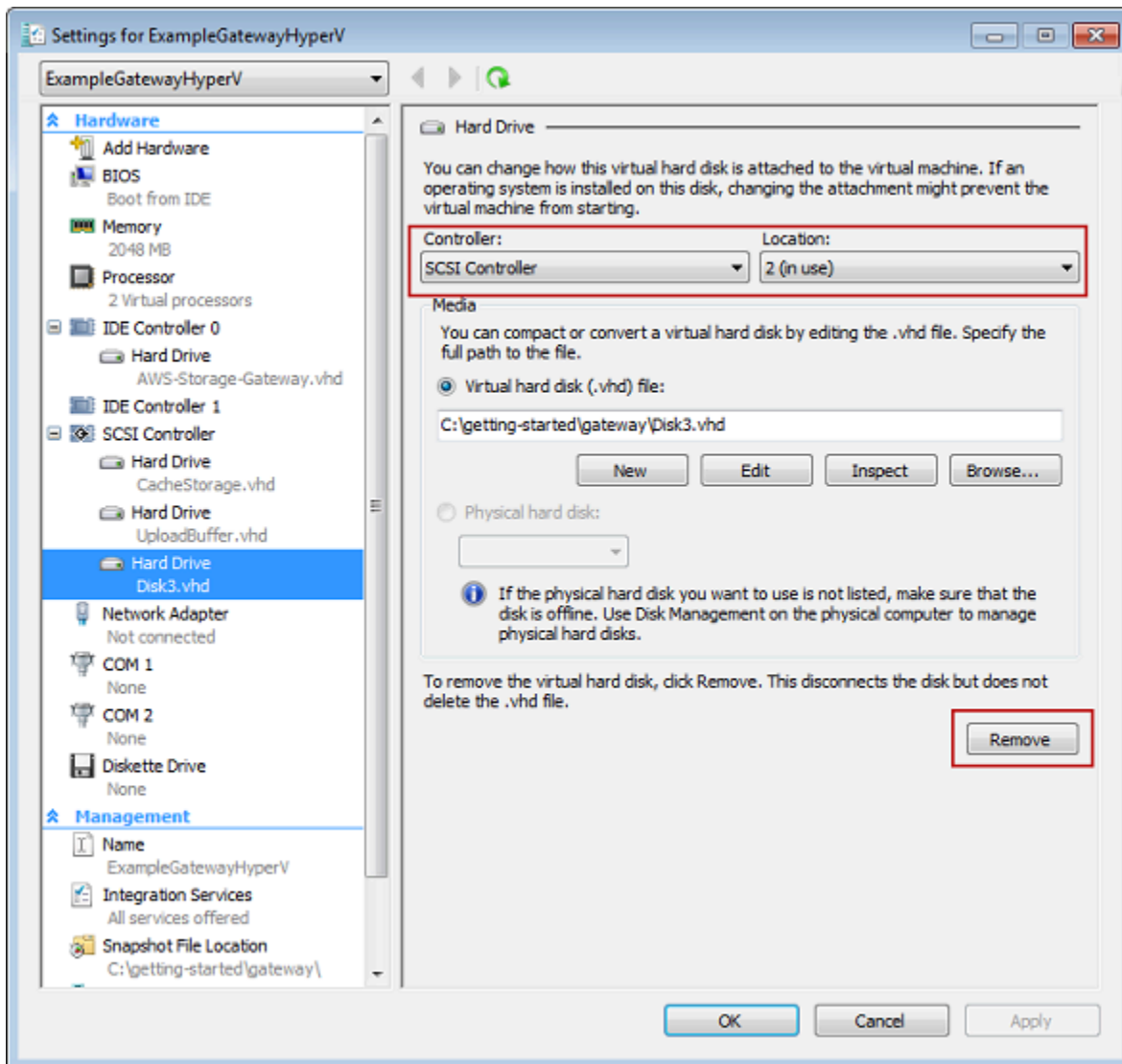
Por meio do procedimento a seguir, você pode remover um disco de seu gateway hospedado em um hipervisor Microsoft Hyper-V.

Para remover um disco subjacente alocado ao buffer de upload (Microsoft Hyper-V)

1. No Microsoft Hyper-V Manager, abra o menu de contexto (clique com o botão direito do mouse) e escolha o nome da VM do gateway e em seguida Settings.
2. Na lista Hardware da caixa de diálogo Settings, selecione o disco a ser removido e escolha Remove.

Os discos que você adiciona a um gateway aparecem na entrada SCSI Controller na lista Hardware. Verifique se os valores em Controller e Location são iguais ao valor que você anotou anteriormente. Isso ajuda a garantir a remoção do disco correto.

O primeiro controlador SCSI exibido no Microsoft Hyper-V Manager é controlador 0.



3. Escolha OK para aplicar a alteração.

Remover um disco de um gateway hospedado no Linux KVM

Para desanexar um disco do gateway hospedado no hipervisor de Linux Kernel-based Virtual Machine (KVM), é possível usar um comando `virsh` semelhante ao seguinte.

```
$ virsh detach-disk domain_name /device/path
```

Para obter mais detalhes sobre como gerenciar discos da KVM, consulte a documentação da sua distribuição do Linux.

Como adicionar e remover volumes do Amazon EBS para um gateway hospedado no Amazon EC2.

Ao configurar inicialmente seu gateway para ser executado como uma instância do Amazon EC2, você reservou volumes do Amazon EBS para uso como buffer de upload e armazenamento em cache. Com o passar do tempo, quando as necessidades de sua aplicação mudarem, é possível reservar mais volumes do Amazon EBS para esse uso. Também é possível reduzir o armazenamento reservado removendo volumes do Amazon EBS alocados anteriormente. Para obter mais informações sobre o Amazon EBS, consulte [Amazon Elastic Block Store \(Amazon EBS\) no Guia do usuário do Amazon EC2](#).

Antes de ampliar o armazenamento do gateway, você deve analisar de que forma precisa dimensionar o buffer de upload e o armazenamento em cache de acordo com as necessidades de seu aplicativo com relação a um gateway. Para fazer isso, consulte [Como determinar o tamanho do buffer de upload para alocar](#) e [Como determinar o tamanho do armazenamento em cache para alocar](#).


Não há cotas para o armazenamento máximo que você pode alocar como buffer de upload e armazenamento em cache. É possível anexar quantos volumes do Amazon EBS desejar à sua instância, mas só é possível configurar esses volumes como buffer de upload e espaço de armazenamento em cache de acordo com essas cotas de armazenamento. Para ter mais informações, consulte [AWS Storage Gateway cotas](#).

Para adicionar um volume do Amazon EBS e configurá-lo para o gateway

1. Crie um volume do Amazon EBS. Para obter instruções, consulte [Como criar ou restaurar um volume do Amazon EBS no Guia do usuário do Amazon EC2](#).
2. Anexe o volume do Amazon EBS à instância do Amazon EC2. Para obter instruções, consulte [Como anexar um volume do Amazon EBS a uma instância no Guia do usuário do Amazon EC2](#).
3. Configure o volume do Amazon EBS que você adicionou como um buffer de upload ou armazenamento em cache. Para obter instruções, consulte [Como gerenciar discos locais para o Storage Gateway](#).

Pode ser que em algum momento você conclua que não precisa do espaço de armazenamento alocado no buffer de upload.

Para remover um volume do Amazon EBS


 Warning

Estas etapas se aplicam somente aos volumes do Amazon EBS alocados como espaço de buffer de upload, não aos volumes alocados ao cache..

1. Encerre o gateway seguindo o procedimento descrito na seção [Encerramento da VM do gateway](#).
2. Separe os volumes do Amazon EBS da instância do Amazon EC2. Para obter instruções, consulte [Separar um volume do Amazon EBS de uma instância no Guia](#) do usuário do Amazon EC2.
3. Exclua o volume do Amazon EBS. Para obter instruções, consulte [Excluir um volume do Amazon EBS no Guia](#) do usuário do Amazon EC2.
4. Inicie o gateway seguindo o procedimento descrito na seção [Encerramento da VM do gateway](#).

Como obter a chave de ativação para o gateway

Para receber uma chave de ativação para seu gateway, faça uma solicitação pela web para a máquina virtual (VM) do gateway. A VM retorna um redirecionamento que contém a chave de ativação, que é passada como um dos parâmetros da ação `ActivateGateway` da API para especificar a configuração do seu gateway. Para obter mais informações, consulte [ActivateGateway](#) na Referência da API do Storage Gateway.

 Note

Se não forem usadas, as chaves de ativação do gateway expiram em 30 minutos.

A solicitação que você faz à VM do gateway inclui a AWS região em que a ativação ocorre. O URL que é retornado pelo redirecionamento na resposta contém um parâmetro de string de consulta denominado `activationkey`. Esse parâmetro de string de consulta é a sua chave de ativação. O formato da string de consulta é semelhante ao seguinte: `http://gateway_ip_address/?`

activationRegion=*activation_region*. A saída dessa consulta retorna a região de ativação e a chave.

O URL também inclui vpcEndpoint o ID do endpoint da VPC para gateways que se conectam usando o tipo de endpoint da VPC.

Note

O dispositivo de hardware do Storage Gateway, os modelos de imagem de VM e as imagens de máquina da Amazon (AMI) do Amazon EC2 vêm pré-configurados com os serviços HTTP necessários para receber e responder às solicitações da web descritas nesta página. Não é necessário nem recomendado instalar nenhum serviço adicional em seu gateway.

Tópicos

- [Linux \(curl\)](#)
- [Linux \(bash/zsh\)](#)
- [Microsoft Windows PowerShell](#)
- [Como usar seu console local](#)

Linux (curl)

Os exemplos a seguir mostram como obter uma chave de ativação com o Linux (curl).

Note

Substitua as variáveis destacadas por valores reais para o gateway. Os valores aceitáveis são os seguintes:

- *gateway_ip_address*: o endereço IPv4 do seu gateway, por exemplo, 172.31.29.201
- *gateway_type* - O tipo de gateway que você deseja ativar, como, STORED, CACHEDVTL, FILE_S3 ou. FILE_FSX_SMB
- *region_code*: a região em que você deseja ativar seu gateway. Consulte os [endpoints regionais](#) no Guia de referência geral da AWS . Se esse parâmetro não for especificado ou se o valor fornecido estiver escrito incorretamente ou não corresponder a uma região válida, o comando usará a região como padrão. us-east-1

- ***vpc_endpoint***: o nome do endpoint da VPC para seu gateway, por exemplo, `vpce-050f90485f28f2fd0-iep0e8vq.storagegateway.us-west-2.vpce.amazonaws.com`.

Para obter a chave de ativação de um endpoint público:

```
curl "http://gateway_ip_address?activationRegion=region_code&no_redirect"
```

Para obter a chave de ativação de um endpoint da VPC:

```
curl "http://gateway_ip_address?  
activationRegion=region_code&vpcEndpoint=vpc_endpoint&no_redirect"
```

Linux (bash/zsh)

O exemplo a seguir mostra como usar o Linux (bash/zsh) para buscar a resposta HTTP, analisar cabeçalhos HTTP e obter a chave de ativação.

```
function get-activation-key() {  
  local ip_address=$1  
  local activation_region=$2  
  if [[ -z "$ip_address" || -z "$activation_region" || -z "$gateway_type" ]]; then  
    echo "Usage: get-activation-key ip_address activation_region gateway_type"  
    return 1  
  fi  
  
  if redirect_url=$(curl -f -s -S -w '%{redirect_url}' "http://$ip_address/?  
activationRegion=$activation_region&gatewayType=$gateway_type"); then  
    activation_key_param=$(echo "$redirect_url" | grep -oE 'activationKey=[A-Z0-9-]+')  
    echo "$activation_key_param" | cut -f2 -d=  
  else  
    return 1  
  fi  
}
```

Microsoft Windows PowerShell

O exemplo a seguir mostra como usar o Microsoft Windows PowerShell para buscar a resposta HTTP, analisar cabeçalhos HTTP e obter a chave de ativação.

```
function Get-ActivationKey {
    [CmdletBinding()]
    Param(
        [parameter(Mandatory=$true)][string]$IpAddress,
        [parameter(Mandatory=$true)][string]$ActivationRegion,
        [parameter(Mandatory=$true)][string]$GatewayType
    )
    PROCESS {
        $request = Invoke-WebRequest -UseBasicParsing -Uri "http://$IpAddress/?
activationRegion=$ActivationRegion&gatewayType=$GatewayType" -MaximumRedirection 0 -
ErrorAction SilentlyContinue
        if ($request) {
            $activationKeyParam = $request.Headers.Location | Select-String -Pattern
"activationKey=([A-Z0-9-]+)"
            $activationKeyParam.Matches.Value.Split("=")[1]
        }
    }
}
```

Como usar seu console local

Os exemplos a seguir mostram como usar o console local para gerar e exibir uma chave de ativação.

Para obter uma chave de ativação para o gateway do seu console local

1. Faça login no console local. Se você estiver se conectando à instância do Amazon EC2 em um computador Windows, faça login como administrador.
2. Depois de fazer login e ver o menu principal de Ativação de dispositivos da AWS : configuração, selecione 0 para escolher Obter chave de ativação.
3. Selecione Storage Gateway para a opção da família de gateways.
4. Quando solicitado, insira a AWS região em que você deseja ativar seu gateway.
5. Insira 1 para pública ou 2 para um endpoint da VPC como o tipo de rede.
6. Insira 1 para padrão ou 2 para FIPS (Padrões Federais de Processamento de Informações) como o tipo de endpoint.

Como conectar iniciadores iSCSI

Ao gerenciar seu gateway, você trabalha com volumes ou dispositivos da biblioteca de fitas virtuais (VTL) expostos como destinos Internet Small Computer System Interface (iSCSI). Em gateways de volumes, os destinos iSCSI são volumes. Em gateways de fitas, os destinos são dispositivos de VTL. Como parte deste trabalho, você executará tarefas como se conectar a esses destinos, personalizar as configurações de iSCSI, conectar-se a um cliente Red Hat Linux e configurar o Challenge Handshake Authentication Protocol (CHAP).

Tópicos

- [Como conectar volumes a um cliente Windows](#)
- [Como conectar volumes ou dispositivos de VTL a um cliente Linux](#)
- [Como personalizar as configurações iSCSI](#)
- [Como configurar a autenticação CHAP para destinos iSCSI](#)

O padrão iSCSI é um padrão de rede de armazenamento baseado no protocolo de Internet (IP) para iniciar e gerenciar conexões baseadas em IP entre dispositivos de armazenamento e clientes. A lista a seguir define alguns dos termos usados para descrever a conexão iSCSI e os componentes envolvidos.

Iniciador iSCSI

O componente cliente de uma rede iSCSI. O iniciador envia solicitações ao destino iSCSI. Os iniciadores podem ser implementados em software ou hardware. O Storage Gateway é compatível somente com iniciadores de software.

Destino iSCSI

O componente de servidor da rede iSCSI que recebe e responde a solicitações de iniciadores. Todo volume é exposto como um destino de iSCSI. Conecte apenas um iniciador iSCSI a cada destino iSCSI.

Iniciador iSCSI da Microsoft

O programa de software em computadores Microsoft Windows que permite que você conecte um computador cliente (ou seja, o computador que executa a aplicação cujos dados você deseja gravar no gateway) a uma matriz externa e baseado em iSCSI (ou seja, o gateway). A conexão é feita por meio do adaptador de rede Ethernet do computador host. O iniciador do Microsoft

iSCSI foi validado com o Storage Gateway no Windows 8.1, Windows 10, Windows Server 2012 R2, Windows Server 2016 e Windows Server 2019. O iniciador é incorporado a esses sistemas operacionais.

Iniciador iSCSI da Red Hat

O pacote Resource Package Manager (RPM) do `iscsi-initiator-utils` fornece um iniciador iSCSI implementado em software para o Red Hat Linux. Esse pacote inclui um daemon de servidor para o protocolo iSCSI.

Todo tipo de gateway pode se conectar a dispositivos iSCSI, e você pode personalizar essas conexões como descrito a seguir.

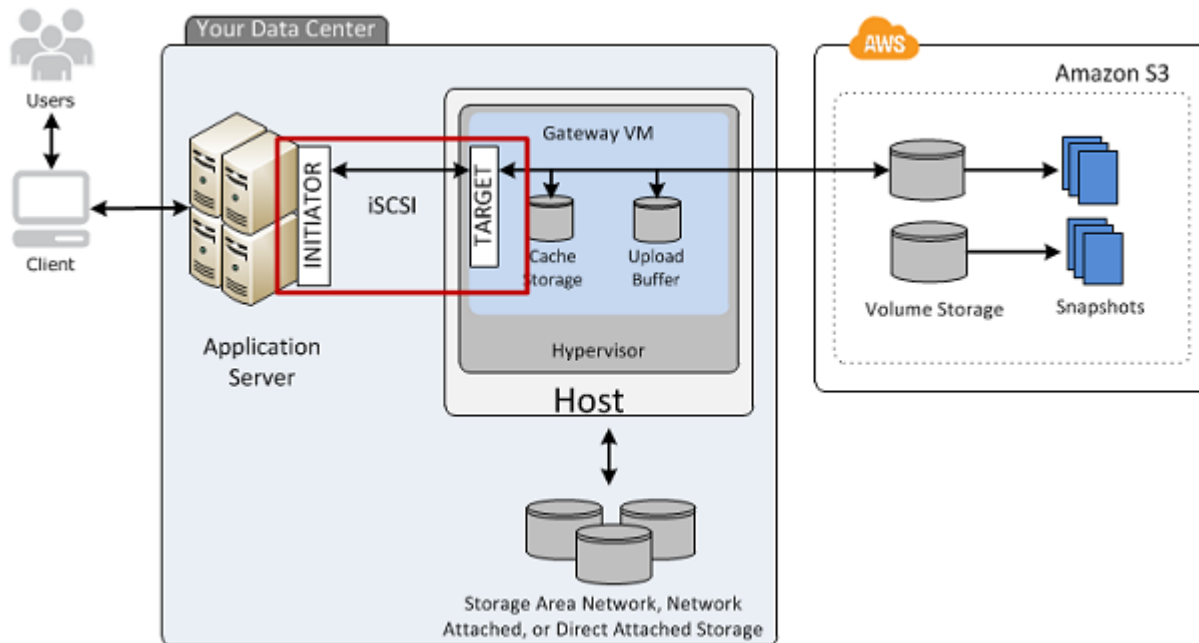
Como conectar volumes a um cliente Windows

Um Gateway de Volumes expõe os volumes que você criou para o gateway, como destinos iSCSI. Para ter mais informações, consulte [Como conectar volumes ao cliente](#).

Note

Para se conectar ao destino do volume, seu gateway deve ter um buffer de upload configurado. Se não houver um buffer de upload configurado para seu gateway, o status de seus volumes será exibido como `UPLOAD BUFFER NOT CONFIGURED`. Para configurar um buffer de upload para um gateway em uma configuração de volumes armazenados, consulte [Para configurar um buffer de upload ou armazenamento em cache adicionais para o gateway](#). Para configurar um buffer de upload para um gateway em uma configuração de volumes armazenados em cache, consulte [Para configurar um buffer de upload ou armazenamento em cache adicionais para o gateway](#).

O diagrama a seguir destaca o destino iSCSI no contexto mais amplo da arquitetura do Storage Gateway. Para ter mais informações, consulte [Como funciona o gateway de volumes \(arquitetura\)](#).



Você pode se conectar a um volume em um cliente Windows ou Red Hat Linux. Opcionalmente, você pode configurar o CHAP para ambos os tipos de cliente.

Seu gateway expõe o volume como um destino de iSCSI com um nome especificado por você, precedido de `iqn.1997-05.com.amazon:`. Por exemplo, se você especificar um nome de destino `myvolume`, o destino iSCSI que você usará para se conectar ao volume será `iqn.1997-05.com.amazon:myvolume`. Para obter mais informações sobre como configurar seus aplicativos para montar volumes em iSCSI, consulte [Como conectar volumes a um cliente Windows](#).

Para	Consulte
Conecte-se a um volume no Windows.	Como se conectar ao cliente Microsoft Windows
Conecte-se a um volume no Red Hat Linux.	Como se conectar ao cliente Red Hat Enterprise Linux
Configure a autenticação CHAP para Windows e Red Hat Linux.	Como configurar a autenticação CHAP para destinos iSCSI

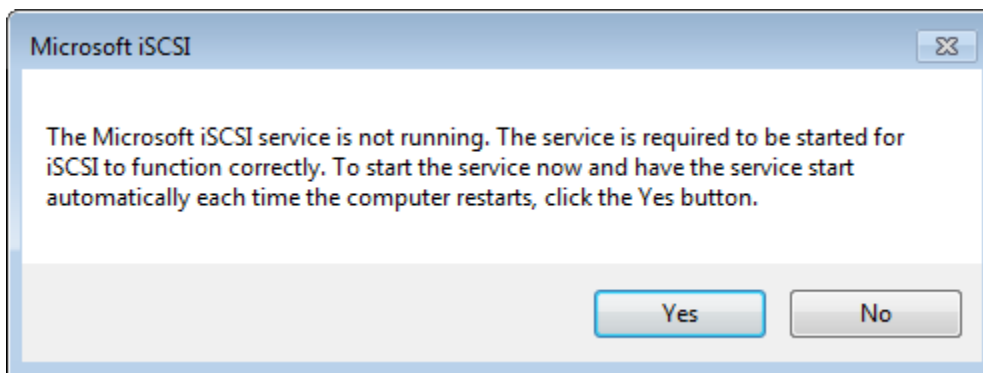
Como conectar um volume de armazenamento ao cliente Windows

1. No menu Iniciar do computador do cliente Windows, insira **iscsicpl.exe** na caixa Pesquisar programas e arquivos, localize o programa iniciador iSCSI e execute-o.

