Guia do usuário

AWSStorage Gateway

Versão da API 2013-06-30

AWSStorage Gateway: Guia do usuário

Table of Contents

O que é o Amazon S3 File Gateway

AWSO Storage Gateway conecta um dispositivo de software local a um armazenamento em nuvem para oferecer uma integração perfeita e segura entre um ambiente de TI local e oAWSInfraestrutura de armazenamento. Você pode usar o serviço para armazenar dados naAWSNuvem para armazenamento escalável e econômico que ajuda a manter a segurança dos dados.AWS O Storage Gateway oferece soluções de armazenamento em arquivos, volumes e fitas.

Tópicos

Amazon S3 File Gateway

Amazon S3 File Gateway—O Amazon S3 File Gateway oferece suporte a uma interface de arquivo noAmazon Simple Storage Service (Amazon S3)E combina um serviço e um dispositivo de software virtual. Ao usar essa combinação, você pode armazenar e recuperar objetos no Amazon S3 por meio de protocolos de arquivo padrão do setor, como o Network File System (NFS) e Server Message Block (SMB). O dispositivo de software ou gateway é implantado no ambiente no local como uma máquina virtual (VM) em execução no hipervisor VMware ESXi, Microsoft Hyper-V ou Linux Kernel-based Virtual Machine (KVM). O gateway oferece acesso a objetos no S3 como arquivos ou pontos de montagem de compartilhamento de arquivo. Com o S3 File Gateway, você pode fazer o seguinte:

- Agora você pode armazenar e recuperar arquivos diretamente usando o protocolo NFS versão 3 ou 4.1.
- Agora você pode armazenar e recuperar arquivos diretamente usando a versão de sistema de arquivo SMB, protocolo 2 e 3.
- Você pode acessar seus dados diretamente no Amazon S3AWSAplicativo ou serviço em nuvem.
- Você pode gerenciar seus dados do Amazon por meio de políticas de ciclo de vida, replicação entre regiões e controle de versões. Você pode pensar no S3 File Gateway como uma montagem de sistema de arquivo no Amazon S3.

O S3 File Gateway simplifica o armazenamento de arquivos no Amazon S3, integra-se a aplicativos existentes por meio de protocolos de sistema de arquivos padrão do setor e constitui uma alternativa econômica de armazenamento local. Além disso, oferece acesso de baixa latência aos dados por meio de armazenamento em cache local transparente. Um gateway de arquivos S3 gerencia

a transferência de dados de e paraAWS, protege os aplicativos contra congestionamentos de rede, otimiza e transmite dados em paralelo e gerencia o consumo de largura de banda. O S3 File Gateway integra-se comAWSserviços, por exemplo, com o seguinte:

- Gerenciamento de acesso comum usando o AWS Identity and Access Management (IAM)
- Uso de Criptografia AWS Key Management Service (AWS KMS)
- Monitoramento usando o Amazon CloudWatch (CloudWatch)
- Uso de auditoriaAWS CloudTrail(CloudTrail)
- Operações usando o AWS Management Console e a AWS Command Line Interface (AWS CLI)
- Faturamento e gerenciamento de custos

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:

- fornece instruções sobre como criar e usar um gateway de arquivos do S3. Mostra como criar um compartilhamento de arquivos, mapear sua unidade para um bucket do Amazon S3 e fazer upload de arquivos e pastas para o Amazon S3.

- descreve como executar tarefas de gerenciamento para todos os tipos de gateway e recurso.

Neste guia, você encontra principalmente instruções sobre como trabalhar com operações de gateway usando o AWS Management Console. Se você quiser executar essas operações de forma programática, consulteAWSReferência da Storage Gateway.

Como o Storage Gateway funciona (arquitetura)

A seguir, você encontrará uma visão geral da arquitetura das soluções disponíveis Storage Gateway.

Tópicos

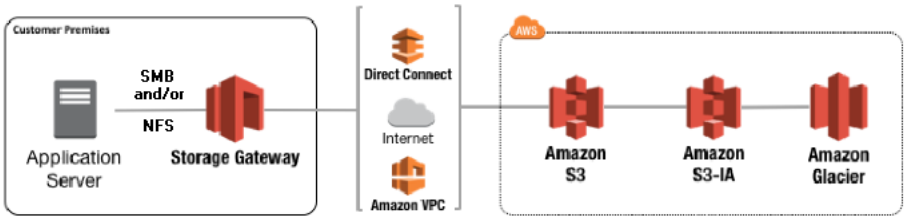
Gateways de arquivos do Amazon S3

Para usar um S3 File Gateway, você precisa primeiro fazer download de uma imagem da VM para o gateway. Em seguida, você ativa o gateway a partir doAWS Management Consoleou por meio da Storage Gateway API. Também é possível criar um S3 File Gateway usando uma imagem do Amazon EC2.

Depois que o S3 File Gateway for ativado, crie e configure o compartilhamento de arquivos e associe-o ao bucket do Amazon Simple Storage Service (Amazon S3). Isso torna o compartilhamento acessível por clientes usando o protocolo Network File System (NFS) ou Server Message Block (SMB). Os arquivos gravados em um compartilhamento de arquivos tornam-se objetos no Amazon S3, com o caminho como chave. Há um mapeamento individualizado entre arquivos e objetos, e o gateway atualiza assincronamente os objetos no Amazon S3 à medida que você altera os arquivos. Os objetos existentes no bucket do Amazon S3 aparecem como arquivos no sistema de arquivos e a chave transforma-se o caminho. Os objetos são criptografados com o Amazon S3 — chaves de criptografia no lado do servidor (SSE-S3). Todas as transferências de dados são feitas por meio de HTTPS.

O serviço otimiza a transferência de dados entre o gateway eAWSUsando multipart uploads paralelos ou downloads de intervalo de bytes para usar melhor a largura de banda disponível. O cache local é mantido para fornecer acesso de baixa latência aos dados acessados recentemente e reduzir os encargos de saída de dados. As métricas do CloudWatch fornecem informações sobre o uso de recursos na VM e a transferência de dados para e deAWS. O CloudTrail rastreia todas as chamadas da API.

Com o armazenamento do S3 File Gateway, é possível realizar tarefas como ingerir cargas de trabalho da nuvem para o Amazon S3, fazer backup e arquivamento, estratificação e migração de dados de armazenamento para oAWSNuvem. O diagrama a seguir fornece uma visão geral da implantação do armazenamento do Storage Gateway.



O S3 File Gateway converte arquivos em objetos S3 ao fazer upload de arquivos para o Amazon S3. A interação entre as operações de arquivos executadas em compartilhamentos de arquivos no S3 File Gateway e objetos S3 exige que determinadas operações sejam cuidadosamente consideradas ao converter entre arquivos e objetos.

As operações de arquivo comuns alteram os metadados do arquivo, o que resulta na exclusão do objeto S3 atual e na criação de um novo objeto S3. A tabela a seguir mostra exemplos de operações de arquivo e o impacto nos objetos do S3.

Operação de arquivos	Impacto no objeto do S3	Implicação da classe de armazenamento
Renomear arquivo	Substitui o objeto S3 existente e cria um novo objeto S3 para cada arquivo	Taxas de exclusão antecipada e taxas de recuperação podem ser aplicadas
Renomear pasta	Substitui todos os objetos do S3 existentes e cria novos objetos do S3 para cada pasta e arquivos na estrutura de pastas	Taxas de exclusão antecipada e taxas de recuperação podem ser aplicadas
Alterar permissões de arquivo/pasta	Substitui o objeto S3 existente e cria um novo objeto S3 para cada arquivo ou pasta	Taxas de exclusão antecipada e taxas de recuperação podem ser aplicadas
Alterar a propriedade de arquivo/pasta	Substitui o objeto S3 existente e cria um novo objeto S3 para cada arquivo ou pasta	Taxas de exclusão antecipada e taxas de recuperação podem ser aplicadas

Operação de arquivos	Impacto no objeto do S3	Implicação da classe de armazenamento
Anexar a um arquivo	Substitui o objeto S3 existente e cria um novo objeto S3 para cada arquivo	Taxas de exclusão antecipada e taxas de recuperação podem ser aplicadas

Quando um arquivo é gravado no S3 File Gateway por um cliente NFS ou SMB, o gateway de arquivos carrega os dados do arquivo para o Amazon S3 seguidos de seus metadados (proprietários, carimbos de data/hora, etc.). O upload dos dados do arquivo cria um objeto S3 e o upload dos metadados do arquivo atualiza os metadados do objeto S3. Esse processo cria outra versão do objeto, resultando em duas versões de um objeto. Se o Versionamento do S3 estiver habilitado, ambas as versões serão armazenadas.

Quando um arquivo é modificado no S3 File Gateway por um cliente NFS ou SMB depois de ter sido carregado para o Amazon S3, o S3 File Gateway carrega os dados novos ou modificados em vez de fazer upload do arquivo inteiro. A modificação do arquivo resulta em uma nova versão do objeto S3 que está sendo criada.

Quando o S3 File Gateway carrega arquivos maiores, talvez seja necessário fazer upload de blocos menores do arquivo antes que o cliente termine de gravar no S3 File Gateway. Alguns motivos para isso incluem liberar espaço em cache ou uma alta taxa de gravações em um compartilhamento de arquivos. Isso pode resultar em várias versões de um objeto no bucket do S3.

Você deve monitorar o bucket do S3 para determinar quantas versões de um objeto existem antes de configurar políticas de ciclo de vida para mover objetos para diferentes classes de armazenamento. Você deve configurar a expiração do ciclo de vida para versões anteriores para minimizar o número de versões que você tem para um objeto no bucket do S3. O uso de replicação de mesma região (SRR) ou CRR (replicação entre regiões) entre buckets do S3 aumentará o armazenamento usado.

Configuração do Amazon S3 File Gateway

Esta seção fornece instruções para começar a usar o Amazon S3 File Gateway. Para começar a usá-lo, primeiro registre-se noAWS. Se você estiver usando o pela primeira vez, recomendamos que você leia oRegiões daeRequisitosSeções.

Tópicos

Cadastre-se na Amazon Web Services

Se você ainda não tem uma Conta da AWS, siga as etapas a seguir para criar uma.

Para se cadastrar em uma Conta da AWS

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

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

Criar um usuário do IAM

Depois de criar oAWSconta, use as etapas a seguir para criar umAWS Identity and Access Management(IAM) usuário para você. Em seguida, você adiciona esse usuário a um grupo que tem permissões administrativas.

Para criar um usuário administrador para você mesmo e adicionar o usuário a um grupo de administradores (console)

1. Faça login no console do IAM como proprietário da conta escolhendo Root user (Usuário root) e inserindo o endereço de e-mail da sua Conta da AWS. Na próxima página, insira sua senha.

> **Note**
>
> Recomendamos seguir as práticas recomendadas para utilizar o usuário do IAM **`Administrator`** a seguir e armazenar as credenciais do usuário raiz com segurança. Cadastre-se como o usuário raiz apenas para executar algumas tarefas de gerenciamento de serviços e contas.

2. No painel de navegação, escolha Usuários e depois Adicionar usuário.
3. Em User name (Nome do usuário), digite **`Administrator`**.
4. Marque a caixa de seleção ao lado do acesso ao AWS Management Console. Então, selecione Custom password (Senha personalizada), e insira sua nova senha na caixa de texto.
5. (Opcional) Por padrão, a AWS exige que o novo usuário crie uma senha ao fazer login pela primeira vez. Você pode desmarcar a caixa de seleção próxima de User must create a new password at next sign-in (O usuário deve criar uma senha no próximo login) para permitir que o novo usuário redefina a senha depois de fazer login.
6. Selecione Next (Próximo): Permissions
7. Em Set permissions (Conceder permissões), escolha Add user to group (Adicionar usuário ao grupo).
8. Escolha Create group (Criar grupo).
9. Na caixa de diálogo Create group (Criar grupo), em Group name (Nome do grupo), digite **`Administrators`**.
10. Escolha Filter policies (Filtrar políticas) e, em seguida, selecione AWS managed - job function (Função de trabalho gerenciada da AWS) para filtrar o conteúdo da tabela.
11. Na lista de políticas, marque a caixa de seleção AdministratorAccess. A seguir escolha Criar grupo.

> **Note**
>
> Você deve ativar o acesso de usuário do IAM e da função para Billing (Faturamento) antes de usar as permissões de `AdministratorAccess` para acessar o console do AWS Billing and Cost Management. Para fazer isso, siga as instruções na etapa 1 do tutorial sobre como delegar acesso ao console de faturamento.

12. Suporte a lista de grupos, selecione a caixa de seleção para seu novo grupo. Escolha Refresh (Atualizar) caso necessário, para ver o grupo na lista.

13. Selecione Next (Próximo): Tags.
14. (Opcional) Adicione metadados ao usuário anexando tags como pares de chave-valor. Para obter mais informações sobre como usar tags no IAM, consulte Marcar entidades do IAM no Manual do usuário do IAM.
15. Selecione Next (Próximo): Review (Revisar)Para ver uma lista de associações a grupos a serem adicionadas ao novo usuário. Quando você estiver pronto para continuar, selecione Criar usuário.

Você pode usar esse mesmo processo para criar mais grupos e usuários e conceder aos seus usuários acesso aos recursos da sua Conta da AWS. Para saber como usar políticas para restringir as permissões de usuário a recursos específicos da AWS, consulte Gerenciamento de acesso e Exemplos de políticas.

Requisitos de configuração do gateway

A menos que especificado de outra forma, os seguintes requisitos são comuns a todos os tipos de gateway de arquivos noAWS Storage Gateway. Sua configuração deve atender aos requisitos desta seção. Revise os requisitos que se aplicam à configuração do gateway antes de implantar o gateway.

Tópicos

Pré-requisitos necessários

Antes de usar um Amazon FSx File Gateway (FSx File Gateway), você deve atender aos seguintes requisitos:

- Crie e configure um sistema de arquivos FSx for Windows File Server. Para obter instruções, consulteEtapa 1: Criar seu sistema de arquivosnoGuia do usuário do Amazon FSx for Windows File Server.
- Configure o Microsoft Active Directory (AD).
- Certifique-se de que haja largura de banda de rede suficiente entre o gateway eAWS. É necessário um mínimo de 100 Mbps para baixar, ativar e atualizar o gateway com êxito.
- Configure sua rede privada, VPN ouAWS Direct ConnectEntre a Amazon Virtual Private Cloud (Amazon VPC) e o ambiente no local onde você está implantando seu FSx File Gateway.
- Verifique se o gateway pode resolver o nome do Controlador de Domínio Active Directory. Você pode usar o DHCP no domínio do Active Directory para lidar com a resolução ou especificar um servidor DNS manualmente no menu de configurações de rede no console local do gateway.

Requisitos de hardware e armazenamento

As seções a seguir fornecem informações sobre os requisitos mínimos de hardware e configuração do seu gateway e a quantidade mínima de espaço em disco para alocar ao armazenamento requerido.

Para obter informações sobre as melhores práticas para o desempenho do gateway de arquivos, consulte Orientação de desempenho para gateways de arquivos.

Requisitos de hardware para VMs locais

Ao implantar seu gateway no local, verifique se o hardware subjacente no qual está implantando a máquina virtual do gateway (VM) pode oferecer os seguintes recursos mínimos:

- Quatro processadores virtuais designados para a VM
- 16 GiB de memória RAM reservada para gateways de arquivos
- 80 GiB de espaço em disco para instalação da imagem da VM e dados do sistema

Para obter 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 Cotas para compartilhamentos de arquivos.

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 seu gateway funcione. No entanto, para a família de instâncias otimizadas para computação, o tamanho deve ser pelo menos**`2xlarge`**. Use um dos seguintes tipos de instância recomendados para o seu tipo de gateway.

Recomendado para tipos de gateway de arquivos

- Família de instâncias para uso geral: tipos de instância m4 ou m5.
- Família de instâncias otimizadas para computação — tipos de instância c4 ou c5. 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.
- Família de instâncias otimizadas para o armazenamento — tipos de instância i3.

> **Note**
>
> Quando você inicia seu gateway no Amazon EC2 e o tipo de instância escolhido é compatível com o armazenamento temporário, os discos são listados automaticamente. Para obter mais informações sobre o armazenamento de instâncias do Amazon EC2, consulteArmazenamento de instânciasnoGuia do usuário do Amazon EC2.
> As gravações do aplicativo são armazenadas no cache de maneira síncrona e, depois, carregadas de modo assíncrono no armazenamento durável no Amazon S3. Se o armazenamento temporário for perdido porque uma instância do é interrompida antes da conclusão do upload, os dados que ainda residem no cache e ainda não foram gravados no Amazon Simple Storage Service (Amazon S3) podem ser perdidos. Antes de interromper a instância que hospeda o gateway, verifique se o`CachePercentDirty`A métrica do CloudWatch é`0`. Para obter informações sobre o armazenamento temporário, consulte Usando armazenamento efêmero com gateways EC2. Para obter informações sobre métricas de monitoramento para seu Storage Gateway, consulteMonitorando seu gateway de arquivos.
> Se você tiver mais de 5 milhões de objetos no seu bucket do S3 e estiver usando um volume SSD de uso geral, é necessário um volume mínimo de EBS de 350 GiB para o desempenho aceitável do seu gateway durante a inicialização. Para obter informações sobre como aumentar o tamanho do volume, consulteModificar um volume do EBS usando volumes elásticos (console).

Requisitos de armazenamento

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

Tipo de gateway	Cache (mínimo)	Cache (máximo)			
Gateway de arquivos	150 GiB	64 TiB			

> **Note**
>
> Você pode configurar uma ou mais unidades locais para o cache, até a capacidade máxima. Ao adicionar cache a um gateway existente, é importante criar novos discos no host (hipervisor ou instância do Amazon EC2). Não altere o tamanho de discos existentes caso os discos tenham sido alocados anteriormente como cache.

Para obter informações sobre cotas de gateway, consulte Cotas para compartilhamentos de arquivos.