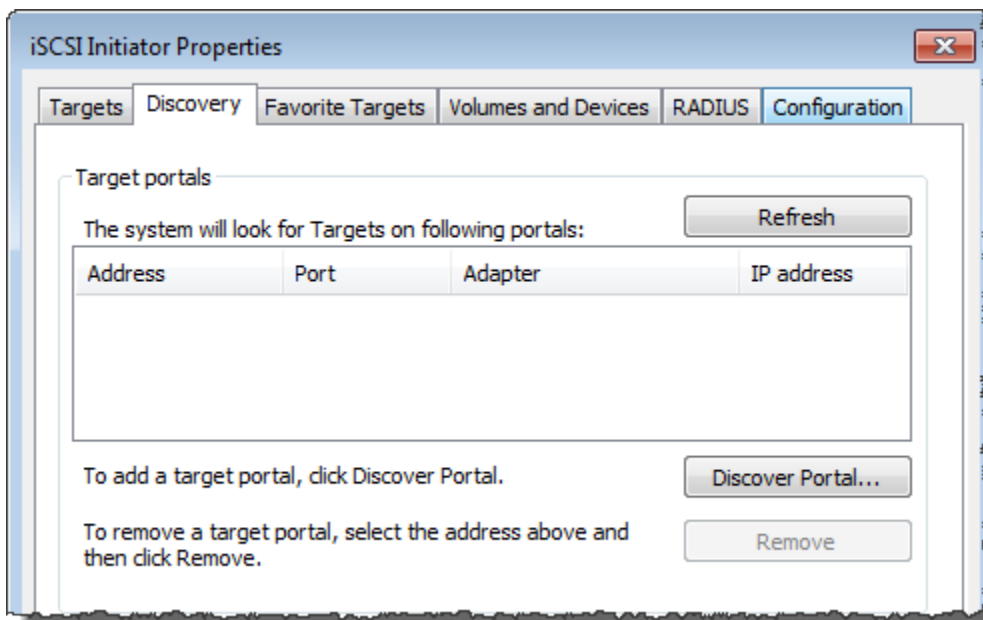
Note

Você deve ter direitos de administrador no computador cliente para executar o iniciador iSCSI.

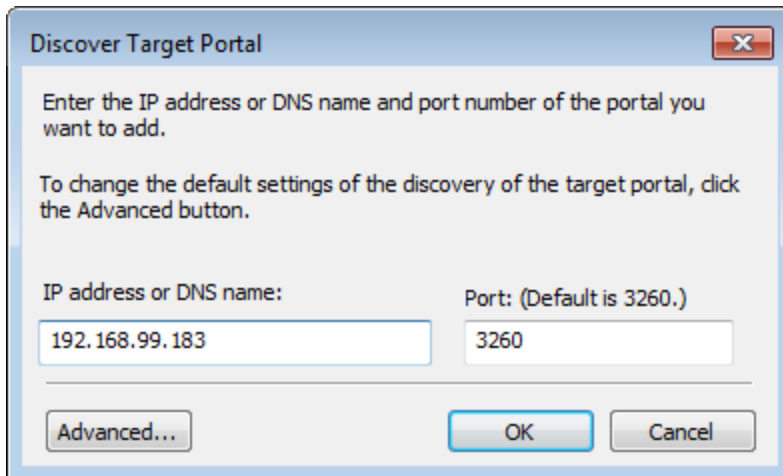
2. Quando solicitado, escolha Sim para iniciar o serviço do iniciador iSCSI da Microsoft.



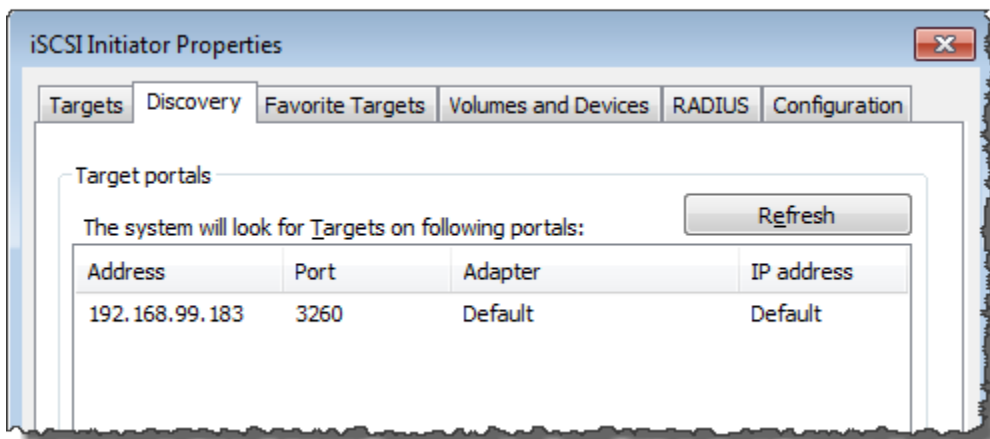
3. Na caixa de diálogo iSCSI Initiator Properties (Propriedades do Iniciador iSCSI), escolha a guia Discovery (Descoberta) e, em seguida, Discover Portal (Descobrir Portal).



- Na caixa de diálogo Descobrir Portal de Destino, insira o endereço IP do destino iSCSI em Endereço IP ou nome DNS e escolha OK. Para obter o endereço IP de seu gateway, examine a guia Gateway no console do Storage Gateway. Se você tiver implantado o gateway em uma instância do Amazon EC2 poderá encontrar o endereço IP ou DNS público na guia Descrição no console do Amazon EC2.



O endereço IP é então exibido na lista Portais de Destino na guia Descoberta.



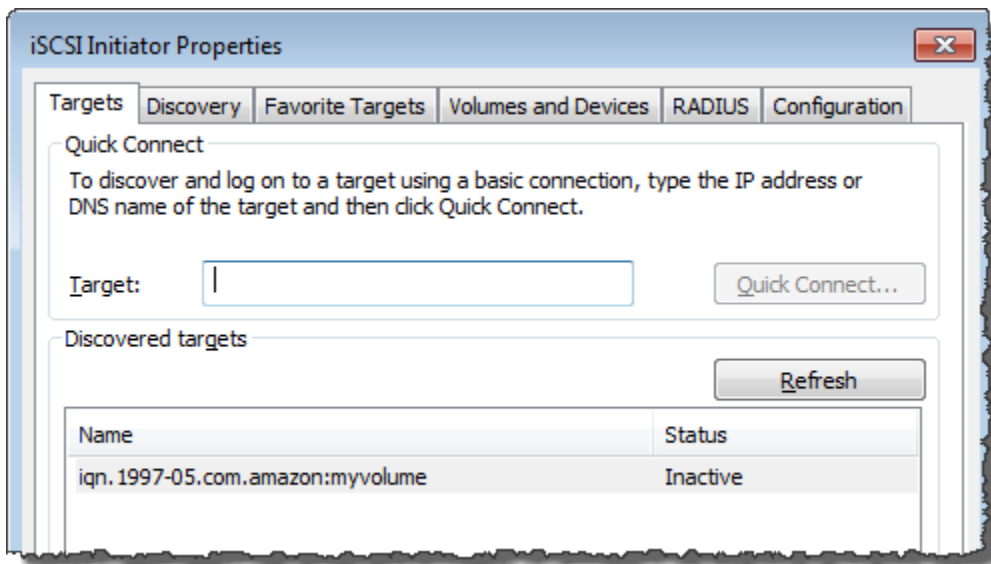
Warning

Para gateways implantados em uma instância do Amazon EC2, não é possível acessar o gateway por meio de uma conexão de Internet pública. O endereço IP elástico da instância do Amazon EC2 não pode ser usado como o endereço de destino.

- Conecte o novo portal de destino ao destino do volume de armazenamento no gateway:

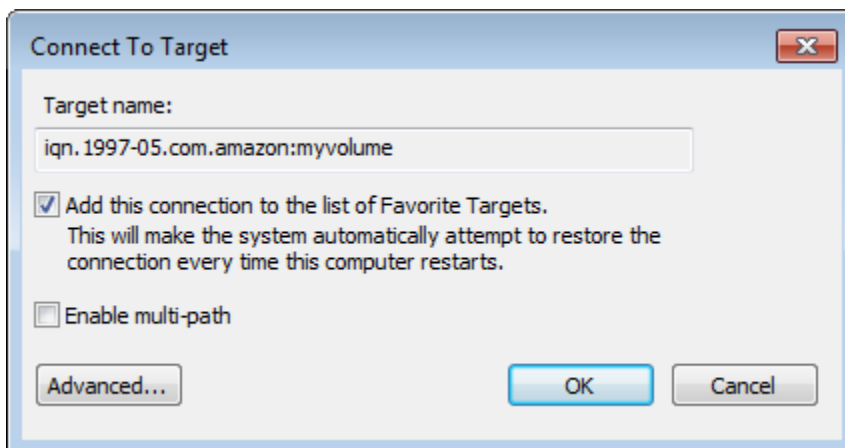
- a. Escolha a guia Destinos.

O novo portal de destino é mostrado com status inativo. O nome do destino mostrado deve ser igual ao nome especificado para seu volume de armazenamento na etapa 1.

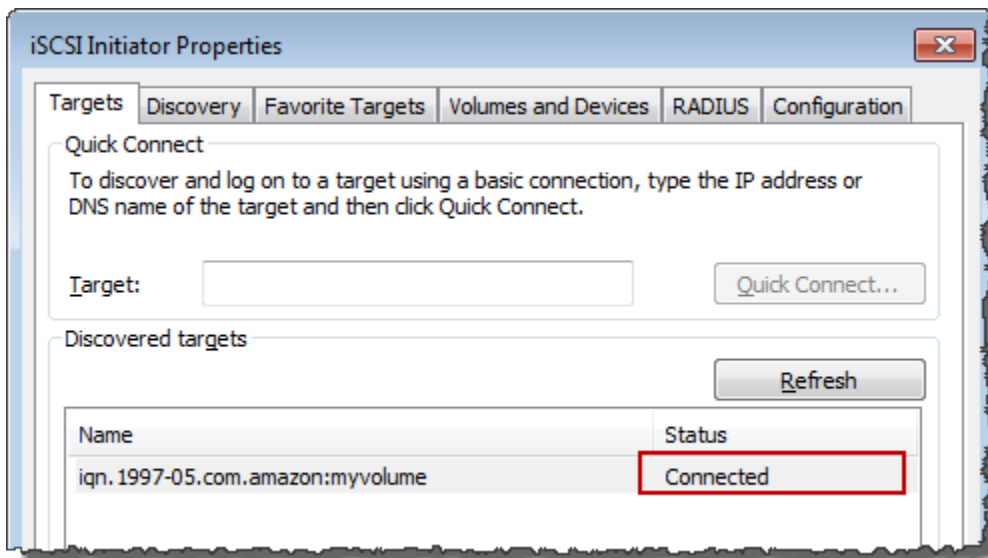


- b. Selecione o destino e escolha Conectar.

Se o nome do destino ainda não estiver preenchido, insira o nome do destino conforme mostrado na etapa 1. Na caixa de diálogo Conectar ao destino, selecione Adicionar esta conexão à lista de destinos favoritos e escolha OK.



- c. Na guia Destinos, confirme se o Status do destino está com o valor Conectado, que indica que o destino está conectado, e clique em OK.



Agora é possível inicializar e formatar esse volume de armazenamento para o Windows para que possa começar a salvar os dados nele. Você pode fazer isso usando a ferramenta Gerenciamento de Disco do Windows.

Note

Embora isso não seja necessário para este exercício, é altamente recomendável personalizar suas configurações de iSCSI para um aplicativo real, tal como discutido em [Como personalizar as configurações iSCSI do Windows](#).

Como conectar volumes ou dispositivos de VTL a um cliente Linux

Ao usar o Red Hat Enterprise Linux (RHEL), é possível usar o pacote RPM `iscsi-initiator-utils` para se conectar aos destinos iSCSI do gateway (volumes ou dispositivos de VTL).

Para conectar um cliente Linux a destinos iSCSI

1. Instale o pacote RPM `iscsi-initiator-utils`, caso ele ainda não esteja instalado no cliente.

Você pode usar o comando a seguir para instalar o pacote.

```
sudo yum install iscsi-initiator-utils
```

2. O daemon iSCSI deve estar em execução.

- a. Verifique se o daemon iSCSI está em execução usando um dos comandos a seguir.

Para o RHEL 5 ou 6, use o comando a seguir.

```
sudo /etc/init.d/iscsi status
```

Para o RHEL 7, use o comando a seguir.

```
sudo service iscsid status
```

- b. Se o status do comando não retornar o status em execução, inicie o daemon usando um dos comandos a seguir.

Para o RHEL 5 ou 6, use o comando a seguir.

```
sudo /etc/init.d/iscsi start
```

Para o RHEL 7, use o comando a seguir. Para o RHEL 7, não é necessário iniciar explicitamente o serviço `iscsid`.

```
sudo service iscsid start
```

3. Para detectar os destinos de volume ou dispositivo de VTL definidos para um gateway, use o comando de descoberta a seguir.

```
sudo /sbin/iscsiadm --mode discovery --type sendtargets --portal [GATEWAY_IP]:3260
```

Substitua o endereço IP do gateway para a variável **[GATEWAY_IP]** no comando anterior. É possível encontrar o IP do gateway nas propriedades de Informações de destino iSCSI de um volume no console do Storage Gateway.

A saída do comando de descoberta será semelhante à saída do exemplo a seguir.

Em gateways de volumes: **[GATEWAY_IP]**:3260, 1
iqn.1997-05.com.amazon:myvolume

Em gateway de fitas: iqn.1997-05.com.amazon:**[GATEWAY_IP]**-tapedrive-01

O nome qualificado de iSCSI (IQN) será diferente do que é mostrado anteriormente porque os valores de IQN são exclusivos para uma organização. O nome do destino é o nome que você especificou quando criou o volume. Também é possível encontrar esse nome de destino nas propriedades Informação do destino ao selecionar um volume no console do Storage Gateway.

4. Para se conectar a um destino, use o comando a seguir.

Observe que você precisa especificar o `[GATEWAY_IP]` e IQN corretos no comando de conexão.

Warning

Para gateways implantados em uma instância do Amazon EC2, não é possível acessar o gateway por meio de uma conexão de Internet pública. O endereço IP elástico da instância do Amazon EC2 não pode ser usado como o endereço de destino.

```
sudo /sbin/iscsiadm --mode node --targetname  
iqn.1997-05.com.amazon:[ISCSI_TARGET_NAME] --portal [GATEWAY_IP]:3260,1 --login
```

5. Para verificar se o volume está anexado ao computador cliente (o iniciador), use o comando a seguir.

```
ls -l /dev/disk/by-path
```

A saída do comando será semelhante à saída do exemplo a seguir.

```
lrwxrwxrwx. 1 root root 9 Apr 16 19:31 ip-[GATEWAY_IP]:3260-iscsi-  
iqn.1997-05.com.amazon:myvolume-lun-0 -> ../../sda
```

Depois que configurar seu iniciador, é altamente recomendável que você personalize suas configurações iSCSI, conforme discutido em [Como personalizar suas configurações iSCSI Linux](#).

Como personalizar as configurações iSCSI

Após configurar seu iniciador, é altamente recomendável personalizar as configurações iSCSI para evitar que o iniciador desconecte-se dos destinos.

Ao aumentar os valores de tempo limite de iSCSI, conforme mostrado nas etapas a seguir, você torna o aplicativo mais adequado para lidar com operações de gravação demoradas e outros problemas temporários, como interrupções na rede.

Note

Antes de fazer alterações no registro, você deve fazer backup do registro. Para obter informações sobre como fazer uma cópia de backup e outras práticas recomendadas a serem seguidas ao trabalhar com o registro, consulte [Práticas recomendadas do registro](#) na Microsoft TechNet Library.

Tópicos

- [Como personalizar as configurações iSCSI do Windows](#)
- [Como personalizar suas configurações iSCSI Linux](#)
- [Como personalizar suas configurações de tempo limite de disco Linux para gateways de volumes](#)

Como personalizar as configurações iSCSI do Windows

Ao usar um cliente Windows, você usa o iniciador iSCSI da Microsoft para se conectar ao seu volume de gateway. Para obter instruções sobre como se conectar a seus volumes, consulte [Como conectar volumes ao cliente](#).

1. Conecte os dispositivos do gateway de fitas ao seu cliente Windows.
2. Se você estiver usando um aplicativo de backup, configure-o para usar os dispositivos.

Para personalizar as configurações iSCSI do Windows

1. Aumente o tempo máximo durante o qual as solicitações são colocados em fila.
 - a. Inicie o Editor de Registro (`Regedit.exe`).
 - b. Navegue até a chave do identificador global exclusivo (GUID) mostrada a seguir, referente à classe de dispositivo que contém as configurações do controlador iSCSI.

⚠ Warning

Verifique se você está trabalhando na CurrentControlSetsubchave e não em outro conjunto de controle, como ControlSet001 ou ControlSet002.

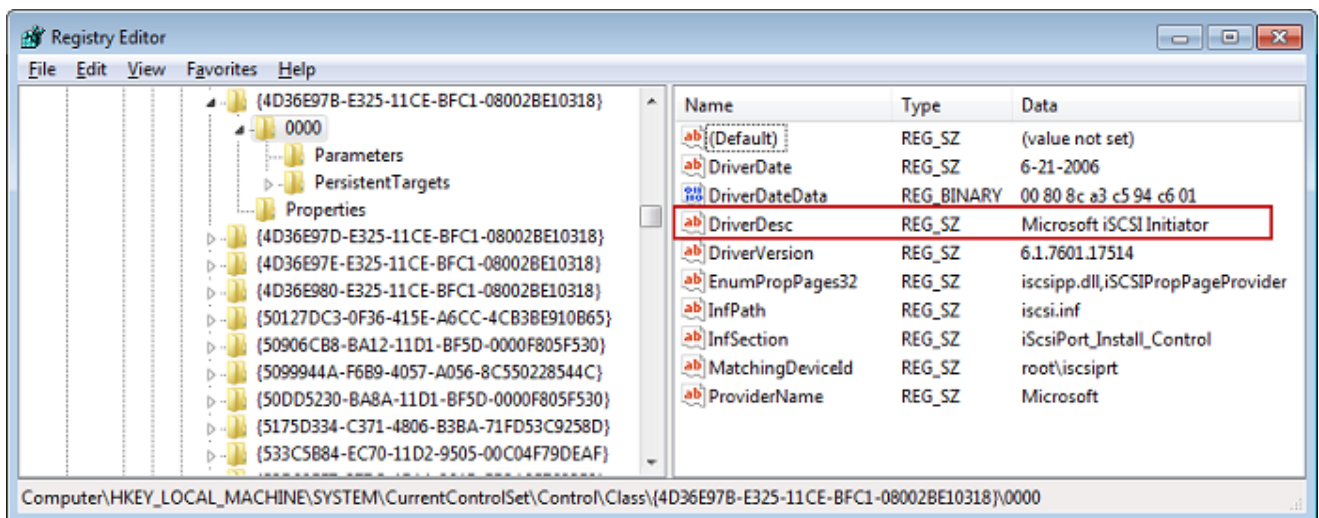
```
HKEY_Local_Machine\SYSTEM\CurrentControlSet\Control\Class\{4D36E97B-E325-11CE-BFC1-08002BE10318}
```

- c. Encontre a subchave para o iniciador Microsoft iSCSI, mostrada a seguir como *[Instance Number]*.