Requisitos de rede e firewall

Seu gateway requer acesso à Internet, redes locais, Domain Name Service (DNS), firewalls, roteadores, servidores etc.

Os requisitos de largura de banda de rede variam de acordo com a quantidade de dados carregados e baixados pelo gateway. É necessário um mínimo de 100 Mbps para baixar, ativar e atualizar o gateway com êxito. Seus padrões de transferência de dados determinarão a largura de banda necessária para suportar sua carga de trabalho.

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 FSx File Gateway no Amazon EC2 ou usar outros tipos de implantação (incluindo locais) com políticas de segurança de rede que restrinjamAWSIntervalos de endereços IP. Seu gateway pode enfrentar problemas de conectividade de serviço quando oAWSOs valores do intervalo de IP mudam. OAWSOs valores do intervalo de endereço IP que você precisa usar estão no subconjunto de serviço da Amazon para oAWSRegião na qual você ativa o gateway. Para obter os valores do intervalo de IP atuais, consulteAWSIntervalos de endereços IPnoAWSReferência geral.

Tópicos

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	Direção	Origem	Destination (Destino)	Como usar
TCP	443 (HTTPS)	Saída	Storage Gateway	AWS	Para comunicação do Storage Gateway com oAWSendpo

Protocolo	Port	Direção	Origem	Destination (Destino)	Como usar
					int de serviço. Para obter informaçõ es sobre endpoints de serviço, consulte Permitir acesso ao AWS Storage Gateway por meio de firewalls e roteadores.

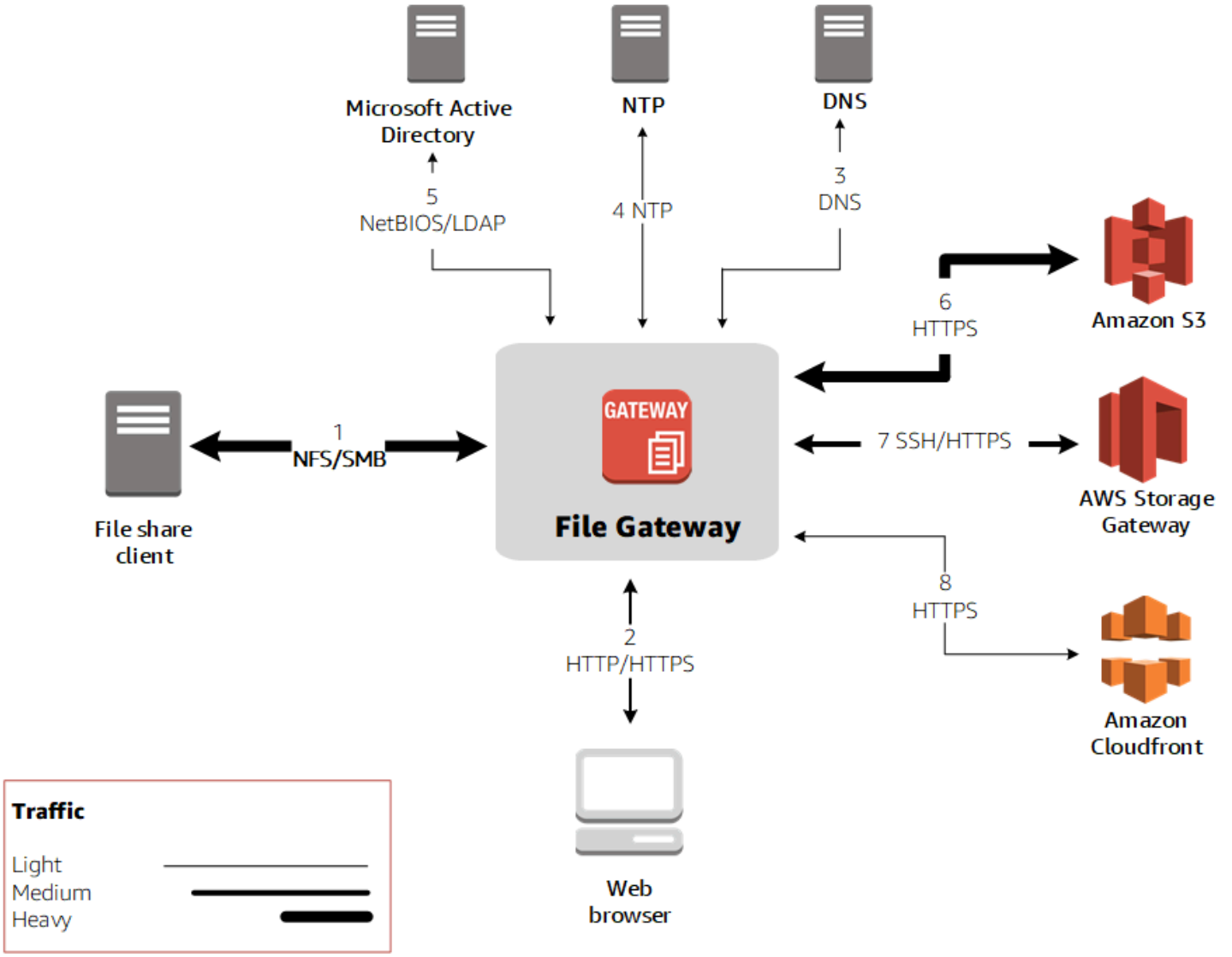
Protocolo	Port	Direção	Origem	Destination (Destino)	Como usar
TCP	80 (HTTP)	Entrada	O host do qual você se conecta aoAWS Management Console.	Storage Gateway	Por sistemas locais para obter a chave de ativação do Storage Gateway. A porta 80 é usada somente durante a ativação do dispositivo Storage Gateway. 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 seu gateway pelo console do Storage Gateway, o host do

Protocolo	Port	Direção	Origem	Destination (Destino)	Como usar
					qual você se conecta ao console deverá ter acesso à porta 80 do gateway.
UDP/UDP	53 (DNS)	Saída	Storage Gateway	Servidor DNS	Para comunicação entre o Storage Gateway e o servidor DNS.

Protocolo	Port	Direção	Origem	Destination (Destino)	Como usar
TCP	22 (Canal de suporte)	Saída	Storage Gateway	AWS Support	PermiteAWS SupportPara acessar seu gateway para ajudar 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.
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 gateways de arquivos

A ilustração a seguir mostra as portas a serem abertas para o gateway de arquivos do S3.



> **Note**
>
> Para obter requisitos específicos de porta, consulteRequisitos de porta.

Para o S3 File Gateway, você só precisa usar o Microsoft Active Directory quando você deseja permitir que os usuários do domínio acessem um compartilhamento de arquivos do Server Message Block (SMB). Seu gateway de arquivos pode ser associado a qualquer domínio Windows válido (solucionado por DNS).

Você também pode usar oAWS Directory Servicepara criar umAWS Managed Microsoft ADNa Nuvem da Amazon Web Services. Para a maioria dosAWS Managed Microsoft ADImplantações, você precisa configurar o serviço do protocolo de configuração do servidor dinâmico (DHCP) para a

VPC. Para obter informações sobre como criar um conjunto de opções de DHCP, consulteCriar um conjunto de opções de DHCPnoAWS Directory ServiceGuia de administração.

Além das portas comuns, o Amazon S3 File Gateway requer as seguintes portas.

Protocolo	Port	Direção	Origem	Destination (Destino)	Como usar
TCP/UDP	2049 (NFS)	Entrada	Clientes NFS	Storage Gateway	Para que sistemas locais se conectem a compartil hamentos NFS expostos pelo gateway.
TCP/UDP	111 (NFSv3)	Entrada	Cliente NFSv3	Storage Gateway	Para que sistemas locais se conectem ao mapeador de portas exposto pelo gateway. **Note** Essa porta é necessári a apenas para NFSv3.

Protocolo	Port	Direção	Origem	Destination (Destino)	Como usar
TCP/UDP	20048 (NFSv3)	Entrada	Cliente NFSv3	Storage Gateway	Para que sistemas locais se conectem a suportes expostos pelo gateway. **Note** Essa porta é necessária apenas para NFSv3.