A chave é representada por um número de quatro dígitos, como 0000.

```
HKEY_Local_Machine\SYSTEM\CurrentControlSet\Control\Class\{4D36E97B-E325-11CE-BFC1-08002BE10318}\[<Instance Number]
```

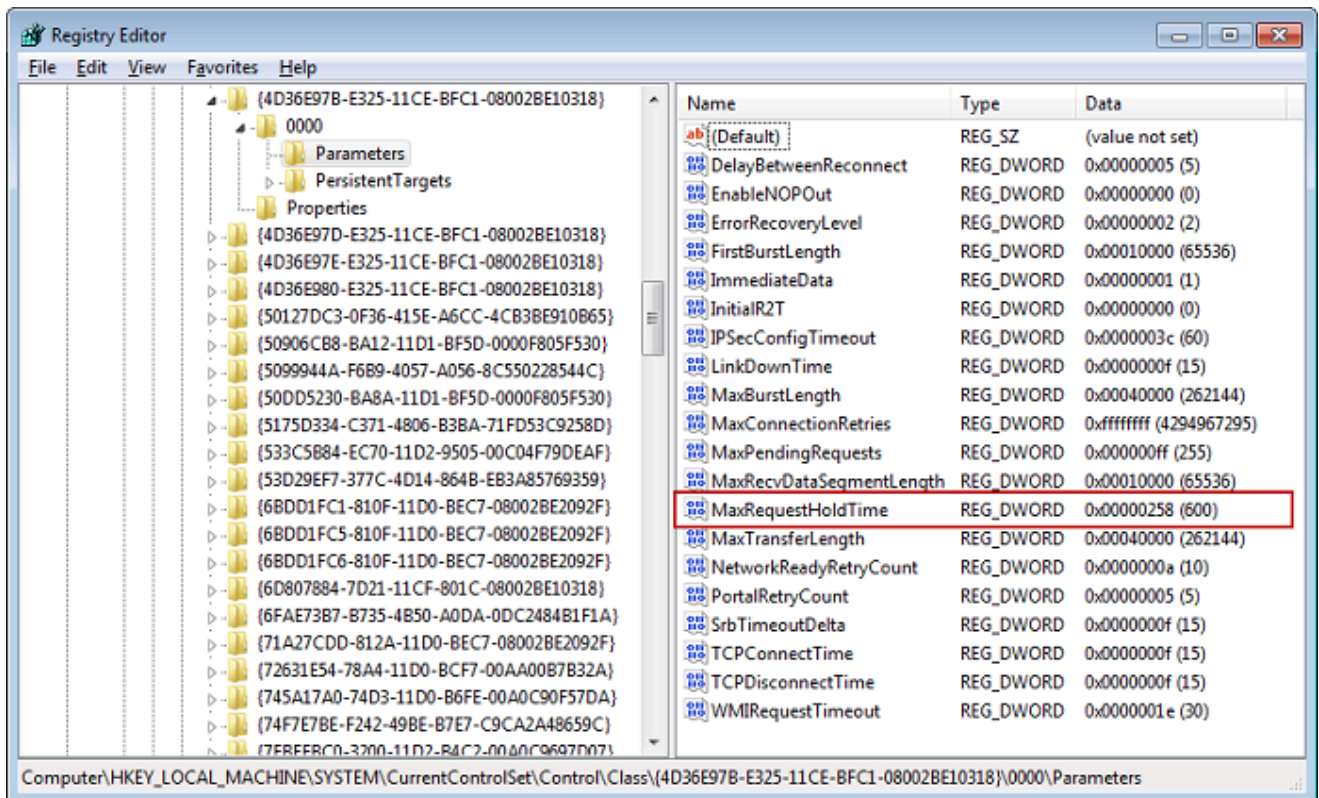
Dependendo do que está instalado em seu computador, o iniciador iSCSI da Microsoft pode não ser a subchave 0000. Para se assegurar de que selecionou a subchave correta, confirme se a string DriverDesc tem o valor Microsoft iSCSI Initiator, como mostrado no exemplo a seguir.



- d. Para exibir as configurações iSCSI, escolha a subchave Parameters (Parâmetros).

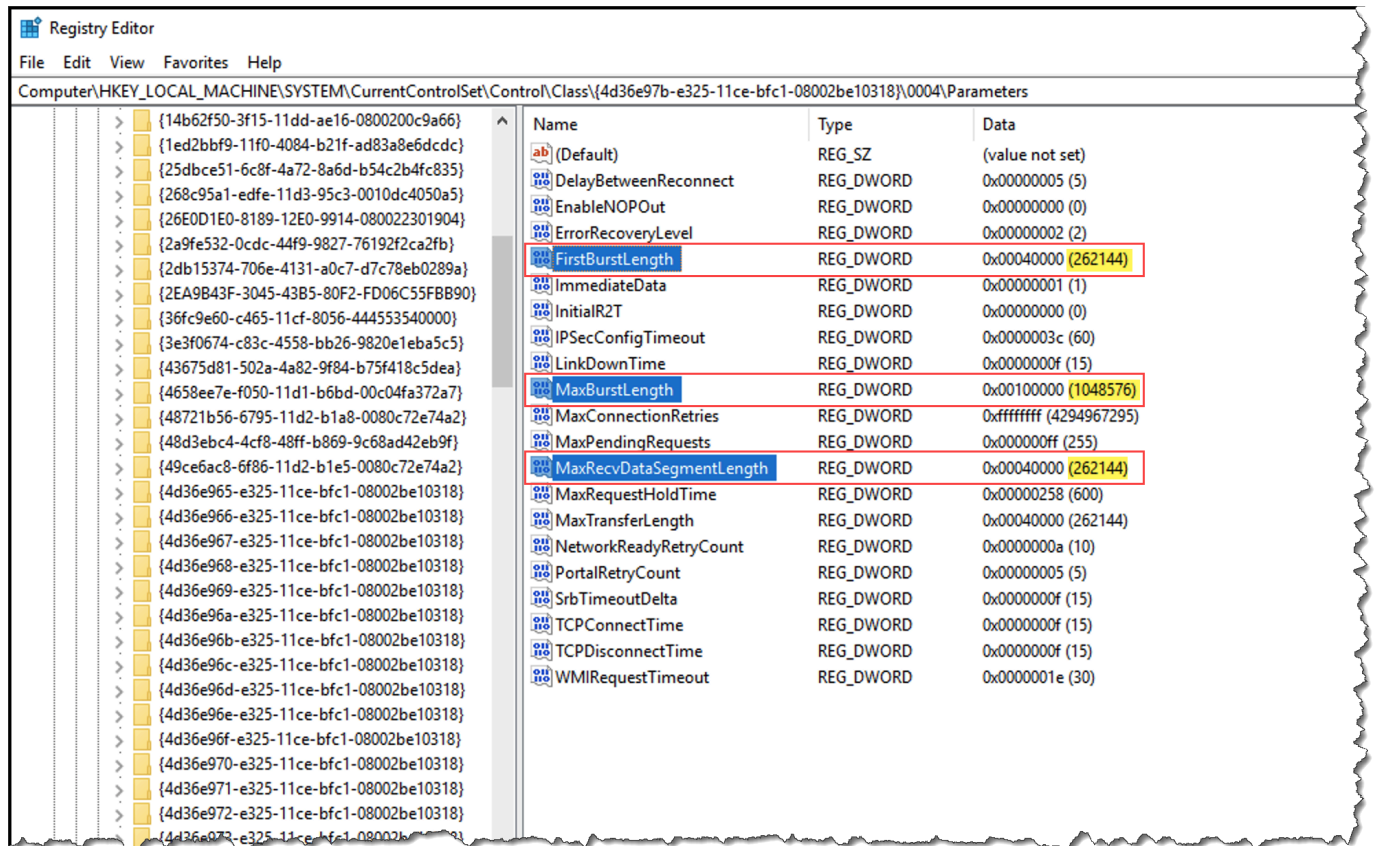
- e. Abra o menu de contexto (clique com o botão direito do mouse) do valor `MaxRequestHoldTimeDWORD` (32 bits), escolha Modificar e altere o valor para **600**

`MaxRequestHoldTime` especifica por quantos segundos o iniciador Microsoft iSCSI deve reter e repetir os comandos pendentes antes de notificar a camada superior sobre um evento. `Device Removal` Esse valor representa um tempo de espera de 600 segundos, conforme mostrado no exemplo a seguir.



2. É possível aumentar a quantidade máxima de dados que podem ser enviados em pacotes iSCSI modificando os seguintes parâmetros:

- `FirstBurstLength` controla a quantidade máxima de dados que podem ser transmitidos em uma solicitação de gravação não solicitada. Defina esse valor como **262144** ou o padrão do sistema operacional Windows, o que for maior.
- `MaxBurstLength` é semelhante a `FirstBurstLength`, mas define a quantidade máxima de dados que podem ser transmitidos nas sequências de gravação solicitadas. Defina esse valor como **1048576** ou o padrão do sistema operacional Windows, o que for maior.
- `MaxRecvDataSegmentLength` controla o tamanho máximo do segmento de dados associado a uma única unidade de dados de protocolo (PDU). Defina esse valor como **262144** ou o padrão do sistema operacional Windows, o que for maior.



Note

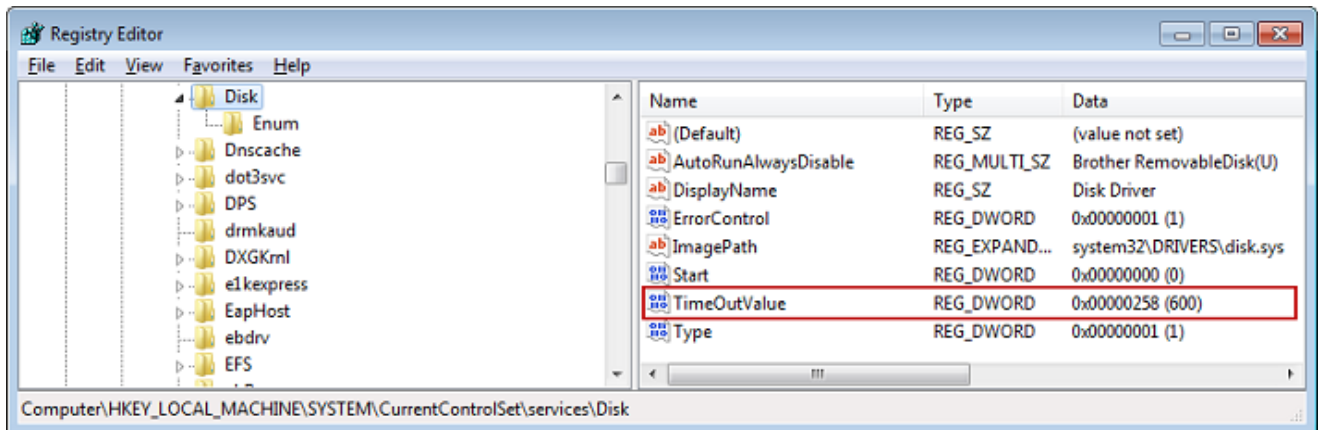
Softwares de backup diferentes podem ser otimizados para funcionar melhor usando configurações iSCSI diferentes. Para verificar quais valores desses parâmetros fornecerão o melhor desempenho, consulte a documentação do software de backup.

3. Aumente o valor do tempo limite do disco, conforme mostrado a seguir:
 - a. Inicie o Editor de Registro (Regedit.exe), se ainda não tiver feito isso.
 - b. Navegue até a subchave Disco na subchave Serviços do CurrentControlSet, mostrada a seguir.

HKEY_Local_Machine\SYSTEM\CurrentControlSet\Services\Disk

- c. Abra o menu de contexto (clique com o botão direito do mouse) do valor TimeoutValueDWORD (32 bits), escolha Modificar e altere o valor para. **600**

TimeoutValue especifica quantos segundos o iniciador iSCSI aguardará por uma resposta do alvo antes de tentar a recuperação da sessão interrompendo e restabelecendo a conexão. Esse valor representa um período de tempo limite de 600 segundos, conforme mostrado no exemplo a seguir.



4. Para garantir que os novos valores de configuração entrem em vigor, reinicie o sistema.

Antes de reiniciar, você deve confirmar se os resultados de todas as operações de gravação nos volumes são descarregadas. Para isso, antes de reiniciar, desative qualquer disco de volume de armazenamento mapeado.

Como personalizar suas configurações iSCSI Linux

Assim que configurar o iniciador do seu gateway, é altamente recomendável personalizar as configurações iSCSI para evitar que o iniciador se desconecte dos destinos. Ao aumentar os valores de tempo limite de iSCSI, conforme mostrado a seguir, você torna o aplicativo mais adequado para lidar com operações de gravação demoradas e outros problemas temporários, como interrupções na rede.

Note

Os comandos podem ser levemente diferentes para outros tipos de Linux. Os exemplos a seguir baseiam-se no Red Hat Linux.

Para personalizar suas configurações iSCSI Linux

1. Aumente o tempo máximo durante o qual as solicitações são colocados em fila.

- a. Abra o arquivo `/etc/iscsi/iscsid.conf` e encontre as linhas a seguir.

```
node.session.timeo.replacement_timeout = [replacement_timeout_value]
node.conn[0].timeo.noop_out_interval = [noop_out_interval_value]
node.conn[0].timeo.noop_out_timeout = [noop_out_timeout_value]
```

- b. Defina o valor `[replacement_timeout_value]` como **600**.

Defina o valor `[noop_out_interval_value]` como **60**.

Defina o valor `[noop_out_timeout_value]` como **600**.

Todos os três valores são em segundos.

Note

As configurações `iscsid.conf` devem ser feitas antes de descobrir o gateway. Se você já tiver descoberto seu gateway ou feito login no destino, ou ambos, poderá excluir a entrada do banco de dados de descoberta usando o comando a seguir. Em seguida, você pode redescobrir ou fazer login novamente para escolher a nova configuração.

```
iscsiadm -m discoverydb -t sendtargets -p [GATEWAY_IP]:3260 -o delete
```

2. Aumente os valores máximos para a quantidade de dados que podem ser transmitidos em cada resposta.

- a. Abra o arquivo `/etc/iscsi/iscsid.conf` e encontre as linhas a seguir.


```
node.session.iscsi.FirstBurstLength = [replacement_first_burst_length_value]
node.session.iscsi.MaxBurstLength = [replacement_max_burst_length_value]
node.conn[0].iscsi.MaxRecvDataSegmentLength
= [replacement_segment_length_value]
```

- b. Recomendamos os seguintes valores para obter um melhor desempenho. O software de backup pode ser otimizado para usar valores diferentes, portanto, consulte a documentação do software de backup para obter melhores resultados.

Defina o valor `[replacement_first_burst_length_value]` como **262144** ou o padrão do sistema operacional Linux, o que for maior.

Defina o valor `[replacement_max_burst_length_value]` como **1048576** ou o padrão do sistema operacional Linux, o que for maior.

Defina o valor `[replacement_segment_length_value]` como **262144** ou o padrão do sistema operacional Linux, o que for maior.

 Note

Softwares de backup diferentes podem ser otimizados para funcionar melhor usando configurações iSCSI diferentes. Para verificar quais valores desses parâmetros fornecerão o melhor desempenho, consulte a documentação do software de backup.

3. Reinicie o sistema para garantir que os novos valores de configuração entrem em vigor.

Antes de reiniciar, você deve confirmar se os resultados de todas as operações de gravação nas fitas são descarregadas. Para fazer isso, desmonte as fitas antes de reiniciar.

Como personalizar suas configurações de tempo limite de disco Linux para gateways de volumes

Se você estiver usando um gateway de volumes, poderá personalizar as seguintes configurações de tempo limite do disco Linux, além das configurações de iSCSI descritas na seção anterior.

Para personalizar suas configurações de tempo limite do disco Linux

1. Aumente o valor de tempo limite no arquivo de regras.
 - a. Se você estiver usando o iniciador RHEL 5, abra o arquivo `/etc/udev/rules.d/50-udev.rules` e localize a linha a seguir.

```
ACTION=="add", SUBSYSTEM=="scsi" , SYSFS{type}=="0|7|14", \  
RUN+="/bin/sh -c 'echo [timeout] > /sys$$DEVPATH/timeout'"
```

Esse arquivo de regras não existe nos iniciadores RHEL 6 ou 7; portanto, você deve criá-lo usando a seguinte regra.

```
ACTION=="add", SUBSYSTEMS=="scsi" , ATTRS{model}=="Storage Gateway",  
RUN+="/bin/sh -c 'echo [timeout] > /sys$$DEVPATH/timeout'"
```

Para modificar o valor do tempo limite no RHEL 6, use o comando a seguir e adicione as linhas de código mostradas anteriormente.

```
sudo vim /etc/udev/rules.d/50-udev.rules
```

Para modificar o valor do tempo limite no RHEL 7, use o comando a seguir e adicione as linhas de código mostradas anteriormente.

```
sudo su -c "echo 600 > /sys/block/[device name]/device/timeout"
```

- b. Defina o valor *[timeout]* como **600**.

Esse valor representa um tempo limite de 600 segundos.

2. Reinicie o sistema para garantir que os novos valores de configuração entrem em vigor.

Antes de reiniciar, você deve confirmar se os resultados de todas as operações de gravação nos volumes são descarregadas. Para fazer isso, desmonte os volumes de armazenamento antes de reiniciar.

3. Você pode testar a configuração usando o comando a seguir.

```
udevadm test [PATH_TO_ISCSI_DEVICE]
```

Esse comando mostra as regras udev aplicadas ao dispositivo iSCSI.

Como configurar a autenticação CHAP para destinos iSCSI

O Storage Gateway oferece suporte à autenticação entre o gateway e os iniciadores iSCSI usando o Challenge-Handshake Authentication Protocol (CHAP). O CHAP fornece proteção contra ataques de reprodução verificando periodicamente a identidade de um iniciador iSCSI como autenticado para acessar um volume e um dispositivo VTL de destino.

Note

A configuração do CHAP é opcional, mas altamente recomendada.

Para configurar o CHAP, você precisa configurá-lo tanto no console do Storage Gateway quanto no software do iniciador iSCSI usado para conexão com o destino. O Storage Gateway usa o CHAP mútuo, caso em que o iniciador autentica o destino e o destino autentica o iniciador.

Para configurar o CHAP mútuo para seus destinos

1. Configure o CHAP no console Storage Gateway, conforme discutido em [Para configurar o CHAP para um volume de destino no console do Storage Gateway](#).
2. No software do iniciador do cliente, preencha a configuração do CHAP:
 - Para configurar o CHAP mútuo em um cliente Windows, consulte [Para configurar o CHAP mútuo em um cliente Windows](#).
 - Para configurar o CHAP mútuo em um cliente Red Hat Linux, consulte [Para configurar o CHAP mútuo em um cliente Red Hat Linux](#).

Para configurar o CHAP para um volume de destino no console do Storage Gateway

Neste procedimento, você especifica duas chaves secretas usadas para ler e gravar em um volume. Essas mesmas chaves são usadas no procedimento para configurar o iniciador do cliente.

1. No console do Storage Gateway, escolha Volumes no painel de navegação.
2. Em Actions (Ações), escolha Configure CHAP authentication (Configurar autenticação do CHAP).
3. Forneça as informações solicitadas na caixa de diálogo Configurar autenticação CHAP, mostrada na captura de tela a seguir.
 - a. Em Nome do iniciador, digite o nome do iniciador iSCSI. Esse nome é um nome qualificado Amazon iSCSI (IQN) que é precedido por `iqn.1997-05.com.amazon:` e seguido pelo nome de destino. Veja um exemplo a seguir.

`iqn.1997-05.com.amazon:your-volume-name`

Você pode localizar o nome do iniciador usando o software do iniciador iSCSI. Por exemplo, para clientes Windows, o nome é o valor na guia Configuração do iniciador iSCSI. Para ter mais informações, consulte [Para configurar o CHAP mútuo em um cliente Windows](#).

Note

Para alterar um nome de iniciador, você deve primeiro desativar o CHAP, alterar o nome do iniciador no software do iniciador iSCSI e, em seguida, ativar o CHAP com o novo nome.

- b. Em Segredo usado para autenticar o iniciador, digite o segredo solicitado.

Esse segredo deve ter no mínimo 12 caracteres e no máximo 16 caracteres de extensão. Esse valor é a chave secreta que o iniciador (ou seja, o cliente Windows) deve conhecer para participar do CHAP com o destino.

- c. Em segredo usado para autenticar o destino (CHAP mútuo), digite o segredo solicitado.

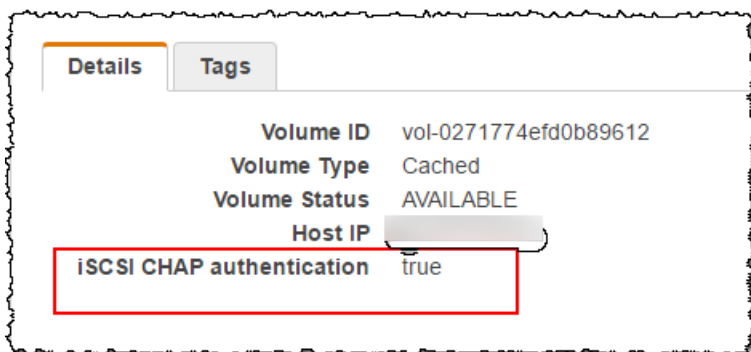
Esse segredo deve ter no mínimo 12 caracteres e no máximo 16 caracteres de extensão. Esse valor é a chave secreta que o destino (ou seja, o cliente Windows) deve conhecer para participar do CHAP com o destino.

Note

O segredo usado para autenticar o destino deve ser diferente do segredo para autenticar o iniciador.

- d. Escolha Salvar.

4. Escolha a guia Details e confirme se iSCSI CHAP authentication está definida como true.



Para configurar o CHAP mútuo em um cliente Windows

Neste procedimento, você configurará o CHAP no iniciador iSCSI da Microsoft usando as mesmas chaves que usou para configurar o CHAP para o volume no console.

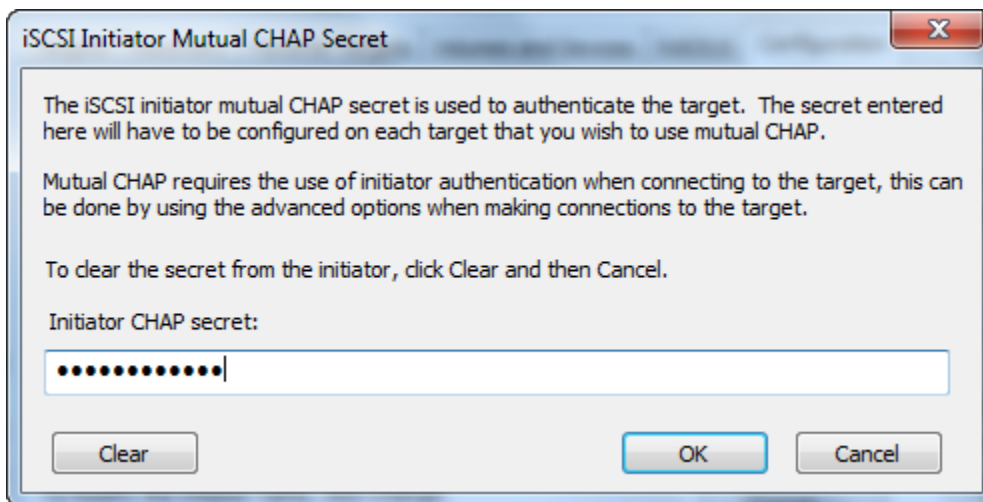
1. Se o iniciador iSCSI ainda não tiver sido iniciado, no menu Iniciar do computador cliente Windows, escolha Executar, digite **iscsicpl.exe** e escolha OK para executar o programa.
2. Defina a configuração de CHAP mútuo para o iniciador (isto é, o cliente Windows):
 - a. Escolha a guia Configuração.