Requisitos de rede e firewall para o dispositivo de hardware Storage Gateway

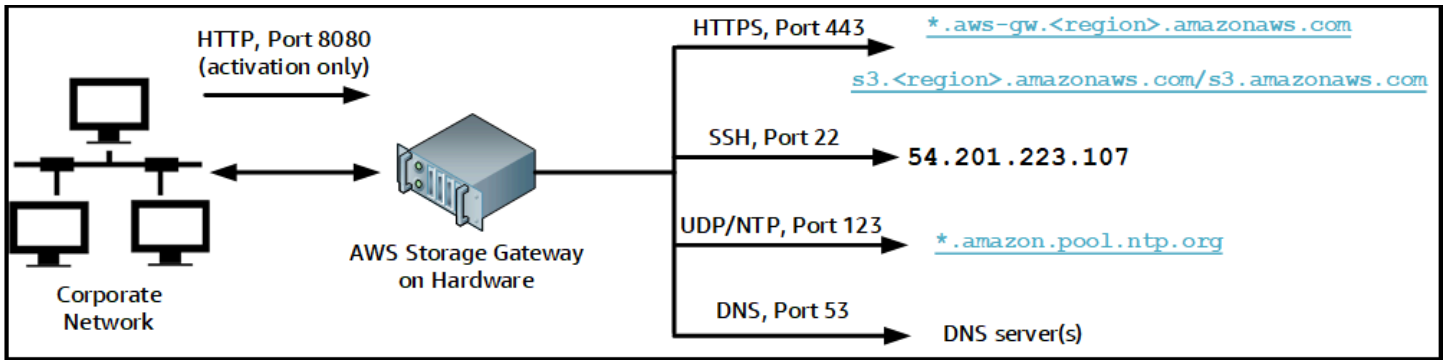
Cada Storage Gateway Hardware Appliance requer os seguintes serviços de rede:

- Acesso à Internet— uma conexão de rede sempre disponível com a Internet por meio de uma interface de rede no servidor.
- Serviços DNS— Serviços DNS para comunicação entre o dispositivo de hardware e o servidor DNS.
- Sincronização de horário— um serviço de horário do Amazon NTP configurado automaticamente deve ser acessível.
- IP address— 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	Direção	Origem	Destination (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

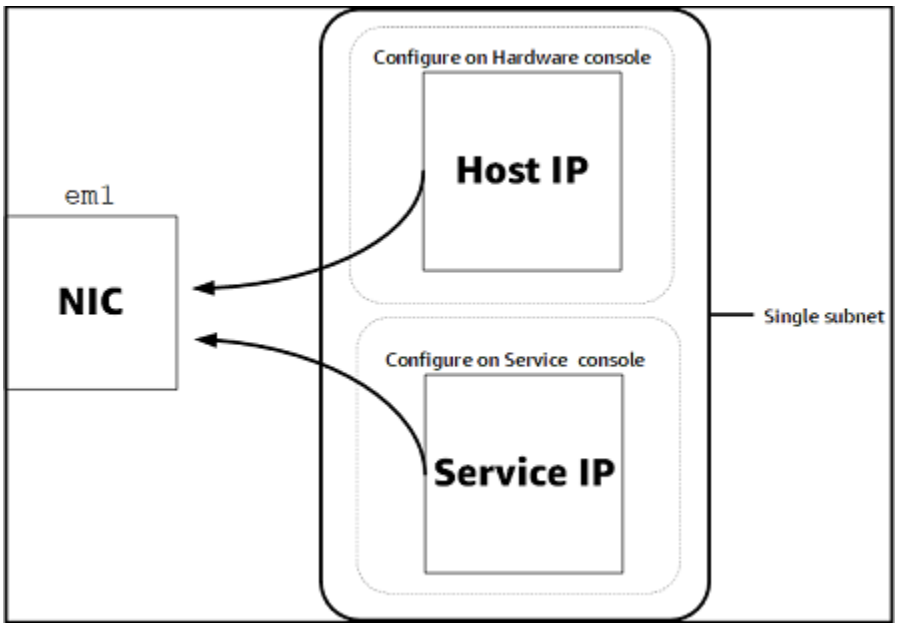
Protocolo	Port	Direção	Origem	Destination (Destino)	Como usar
HTTPS	443	Saída	Equipamento de hardware	`*.amazonaws.com`	Transferência de dados
HTTP	8080	Entrada	AWS	Equipamento de hardware	Ativação (apenas brevemente)

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 obter mais informações, consulte Configuração de parâmetros de rede.

> **Note**
>
> Para ver uma ilustração mostrando a parte posterior do servidor com suas portas, consulteMontagem em rack seu aparelho 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, consulteUso do dispositivo de hardware Storage Gateway.

Permitir acesso ao AWS Storage Gateway por meio de firewalls e roteadores

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

> **Important**
>
> Dependendo do gatewayAWSRegião, substitua*região*no endpoint de serviço com a cadeia de caracteres Region correta.

Veja a seguir o endpoint de serviço necessário por todos os gateways para operações de head-bucket.

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

Os seguintes endpoints de serviço são necessários por todos os gateways para o caminho de controle (`anon-cp`,`client-cp`,`proxy-app`) e caminho de dados (`dp-1`) operações.

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

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

```
storagegateway.region.amazonaws.com:443
```

O exemplo a seguir é um endpoint de serviço do gateway na região Oeste dos EUA (Oregon) (Oregon) (`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. Um gateway de arquivos requer que esse endpoint acesse o bucket do Amazon S3 para o qual o compartilhamento de arquivos está mapeado.

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

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

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

> **Note**
>
> Se o gateway não puder determinar oAWSRegião em que seu bucket do S3 está localizado, esse endpoint de serviço usa como padrão`s3.us-east-1.amazonaws.com`. Recomendamos que você permita o acesso à região US East (N. Virginia) (N. Virginia)`us-east-1`), além das regiões onde o gateway está ativado e do local onde seu bucket do S3 se encontra.

Veja a seguir os endpoints de serviço do Amazon S3 paraAWS GovCloud (US)Regiões.

```
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 de FIPS para um bucket do S3 noAWSRegião GovCloud (Oeste dos EUA).

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

Veja a seguir o endpoint do Amazon CloudFront necessário para o Storage Gateway obter a lista de disponíveisAWSRegiões.

```
https://d4kdq0yaxexbo.cloudfront.net/
```

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

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

- Gateway de armazenamento — para suporteAWSRegiões e uma lista deAWSendpoints de serviço que você pode usar com o Storage Gateway, consulteAWS Storage GatewayEndpoints e cotas donoAWSReferência geral.
- Dispositivo de hardware do Storage Gateway — Para suporteAWSRegiões que você pode usar com o equipamento de hardware, consulteRegiões do appliance de hardware do StoragenoAWSReferência geral.

Configurar grupos de segurança para sua instância de gateway Amazon EC2

DentroAWS Storage Gateway, um security group controla o tráfego para sua instância de gateway 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 Amazon EC2 fora do security group 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 acesso à porta 22 somente se estiver usando o AWS Support para finalidades de solução de problemas. Para obter mais informações, consulte Você querAWS Supportpara ajudar a solucionar problemas do gateway EC2.

Em alguns casos, você pode 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

É possível executar o Storage Gateway no local como um dispositivo de máquina virtual (VM) ou um dispositivo de hardware físico, ou noAWSComo instância do Amazon EC2.

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

- VMware ESXi Hypervisor (versões 6.0, 6.5 ou 6.7) — uma versão gratuita do VMware está disponível noSite da VMware. Para esta configuração, você precisa também de um cliente VMware vSphere para se conectar ao host.
- Microsoft Hyper-V Hypervisor (versão 2012 R2 ou 2016) — uma versão gratuita e independente do Hyper-V está disponível noCentro de downloads da Microsoft. Para esta configuração, você precisará de um Microsoft Hyper-V Manager em um computador cliente Microsoft Windows para se conectar ao host.
- Linux Kernelel-based Virtual Machine (KVM) — 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 recente. O Storage Gateway é testado e compatível com as 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 Amazon EC2 — o Storage Gateway fornece uma Imagem de máquina da Amazon (AMI) que contém a imagem da VM do gateway. Para obter informações sobre como implantar um gateway no Amazon EC2, consulteImplantar um gateway de arquivos em um host do Amazon EC2.
- Storage Gateway Hardware Appliance — O Storage Gateway fornece um dispositivo de hardware físico como uma opção de implantação no local 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 obter mais informações, consulte Recuperando de um desligamento inesperado de máquina virtual.
> O Storage Gateway não oferece suporte à memória dinâmica nem à expansão da memória virtual.

Clientes NFS compatíveis para um gateway de arquivos

Gateways de arquivo compatíveis com os seguintes clientes NFS (Network File System):

- Amazon Linux
- Mac OS X

> **Note**
>
> Recomendamos definir `orsizeewsize`opções de montagem para 64 KB para melhorar o desempenho ao montar compartilhamentos de arquivos NFS no Mac OS X.

- RHEL 7
- SUSE Linux Enterprise Server 11 e SUSE Linux Enterprise Server 12
- Ubuntu 14.04
- Microsoft Windows 10 Enterprise, Windows Server 2012 e Windows Server 2016. Clientes nativos comportam somente o NFS versão 3.

- Windows 7 Enterprise e Windows Server 2008.

  Clientes nativos comportam somente o NFS versão 3. O tamanho máximo de E/S NFS comportado é 32 KB; por isso, é provável que haja uma queda de desempenho nessas versões do Windows.

> **Note**
>
> Agora, você pode usar compartilhamentos de arquivos SMB quando o acesso é exigido por meio de clientes Windows (SMB), em vez de usar os clientes Windows NFS.

Clientes SMB compatíveis para um gateway de arquivos

Os gateways de arquivos oferecem suporte aos clientes de Service Message Block (SMB) a seguir:

- Microsoft Windows Server 2008 e posterior
- Versões de área de trabalho do Windows: 10, 8 e 7.
- Terminal do Windows Server em execução no Windows Server 2008 e posterior

> **Note**
>
> A criptografia de bloco de mensagens do servidor requer clientes compatíveis com o SMB v2.1.

Operações do sistema de arquivos compatíveis para um gateway de arquivos

Seu cliente NFS ou SMB pode gravar, ler, excluir e truncar arquivos. Quando os clientes enviam gravações paraAWS Storage Gateway, ele grava no cache local de maneira síncrona. Em seguida, ele grava no Amazon S3 de maneira assíncrona por meio de transferências otimizadas. As leituras são primeiro atendidas pelo cache local. Quando não existem dados disponíveis, eles são obtidos por meio do S3 como cache de leitura.

As gravações e leituras são otimizadas de modo que somente as partes alteradas ou solicitadas sejam transferidas pelo gateway. Exclui objetos de remoção do Amazon S3. Os diretórios são gerenciados como objetos de pasta no S3, usando a mesma sintaxe que o console do Amazon S3.

As operações de HTTP, como GETPUT, UPDATE e DELETE, podem modificar arquivos em um compartilhamento de arquivos. Essas operações estão em conformidade com as funções atômicas de criação, leitura, atualização e exclusão (CRUD).

Como acessar o AWS Storage Gateway

Você pode usar oAWS Storage GatewayconsolePara 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.

Além disso, você pode usar a API do AWS Storage Gateway para configurar e gerenciar programaticamente seus gateways. Para obter mais informações sobre a API, consulte Referência de API para Storage Gateway.

Você também pode usar oAWSSDKs para desenvolver aplicativos que interajam com o Storage Gateway. OAWSOs 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, consulteAWSCentro de desenvolvedores.

Para obter mais informações sobre preços, consulte Preços do AWS Storage Gateway.

Regiões do AWS com suporte

- Storage Gateway — Para suporteAWSRegiões e uma lista deAWSendpoints de serviço que você pode usar com o Storage Gateway, consulteAWS Storage GatewayEndpoints e cotas donoAWSReferência geral.
- Storage Gateway Hardware Appliance — para saber as regiões compatíveis com o dispositivo de hardware, consulteAWS Storage GatewayRegiões do dispositivo de hardwarenoAWSReferência geral.

Uso do dispositivo de hardware Storage Gateway

O dispositivo de hardware do Storage Gateway é um dispositivo de hardware físico que traz o software Storage Gateway pré-instalado em uma configuração de servidor validada. Você pode gerenciar seu dispositivo de hardware doHardwarePágina noAWS Storage Gatewayconsole do .

O dispositivo de hardware é um servidor 1U de alto desempenho que você pode implantar em seu datacenter ou localmente dentro do seu firewall corporativo. Ao comprar e ativar o dispositivo de hardware, o processo de ativação associa seu dispositivo de hardware aoAWSconta. Após a ativação, seu dispositivo de hardware será exibido no console como um gateway noHardware. Você pode configurar o dispositivo de hardware como um gateway de arquivos, de fitas ou de volume. O procedimento usado para implantar e ativar esses tipos de gateway em um equipamento de hardware é o mesmo utilizado em plataformas virtuais.

O Storage Gateway Hardware Appliance pode ser solicitado diretamente doAWS Storage Gatewayconsole do .

Para solicitar um dispositivo de hardware

1. Abra o console Storage Gateway emhttps://console.aws.amazon.com/storagegateway/homee escolha oAWSRegião na qual você deseja seu dispositivo.
2. SelecioneHardwareNo painel de navegação.