Note

O valor Initiator Name é exclusivo para o iniciador e a empresa. O nome mostrado anteriormente é o valor que você usou na caixa de diálogo Configurar autenticação CHAP do console do Storage Gateway.

O nome mostrado na imagem de exemplo é apenas demonstrativo.

- b. Selecione CHAP.
- c. Na caixa de diálogo iSCSI Initiator Mutual Chap Secret, digite o valor secreto do CHAP mútuo.

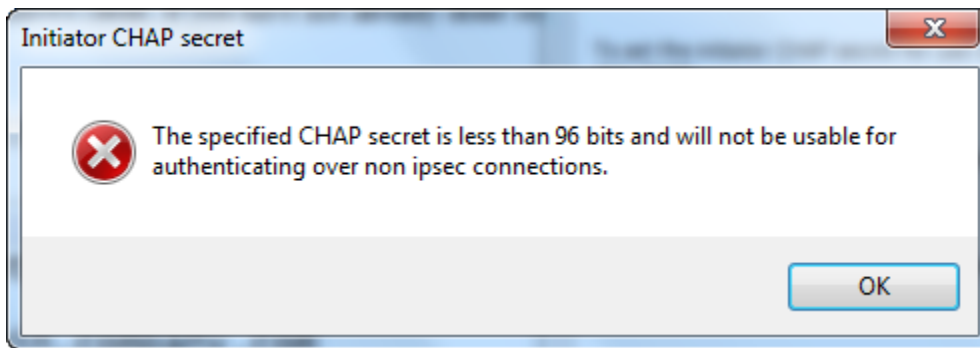


Nessa caixa de diálogo, insira o segredo que o iniciador (o cliente Windows) usa para autenticar o destino (o volume de armazenamento). Esse segredo permite que o destino leia e grave no iniciador. Esse segredo é o mesmo que o segredo digitado na caixa Segredo usado para autenticar o destino (CHAP mútuo) na caixa de diálogo Configurar autenticação

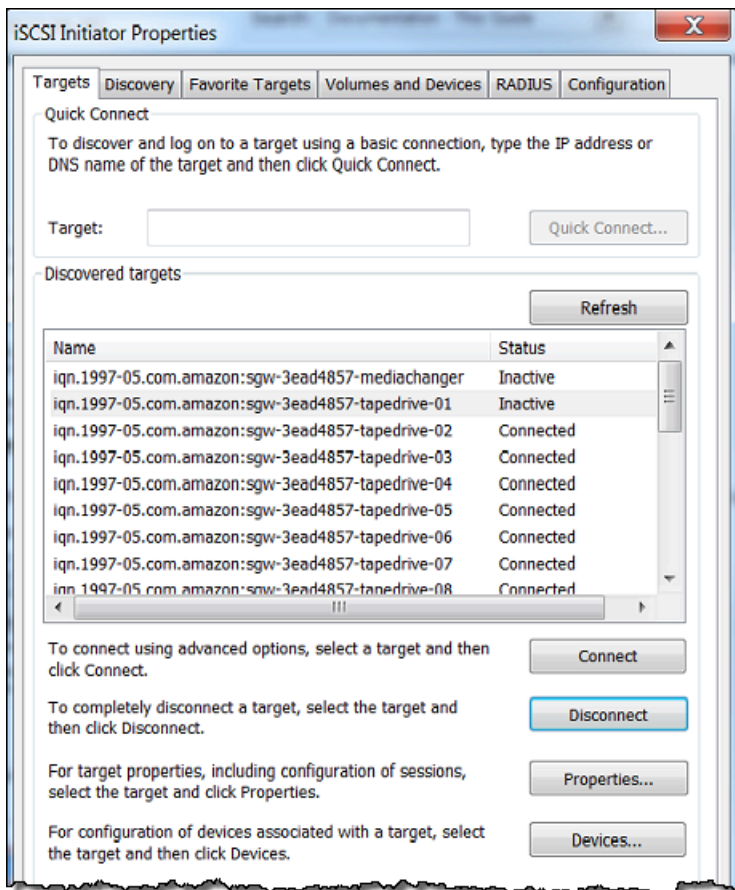
do CHAP. Para ter mais informações, consulte [Como configurar a autenticação CHAP para destinos iSCSI](#).

- d. Se a chave que você digitou tiver menos de 12 caracteres ou mais de 16 caracteres de extensão, será exibida a caixa de diálogo de erro Segredo do iniciador CHAP.

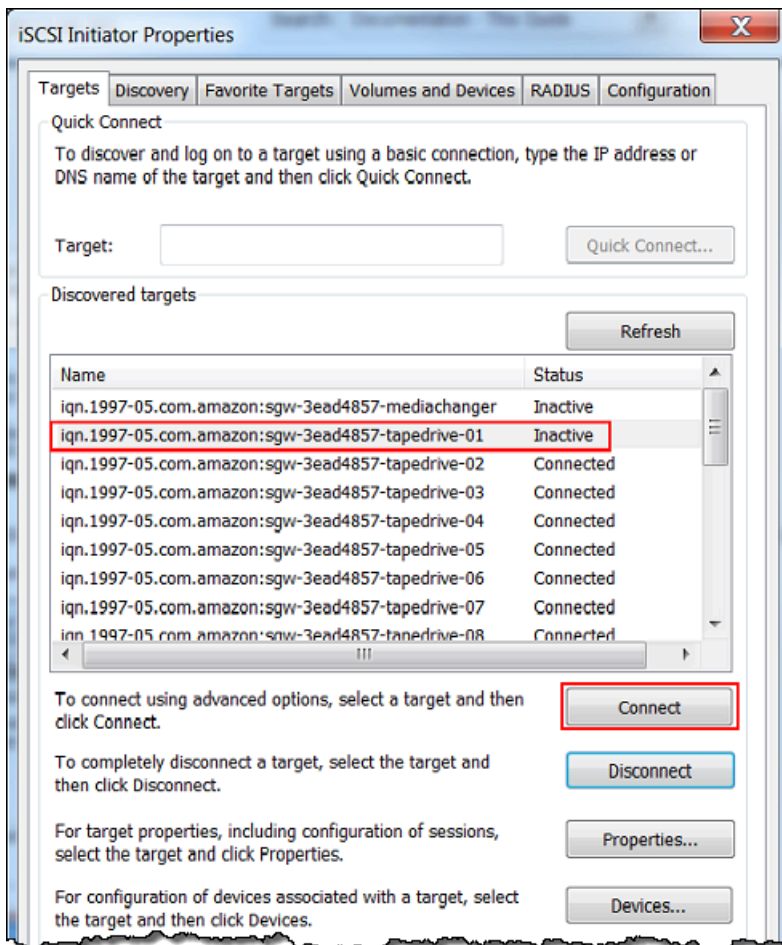
Escolha OK e digite a chave novamente.



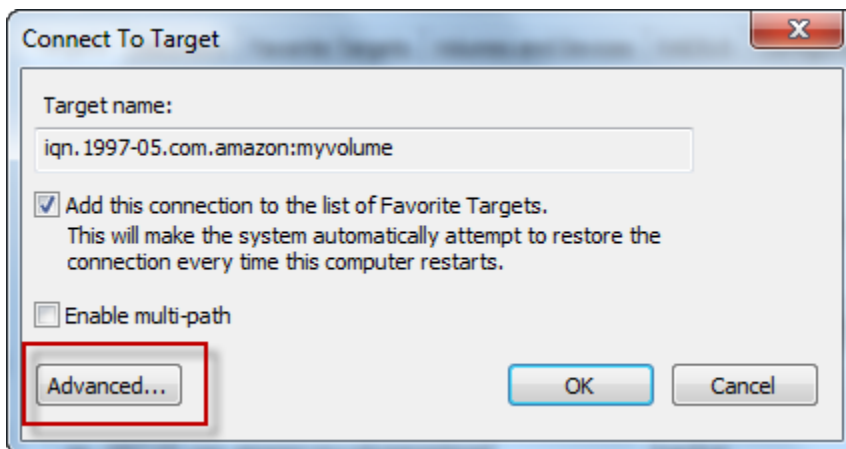
3. Configure o destino com o segredo do iniciador para concluir a configuração do CHAP mútuo.
 - a. Escolha a guia Destinos.



- b. Se o destino que você deseja configurar para o CHAP estiver conectado no momento, desconecte-o. Para isso, selecione-o e escolha Desconectar.
- c. Selecione o destino para o qual você deseja configurar o CHAP e, em seguida, escolha Conectar.

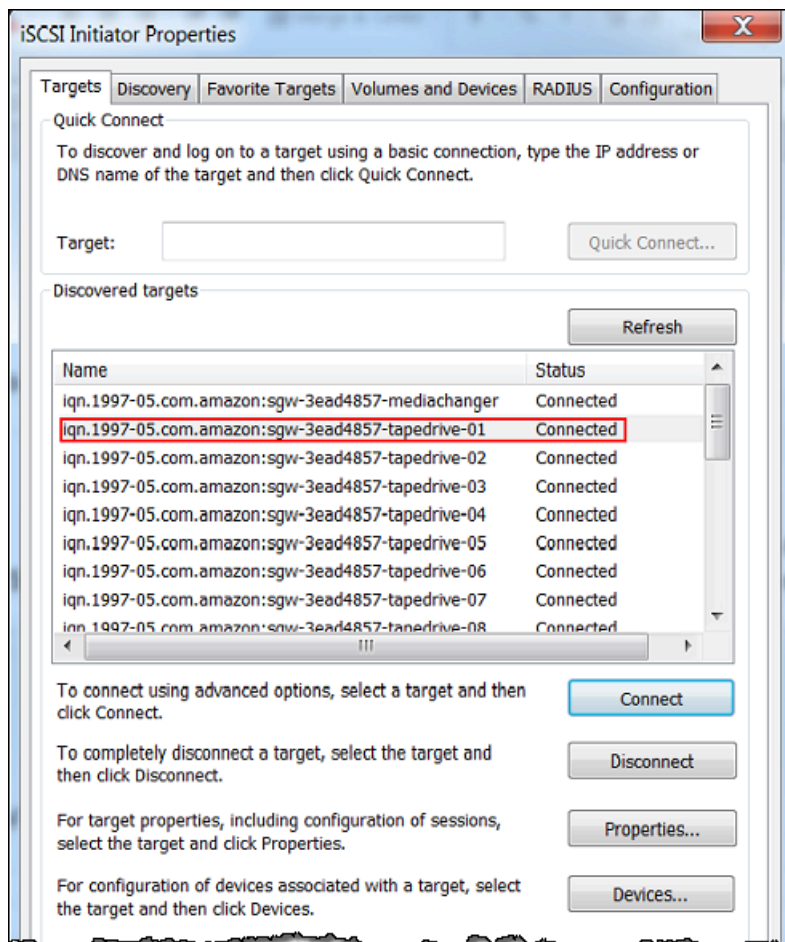


- d. Na caixa de diálogo Conectar-se Ao Destino, escolha Avançado.



- e. Na caixa de diálogo Configurações avançadas, configure o CHAP.
- i. Selecione Ativar login do CHAP.

- ii. Insira o segredo que é exigido para autenticar o iniciador. Este segredo é o mesmo que o segredo digitado na caixa Segredo usado para autenticar o iniciador na caixa de diálogo Configurar a autenticação CHAP. Para ter mais informações, consulte [Como configurar a autenticação CHAP para destinos iSCSI](#).
 - iii. Selecione Executar autenticação mútua.
 - iv. Para aplicar as alterações, escolha OK.
- f. Na caixa de diálogo Conectar-se Ao Destino, escolha OK.
4. Se você forneceu a chave secreta, o destino correto exibirá o status Conectado.



Para configurar o CHAP mútuo em um cliente Red Hat Linux

Neste procedimento, você configurará o CHAP no iniciador iSCSI Linux usando as mesmas chaves que usou para configurar o CHAP para o volume no console do Storage Gateway.

1. Primeiramente, o daemon iSCSI deve estar em execução e você já deve estar conectado a um destino. Se você não tiver concluído essas duas tarefas, consulte [Como se conectar a um cliente Red Hat Enterprise Linux](#).
2. Desconecte e remova qualquer configuração existente para o destino para o qual você está prestes a configurar o CHAP.
 - a. Para encontrar o nome do destino e garantir que se trata de uma configuração definida, relacione as configurações salvas usando o comando a seguir.

```
sudo /sbin/iscsiadm --mode node
```

- b. Desconecte-se do destino.

O comando a seguir desconecta o destino chamado **myvolume** definido no nome qualificado de iSCSI (IQN) da Amazon. Altere o nome do destino e o IQN conforme sua situação exigir.

```
sudo /sbin/iscsiadm --mode node --logout GATEWAY_IP:3260,1  
iqn.1997-05.com.amazon:myvolume
```

- c. Remova a configuração do destino.

O comando a seguir remove a configuração do destino **myvolume**.

```
sudo /sbin/iscsiadm --mode node --op delete --targetname  
iqn.1997-05.com.amazon:myvolume
```

3. Edite o arquivo de configuração iSCSI para ativar o CHAP.
 - a. Obtenha o nome do iniciador (ou seja, o cliente que você está usando).

O comando a seguir obtém o nome do iniciador do arquivo `/etc/iscsi/initiatorname.iscsi`.

```
sudo cat /etc/iscsi/initiatorname.iscsi
```

A saída desse comando é semelhante a esta:

```
InitiatorName=iqn.1994-05.com.redhat:8e89b27b5b8
```

- b. Abra o arquivo `/etc/iscsi/iscsid.conf`.

- c. Retire as seguintes linhas no arquivo e especifique os valores corretos para *nome de usuário*, *senha*, *username_in* e *password_in*.

```
node.session.auth.authmethod = CHAP
node.session.auth.username = username
node.session.auth.password = password
node.session.auth.username_in = username_in
node.session.auth.password_in = password_in
```

Para obter orientações sobre os valores que deve especificar, consulte a tabela a seguir.

Definição da configuração	Valor
<i>nome de usuário</i>	O nome do iniciador que você encontrou na etapa anterior deste procedimento. O valor começa com iqn. Por exemplo, iqn.1994-05.com.redhat:8e89b27b5b8 é um valor de nome de <i>username</i> válido.
<i>password</i>	A chave secreta usada para autenticar o iniciador (o cliente que você está usando) quando ele se comunica com o volume.
<i>username_in</i>	O IQN do volume de destino. O valor começa com iqn e termina com o nome do destino. Por exemplo, iqn.1997-05.com.amazon:myvolume é um valor de nome de <i>username_in</i> válido.
<i>password_in</i>	A chave secreta usada para autenticar o destino (o volume) quando ele se comunica com o iniciador.

- d. Salve as alterações no arquivo de configuração e, em seguida, feche o arquivo.
4. Descubra e faça login no destino. Para fazer isso, siga as etapas em [Como se conectar a um cliente Red Hat Enterprise Linux](#).

Usando AWS Direct Connect com o Storage Gateway

AWS Direct Connect vincula sua rede interna à Amazon Web Services Cloud. Ao usar AWS Direct Connect com o Storage Gateway, você pode criar uma conexão para necessidades de carga de trabalho de alto rendimento, fornecendo uma conexão de rede dedicada entre seu gateway local e AWS.

O Storage Gateway usa endpoints públicos. Com uma AWS Direct Connect conexão estabelecida, você pode criar uma interface virtual pública para permitir que o tráfego seja roteado para os endpoints do Storage Gateway. A interface virtual pública evita os provedores de serviço de Internet do caminho da sua rede. O endpoint público do serviço Storage Gateway pode estar na mesma AWS região do AWS Direct Connect local ou em uma AWS região diferente.

A ilustração a seguir mostra um exemplo de como AWS Direct Connect funciona com o Storage Gateway.

arquitetura de rede mostrando o Storage Gateway conectado à nuvem usando conexão AWS direta.

O procedimento a seguir pressupõe que você tenha criado um gateway operacional.

Para usar AWS Direct Connect com o Storage Gateway

1. Crie e estabeleça uma AWS Direct Connect conexão entre seu data center local e seu endpoint do Storage Gateway. Para obter mais informações sobre como criar uma conexão, consulte [Conceitos básicos do AWS Direct Connect](#) no Guia do usuário do AWS Direct Connect .
2. Conecte seu dispositivo Storage Gateway local ao AWS Direct Connect roteador.
3. Crie uma interface virtual pública e configure seu roteador local de forma adequada. Mesmo com o Direct Connect, os endpoints da VPC devem ser criados com o HAProxy. Para obter mais informações, consulte [Como criar uma interface virtual](#) no Guia do usuário do AWS Direct Connect .

Para obter detalhes sobre AWS Direct Connect, consulte [O que é AWS Direct Connect?](#) no Guia do AWS Direct Connect usuário.

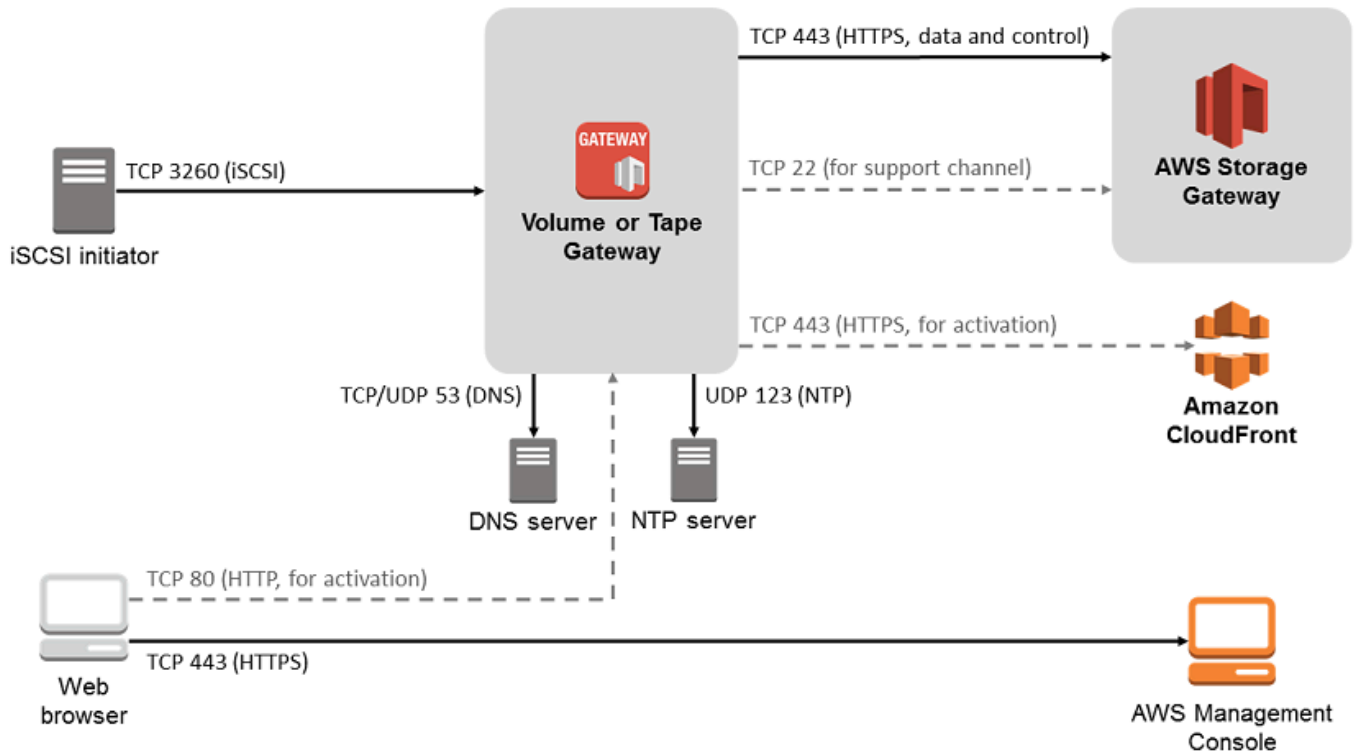
Requisitos de porta

O Storage Gateway requer as portas a seguir para sua operação. Algumas portas são comuns e necessárias por todos os tipos de gateway. Outras portas são necessárias por tipos de gateway

específicos. Nesta seção, é possível encontrar uma ilustração e uma lista das portas necessárias para o gateway de volumes.

gateway de volumes

A ilustração a seguir mostra as portas a serem abertas para a operação de gateway de volumes



As portas a seguir são comuns e necessárias a todos os tipos de gateway.

De	Para	Protocolo	Port	Como usar
VM do Storage Gateway	AWS	Transmission Control Protocol (TCP)	443 (HTTPS)	Para comunicação de uma VM de saída do Storage Gateway com um endpoint de AWS serviço. Para obter

De	Para	Protocolo	Port	Como usar
				informações sobre endpoints de serviço, consulte Permitindo AWS Storage Gateway acesso por meio de firewalls e roteadores.