3. SelecionePedido dispositivoe, depois, escolhaProsseguir. Você será redirecionado para oAWSElemental Appliances e Software Management Console para solicitar uma cotação de vendas.
4. Preencha as informações necessárias e escolhaEnviar.

Depois que as informações forem analisadas, uma cotação de venda é gerada e você poderá prosseguir com o processo de pedido e enviar uma Ordem de Compra ou providenciar o pagamento antecipado.

Para exibir uma cotação de vendas ou histórico de pedidos para o equipamento de hardware

1. Abra o console Storage Gateway emhttps://console.aws.amazon.com/storagegateway/home.
2. SelecioneHardwareNo painel de navegação.

3. SelecioneCotações e pedidose, depois, escolhaProsseguir. Você será redirecionado para oAWSElemental Appliances e Software Management Console para revisar as cotações de vendas e o histórico de pedidos.

Nas seções a seguir, você encontra instruções sobre como configurar, ativar, executar e usar um dispositivo de hardware do Storage Gateway.

Tópicos

Regiões do AWS com suporte

O Storage Gateway Hardware Appliance está disponível para envio em todo o mundo onde é legalmente permitido e permitido para exportação pelo governo dos EUA. Para obter informações sobre suporteAWSRegiões, consulteRegiões Storage GatewaynoAWSReferência geral.

Configuração do dispositivo de hardware

Depois de receber o dispositivo de hardware do Storage Gateway, use o console do dispositivo de hardware para configurar a rede e fornecer uma conexão permanente aoAWSe ative seu aparelho. A ativação associa seu equipamento com oAWSConta usada durante o processo de ativação. Depois que ele for ativado, execute um gateway de arquivo ou de volume no console do Storage Gateway.

Para instalar e configurar seu dispositivo de hardware

1. Monte o dispositivo em rack e conecte-o à energia e à rede. Para obter mais informações, consulte Montagem em rack seu aparelho de hardware e conectá-lo à alimentação.
2. Defina os endereços IPv4 (Protocolo de Internet versão 4) para o dispositivo de hardware (host) e o Storage Gateway (o serviço). Para obter mais informações, consulte Configuração de parâmetros de rede.
3. Ativar o equipamento de hardware no consoleHardwarePágina noAWSRegião de sua escolha. Para obter mais informações, consulte Como ativar o dispositivo de hardware.
4. Instale o Storage Gateway no dispositivo de hardware. Para obter mais informações, consulte Configuração do gateway.

   Os gateways são instalados no dispositivo de hardware da mesma forma que no VMware ESXi, no Microsoft Hyper-V, na Linux Kernel-based Virtual Machine (KVM) ou no Amazon EC2.

Aumento do armazenamento em cache utilizável

Você pode aumentar o armazenamento utilizável no dispositivo de hardware de 5 TB para 12 TB. Isso proporciona um maior espaço em cache para acesso de baixa latência aos dados noAWS. Se você tiver solicitado o modelo de 5 TB, poderá aumentar o armazenamento utilizável para 12 TB comprando cinco SSDs de 1,92 TB (unidades de estado sólido), que estão disponíveis para pedidos no consoleHardware. Você pode solicitar os SSDs adicionais seguindo o mesmo processo de pedido que solicitar um dispositivo de hardware e solicitar uma cotação de vendas no console do Storage Gateway.

Você pode então 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 para 12 TB, faça o seguinte:

1. Redefina o dispositivo de hardware para suas configurações de fábrica. ContatoAWSSupport para obter instruções sobre como fazer isso.
2. Adicione cinco SSDs de 1,92 TB ao dispositivo.

Opções da placa de interface de rede

Dependendo do modelo de equipamento que você pediu, 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 da NIC 10G DA/SFP+:
  - Use cabos de conexão direta de cobre Twinax até 5 metros
  - Módulos ópticos SFP+ compatíveis com Dell/Intel (SR ou LR)
  - Transceptor de cobre SFP/SFP+ para 1G-Base-T ou 10G-Base-T

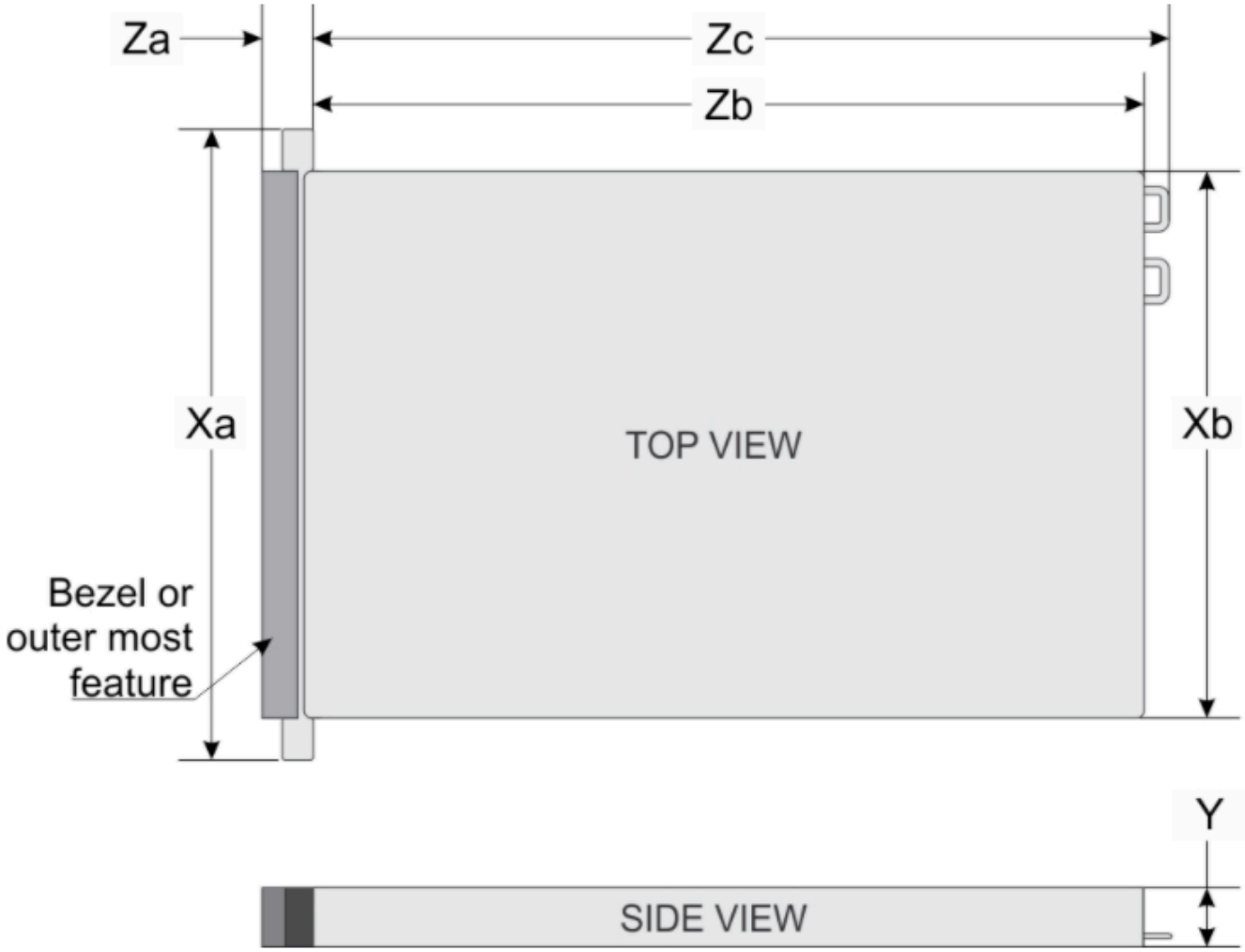
Montagem em rack seu aparelho de hardware e conectá-lo à alimentação

Depois de tirar o dispositivo de hardware do Storage Gateway, siga as instruções contidas na caixa para montar o servidor no rack. Seu dispositivo tem formato 1U e é compatível com racks de 19 polegadas em conformidade com a International Electrotechnical Commission (IEC).

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

- Cabos de alimentação: 1 (necessário); 2 (recomendado).
- Cabeamento de rede suportado (dependendo de qual placa de interface de rede (NIC) está incluída no dispositivo de hardware). Twinax Copper DAC, módulo óptico 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



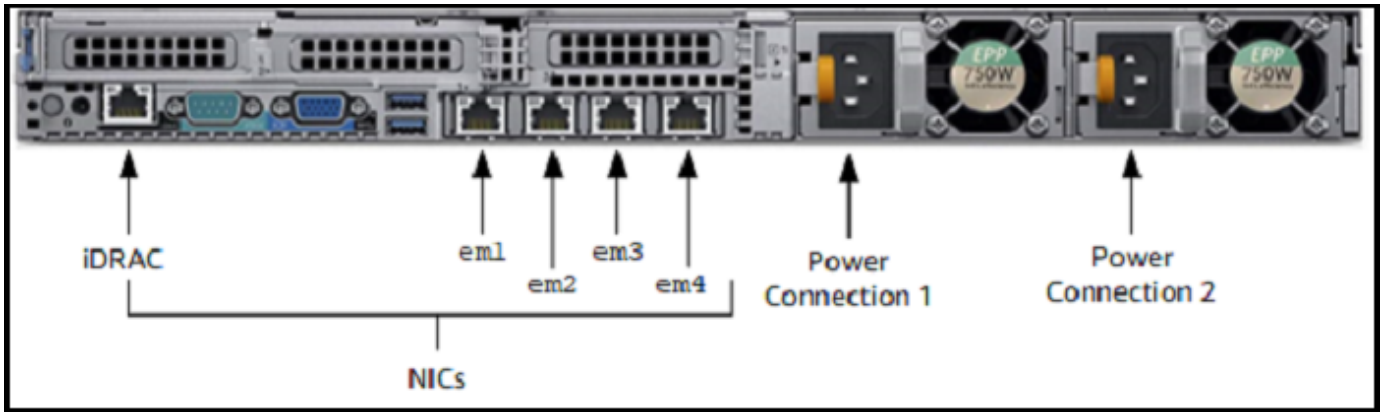
System	Xa	Xb	Y	Za (with bezel)	Za (without bezel)	Zb*	Zc
10 x 2.5-inches	482.0 mm (18.97-inches)	434.0 mm (17.08-inches)	42.8 mm (1.68-inches)	35.84 mm (1.41-inches)	22.0 mm (0.87-inches)	733.82 mm (29.61-inches)	772.67 mm (30.42-inches)

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 dispositivo de hardware do Storage Gateway como descrito emRequisitos de rede e firewall para o dispositivo de hardware Storage Gateway.

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 ambras as fontes.

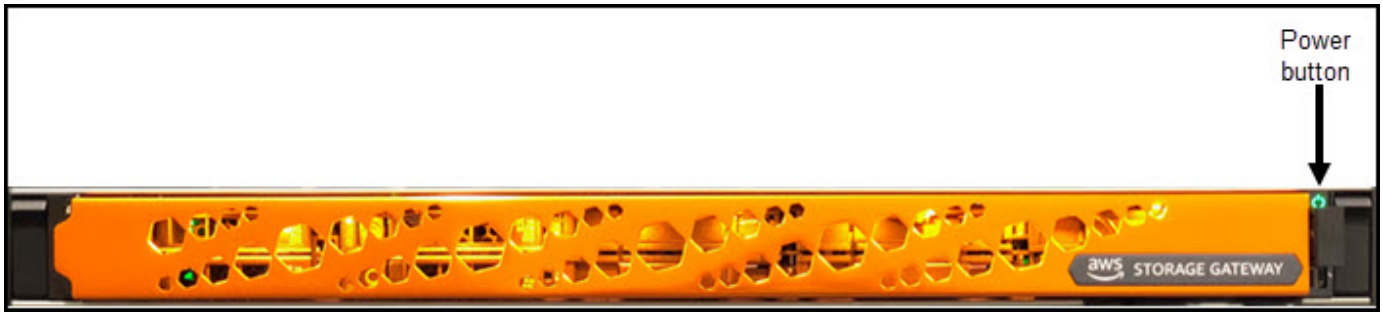
   Na imagem a seguir, você pode ver o dispositivo de hardware com diferentes conexões.



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 oferece suporte ao entroncamento 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.



Depois que o servidor é inicializado, o console de hardware é exibido na tela. O console de hardware apresenta uma interface de usuário específica paraAWSVocê pode usar para configurar os parâmetros iniciais da rede. Você configura esses parâmetros para conectar o dispositivo aoAWSE abra um canal de suporte para solução de problemas porAWSSupport.

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).

Nesse momento você visualiza o console do hardware, que mostra o seguinte:

Próxima etapa

[Configuração de parâmetros de rede]

Configuração de parâmetros de rede

Depois que o servidor é inicializado, você pode inserir a primeira senha no console de hardware, como descrito em [Montagem em rack seu aparelho de hardware e conectá-lo à alimentação].

Depois, no console de hardware, siga estas etapas para configurar os parâmetros de rede e conectar o dispositivo de hardwareAWS.

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.

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 deve fornecer a mesma conexão permanente com oAWSendpoints listados nos requisitos.

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, insira o mesmo endereço no console, na página Hardware, como descrito a seguir. O processo de ativação confirma que o dispositivo de hardware tem as credenciais de segurança apropriadas e registra o dispositivo noAWSconta.

Você pode optar por ativar seu dispositivo de hardware em qualquer um dos compatíveisAWSRegiões. Para ver uma lista dos compatíveisAWSRegiões, consulteRegiões Storage GatewaynoAWSReferência geral.

Para ativar seu dispositivo pela primeira vez ou em umAWSRegião em que você não tem gateways implantados

1. Faça login noAWS Management Consolee abra o console do Storage Gateway emAWS Storage GatewayManagement ConsoleCom as credenciais da conta a serem usadas para ativar seu hardware.

   Se este for seu primeiro gateway em umAWSRegion, você vê uma tela inicial. Depois de criar um gateway nesteAWSRegião, a tela não é mais exibida.