De	Para	Protocolo	Port	Como usar
Seu navegador da web	VM do Storage Gateway	TCP	80 (HTTP)	<p>Por sistemas locais para obter a chave de ativação do Storage Gateway. A porta 80 só é usada durante a ativação de um dispositivo do Storage Gateway.</p> <p>Uma VM do Storage Gateway não exige que a porta 80 seja publicamente acessível. O nível necessário de acesso à porta 80 depende da configuração da rede. Se você ativar o gateway pelo Storage Gateway Management Console,</p>

De	Para	Protocolo	Port	Como usar
				o host pelo qual se conecta ao console deverá ter acesso à porta 80 do gateway.
VM do Storage Gateway	Servidor Domain Name Service (DNS – Serviço do nome de domínio)	User Datagram Protocol (UDP)/UDP	53 (DNS)	Para a comunicação entre a VM do Storage Gateway e o servidor DNS.

De	Para	Protocolo	Port	Como usar	
VM do Storage Gateway	AWS	TCP	22 (Canal de suporte)	Permite AWS Support acessar seu gateway para ajudá-lo a solucionar problemas de gateway. Você não precisa dessa porta aberta para a operação normal do gateway, mas ela é necessária para a solução de problemas.	

De	Para	Protocolo	Port	Como usar
VM do Storage Gateway	Servidor de Network Time Protocol (NTP)	UDP	123 (NTP)	<p>Usado por sistemas locais para sincronizar a hora da VM com a hora do host. Uma VM do Storage Gateway está configurada para usar os seguintes servidores NTP:</p> <ul style="list-style-type: none">• 0.amazon.pool.ntp.org• 1.amazon.pool.ntp.org• 2.amazon.pool.ntp.org• 3.amazon.pool.ntp.org
Dispositivo de hardware do Storage Gateway	Proxy de protocolo de transferência de hipertexto (HTTP)	TCP	8080 (HTTP)	Necessário brevemente e para ativação.

Além das portas comuns, o gateway de volumes também precisam das portas a seguir.

De	Para	Protocolo	Port	Como usar
Iniciadores iSCSI	VM do Storage Gateway	TCP	3260 (iSCSI)	Por sistemas locais para se conectar a destinos iSCSI expostos pelo gateway.

Como conectar seu gateway

Assim que escolher um host e implantar a VM do gateway, conecte e ative seu gateway. Para isso, você precisará do endereço IP VM do gateway. O endereço IP pode ser obtido no console local de seu gateway. Faça login no console local e obtenha o endereço IP na parte superior da página do console.

Para gateways implantados no local, é também possível obter o endereço IP no hipervisor. Para gateways do Amazon EC2, é possível obter o endereço IP da instância do Amazon EC2, no Amazon EC2 Management Console. Para saber como obter o endereço IP do gateway, consulte uma das opções a seguir:

- Host do VMware: [Acesso ao console local do gateway com o VMware ESXi](#)
- Host do HyperV: [Acessar o console local do gateway com o Microsoft Hyper-V](#)
- Host da Linux Kernel-based Virtual Machine (KVM): [Acessar o console local do gateway com o Linux KVM](#)
- Host do EC2: [Como obter um endereço IP em um host do Amazon EC2](#)

Quando você localizar o endereço IP, anote-o. Em seguida, retorne ao console do Storage Gateway e digite o endereço IP no console.

Como obter um endereço IP em um host do Amazon EC2

Para obter o endereço IP da instância do Amazon EC2 na qual seu gateway está implantado, faça login no console local da instância do EC2. Obtenha então o endereço IP na parte superior da página do console. Para obter instruções, consulte [Como fazer login no console local do gateway do Amazon EC2](#).

Também é possível obter o endereço IP no Amazon EC2 Management Console. É recomendável usar o endereço IP público na ativação. Para obter o endereço IP público, use o procedimento 1. Se você optar por usar o endereço IP elástico, consulte o procedimento 2.

Procedimento 1: para se conectar ao gateway usando o endereço IP público

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 EC2 na qual seu gateway está implantado.
3. Escolha a guia Description na parte inferior e anote o endereço IP público. Você usará esse endereço IP para se conectar ao gateway. Retorne ao console do Storage Gateway e insira o endereço IP.

Se você desejar usar o endereço IP elástico na ativação, use o procedimento a seguir.

Procedimento 2: para se conectar ao gateway usando o endereço IP elástico

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 EC2 na qual seu gateway está implantado.
3. Escolha a guia Description na parte inferior e tome nota do número presente em Elastic IP. Você usa o endereço IP elástico para se conectar ao gateway. Retorne ao console do Storage Gateway e insira o endereço IP elástico.
4. Depois de ativar seu gateway, escolha esse gateway recém-ativado e em seguida a guia VTL devices no painel inferior.
5. Obtenha os nomes de todos os seus dispositivos de VTL.
6. Para cada destino, execute o comando a seguir para configurá-lo.

```
iscsiadm -m node -o new -T [$TARGET_NAME] -p [$Elastic_IP]:3260
```

7. Para cada destino, execute o comando a seguir para registrá-lo.

```
iscsiadm -m node -p [ELASTIC_IP]:3260 --login
```

Seu gateway agora está conectado por meio do endereço IP elástico da Instância EC2.

Como entender os recursos e IDs de recursos do Storage Gateway

No Storage Gateway, o recurso principal é um gateway, mas existem outros tipos de recurso, como: volume, fita virtual, destino iSCSI e dispositivo de vtl. Eles são chamados de sub-recursos e só existem se associados a um gateway.

Esses recursos e sub-recursos têm Nomes de recursos da Amazon (ARNs) exclusivos associados a eles, conforme mostrado na tabela a seguir.

Tipo de recurso	Formato do ARN
ARN de gateway	arn:aws:storagegateway: <i>region:account-id</i> :gateway/ <i>gateway-id</i>
ARN de volume	arn:aws:storagegateway: <i>region:account-id</i> :gateway/ <i>gateway-id</i> /volume/ <i>volume-id</i>
ARN de destino (destino iSCSI)	arn:aws:storagegateway: <i>region:account-id</i> :gateway/ <i>gateway-id</i> /target/ <i>iSCSITarget</i>

O Storage Gateway também é compatível com o uso de instâncias EC2 e volumes e snapshots do EBS. Estes são os recursos do Amazon EC2 usados no Storage Gateway.

Como trabalhar com IDs de recurso

Ao criar um recurso, o Storage Gateway atribui ao recurso um ID de recurso exclusivo. Esse ID de recurso faz parte do ARN do recurso. Um ID de recurso assume a forma de um identificador de recurso, seguido de um hífen e uma combinação única de oito letras e números. Por exemplo, um ID de gateway ID assume a forma `sgw-12A3456B`, em que `sgw` é o identificador de recursos

para gateways. Um ID de volume assume a forma `vol-3344CCDD`, em que `vol` é o identificador de recursos para volumes.

Para fitas virtuais, você pode acrescentar um prefixo de até quatro caracteres ao ID do código de barras para ajudá-lo a organizar suas fitas.

Os IDs de recursos do Storage Gateway estão em letras maiúsculas. No entanto, quando você usa esses IDs de recurso com a API do Amazon EC2, o Amazon EC2 espera que os IDs de recurso estejam em letra minúscula. Você deve alterar o ID do recurso para minúscula para usá-lo com a API do EC2. Por exemplo, no Storage Gateway o ID de um volume deve ser `vol-1122AABB`. Ao usar esse ID com a API do EC2, você deve alterá-lo para `vol-1122aabb`. Do contrário, a API do EC2 talvez não se comporte como esperado.

Como atribuir tags a recursos do Storage Gateway

No Storage Gateway, é possível usar tags para gerenciar seus recursos. As tags permitem que você adicione metadados e categorize seus recursos para torná-los mais fáceis de gerenciar. Toda tag é composta de um par de valores de chave, que são definidos por você. Você pode adicionar tags a gateways, volumes e fitas virtuais. Você pode pesquisar e filtrar esses recursos de acordo com as tags que adicionar.

Por exemplo, é possível usar tags para identificar quais recursos do Storage Gateway são usados por cada departamento em sua organização. Você pode atribuir tags a gateways e volumes usados pelo departamento de contabilidade da seguinte forma: (`key=department` e `value=accounting`). Em seguida, você pode usar essa tag como filtro para identificar todos os gateways e volumes usados pelo departamento de contabilidade e usar essas informações para determinar o custo. Para obter mais informações, consulte [Usar tags de alocação de custos](#) e [Trabalhar com o Tag Editor](#).

Se você arquivar uma fita virtual marcada, ela manterá a tag no arquivo. Da mesma forma, se você recuperar uma fita do arquivo em outro gateway, as tags serão mantidas no novo gateway.

As tags não têm nenhum significado semântico, mas são interpretadas como string de caracteres.

As restrições a seguir se aplicam às tags:

- As chaves e os valores de tags diferenciam maiúsculas de minúsculas.
- O número máximo de tags para cada recurso é 50.
- As chaves de tag não podem começar com `aws:`. Esse prefixo está reservado para AWS uso.

- Os caracteres válidos para a propriedade da chave são letras e números UTF-8, espaço e os caracteres especiais + - = . _ : / e @.

Como trabalhar com tags

É possível trabalhar com tags usando o console, a API ou a [interface de linha de comandos \(CLI\) do Storage Gateway](#). Os procedimentos a seguir mostram como adicionar, editar e excluir uma tag no console.

Para adicionar uma tag

1. Abra o console do Storage Gateway em <https://console.aws.amazon.com/storagegateway/home>.
2. No painel de navegação, escolha o recurso o qual você deseja atribuir uma tag.

Por exemplo, para atribuir uma tag a um gateway, escolha Gateways e, na lista de gateways, escolha o gateway ao qual deseja atribuir a tag.

3. Escolha Tags e em seguida Add/edit tags.
4. Na caixa de diálogo Add/edit tags, escolha Create tag.
5. Digite uma chave em Key e um valor em Value. Por exemplo, você pode digitar **Department** para a chave e **Accounting** para o valor.

Note

Você pode deixar a caixa Value em branco.

6. Escolha Create Tag para adicionar mais tags. Você pode adicionar várias tags a um recurso.
7. Quando terminar de adicionar tags, escolha Save.

Para editar uma tag

1. Abra o console do Storage Gateway em <https://console.aws.amazon.com/storagegateway/home>.
2. Escolha o recurso cuja tag você deseja editar.
3. Escolha Tags para abrir a caixa de diálogo Add/edit tags.
4. Escolha o ícone de lápis ao lado da tag que você deseja editar e em seguida edite a tag.
5. Quando terminar de editar a tag, escolha Save.

Para excluir uma tag

1. Abra o console do Storage Gateway em <https://console.aws.amazon.com/storagegateway/home>.
2. Escolha o recurso cuja tag você deseja excluir.
3. Escolha Tags e em seguida Add/edit tags para abrir a caixa de diálogo Add/edit tags.
4. Escolha o ícone X ao lado da tag que você deseja excluir e escolha Save.

Como trabalhar com componentes de código aberto para o AWS Storage Gateway

Esta seção descreve as ferramentas e licenças de terceiros das quais dependemos para oferecer a funcionalidade do Storage Gateway.

O código-fonte de determinados componentes de software de código aberto incluídos com o software AWS Storage Gateway está disponível para download nos seguintes locais:

- Para gateways implantados no VMware ESXi, faça download de [sources.tar](#)
- Para gateways implantados no Microsoft Hyper-V, faça download de [sources_hyperv.tar](#)
- Para gateways implantados na Máquina virtual baseada em Kernel (KVM) do Linux, faça download de [sources_kVM.tar](#)

Esse produto inclui software desenvolvido pelo OpenSSL Project para uso no OpenSSL Toolkit (<http://www.openssl.org/>). Para obter as licenças relevantes para todas as ferramentas de terceiros dependentes, consulte [Licenças de terceiros](#).

AWS Storage Gateway cotas


Neste tópico, é possível encontrar informações sobre compartilhamento de arquivos, volume, fita, configuração e limites desempenho no Storage Gateway.

Tópicos

- [Cotas para volumes](#)
- [Tamanhos de disco local recomendados para seu gateway](#)

Cotas para volumes

A tabela a seguir relaciona as cotas para volumes.

Descrição	Volumes armazenados em cache	Volumes armazenados
Tamanho máximo de um volume	32 TiB	16 TiB
<div data-bbox="142 594 266 632">  Note </div> <div data-bbox="185 648 638 1022"> <p>Se criar um snapshot de um volume armazenado em cache com um tamanho superior a 16 TiB, você não poderá restaurá-lo em um volume do Storage Gateway, mas não para um volume do Amazon Elastic Block Store (Amazon EBS).</p> </div>		
Número máximo de volumes por gateway	32	32
Tamanho total de todos os volumes por gateway	1,024 TiB	512 TiB

Tamanhos de disco local recomendados para seu gateway

A tabela a seguir recomenda tamanhos para armazenamento em disco local para o gateway implantado.

Tipo de gateway	Cache (mínimo)	Cache (máximo)	Buffer de upload (mínimo)	Buffer de upload (máximo)	Outros discos locais necessários
Gateway de volumes em cache	150 GiB	64 TiB	150 GiB	2 TiB	—
Gateway de volumes armazenado	—	—	150 GiB	2 TiB	Um ou mais para volume ou volumes armazenados

Note

É possível configurar uma ou mais unidades locais para seu cache e buffer de upload, até a capacidade máxima.

Ao adicionar cache ou fazer upload de buffer para um gateway existente, é importante criar novos discos no host (instância do hipervisor ou do Amazon EC2). Não altere o tamanho de discos existentes caso os discos tenham sido alocados anteriormente como um cache ou um buffer de upload.

Referência de API para o Storage Gateway

Além de usar o console, você pode usar a AWS Storage Gateway API para configurar e gerenciar programaticamente seus gateways. Esta seção descreve as AWS Storage Gateway operações, a assinatura de solicitações para autenticação e o tratamento de erros. Para obter informações sobre os endpoints disponíveis para o Storage Gateway, consulte [Endpoints e cotas do AWS Storage Gateway](#) na Referência geral da AWS.

Note

Você também pode usar os AWS SDKs ao desenvolver aplicativos com o AWS Storage Gateway. Os AWS SDKs para Java, .NET e PHP envolvem a AWS Storage Gateway API subjacente, simplificando suas tarefas de programação. Para obter informações sobre como fazer download de bibliotecas de SDKs, consulte [Bibliotecas de códigos de exemplo](#).

Tópicos

- [Cabeçalhos de solicitação requeridos no Storage Gateway](#)
- [Solicitações de assinatura](#)
- [Respostas de erro](#)
- [Ações](#)

Cabeçalhos de solicitação requeridos no Storage Gateway

Esta seção descreve os cabeçalhos requeridos que você deve enviar em cada solicitação POST ao Storage Gateway. Os cabeçalhos HTTP são incluídos para identificar as principais informações sobre a solicitação, como a operação que você deseja invocar, a data da solicitação e informações que indicam sua autorização como remetente da solicitação. Os cabeçalhos diferenciam minúsculas e maiúsculas e a ordem dos cabeçalhos não é importante.

O exemplo a seguir mostra os cabeçalhos que são usados na [ActivateGateway](#) operação.

```
POST / HTTP/1.1
Host: storagegateway.us-east-2.amazonaws.com
```



```
Content-Type: application/x-amz-json-1.1
Authorization: AWS4-HMAC-SHA256 Credential=AKIAIOSFODNN7EXAMPLE/20120425/us-east-2/
storagegateway/aws4_request, SignedHeaders=content-type;host;x-amz-date;x-amz-target,
Signature=9cd5a3584d1d67d57e61f120f35102d6b3649066abdd4bf4bbcf05bd9f2f8fe2
x-amz-date: 20120912T120000Z
x-amz-target: StorageGateway_20120630.ActivateGateway
```

A seguir estão os cabeçalhos que devem ser incluídos em suas solicitações POST ao Storage Gateway. Os cabeçalhos mostrados abaixo que começam com “x-amz” são AWS cabeçalhos específicos. Todos os outros cabeçalhos listados são cabeçalhos comuns usados em transações HTTP.

Cabeçalho	Descrição
Authorization	<p>O cabeçalho de autorização contém várias informações sobre a solicitação que permitem que o Storage Gateway determine se a solicitação é uma ação válida para o solicitante. O formato desse cabeçalho é o seguinte (as quebras de linha foram adicionadas por motivo de legibilidade):</p> <pre>Authorization: AWS4-HMAC_SHA456 Credentials= <i>YourAccessKey</i> /<i>yyyymmdd</i>/<i>region</i>/storagegateway/aw s4_request, SignedHeaders=content-type;host;x-amz-date;x-amz-targ et, Signature= <i>CalculatedSignature</i></pre> <p>Na sintaxe anterior, você especifica o ano <i>YourAccessKey</i>, mês e dia (<i>aaaammdd</i>), a região e o <i>CalculatedSignature</i>. O formato do cabeçalho de autorização é determinado pelos requisitos do processo de assinatura a AWS V4. Os detalhes da assinatura são discutidos no tópico Solicitações de assinatura.</p>
Content-Type	<p>Use <code>application/x-amz-json-1.1</code> como tipo de conteúdo para todas as solicitações ao Storage Gateway.</p> <pre>Content-Type: application/x-amz-json-1.1</pre>

Cabeçalho	Descrição
Host	<p>Use o cabeçalho do host para especificar o endpoint do Storage Gateway em que você envia sua solicitação. Por exemplo, <code>storagegateway.us-east-2.amazonaws.com</code> é o endpoint para a região Leste dos EUA (Ohio). Para obter mais informações sobre os endpoints disponíveis para o Storage Gateway, consulte Endpoints e cotas do AWS Storage Gateway na Referência geral da AWS.</p> <pre data-bbox="472 569 1507 646">Host: storagegateway. <i>region</i>.amazonaws.com</pre>
x-amz-date	<p>Você deve fornecer o carimbo de data/hora no Date cabeçalho HTTP ou no AWS x-amz-date cabeçalho. (Algumas bibliotecas de cliente HTTP não permitem a definição do cabeçalho Date.) Quando existe um cabeçalho x-amz-date, o Storage Gateway ignora qualquer cabeçalho Date durante a autenticação de uma solicitação. O formato x-amz-date deve ser o formato básico ISO8601, no formato <code>YYYYMMDD'T'HHMMSS'Z'</code>. Quando forem usados os cabeçalhos Date e x-amz-date, o formato do cabeçalho de data não precisa ser o ISO8601.</p> <pre data-bbox="472 1178 1507 1255">x-amz-date: <i>YYYYMMDD'T'HHMMSS'Z'</i></pre>
x-amz-target	<p>Esse cabeçalho especifica a versão da API e a operação que você está solicitando. Os valores do cabeçalho de destino são formados por concatenação da versão da API e do nome da API e têm o formato a seguir.</p> <pre data-bbox="472 1541 1507 1619">x-amz-target: StorageGateway_ <i>APIversion</i> .<i>operationName</i></pre> <p>O valor <code>operationName</code> (por exemplo, <code>ActivateGateway</code>) pode ser encontrado na lista de APIs,. Referência de API para o Storage Gateway</p>

Solicitações de assinatura

O Storage Gateway exige que toda solicitação enviada seja autenticada com uma assinatura. Para assinar uma solicitação, calcule uma assinatura digital usando a função de hash criptográfico. Hash criptográfico é uma função que retorna um valor de hash exclusivo com base na entrada. A entrada da função de hash inclui o texto da solicitação e a chave de acesso secreta. A função de hash retorna um valor de hash que você inclui na solicitação como sua assinatura. A assinatura é parte do cabeçalho `Authorization` de sua solicitação.

Depois de receber a solicitação, o Storage Gateway recalculará a assinatura usando a mesma função de hash e a entrada que você usou para assinar a solicitação. Quando a assinatura resultante corresponde à assinatura na solicitação, o Storage Gateway processa a solicitação. Do contrário, a solicitação é rejeitada.

O Storage Gateway é compatível com a autenticação usando o [Signature versão 4 da AWS](#). O processo para calcular uma assinatura pode ser dividido em três tarefas:

- [Tarefa 1: Criar uma solicitação canônica](#)

Reorganize sua solicitação HTTP em um formato canônico. É necessário usar uma forma canônica, pois o Storage Gateway usa a mesma forma canônica quando recalcula uma assinatura para compará-la com a que você enviou.

- [Tarefa 2: Criar uma string para assinar](#)

Crie uma string que será usada como um dos valores de entrada para sua função hash criptográfica. A string, chamada `string-to-sign`, é uma concatenação do nome do algoritmo hash, da data da solicitação, de uma string do escopo da credencial e da solicitação canonizada da tarefa anterior. A string do escopo credencial em si é uma concatenação da data, da região e de informações do serviço.

- [Tarefa 3: Crie uma assinatura](#)

Crie uma assinatura para sua solicitação usando uma função hash criptográfica que aceita duas strings de entrada: sua string para assinar e uma chave derivada. Para calcular a chave derivada, inicie sua chave de acesso secreta e use a string do escopo da credencial para criar uma série de códigos de autenticação de mensagem baseados em hash (HMACs).

Cálculo de assinatura de exemplo

O exemplo a seguir mostra os detalhes da criação de uma assinatura para [ListGateways](#). Esse exemplo pode ser usado como referência para verificar o método de cálculo da assinatura. Outros cálculos de referência estão incluídos no [Signature Version 4 Test Suite](#) do Amazon Web Services Glossary.

O exemplo supõe o seguinte:

- O time stamp da solicitação é "Mon, 10 Sep 2012 00:00:00" GMT.
- O endpoint é a região Leste dos EUA (Ohio).

A sintaxe de solicitação geral (incluindo o corpo JSON) é:

```
POST / HTTP/1.1
Host: storagegateway.us-east-2.amazonaws.com
x-amz-Date: 20120910T000000Z
Authorization: SignatureToBeCalculated
Content-type: application/x-amz-json-1.1
x-amz-target: StorageGateway_20120630.ListGateways
{}
```

O formato canônico da solicitação calculada para [Tarefa 1: Criar uma solicitação canônica](#) é:

```
POST
/

content-type:application/x-amz-json-1.1
host:storagegateway.us-east-2.amazonaws.com
x-amz-date:20120910T000000Z
x-amz-target:StorageGateway_20120630.ListGateways

content-type;host;x-amz-date;x-amz-target
44136fa355b3678a1146ad16f7e8649e94fb4fc21fe77e8310c060f61caaff8a
```

A última linha da solicitação canônica é o hash do corpo da solicitação. Além disso, observe a terceira linha vazia na solicitação canônica. Isso ocorre porque não há parâmetros de consulta para essa API (ou qualquer API do Storage Gateway).

A string-to-sign para [Tarefa 2: Criar uma string para assinar](#) é:

```
AWS4-HMAC-SHA256
20120910T000000Z
20120910/us-east-2/storagegateway/aws4_request
92c0effa6f9224ac752ca179a04cecbde3038b0959666a8160ab452c9e51b3e
```

A primeira linha da string-to-sign é o algoritmo, a segunda é o time stamp, a terceira é o escopo da credencial e a última é um hash da solicitação canônica da Tarefa 1.

Para [Tarefa 3: Crie uma assinatura](#), a chave derivada pode ser representada como:

```
derived key = HMAC(HMAC(HMAC(HMAC("AWS4" + YourSecretAccessKey, "20120910"), "us-
east-2"), "storagegateway"), "aws4_request")
```

Se a chave de acesso secreta, bPxRfi wjalrxutnfEMI/k7mdeng/ CYEXAMPLEKEY, for usada, a assinatura calculada será:

```
6d4c40b8f2257534dbdca9f326f147a0a7a419b63aff349d9d9c737c9a0f4c81
```

A etapa final é construir o cabeçalho Authorization. Para a chave de acesso de demonstração AKIAIOSFODNN7EXAMPLE, o cabeçalho (com quebras de linha adicionadas por motivo de legibilidade) é:

```
Authorization: AWS4-HMAC-SHA256 Credential=AKIAIOSFODNN7EXAMPLE/20120910/us-east-2/
storagegateway/aws4_request,
SignedHeaders=content-type;host;x-amz-date;x-amz-target,
Signature=6d4c40b8f2257534dbdca9f326f147a0a7a419b63aff349d9d9c737c9a0f4c81
```

Respostas de erro

Tópicos

- [Exceções](#)
- [Códigos de erro de operação](#)
- [Respostas de erro](#)

Esta seção fornece informações de referência sobre AWS Storage Gateway erros. Esses erros são representados por uma exceção de erro e um código de erro de operação. Por exemplo, a exceção de erro `InvalidSignatureException` é retornada por qualquer resposta à API se houver um problema na assinatura da solicitação. No entanto, o código de erro da operação `ActivationKeyInvalid` é retornado somente para a [ActivateGatewayAPI](#).

Dependendo do tipo de erro, o Storage Gateway pode retornar somente uma exceção ou então um código de erro de exceção e de operação. Exemplos de respostas de erro são mostrados em [Respostas de erro](#).

Exceções

A tabela a seguir lista as exceções AWS Storage Gateway da API. Quando uma AWS Storage Gateway operação retorna uma resposta de erro, o corpo da resposta contém uma dessas exceções. As exceções `InternalServerError` e `InvalidGatewayRequestException` retornam um dos códigos de mensagem de [Códigos de erro de operação](#) que geram os códigos de erro de operação específicos.

Exceção	Message	Código de status HTTP
<code>IncompleteSignatureException</code>	A assinatura especificada está incompleta.	400 solicitação inválida
<code>InternalFailure</code>	O processamento da solicitação falhou por algum erro ou alguma exceção ou falha desconhecida.	500 Internal Server Error
<code>InternalServerError</code>	Uma das mensagens de código de erro de operação em Códigos de erro de operação .	500 Internal Server Error
<code>InvalidAction</code>	A ação ou operação solicitada é inválida.	400 solicitação inválida
<code>InvalidClientTokenId</code>	O certificado X.509 ou ID da chave de AWS acesso fornecido não existe em nossos registros.	403 proibido

Exceção	Message	Código de status HTTP
<code>InvalidGatewayRequestException</code>	Uma das mensagens de código de erro de operação em Códigos de erro de operação .	400 solicitação inválida
<code>InvalidSignatureException</code>	A assinatura da solicitação que calculamos não corresponde à assinatura que você forneceu. Verifique sua chave de AWS acesso e método de assinatura.	400 solicitação inválida
<code>MissingAction</code>	Está faltando um parâmetro de ação ou operação na solicitação.	400 solicitação inválida
<code>MissingAuthenticationToken</code>	A solicitação deve conter uma ID de chave de AWS acesso válida (registrada) ou um certificado X.509.	403 proibido
<code>RequestExpired</code>	A solicitação ultrapassa data de expiração ou a data de solicitação (ambas com acréscimo de 15 minutos) ou a data de solicitação ultrapassa 15 minutos no futuro.	400 solicitação inválida
<code>SerializationException</code>	Ocorreu um erro durante a serialização. Verifique se a carga JSON está bem formada.	400 solicitação inválida
<code>ServiceUnavailable</code>	Falha na solicitação devido a um erro temporário do servidor.	503 Service Unavailable (503 Serviço não disponível)
<code>SubscriptionRequiredException</code>	O ID da chave de AWS acesso precisa de uma assinatura para o serviço.	400 solicitação inválida

Exceção	Message	Código de status HTTP
ThrottlingException	Taxa excedida.	400 solicitação inválida
UnknownOperationException	Foi especificada uma operação desconhecida. As operações válidas estão relacionadas em Operações no Storage Gateway .	400 solicitação inválida
UnrecognizedClientException	O token de segurança incluído na solicitação é inválido.	400 solicitação inválida
ValidationException	O valor de um parâmetro de entrada é inválido ou está fora do intervalo.	400 solicitação inválida

Códigos de erro de operação

A tabela a seguir mostra o mapeamento entre os códigos de erro de AWS Storage Gateway operação e as APIs que podem retornar os códigos. Todos os códigos de erro de operação são retornados com uma das duas exceções gerais – `InternalServerError` e `InvalidGatewayRequestException` – descritas em [Exceções](#).

Código de erro de operação	Message	Operações que retornam esse código de erro
ActivationKeyExpired	A chave de ativação especificada expirou.	ActivateGateway
ActivationKeyInvalid	A chave de ativação especificada é inválida.	ActivateGateway
ActivationKeyNotFound	Não foi possível encontrar a chave de ativação especificada.	ActivateGateway

Código de erro de operação	Message	Operações que retornam esse código de erro
BandwidthThrottlesScheduleNotFound	Não foi possível encontrar a limitação de largura de banda.	DeleteBandwidthRateLimit
CannotExportSnapshot	Não é possível exportar o snapshot especificado.	CreateCachediVolume SCSI CreateStorediVolume SCSI
InitiatorNotFound	Não foi possível encontrar o iniciador especificado.	DeleteChapCredentials
DiskAlreadyAllocated	O disco especificado já está alocado.	AddCache AddUploadBuffer AddWorkingStorage CreateStorediVolume SCSI
DiskDoesNotExist	O disco especificado não existe.	AddCache AddUploadBuffer AddWorkingStorage CreateStorediVolume SCSI
DiskSizeNotGigAligned	O disco especificado não está alinhado em gigabyte.	CreateStorediVolume SCSI
DiskSizeGreaterThanVolumeMaxSize	O tamanho do disco é superior ao tamanho máximo de volume.	CreateStorediVolume SCSI

Código de erro de operação	Message	Operações que retornam esse código de erro
DiskSizeLessThanVolumeSize	O tamanho do disco especificado é superior ao tamanho do volume.	CreateStorediVolume SCSI
DuplicateCertificateInfo	As informações de certificado especificadas estão duplicadas.	ActivateGateway

Código de erro de operação	Message	Operações que retornam esse código de erro
GatewayInternalError	Ocorreu um erro interno no gateway.	AddCache AddUploadBuffer AddWorkingStorage CreateCachediVolume SCSI CreateSnapshot CreateStorediVolume SCSI CreateSnapshotFromVolumeRecoveryPoint DeleteBandwidthRateLimit DeleteChapCredentials DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediVolumes SCSI DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediVolumes SCSI DescribeWorkingStorage ListLocalDisks

Código de erro de operação	Message	Operações que retornam esse código de erro
		ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewaySoftwareNow UpdateSnapshotSchedule

Código de erro de operação	Message	Operações que retornam esse código de erro
GatewayNotConnected	O gateway especificado não está conectado.	AddCache AddUploadBuffer AddWorkingStorage CreateCachediVolume SCSI CreateSnapshot CreateStorediVolume SCSI CreateSnapshotFromVolumeRecoveryPoint DeleteBandwidthRateLimit DeleteChapCredentials DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediVolumes SCSI DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediVolumes SCSI DescribeWorkingStorage ListLocalDisks

Código de erro de operação	Message	Operações que retornam esse código de erro
		ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewaySoftwareNow UpdateSnapshotSchedule

Código de erro de operação	Message	Operações que retornam esse código de erro
GatewayNotFound	O gateway especificado não foi encontrado.	AddCache AddUploadBuffer AddWorkingStorage CreateCachediVolume SCSI CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediVolume SCSI DeleteBandwidthRateLimit DeleteChapCredentials DeleteGateway DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediVolumes SCSI DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediVolumes SCSI DescribeWorkingStorage

Código de erro de operação	Message	Operações que retornam esse código de erro
		ListLocalDisks
		ListVolumes
		ListVolumeRecoveryPoints
		ShutdownGateway
		StartGateway
		UpdateBandwidthRateLimit
		UpdateChapCredentials
		UpdateMaintenanceStartTime
		UpdateGatewaySoftwareNow
		UpdateSnapshotSchedule

Código de erro de operação	Message	Operações que retornam esse código de erro
GatewayProxyNetworkConnectionBusy	A conexão de rede proxy do gateway especificado está ocupada.	AddCache AddUploadBuffer AddWorkingStorage CreateCachediVolume SCSI CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediVolume SCSI DeleteBandwidthRateLimit DeleteChapCredentials DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediVolumes SCSI DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediVolumes SCSI DescribeWorkingStorage ListLocalDisks

Código de erro de operação	Message	Operações que retornam esse código de erro
		ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewaySoftwareNow UpdateSnapshotSchedule

Código de erro de operação	Message	Operações que retornam esse código de erro
InternalError	Ocorreu um erro interno.	ActivateGateway AddCache AddUploadBuffer AddWorkingStorage CreateCachediVolume SCSI CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediVolume SCSI DeleteBandwidthRateLimit DeleteChapCredentials DeleteGateway DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediVolumes SCSI DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediVolumes SCSI

Código de erro de operação	Message	Operações que retornam esse código de erro
		DescribeWorkingStorage ListLocalDisks ListGateways ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewayInformation UpdateGatewaySoftwareNow UpdateSnapshotSchedule

Código de erro de operação	Message	Operações que retornam esse código de erro
InvalidParameters	A solicitação especificada contém parâmetros incorretos.	ActivateGateway AddCache AddUploadBuffer AddWorkingStorage CreateCachediVolume SCSI CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediVolume SCSI DeleteBandwidthRateLimit DeleteChapCredentials DeleteGateway DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediVolumes SCSI DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediVolumes SCSI

Código de erro de operação	Message	Operações que retornam esse código de erro
		DescribeWorkingStorage ListLocalDisks ListGateways ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewayInformation UpdateGatewaySoftwareNow UpdateSnapshotSchedule
LocalStorageLimitExceeded	O limite de armazenamento local foi excedido.	AddCache AddUploadBuffer AddWorkingStorage
LunInvalid	O LUN especificado está incorreto.	CreateStorediVolume SCSI

Código de erro de operação	Message	Operações que retornam esse código de erro
MaximumVolumeCount Exceeded	A contagem máxima de volume foi excedida.	CreateCachediVolume SCSI CreateStorediVolume SCSI DescribeCachediVolumes SCSI DescribeStorediVolumes SCSI
NetworkConfigurati onChanged	A configuração de rede do gateway mudou.	CreateCachediVolume SCSI CreateStorediVolume SCSI

Código de erro de operação	Message	Operações que retornam esse código de erro
NotSupported	A operação especificada não é comportada.	ActivateGateway AddCache AddUploadBuffer AddWorkingStorage CreateCachediVolume SCSI CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediVolume SCSI DeleteBandwidthRateLimit DeleteChapCredentials DeleteGateway DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediVolumes SCSI DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediVolumes SCSI

Código de erro de operação	Message	Operações que retornam esse código de erro
		DescribeWorkingStorage ListLocalDisks ListGateways ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewayInformation UpdateGatewaySoftwareNow UpdateSnapshotSchedule
OutdatedGateway	O gateway especificado está desatualizado.	ActivateGateway
SnapshotInProgressException	O snapshot especificado está em andamento.	DeleteVolume
SnapshotIdInvalid	O snapshot especificado é inválido.	CreateCachediVolume SCSI CreateStorediVolume SCSI

Código de erro de operação	Message	Operações que retornam esse código de erro
StagingAreaFull	A área de preparação está cheia.	CreateCachediVolume SCSI CreateStorediVolume SCSI
TargetAlreadyExists	O destino especificado já existe.	CreateCachediVolume SCSI CreateStorediVolume SCSI
TargetInvalid	O destino especificado é inválido.	CreateCachediVolume SCSI CreateStorediVolume SCSI DeleteChapCredentials DescribeChapCredentials UpdateChapCredentials
TargetNotFound	O destino especificado não foi encontrado.	CreateCachediVolume SCSI CreateStorediVolume SCSI DeleteChapCredentials DescribeChapCredentials DeleteVolume UpdateChapCredentials

Código de erro de operação	Message	Operações que retornam esse código de erro
<code>UnsupportedOperationForGatewayType</code>	A operação especificada não é válida para o tipo de gateway.	AddCache AddWorkingStorage CreateCachediVolume SCSI CreateSnapshotFromVolumeRecoveryPoint CreateStorediVolume SCSI DeleteSnapshotSchedule DescribeCache DescribeCachediVolumes SCSI DescribeStorediVolumes SCSI DescribeUploadBuffer DescribeWorkingStorage ListVolumeRecoveryPoints
<code>VolumeAlreadyExists</code>	O volume especificado já existe.	CreateCachediVolume SCSI CreateStorediVolume SCSI
<code>VolumeIdInvalid</code>	O volume especificado é inválido.	DeleteVolume
<code>VolumeInUse</code>	O volume especificado já está em uso.	DeleteVolume

Código de erro de operação	Message	Operações que retornam esse código de erro
VolumeNotFound	O volume especificado não foi encontrado.	CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint DeleteVolume DescribeCachedVolumes SCSI DescribeSnapshotSchedule DescribeStoredVolumes SCSI UpdateSnapshotSchedule
VolumeNotReady	O volume especificado não está pronto.	CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint

Respostas de erro

Quando existe um erro, as informações no cabeçalho da resposta contêm:

- Tipo de conteúdo: aplicativo/ -1,1 x-amz-json
- Um código de status HTTP 4xx ou 5xx apropriado

O corpo de uma resposta de erro contém informações sobre o erro que ocorreu. A resposta de erro de exemplo a seguir mostra a sintaxe de saída dos elementos comuns a todas as respostas de erro.

```
{
  "__type": "String",
  "message": "String",
  "error":
    { "errorCode": "String",
      "errorDetails": "String"
    }
}
```

```
}
```

A tabela a seguir explica os campos de resposta de erro JSON mostrados na sintaxe anterior.

`__type`

Uma das exceções de [Exceções](#).

Tipo: string

`error`

Contém detalhes de erro específicos à API. Em erros genéricos (isto é, não específicos a nenhuma API), essa informação não é mostrada.

Tipo: Coleção

`errorCode`

Um dos códigos de erro de operação .

Tipo: string

`errorDetails`

Esse campo não é usado na versão atual da API.

Tipo: string

`mensagem`

Uma das mensagens de código de erro de operação em .

Tipo: string

Exemplos de resposta de erro

O corpo JSON a seguir será retornado se você usar a API `DescribeStorediSCSIVolumes` e especificar uma entrada de solicitação ARN do gateway que não existe.

```
{
  "__type": "InvalidGatewayRequestException",
  "message": "The specified volume was not found.",
  "error": {
```

```
"errorCode": "VolumeNotFound"
}
```

O seguinte corpo JSON será retornado se o Storage Gateway calcular uma assinatura que não corresponda à assinatura enviada com uma solicitação.

```
{
  "__type": "InvalidSignatureException",
  "message": "The request signature we calculated does not match the signature you
provided."
}
```

Operações no Storage Gateway

Para conferir uma lista completa de operações da API do Storage Gateway, consulte [Ações](#) na Referência de API do AWS Storage Gateway .

Histórico de documentos do Guia do usuário do gateway de volumes

- Versão da API: 30/6/2013
- Última atualização da documentação: 24 de novembro de 2020

A tabela a seguir descreve as alterações importantes em cada versão do Guia do usuário do AWS Storage Gateway depois de abril de 2018. Para receber notificações sobre atualizações dessa documentação, você poderá se inscrever em um feed RSS.

Alteração	Descrição	Data
Opção adicionada para ativar ou desativar as atualizações de manutenção	O Storage Gateway recebe atualizações de manutenção regulares que podem incluir atualizações de sistema operacional e software, correções para tratar de estabilidade, desempenho e segurança, além de acesso a novos recursos. Agora você pode definir uma configuração para ativar ou desativar essas atualizações para cada gateway individual em sua implantação. Para obter mais informações, consulte Gerenciando atualizações de gateway usando o AWS Storage Gateway console .	6 de junho de 2024
Suporte obsoleto para o Tape Gateway no Snowball Edge	Não é mais possível hospedar o Tape Gateway em dispositivos Snowball Edge.	14 de março de 2024

[Instruções atualizadas para testar a configuração do gateway usando aplicações de terceiros](#)

As instruções para testar a configuração do gateway usando aplicações de terceiros agora descrevem o comportamento esperado se o gateway for reiniciado durante um trabalho de backup em andamento. Para obter mais informações, consulte .

24 de outubro de 2023

[CloudWatch Alarmes recomendados atualizados](#)

O CloudWatch HealthNotifications alarme agora se aplica e é recomendado para todos os tipos de gateway e plataformas de host. As configurações recomendadas também foram atualizadas para HealthNotifications e AvailabilityNotifications . Para obter mais informações, consulte .

2 de outubro de 2023

[Guias do usuário separadas do gateway de fitas e volumes](#)

O Guia do Usuário do Storage Gateway, que anteriormente continha informações sobre os tipos de fita e gateway de volumes, foi dividido entre Guia do Usuário do gateway de fitas e Guia do Usuário do gateway de volumes, em que cada um contém informações sobre apenas um tipo de gateway. Para obter mais informações, consulte o [Guia do usuário do gateway de fitas](#) e o [Guia do usuário do gateway de volumes](#).

23 de março de 2022

[Procedimentos atualizados de criação de gateway](#)

Os procedimentos para criar todos os tipos de gateway usando o console do Storage Gateway foram atualizados. Para obter mais informações, consulte [Como criar um gateway](#).

18 de janeiro de 2022

[Nova interface de fitas](#)

A página de visão geral da fita no AWS Storage Gateway console foi atualizada com novos recursos de pesquisa e filtragem. Todos os procedimentos relevantes deste guia foram atualizados para descrever a nova funcionalidade. Para obter mais informações, consulte [Como gerenciar um gateway de fitas](#).

23 de setembro de 2021

[Support para Quest NetVault Backup 13 for Tape Gateway](#)

Os gateways de fita agora oferecem suporte ao Quest NetVault Backup 13 em execução no Microsoft Windows Server 2012 R2 ou no Microsoft Windows Server 2016. Para obter mais informações, consulte [Testando sua configuração usando o Quest NetVault Backup](#).

22 de agosto de 2021

[Tópicos do gateway de arquivos do S3 removidos das guias de gateways de fitas e de volumes](#)

Para ajudar a facilitar o acompanhamento dos guias do usuário do gateway de fitas e do gateway de volumes para os clientes que estão configurando seus respectivos tipos de gateway, alguns tópicos desnecessários foram removidos.

21 de julho de 2021

[Compatibilidade com o IBM Spectrum Protect 8.1.10 no Windows e no Linux para o gateway de fitas](#)

Agora os gateways de fitas são compatíveis com o IBM Spectrum Protect versão 8.1.10 em execução no Microsoft Windows Server e Linux. Para obter mais informações, consulte [Como testar sua configuração usando o IBM Spectrum Protect](#).

24 de novembro de 2020

[Conformidade com o FedRAMP](#)

O Storage Gateway agora está em conformidade com o FedRAMP. Para obter mais informações, consulte [Validação de conformidade para o Storage Gateway](#).