   > **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. Escolha Get started (Começar) para ver o assistente de criação de gateway e, depois, escolha Hardware Appliance (Dispositivo de hardware) na página Select host platform (Selecionar plataforma de host), como mostrado a seguir.
3. Escolha Next (Próximo) para ver a tela Connect to hardware (Conectar-se ao hardware) mostrada a seguir.
4. para oEndereço IPnoConnect ao dispositivo de hardware, insira o endereço IPv4 do seu dispositivo e selecioneConecte-sePara acessar a tela Ativar hardware mostrada a seguir.
5. Em Hardware name (Nome do hardware), insira um nome para o seu dispositivo. Os nomes podem ter até 255 caracteres e não podem conter barras.
6. para oFuso horário do hardware, insira suas configurações locais.

O fuso horário controla quando ocorrem atualizações de hardware: o horário definido para elas é 2h (horário local).

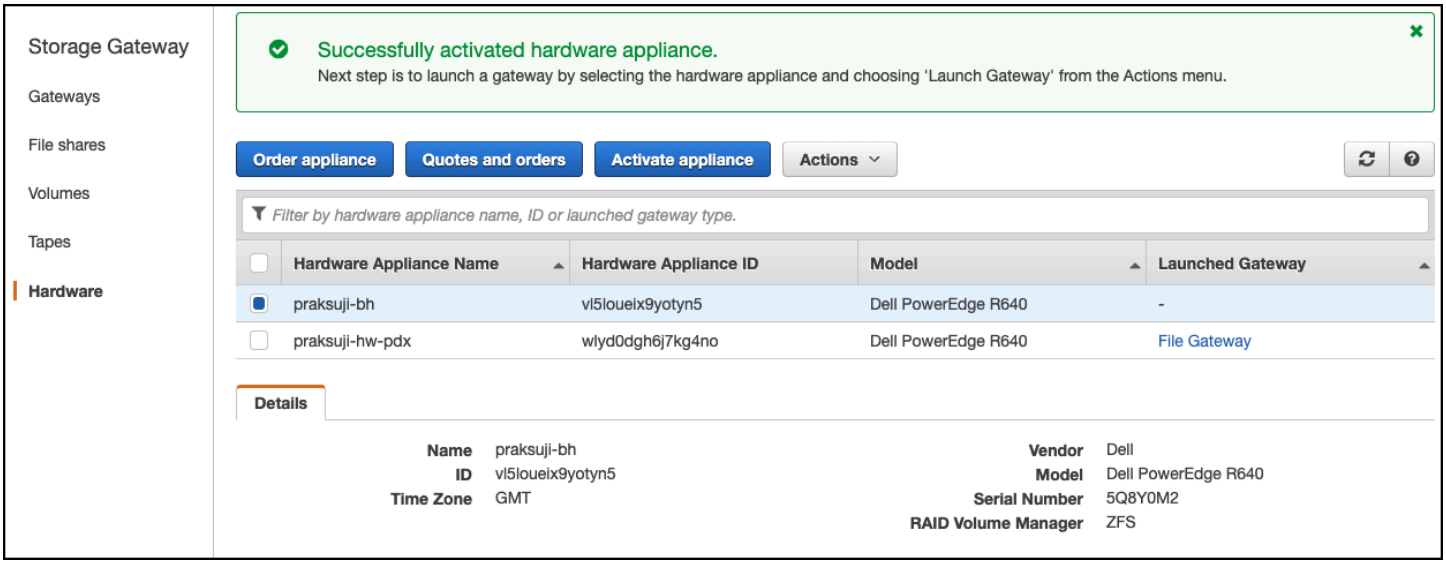
> **Note**
>
> Recomendamos definir o fuso horário do seu dispositivo para garantir que as atualizações ocorram fora do seu horário de trabalho.

7. (Opcional) Mantenha o RAID Volume Manager (Gerenciador de volumes do RAID) definido como ZFS.

   O ZFS é usado como gerenciador de volumes RAID no dispositivo de hardware para fornecer melhor desempenho e proteção de dados. O ZFS é um sistema de arquivos e gerenciador de volumes lógico, de código de aberto e baseado em software. O dispositivo de hardware é ajustado especificamente para o RAID ZFS. Para obter mais informações sobre o RAID ZFS, consulte a página do ZFS na Wikipedia.
8. Escolha Next (Próximo) para finalizar a ativação.

Um banner do console é exibido na página Hardware, indicando que o dispositivo foi ativado com êxito, como mostrado a seguir.

Nesse momento, o dispositivo está associado à sua conta. A próxima etapa é executar um gateway de arquivo, fita ou volume armazenado em cache no seu dispositivo.



Próxima etapa

Como executar o gateway

Como executar o gateway

Você pode executar qualquer um dos três Storage Gateways no dispositivo: gateway de arquivos, de volume (armazenado em cache) ou de fita.

Para executar um gateway no seu dispositivo de hardware

1. Faça login noAWS Management Consolee abra o console do Storage Gateway emhttps://console.aws.amazon.com/storagegateway/home.
2. Escolha Hardware.
3. Em Actions (Ações), escolha Launch Gateway (Executar gateway).
4. Para Gateway Type (Tipo de gateway), escolha File Gateway (Gateway de arquivo), Tape Gateway (Gateway de fita) ou Volume Gateway (Cached) (Gateway de volume armazenado em cache).
5. Em Gateway name (Nome do gateway), insira um nome para o seu gateway. Os nomes podem ter até 255 caracteres e não podem conter barras.
6. Escolha Launch Gateway (Executar gateway).

O software Storage Gateway para o tipo de gateway escolhido é instalado no dispositivo. Pode levar até 5 a 10 minutos para que um gateway apareça comoconectadosNo console do.

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

Próxima etapa

Configuração de um endereço IP para o gateway

Configuração de um endereço IP para o gateway

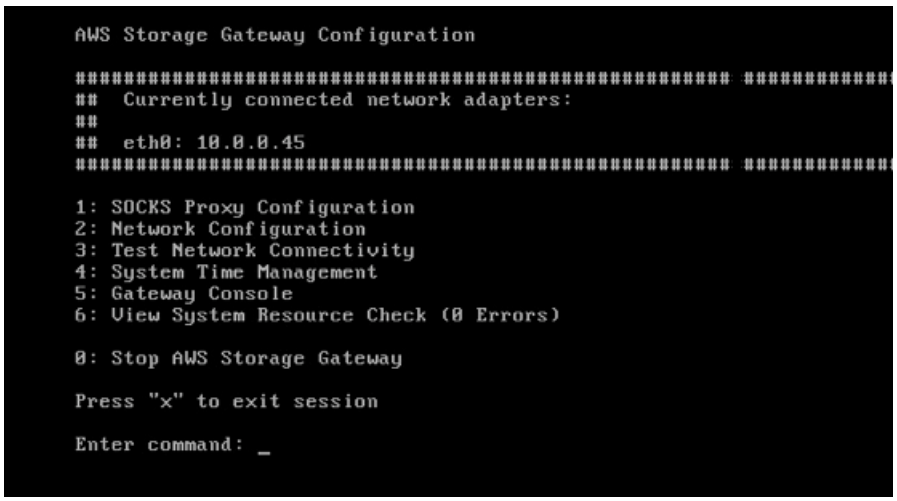
Antes de ativar o equipamento de hardware, você atribuiu um endereço IP à interface de rede física. Agora que você ativou o appliance e iniciou o Storage Gateway nele, você precisa atribuir outro endereço IP à máquina virtual do Storage Gateway que é executada no dispositivo de hardware. Para atribuir um endereço IP estático a um gateway instalado no dispositivo de hardware, configure

o endereço IP no console local para esse 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 Montagem em rack seu aparelho de hardware e conectá-lo à alimentação.
5. Navegue até a página de configurações de rede do console local do gateway, como mostrado a seguir.



6. Digite 2 para acessar a página Network Configuration (Configuração de rede) mostrada a seguir.

7. Configure um endereço IP estático ou DHCP para a porta de rede no seu dispositivo de hardware para apresentar um gateway de arquivo, volume ou fita para os aplicativos. 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

Configuração do gateway

Configuração do 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 do tipo gateway. Para obter instruções, consulte Configurar o Amazon S3 File Gateway.

Removendo 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. Escolha a caixa de seleção para o gateway.
2. Em Actions, selecione Remove Gateway.
3. Na caixa de diálogo no dispositivo de hardware Remover gateway , escolha Confirmar.

> **Note**
>
> Ao excluir um gateway, você não pode 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 exclusão de um gateway não exclue o dispositivo de hardware do console. O dispositivo de hardware permanece para futuras implantações do gateway.

Exclua seu dispositivo de hardware

Depois de ativar o equipamento de hardware em seuAWSConta, talvez você precise movê-la e ativá-la em outraAWSconta. Nesse caso, primeiro exclua o dispositivo doAWSconta e ative-a em outraAWSconta. Você também pode querer excluir o dispositivo completamente do seuAWSConta porque você não precisa mais dela. Siga estas instruções para excluir o dispositivo de hardware.

Para excluir seu equipamento 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 dispositivo de hardware, consulteRemovendo um gateway do dispositivo de hardware.
2. Na página Hardware, escolha o dispositivo de hardware que deseja excluir.
3. Em Actions (Ações), escolha Delete Appliance (Excluir dispositivo).
4. Na caixa de diálogo Confirm deletion of resource(s) (Confirmar exclusão de recursos), marque a caixa de verificação de confirmação e escolha Delete (Excluir). Uma mensagem indicando a exclusão bem-sucedida é exibida.

Ao excluir o dispositivo de hardware, todos os recursos associados ao gateway que está instalado no dispositivo também serão excluídos, exceto os dados no dispositivo de hardware em si não serão excluídos.

Conceitos básicos do AWS Storage Gateway

Nesta seção, é possível encontrar instruções sobre como criar e ativar um gateway de arquivos noAWS Storage Gateway. Antes de começar, certifique-se de que sua configuração atenda aos pré-requisitos necessários e outros requisitos descritos noConfiguração do Amazon S3 File Gateway.

Tópicos

- Criar e ativar um Amazon S3 File Gateway

Criar e ativar um Amazon S3 File Gateway

Nesta seção, é possível encontrar instruções sobre como criar, implantar e ativar um gateway de arquivos noAWS Storage Gateway.

Tópicos

- Configurar um gateway de arquivos do Amazon S3
- Connect seu Amazon S3 File Gateway aoAWS
- Revise as configurações e ative o Amazon S3 File Gateway
- Configurar o Amazon S3 File Gateway

Configurar um gateway de arquivos do Amazon S3

Como configurar um novo gateway de arquivos do S3

1. Abrir oAWS Management Consoleemhttps://console.aws.amazon.com/storagegateway/home/, e escolha oRegião da AWSOnde você deseja criar seu gateway.
2. SelecioneCriar gatewayPara abrir oConfigurar gateway.
3. NoConfigurações do gatewaySeção, faça o seguinte:

    a. Em Gateway name (Nome do gateway), insira um nome para o seu gateway. Depois que seu gateway for criado, você pode procurar esse nome para encontrar seu gateway nas páginas de lista naAWS Storage Gatewayconsole do .

    b. para oFuso horário do gateway, escolha o fuso horário local para a parte do mundo em que você deseja implantar seu gateway.