24 de novembro de 2020

[Controle de utilização da largura de banda baseada em agendamento](#)

Agora o Storage Gateway é compatível com o controle de utilização de largura de banda baseada em agendamento para gateways de fitas e volumes. Para obter mais informações, consulte [Como programar o controle de utilização usando o console do Storage Gateway](#).

9 de novembro de 2020

[O volume em cache e o armazenamento em cache local dos gateways de fitas aumentam em quatro vezes](#)

O Storage Gateway agora é compatível com um cache local de até 64 TB para volumes em cache e gateways de fitas, melhorando o desempenho de aplicações on-premises ao fornecer acesso de baixa latência a conjuntos de dados de trabalho maiores. Para obter mais informações, consulte [Tamanhos de disco local recomendados para o gateway](#).

9 de novembro de 2020

Migração de gateway

Agora o Storage Gateway é compatível com a migração de gateways de volumes em cache para novas máquinas virtuais. Para obter mais informações, consulte [Como mover volumes em cache para uma nova máquina virtual do gateway de volumes em cache](#).

10 de setembro de 2020

[Support para bloqueio de retenção de fita e write-once-read-many proteção de fita \(WORM\)](#)

O Storage Gateway é compatível com o bloqueio de retenção de fitas em fitas virtuais e ao gravação única e várias leituras (WORM). O bloqueio de retenção de fitas permite especificar o modo e o período de retenção em fitas virtuais arquivadas, evitando que elas sejam excluídas por um período fixo de até 100 anos. Inclui controles de permissão sobre quem pode excluir fitas ou modificar as configurações de retenção. Para obter mais informações, consulte [Como usar o bloqueio de retenção de fitas](#). As fitas virtuais ativadas por WORM ajudam a garantir que os dados nas fitas ativas em sua biblioteca de fitas virtuais não possam ser sobrescritos ou apagados. Para obter mais informações, consulte [Proteção de fitas de gravação única e várias leituras \(WORM\)](#).

19 de agosto de 2020

[Solicite o dispositivo de hardware por meio do console](#)

Agora você pode solicitar o dispositivo de hardware por meio do AWS Storage Gateway console. Para obter mais informações, consulte [Como usar o Storage Gateway Hardware Appliance](#).

12 de agosto de 2020

[Compatibilidade com endpoints do padrão FIPS \(Padrão federal de processamento de informações\) em novas regiões da AWS](#)

Agora é possível ativar um gateway com endpoints FIPS nas regiões Leste dos EUA (Ohio), Leste dos EUA (Norte da Virgínia), Oeste dos EUA (Norte da Califórnia), Oeste dos EUA (Oregon) e Canadá (Central). Para obter mais informações, consulte [endpoints e cotas do AWS Storage Gateway](#) na Referência geral da AWS.

31 de julho de 2020

[Migração de gateway](#)

Agora o Storage Gateway é compatível com a migração de fitas e gateways de volumes armazenados para novas máquinas virtuais. Para obter mais informações, consulte [Como mover seus dados para um novo gateway](#).

31 de julho de 2020

[Veja os CloudWatch alarmes da Amazon no console do Storage Gateway](#)

Agora você pode ver CloudWatch os alarmes no console do Storage Gateway. Para obter mais informações, consulte .

29 de maio de 2020

[Compatibilidade com endpoints do padrão FIPS \(Padrão federal de processamento de informações\)](#)

Agora, é possível ativar um gateway com endpoints de FIPS nas regiões AWS GovCloud (US) . Para escolher um endpoint de FIPS para um gateway de volumes, consulte [Como escolher um endpoint de serviço](#). Para escolher um endpoint FIPS para um gateway de fitas, consulte [Conectar seu gateway de fitas à AWS](#).

22 de maio de 2020

[Novas AWS regiões](#)

Agora o Storage Gateway está disponível nas regiões África (Cidade do Cabo) e Europa (Milão). Para obter mais informações, consulte [endpoints e cotas do AWS Storage Gateway](#) na Referência geral da AWS.

7 de maio de 2020

[Compatibilidade com a classe de armazenamento S3 Intelligent-Tiering](#)

Agora o Storage Gateway é compatível com a classe de armazenamento S3 Intelligent-Tiering. A classe de armazenamento S3 Intelligent-Tiering otimiza os custos de armazenamento movendo automaticamente os dados para o nível de acesso ao armazenamento mais econômico, sem impacto no desempenho ou sobrecarga operacional. Para obter mais informações, consulte [Classe de armazenamento para otimizar automaticamente os objetos acessados com frequência e pouca frequência](#) no Guia do usuário do Amazon Simple Storage Service.

30 de abril de 2020

[Desempenho duas vezes maior de gravação e leitura do gateway de fitas](#)

O Storage Gateway aumenta em duas vezes o desempenho de leitura e gravação em fitas virtuais no gateway de fitas, permitindo que você realize backups e recuperações de maneira mais rápida que antes. Para obter mais informações, consulte [Orientação de desempenho para gateways de fitas](#) no Guia do usuário do Storage Gateway.

23 de abril de 2020

[Compatibilidade com a criação automática de fitas](#)

Agora o Storage Gateway oferece a capacidade de criar automaticamente novas fitas virtuais. O gateway de fitas cria automaticamente novas fitas virtuais para manter o número mínimo de fitas disponíveis configuradas e disponibiliza essas novas fitas para importação pela aplicação de backup, permitindo que seus trabalhos de backup sejam executados sem interrupção. Para obter mais informações, consulte [Como criar fitas automaticamente](#) no Guia do usuário do Storage Gateway.

23 de abril de 2020

[Nova AWS região](#)

O Storage Gateway agora está disponível na região AWS GovCloud (Leste dos EUA). Para obter mais informações, consulte [Endpoints e cotas do AWS Storage Gateway](#) na Referência geral da AWS.

12 de março de 2020

[Compatibilidade com o hipervisor de máquina virtual baseada em kernel \(KVM\) do Linux](#)

Agora o Storage Gateway oferece a possibilidade de implantar um gateway on-premises na plataforma de virtualização da KVM. Os gateways implantados na KVM têm todas as mesmas funcionalidades e recursos que os gateways locais existentes. Para obter mais informações, consulte [Hypervisores compatíveis e requisitos de host](#) no Guia do usuário do Storage Gateway.

4 de fevereiro de 2020

[Compatibilidade com o VMware vSphere High Availability](#)

Agora o Storage Gateway oferece suporte para alta disponibilidade no VMware para ajudar a proteger as workloads de armazenamento contra falhas de hardware, de hipervisor ou de rede. Para obter mais informações, consulte [Como usar o VMware vSphere High Availability com o Storage Gateway](#) no Guia do usuário do Storage Gateway. Esta versão também inclui melhorias de desempenho. Para obter mais informações, consulte [Desempenho](#) no Guia do usuário do Storage Gateway.

20 de novembro de 2019

[Nova AWS região para gateway de fitas](#)

Agora o gateway de fitas está disponível na região América do Sul (São Paulo). Para obter mais informações, consulte [Endpoints e cotas do AWS Storage Gateway](#) na Referência geral da AWS.

24 de setembro de 2019

[Compatibilidade com o IBM Spectrum Protect versão 7.1.9 no Linux e gateways de fitas com tamanho máximo de fita aumentado para 5 TiB](#)

Agora, os gateways de fitas são compatíveis com o IBM Spectrum Protect (Tivoli Storage Manager) versão 7.1.9 executado no Linux, além do executado no Microsoft Windows. Para obter mais informações, consulte [Como testar sua configuração com o IBM Spectrum Protect](#) no Guia do usuário do Storage Gateway. Além disso, para os gateways de fitas, o tamanho máximo de uma fita virtual agora aumenta de 2,5 TiB para 5 TiB. Para obter mais informações, consulte [Cotas para fitas](#) no Guia do usuário do Storage Gateway.

10 de setembro de 2019

[Support para Amazon CloudWatch Logs](#)

Agora você pode configurar gateways de arquivos com Amazon CloudWatch Log Groups para ser notificado sobre erros e a integridade do seu gateway e de seus recursos. Para obter mais informações, consulte [Receber notificações sobre a integridade e os erros do Gateway com grupos de CloudWatch log da Amazon](#) no Guia do usuário do Storage Gateway.

4 de setembro de 2019

[Nova AWS região](#)

Agora o Storage Gateway está disponível na região Ásia-Pacífico (Hong Kong) . Para obter mais informações, consulte [Endpoints e cotas do AWS Storage Gateway](#) na Referência geral da AWS.

14 de agosto de 2019

[Nova AWS região](#)

Agora o Storage Gateway está disponível na região do Oriente Médio (Bahrein) . Para obter mais informações, consulte [Endpoints e cotas do AWS Storage Gateway](#) na Referência geral da AWS.

29 de julho de 2019

[Compatibilidade com a ativação de um gateway em uma nuvem privada virtual \(VPC\)](#)

Agora é possível ativar um gateway em uma VPC. É possível criar uma conexão privada entre o dispositivo de software local e a infraestrutura de armazenamento baseada em nuvem. Para obter mais informações, consulte [Ativar um gateway em uma nuvem privada virtual.](#)

20 de junho de 2019

[Compatibilidade com a movimentação de uma fita do S3 Glacier Flexible Retrieval para o S3 Glacier Deep Archive](#)

Agora é possível mover suas fitas virtuais que estão arquivadas na classe de armazenamento S3 Glacier Flexible Retrieval para a classe de armazenamento S3 Glacier Deep Archive para ter retenção de dados econômica e a longo prazo. Para obter mais informações, consulte [Como mover uma fita do S3 Glacier Flexible Retrieval para o S3 Glacier Deep Archive.](#)

28 de maio de 2019

[Compatibilidade do compartilhamento de arquivos SMB para ACLs do Microsoft Windows](#)

Para os gateways de arquivos, agora é possível usar listas de controle de acesso (ACLs) do Microsoft Windows para controlar o acesso ao compartilhamento de arquivos Server Message Block (SMB). Para obter mais informações, consulte [Usar ACLs do Microsoft Windows para controlar o acesso a um compartilhamento de arquivos SMB](#).

8 de maio de 2019

[Integração com o S3 Glacier Deep Archive](#)

O gateway de fitas é integrado ao S3 Glacier Deep Archive. Agora é possível arquivar fitas virtuais no S3 Glacier Deep Archive para a retenção de dados em longo prazo. Para obter mais informações, consulte [Arquivar fitas virtuais](#).

27 de março de 2019

[Disponibilidade do Storage Gateway Hardware Appliance na Europa](#)

O Storage Gateway Hardware Appliance agora está disponível na Europa. Para obter mais informações, consulte [Regiões do equipamento de hardware do AWS Storage Gateway](#) na Referência geral da AWS. Além disso, agora é possível aumentar o armazenamento utilizável no Storage Gateway Hardware Appliance de 5 TB para 12 TB e substituir o cartão de rede de cobre instalado por um cartão de rede de fibra óptica de 10 gigabits. Para obter mais informações, consulte [Configurar seu dispositivo de hardware](#).

25 de fevereiro de 2019

[Integração com AWS Backup](#)

O Storage Gateway se integra com o AWS Backup. Agora você pode usar AWS Backup para fazer backup de aplicativos comerciais locais que usam volumes do Storage Gateway para armazenamento baseado em nuvem. Para obter mais informações, consulte [Fazer backup de seus volumes](#).

16 de janeiro de 2019

[Compatibilidade com Bacula Enterprise e IBM Spectrum Protect](#)

Agora os gateways de fitas são compatíveis com o Bacula Enterprise e IBM Spectrum Protect. Agora, o Storage Gateway também oferece suporte a versões mais recentes do backup Veritas NetBackup, Veritas Backup Exec e Quest. NetVault. Agora é possível usar essas aplicações de backup para fazer backup de dados no Amazon S3 e arquivá-los diretamente em armazenamento off-line (S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive). Para obter mais informações, consulte [Usar seu software de backup para testar uma configuração de gateway](#).

13 de novembro de 2018

[Compatibilidade com o Storage Gateway Hardware Appliance](#)

O Storage Gateway Hardware Appliance inclui o Storage Gateway pré-instalado em um servidor de terceiros. Você pode gerenciar o dispositivo do AWS Management Console. O dispositivo pode hospedar gateways de arquivos, fitas e volumes. Para obter mais informações, consulte [Como usar o Storage Gateway Hardware Appliance](#).

18 de setembro de 2018

[Compatibilidade com o Microsoft System Center 2016 Data Protection Manager \(DPM\)](#)

Os gateways de fitas agora são compatíveis com o Microsoft System Center 2016 Data Protection Manager (DPM). Agora é possível usar o Microsoft DPM para fazer backup de dados no Amazon S3 e arquivá-los diretamente em armazenamento off-line (S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive). Para obter mais informações, consulte [Como testar sua configuração com o Microsoft System Center Data Protection Manager](#).

18 de julho de 2018

[Compatibilidade com o protocolo de Server Message Block \(SMB\)](#)

Os gateways de arquivos acrescentaram suporte ao protocolo de Server Message Block (SMB) para compartilhamentos de arquivos. Para obter mais informações, consulte [Como criar um compartilhamento de arquivos](#).

20 de junho de 2018

[Compatibilidade com o compartilhamento de arquivos, volumes armazenados em cache e criptografia de fitas virtuais](#)

Agora você pode usar AWS Key Management Service (AWS KMS) para criptografar dados gravados em um compartilhamento de arquivos, volume em cache ou fita virtual. Atualmente, você pode fazer isso usando a API do AWS Storage Gateway . Para obter mais informações, consulte [Criptografia de dados por meio do AWS KMS](#).

12 de junho de 2018

[Support NovaStor DataCenter para/Network](#)

Os gateways de fita agora oferecem suporte NovaStor DataCenter a /Network. Agora você pode usar NovaStor DataCenter /Network versão 6.4 ou 7.1 para fazer backup de seus dados no Amazon S3 e arquivá-los diretamente no armazenamento off-line (S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive). Para obter mais informações, consulte [Testando sua configuração usando NovaStor DataCenter /Network](#).

24 de maio de 2018

Atualizações anteriores

A tabela a seguir descreve alterações importantes em cada versão do Guia do usuário do AWS Storage Gateway antes de maio de 2018.

Alteração	Descrição	Alterado em
Suporte à classe de armazenamento S3 One Zone_IA	Para os gateways de arquivos, agora é possível escolher o S3 One Zone_IA como a classe de armazenamento padrão para o compartilhamentos de arquivos. Ao usar esta classe de armazenamento, é possível armazenar seus dados de objetos em uma única zona de disponibilidade do Amazon S3. Para obter mais informações, consulte Criar um compartilhamento de arquivos .	4 de abril de 2018
Nova região da	Agora o gateway de fitas está disponível na região Ásia-Pacífico (Singapura). Para obter informações detalhadas, consulte AWS Regiões .	3 de abril de 2018
Compatibilidade com a notificação de atualização de cache, pagamento pelo solicitante e ACLs padrão para buckets do Amazon S3.	<p>Com os gateways de arquivo, é possível enviar notificações quando o gateway termina de atualizar o cache para seu bucket do Amazon S3. Para obter mais informações, consulte RefreshCache.html na Referência da API do Storage Gateway.</p> <p>Agora, os gateways de arquivos permitem que o solicitante ou leitor, em vez do proprietário do bucket, pague as cobranças de acesso.</p> <p>Os gateways de arquivo permitem conceder controle total ao proprietário do bucket do S3 que mapeia para o compartilhamento de arquivos NFS.</p> <p>Para obter mais informações, consulte Criar um compartilhamento de arquivos.</p>	1º de março de 2018
Support para Dell EMC NetWorker V9.x	Os gateways de fita agora oferecem suporte ao Dell EMC NetWorker V9.x. Agora você pode usar o Dell EMC NetWorker V9.x para fazer backup de seus dados no Amazon S3 e arquivá-los diretamente no armazenamento off-line (S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive). Para obter	27 de fevereiro de 2018

Alteração	Descrição	Alterado em
	mais informações, consulte Testando sua configuração usando a Dell EMC NetWorker .	
Nova região da	Agora o Storage Gateway está disponível na região Europa (Paris). Para obter informações detalhadas, consulte AWS Regiões .	18 de dezembro de 2017
Suporte para notificação de upload de arquivos e adivinhação do tipo MIME	<p>Agora, os gateways de arquivos enviam notificações quando todos os arquivos gravados no compartilhamento de arquivos NFS são carregados no Amazon S3. Para obter mais informações, consulte NotifyWhenUploaded na Referência da API do Storage Gateway.</p> <p>Agora, os gateways de arquivos permitem adivinhar o tipo MIME dos objetos carregados com base nas extensões de arquivo. Para obter mais informações, consulte Criar um compartilhamento de arquivos.</p>	21 de novembro de 2017
Compatibilidade com o VMware ESXi Hypervisor versão 6.5	AWS Storage Gateway agora oferece suporte ao VMware ESXi Hypervisor versão 6.5. Além das versões 4.1, 5.0, 5.1, 5.5 e 6.0. Para ter mais informações, consulte Hipervisores compatíveis e requisitos de host .	13 de setembro de 2017
Compatibilidade com o Commvault 11	Agora os gateways de fitas são compatíveis com o Commvault 11. Agora é possível usar o Commvault para fazer backup de dados no Amazon S3 e arquivá-los diretamente em armazenamento off-line (S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive). Para obter mais informações, consulte Como testar sua configuração usando o Commvault .	12 de setembro de 2017

Alteração	Descrição	Alterado em
Compatibilidade com gateway de arquivos do hipervisor do Microsoft Hyper-V	Agora é possível implantar um gateway de arquivos em um hipervisor do Microsoft Hyper-V. Para obter mais informações, consulte Hipervisores compatíveis e requisitos de host .	22 de junho de 2017
Suporte para três a cinco horas de recuperação de fita em arquivo	Em um gateway de fitas, agora é possível recuperar de três a cinco horas de fita do arquivo. Você pode também determinar o volume de dados do aplicativo de backup ou de sua biblioteca de fitas virtuais (VTL) gravados em sua fita. Para obter mais informações, consulte Como visualizar os detalhes da fita .	23 de maio de 2017
Nova região da	Agora o Storage Gateway está disponível na região da Ásia-Pacífico (Mumbai). Para obter informações detalhadas, consulte AWS Regiões .	02 de maio de 2017
Atualizações nas configurações de compartilhamento de arquivos	Agora, os gateway de arquivos adicionam opções de montagem às configurações do compartilhamento de arquivos. Agora você pode definir opções de esmagamento e somente leitura para o compartilhamento de arquivos. Para obter mais informações, consulte Criar um compartilhamento de arquivos .	28 de março de 2017
Compatibilidade com atualização de cache para compartilhamento de arquivos	Agora, os gateways de arquivos agora podem encontrar objetos no bucket do Amazon S3 que foram adicionados ou removidos desde que a última vez em que o gateway indicou conteúdo e resultados armazenados em cache do bucket. Para obter mais informações, consulte RefreshCache a Referência da API.	
Compatibilidade com clonagem de volume	Para gateways de volume em cache, AWS Storage Gateway agora oferece suporte à capacidade de clonar um volume de um volume existente. Para obter mais informações, consulte Como clonar um volume .	16 de março de 2017

Alteração	Descrição	Alterado em
Compatibilidade com gateways de arquivos no Amazon EC2	AWS Storage Gateway agora fornece a capacidade de implantar um gateway de arquivos no Amazon EC2. É possível ativar um gateway de arquivos no Amazon EC2 usando a Imagem de Máquina da Amazon (AMI) do Storage Gateway, agora disponível como uma AMI de comunidade. Para obter informações sobre como criar um gateway de arquivos e implantá-lo em uma instância do EC2, consulte Criar e ativar um Amazon S3 File Gateway ou Criar e ativar um Amazon FSx File Gateway . Para obter informações sobre como iniciar uma AMI de gateway de arquivos, consulte Como implantar um S3 File Gateway em um host do Amazon EC2 ou Como implantar o FSx File Gateway em um host do Amazon EC2 .	08 de fevereiro de 2017
Compatibilidade como Arcserve 17	Agora o gateway de fitas é compatível com o Arcserve 17. Agora é possível usar o Arcserve para fazer backup de seus dados no Amazon S3 e arquivar diretamente no S3 Glacier Flexible Retrieval. Para obter mais informações, consulte Como testar sua configuração usando o Arcserve Backup r17.0 .	17 de janeiro de 2017
Nova região da	Agora o Storage Gateway está disponível na região UE (Londres). Para obter informações detalhadas, consulte AWS Regiões .	13 de dezembro de 2016
Nova região da	Agora o Storage Gateway está disponível na região Canadá (Central). Para obter informações detalhadas, consulte AWS Regiões .	08 de dezembro de 2016

Alteração	Descrição	Alterado em
Suporte para gateway de arquivos	Além dos gateways de volumes e do gateway de fitas, o Storage Gateway agora fornece o gateway de arquivos. O gateway de arquivos é ao mesmo tempo um serviço e um dispositivo de software virtual que permite que você armazene e recupere objetos no Amazon S3 usando protocolos de arquivo padrão do setor, como o Network File System (NFS). O gateway oferece acesso a objetos no Amazon S3 como arquivos em um ponto de montagem NFS.	29 de novembro de 2016
Backup Exec 16	Agora o gateway de fitas é compatível com o Backup Exec 16. Agora é possível usar o Backup Exec 16 para fazer backup de dados no Amazon S3 e arquivá-los diretamente em armazenamento off-line (S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive). Para obter mais informações, consulte Como testar sua configuração com o Veritas Backup Exec .	7 de novembro de 2016
Compatibilidade com o Micro Focus (HPE) Data Protector 9.x	Agora o gateway de fitas é compatível com o Micro Focus (HPE) Data Protector 9.x. Agora é possível usar o HPE Data Protector para fazer backup de seus dados no Amazon S3 e arquivar diretamente no S3 Glacier Flexible Retrieval. Para obter mais informações, consulte Como testar sua configuração por meio do Micro Focus (HPE) Data Protector .	2 de novembro de 2016
Nova região da	Agora o Storage Gateway está disponível na região Leste dos EUA (Ohio). Para obter informações detalhadas, consulte AWS Regiões .	17 de outubro de 2016

Alteração	Descrição	Alterado em
Redefinição do console do Storage Gateway	O Storage Gateway Management Console foi redefinido para facilitar a configuração, o gerenciamento e o monitoramento de gateways, volumes e fitas virtuais. A interface do usuário agora fornece visualizações que podem ser filtradas e fornece links diretos para AWS serviços integrados, como CloudWatch e Amazon EBS. Para ter mais informações, consulte Inscreva-se para AWS Storage Gateway .	30 de agosto de 2016
Compatibilidade com o Veeam Backup & Replication V9 Update 2 ou posterior	Agora o gateway de fitas é compatível com o Veeam Backup & Replication V9 Update 2 ou posterior (isto é, versão 9.0.0.1715 ou posterior). Agora é possível usar o Veeam Backup Replication V9 Update 2 ou posterior para fazer backup de dados no Amazon S3 e arquivá-los diretamente em armazenamento off-line (S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive). Para obter mais informações, consulte Como testar sua configuração com o Veeam Backup & Replication .	15 de agosto de 2016
IDs mais longos de volume e snapshot	O Storage Gateway está introduzindo IDs mais longos para volumes e snapshots. Você pode ativar o formato de ID mais longo para seus volumes, instantâneos e outros AWS recursos compatíveis. Para ter mais informações, consulte Como entender os recursos e IDs de recursos do Storage Gateway .	25 de abril de 2016

Alteração	Descrição	Alterado em
<p>Nova região da</p> <p>Suporte para armazenamento de no máximo de 512 TiB de tamanho para volumes armazenados</p> <p>Outras atualizações de gateway e aperfeiçoamentos no console local do Storage Gateway</p>	<p>Agora o gateway de fitas está disponível na região da Ásia-Pacífico (Seul). Para ter mais informações, consulte AWS Regiões.</p> <p>Para volumes armazenados, agora você pode criar até 32 volumes de armazenamento, cada um com até 16 TiB de tamanho, para um armazenamento máximo de 512 TiB. Para obter mais informações, consulte Arquitetura de volumes armazenados e AWS Storage Gateway cotas.</p> <p>O tamanho total de todas as fitas em uma biblioteca de fitas virtuais foi ampliado para 1 PiB. Para ter mais informações, consulte AWS Storage Gateway cotas.</p> <p>Agora é possível definir a senha para o console local da VM no console do Storage Gateway. Para obter mais informações, consulte Como definir a senha do console local no console do Storage Gateway.</p>	<p>21 de março de 2016</p>
<p>Compatibilidade com para Dell EMC NetWorker 8.x</p>	<p>O Tape Gateway agora é compatível com o Dell EMC NetWorker 8.x. Agora você pode usar a Dell EMC NetWorker para fazer backup de seus dados no Amazon S3 e arquivá-los diretamente no armazenamento off-line (S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive). Para obter mais informações, consulte Testando sua configuração usando a Dell EMC NetWorker.</p>	<p>29 de fevereiro de 2016</p>

Alteração	Descrição	Alterado em
Compatibilidade com o VMware ESXi Hypervisor versão 6.0 e o iniciador iSCSI Red Hat Enterprise Linux 7	AWS Storage Gateway agora suporta o VMware ESXi Hypervisor versão 6.0 e o iniciador iSCSI Red Hat Enterprise Linux 7. Para obter mais informações, consulte Hypervisores compatíveis e requisitos de host e Iniciadores iSCSI compatíveis .	20 de outubro de 2015
Reestruturação de conteúdo	Essa versão inclui a seguinte melhoria: a documentação agora inclui uma seção sobre gerenciamento de gateway ativado que associa tarefas de gerenciamento comuns a todas as soluções de gateway. A seguir você pode encontrar instruções sobre como gerenciar seu gateway depois de implantá-lo e ativá-lo. Para ter mais informações, consulte Como gerenciar seu gateway .	

Alteração	Descrição	Alterado em
<p>Suporte para armazenamento de no máximo de 1.024 TiB de tamanho para volumes armazenados em cache</p> <p>Compatibilidade com o tipo de adaptador de rede VMXNET3 (10 GbE) no hipervisor do VMware ESXi</p> <p>Melhorias de desempenho</p> <p>Diversas melhorias e atualizações no console local do Storage Gateway</p>	<p>Com relação aos volumes armazenados em cache, agora você pode criar até 32 volumes de armazenamento, cada um com até 32 TiB, para um armazenamento máximo de 1.024 TiB. Para obter mais informações, consulte Arquitetura de volumes em cache e AWS Storage Gateway cotas.</p> <p>Se seu gateway estiver hospedado em um hipervisor do VMware ESXi, você poderá reconfigurá-lo para usar o tipo de adaptador VMXNET3. Para ter mais informações, consulte Como configurar adaptadores de rede para seu gateway.</p> <p>A velocidade máxima de upload no Storage Gateway aumentou para 120 MB por segundo e a velocidade máxima de download aumentou para 20 MB por segundo.</p> <p>O console local do Storage Gateway foi atualizado e aprimorado com outros atributos para ajudar você a executar tarefas de manutenção. Para ter mais informações, consulte Como configurar uma rede de gateway.</p>	<p>16 de setembro de 2015</p>
<p>Compatibilidade com atribuição de tags</p>	<p>Agora o Storage Gateway é compatível com a marcação de recursos. Agora você pode adicionar tags a gateways, volumes e fitas virtuais para torná-los mais fácil de gerenciar. Para ter mais informações, consulte Como atribuir tags a recursos do Storage Gateway.</p>	<p>2 de setembro de 2015</p>

Alteração	Descrição	Alterado em
Compatibilidade com o Quest (antigo Dell) NetVault Backup 10.0	O Tape Gateway agora é compatível com o Quest NetVault Backup 10.0. Agora você pode usar o Quest NetVault Backup 10.0 para fazer backup de seus dados no Amazon S3 e arquivá-los diretamente no armazenamento off-line (S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive). Para obter mais informações, consulte Testando sua configuração usando o Quest NetVault Backup .	22 de junho de 2015

Alteração	Descrição	Alterado em
Suporte para volumes de armazenamento de 16 TiB para configurações de gateway de volumes armazenados	Agora o Storage Gateway é compatível com volumes de armazenamento de 16 TiB para configurações de gateway de volumes armazenados. Agora você pode criar 12 volumes de armazenamento de 16 TiB, para um armazenamento máximo de 192 TiB. Para obter mais informações, consulte Arquitetura de volumes armazenados .	3 de junho de 2015
Compatibilidade com as verificações de recursos do sistema no console local do Storage Gateway	Agora você pode determinar se os recursos do sistema (núcleos virtuais de CPU, tamanho do volume raiz e RAM) são suficientes para seu gateway funcionar corretamente. Para obter mais informações, consulte Como exibir o status de recursos de sistema do gateway ou Como exibir o status de recursos de sistema do gateway .	
Compatibilidade com o iniciador iSCSI Red Hat Enterprise Linux 6	<p>Agora o Storage Gateway é compatível com o iniciador iSCSI Red Hat Enterprise Linux 6. Para ter mais informações, consulte Requisitos.</p> <p>Esta versão inclui as seguintes melhorias e atualizações no Storage Gateway:</p> <ul style="list-style-type: none">No console do Storage Gateway, agora é possível ver a data e a hora em que a última atualização de software bem-sucedida foi aplicada ao seu gateway. Para ter mais informações, consulte Gerenciando atualizações de gateway usando o AWS Storage Gateway console.Agora o Storage Gateway oferece uma API que pode ser usada para listar os iniciadores iSCSI conectados aos volumes de armazenamento. Para	

Alteração	Descrição	Alterado em
	<p>obter mais informações, consulte ListVolumelInitiators referência da API.</p>	
<p>Compatibilidade com o hipervisor do Microsoft Hyper-V versões 2012 e 2012 R2</p>	<p>Agora o Storage Gateway é compatível com o hipervisor do Microsoft Hyper-V versões 2012 e 2012 R2. Trata-se de um complemento para compatibilidade com o hipervisor do Microsoft Hyper-V versão 2008 R2. Para ter mais informações, consulte Hipervisores compatíveis e requisitos de host.</p>	<p>30 de abril de 2015</p>
<p>Compatibilidade com o Symantec Backup Exec 15</p>	<p>Agora o gateway de fitas é compatível com o Symantec Backup Exec 15. Agora é possível usar o Symantec Backup Exec 15 para fazer backup de dados no Amazon S3 e arquivá-los diretamente em armazenamento off-line (S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive). Para obter mais informações, consulte Como testar sua configuração com o Veritas Backup Exec.</p>	<p>6 de abril de 2015</p>
<p>Compatibilidade com autenticação CHAP para volumes de armazenamento</p>	<p>Agora o Storage Gateway é compatível com a configuração de autenticação CHAP para volumes de armazenamento. Para obter mais informações, consulte Configurar a autenticação CHAP para os volumes.</p>	<p>2 de abril de 2015</p>
<p>Compatibilidade com o VMware ESXi Hypervisor versões 5.1 e 5.5</p>	<p>Agora o Storage Gateway é compatível com o VMware ESXi Hypervisor versões 5.1 e 5.5. Oferece suporte para VMware ESXi Hypervisor versões 4.1 e 5.0. Para ter mais informações, consulte Hipervisores compatíveis e requisitos de host.</p>	<p>30 de março de 2015</p>

Alteração	Descrição	Alterado em
Compatibilidade com o utilitário o Windows CHKDSK	Agora o Storage Gateway é compatível com o utilitário o Windows CHKDSK. Você pode usar esse utilitário para verificar a integridade e corrigir erros em seus volumes. Para obter mais informações, consulte Como solucionar problemas de volume .	04 de março de 2015
Integração com AWS CloudTrail para capturar chamadas de API	<p>O Storage Gateway agora está integrado com AWS CloudTrail o. AWS CloudTrail captura chamadas de API feitas por ou em nome do Storage Gateway em sua conta da Amazon Web Services e entrega os arquivos de log para um bucket do Amazon S3 que você especificar. Para ter mais informações, consulte Registro e monitoramento em AWS Storage Gateway.</p> <p>Esta versão inclui a seguinte melhoria e atualização no Storage Gateway:</p> <ul style="list-style-type: none">• Agora as fitas virtuais que têm dados sujos no armazenamento em cache (isto é, que guardam conteúdo não carregado para a AWS) são recuperadas quando um disco do gateway armazenado em cache é alterado. Para obter mais informações, consulte Como recuperar uma fita virtual de um gateway irrecuperável.	16 de dezembro de 2014

Alteração	Descrição	Alterado em
Compatibilidade com software de backup e alterador de mídia adicionais	<p>Agora o gateway de fitas é compatível com o software de backup a seguir:</p> <ul style="list-style-type: none">• Symantec Backup Exec 2014• Microsoft System Center 2012 R2 Data Protection Manager• Veeam Backup & Replication V7• Veeam Backup & Replication V8 <p>Agora é possível usar esses quatro produtos de software de backup com a biblioteca de fitas virtuais (VTL) do Storage Gateway para fazer backup no Amazon S3 e arquivar diretamente em armazenamento off-line (S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive). Para obter mais informações, consulte Usar seu software de backup para testar uma configuração de gateway.</p> <p>Agora o Storage Gateway oferece outro conversor de mídia que funciona com o novo software de backup.</p> <p>Esta versão inclui diversas melhorias e atualizações. AWS Storage Gateway</p>	3 de novembro de 2014
Região Europa (Frankfurt)	Agora o Storage Gateway está disponível também na região da Europa (Frankfurt). Para obter informações detalhadas, consulte AWS Regiões .	23 de outubro de 2014

Alteração	Descrição	Alterado em
Reestruturação de conteúdo	Foi criada uma seção de conceitos básicos comum para todas as soluções de gateway. A seguir você pode encontrar instruções que para fazer download, implantar e ativar um gateway. Depois que implantar e ativar um gateway, será possível prosseguir para obter mais instruções específicas para volumes armazenados em cache e configurações do gateway de fitas. Para obter mais informações, consulte Como criar um gateway de fitas .	19 de maio de 2014
Compatibilidade com o Symantec Backup Exec 2012	Agora o gateway de fitas é compatível com o Symantec Backup Exec 2012. Agora é possível usar o Symantec Backup Exec 2012 para fazer backup de dados no Amazon S3 e arquivá-los diretamente em armazenamento off-line (S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive). Para obter mais informações, consulte Como testar sua configuração com o Veritas Backup Exec .	28 de abril de 2014

Alteração	Descrição	Alterado em
Compatibilidade com o Windows Server Failover Clustering	<ul style="list-style-type: none">• Agora o Storage Gateway permite a conexão de vários hosts com um mesmo volume quando os hosts coordenam o acesso por meio do Windows Server Failover Clustering (WSFC). No entanto, você não pode conectar vários hosts com esse mesmo volume sem usar o WSFC.	31 de janeiro de 2014
Compatibilidade com o iniciador do VMware ESX	<ul style="list-style-type: none">• Agora o Storage Gateway permite que você gerencie diretamente a conectividade de armazenamento por meio do host ESX. Com isso, você tem a opção de usar iniciadores residentes no sistema operacional de suas VMs.	
Compatibilidade com a execução de tarefas de configuração no console local do Storage Gateway	<ul style="list-style-type: none">• Agora o Storage Gateway é compatível com a execução de tarefas de configuração no console local do Storage Gateway. Para obter mais informações sobre a execução de tarefas de configuração em gateways implantados no local, consulte Realizar tarefas no console local da VM do ou Realizar tarefas no console local da VM do . Para obter mais informações sobre a execução de tarefas de configuração em gateways implantados em uma Instância EC2, consulte Como realizar tarefas no console local do Amazon EC2 ou Como realizar tarefas no console local do Amazon EC2.	

Alteração	Descrição	Alterado em
Compatibilidade com biblioteca de fitas virtuais (VTL) e introdução da API versão 30/06/2013	<p>O Storage Gateway conecta um dispositivo de software local ao armazenamento baseado em nuvem para integrar seu ambiente de TI local à infraestrutura de armazenamento. Além dos gateways de volumes (volumes armazenados em cache e volumes armazenados), agora o Storage Gateway é compatível com o gateway-biblioteca de fitas virtuais (VTL). É possível configurar o gateway de fitas com até dez unidades virtuais de fita por gateway. Como as unidades virtuais de fita respondem ao conjunto de comandos SCSI, seus aplicativos locais de backup vão continuar funcionando sem nenhuma modificação. Para obter mais informações, consulte os seguintes tópicos no Guia do usuário do AWS Storage Gateway :</p> <ul style="list-style-type: none">• Para uma visão geral da arquitetura, consulte Como funciona o gateway de fitas (arquitetura).• Para começar a usar o gateway de fitas, consulte Como criar gateway de fitas.	5 de novembro de 2013
Compatibilidade com o Microsoft Hyper-V	<p>Agora o Storage Gateway oferece a possibilidade de implantar um gateway on-premises na plataforma de virtualização Microsoft Hyper-V. Os gateways implantados no Microsoft Hyper-V têm os mesmos recursos e atributos do gateway de armazenamento on-premises existente. Para começar a implantar um gateway com o Microsoft Hyper-V, consulte Hipervisores compatíveis e requisitos de host.</p>	10 de abril de 2013

Alteração	Descrição	Alterado em
Compatibilidade com a implantação de um gateway no Amazon EC2	Agora o Storage Gateway fornece a capacidade de implantar um gateway no Amazon Elastic Compute Cloud (Amazon EC2). É possível iniciar uma instância de gateway no Amazon EC2 usando a AMI do Storage Gateway disponível em AWS Marketplace . Para começar a implantar um gateway usando a AMI do Storage Gateway, consulte Como implantar uma instância do Amazon EC2 para hospedar seu gateway de volumes .	15 de janeiro de 2013

Alteração	Descrição	Alterado em
Compatibilidade para volumes armazenados em cache e introdução da API versão 30/06/2012	<p>Nesta versão, o Storage Gateway passa a ser compatível com volumes armazenados em cache. Os volumes armazenados em cache minimizam a necessidade de redimensionar a infraestrutura de armazenamento local e ao mesmo oferece aos seus aplicativos acesso de baixa latência a dados ativos. Você pode criar volumes de armazenamento de até 32 TiB e montá-los como dispositivos iSCSI nos servidores de aplicativos locais. Os dados gravados nesses volumes armazenados em cache são armazenados no Amazon Simple Storage Service (Amazon S3) e apenas um cache dos dados recém-gravados e lidos será armazenado localmente em seu hardware de storage on-premises. Os volumes armazenados em cache permitirão que você use o Amazon S3 para dados em que latências de recuperação mais elevadas são aceitáveis, como dados mais antigos raramente acessados, e ao mesmo manterão o armazenamento on-premises para dados que exigem acesso de baixa latência.</p> <p>Nesta versão, o Storage Gateway também introduz uma nova versão de API que, além de ser compatível com as operações atuais, oferece novas operações para ser compatível com volumes armazenados em cache.</p> <p>Para obter mais informações sobre as duas soluções do Storage Gateway, consulte Como funciona o gateway de volumes (arquitetura).</p> <p>Você pode também experimentar uma configuração de teste. Para obter instruções, consulte Como criar um gateway de fitas.</p>	29 de outubro de 2012

Alteração	Descrição	Alterado em
Compatibilidade com API e o IAM	<p>Nesta versão, o Storage Gateway introduz o suporte à API, bem como o suporte para AWS Identity and Access Management(IAM).</p> <ul style="list-style-type: none">• Compatibilidade da API: agora é possível configurar e gerenciar programaticamente os recursos do Storage Gateway. Para obter mais informações sobre a API, consulte Referência de API para o Storage Gateway no Guia do usuário do AWS Storage Gateway .• Compatibilidade com o IAM: o AWS Identity and Access Management (IAM) permite criar usuários e gerenciar o acesso deles aos recursos do Storage Gateway por meio de políticas do IAM. Para obter políticas demonstrativas do IAM, consulte Identity and Access Management para AWS Storage Gateway. Para mais informações sobre o IAM, consulte a página de detalhes do AWS Identity and Access Management (IAM).	9 de maio de 2012
Compatibilidade com IP estático	<p>Agora você pode especificar um endereço IP estático para seu gateway local. Para ter mais informações, consulte Como configurar uma rede de gateway.</p>	5 de março de 2012
Novo guia	<p>Esta é a primeira versão do Guia do usuário do AWS Storage Gateway .</p>	24 de janeiro de 2012

Notas de versão do software Volume Gateway Appliance

Essas notas de versão descrevem os recursos, aprimoramentos e correções novos e atualizados incluídos em cada versão do dispositivo Volume Gateway. Cada versão do software é identificada por sua data de lançamento e um número de versão exclusivo.

Você pode determinar o número da versão do software de um gateway verificando sua página de detalhes no console do Storage Gateway ou chamando a ação da [DescribeGatewayInformation](#) API usando um AWS CLI comando semelhante ao seguinte:

```
aws storagegateway describe-gateway-information --gateway-arn
"arn:aws:storagegateway:us-west-2:123456789012:gateway/sgw-12A3456B"
```

O número da versão é retornado no `SoftwareVersion` campo da resposta da API.

Note

Um gateway não reportará informações sobre a versão do software nas seguintes circunstâncias:

- O gateway está off-line.
- O gateway está executando um software antigo que não oferece suporte a relatórios de versão.
- O tipo de gateway é FSx File Gateway.

Para obter mais informações sobre as atualizações do Volume Gateway, incluindo como modificar o cronograma padrão de manutenção automática e atualização de um gateway, consulte [Gerenciando atualizações do gateway usando o console do AWS Storage Gateway](#).

Data de lançamento	Versão do software	Notas da versão
2024-05-28	2.9.0	<ul style="list-style-type: none">• Tempo reduzido de reinicialização do gateway durante atualizações de software• Reduziu a quantidade de dados transferidos para

Data de lançamento	Versão do software	Notas da versão
		estimar a largura de banda da rede
2024-05-08	2.8.3	<ul style="list-style-type: none">Foi resolvido um problema de conectividade na nuvem ao usar o proxy SOCKS5
2024-04-10	2.8.1	<ul style="list-style-type: none">Resolveu um problema de uso de memória introduzido na versão 2.8.0Atualizações de patches de segurançaProcesso aprimorado de atualização de softwareSolucionou o component e Network Time Protocol (NTP) ausente para novos gateways
2024-03-06	2.8.0	<ul style="list-style-type: none">Atualizações do sistema operacional para novos gatewaysAtualizações de patches de segurança
2023-12-19	2.7.0	<ul style="list-style-type: none">Atualizações do sistema operacional para novos gateways
2023-12-14	2.6.6	<ul style="list-style-type: none">Versão de manutenção