4. NoOpções de gatewayseção, paraTipo de gateway, escolhaGateway de arquivos Amazon S3.

5. NoOpções para a plataformaSeção, faça o seguinte:

   a. para oPlataforma de hospedagem, escolha a plataforma na qual deseja implantar seu gateway. Em seguida, siga as instruções específicas da plataforma exibidas na página do console do Storage Gateway para configurar sua 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— Faça download, implante e configure a máquina virtual gateway usando Linux Kernel-based Virtual Machine (KVM).
      - Amazon EC2— Configure e execute uma instância do Amazon EC2 para hospedar seu gateway.
      - Equipamento de hardware— Solicite um dispositivo de hardware físico dedicado a partir deAWSComo hospedar seu gateway.

   b. para oConfirmar configurar o gateway, marque a caixa de seleção para confirmar que você executou as etapas de implantação da plataforma host que você escolheu. Esta etapa não se aplica aoEquipamento de hardwarePlataforma de hospedagem.

6. Agora que o gateway está configurado, você deve escolher como deseja que ele se conecte e se comunique comAWS. SelecionePróximopara prosseguir.

Connect seu Amazon S3 File Gateway aoAWS

Para conectar um novo gateway de arquivos S3 aoAWS

1. Caso ainda não tenha feito, conclua o procedimento descrito emConfigurar um gateway de arquivos do Amazon S3. Quando terminar, escolhaPróximoPara abrir oConectar-se aoAWSNa página noAWS Storage Gatewayconsole do .
2. NoOpções de endpointseção, paraEndpoint de serviço, escolha o tipo de endpoint que seu gateway usará para se comunicar com oAWS. Você pode escolher entre as seguintes opções:

   - Publicly accessible— Seu gateway se comunica comAWSNa internet pública. Se selecionar esta opção, use aEndpoint habilitado para FIPSPara especificar se a conexão deve estar em conformidade com o Federal Information Processing Standards (FIPS).

> **Note**
>
> Se você precisar de módulos criptográficos validados pelo FIPS 140-2 ao acessarAWSPor meio de uma interface de linhas de comando ou 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 do FIPS está disponível somente em algunsAWSRegiões. Para obter mais informações, consulteAWS Storage GatewayEndpoints e cotas donoAWSReferência geral.

- VPC hospedada— Seu gateway se comunica comAWSPor meio de uma conexão privada com a nuvem privada virtual (VPC), permitindo que você controle suas configurações de rede. Se você selecionar essa opção, deverá especificar um endpoint de VPC existente escolhendo o ID do endpoint da VPC na lista suspensa. Você também pode fornecer seu VPC endpoint Domain Name System (DNS) ou o endereço IP.

3. NoOpções de conexão do gatewayseção, paraOpções de conexão, escolha como identificar seu gateway paraAWS. Você pode escolher entre as seguintes opções:

   - IP address— Forneça o endereço IP de seu gateway no campo correspondente. Esse endereço IP deve ser público ou acessível a partir de sua rede atual, e você deve ser capaz de se conectar a ele pelo navegador da Web.

     Você pode obter o endereço IP do gateway fazendo login no console local do gateway a partir do cliente hipervisor ou copiando-o da página de detalhes da instância do Amazon EC2.

   - Chave de ativação— Forneça a chave de ativação para seu gateway no campo correspondente. Você pode gerar uma chave de ativação usando o console local do gateway. Se o endereço IP do gateway não estiver disponível, escolha esta opção.

4. Agora que você escolheu como deseja que seu gateway se conecte aoAWS, você deve ativar o gateway. SelecionePróximopara prosseguir.

Revise as configurações e ative o Amazon S3 File Gateway

Para ativar um novo gateway de arquivos S3

1. Caso ainda não tenha feito, conclua os procedimentos descritos nos seguintes tópicos:

- Configurar um gateway de arquivos do Amazon S3
- Connect seu Amazon S3 File Gateway aoAWS

Quando terminar, escolhaPróximoPara abrir oAnalise e ativeNa página noAWS Storage Gatewayconsole do .

2. Revise os detalhes iniciais do gateway de cada seção da página.
3. Se uma seção contiver erros, escolhaEditepara retornar à página de configurações correspondente e fazer alterações.

> **Important**
>
> Não é possível modificar as opções de gateway ou as configurações de conexão depois que o gateway for ativado.

4. Agora que você ativou seu gateway, você deve executar a configuração pela primeira vez para alocar discos de armazenamento local e configurar o log. SelecionePróximopara prosseguir.

Configurar o Amazon S3 File Gateway

Para executar a configuração pela primeira vez em um novo S3 File Gateway

1. Caso ainda não tenha feito, conclua os procedimentos descritos nos seguintes tópicos:

   - Configurar um gateway de arquivos do Amazon S3
   - Connect seu Amazon S3 File Gateway aoAWS
   - Revise as configurações e ative o Amazon S3 File Gateway

   Quando terminar, escolhaPróximoPara abrir oConfigurar gatewayNa página noAWS Storage Gatewayconsole do .
2. NoConfigurar o armazenamento em cache, use as listas suspensas para alocar pelo menos um disco local com pelo menos 150 gibibytes (GiB) capacidade paraCache. Os discos locais listados nesta seção correspondem ao armazenamento físico que você provisionou na plataforma host.
3. NoGrupo de logs do CloudWatch, escolha como configurar o Amazon CloudWatch Logs para monitorar a integridade do seu gateway. Você pode escolher entre as seguintes opções:

- Criar um novo grupo de logs— Configure um novo grupo de logs para monitorar seu gateway.
- Use um grupo de logs existente— Escolha um grupo de logs existente na lista suspensa correspondente.
- Desativar o registro em log— Não use o Amazon CloudWatch Logs para monitorar seu gateway.

4. NoAlarmes do CloudWatch, escolha como configurar os alarmes do Amazon CloudWatch para notificá-lo quando as métricas do gateway se desviarem dos limites definidos. Você pode escolher entre as seguintes opções:

   - Desativar alarmes— Não use alarmes do CloudWatch para ser notificado sobre as métricas do gateway.
   - Criar um alarme do CloudWatch— Configure um novo alarme do CloudWatch para ser notificado sobre as métricas do gateway. SelecioneCriar alarmePara definir métricas e especificar ações de alarme no console do Amazon CloudWatch. Para obter instruções, consulteUsando alarmes do Amazon CloudWatchnoGuia do usuário do Amazon CloudWatch.

5. (Opcional) NoTagsseção, escolhaAdicionar nova tagE, em seguida, insira um par de chave/valor que diferencia maiúsculas de minúsculas e ajuda você a pesquisar e filtrar o gateway nas páginas de lista doAWS Storage Gatewayconsole do . Repita esta etapa para adicionar quantas tags desejar.

6. (Opcional) NoVerifique a configuração do VMware High AvailabilitySe o gateway estiver implantado em um host do VMware como parte de um cluster que está ativado para o VMware High Availability (HA), escolhaVerifique o VMware HApara testar se a configuração do HA está funcionando corretamente.

   > **Note**
   >
   > Esta seção aparece apenas para gateways que estão em execução na plataforma host VMware.
   > Esta etapa não é necessária para concluir o processo de configuração do gateway. Você pode testar a configuração de HA do gateway a qualquer momento. A verificação demora alguns minutos e reinicializa a máquina virtual (VM) do Storage Gateway.

7. SelecioneConfigurePara concluir a criação do gateway.

   Para verificar o status de seu novo gateway, procure-o naGateways doA página doAWS Storage Gatewayconsole do .

Agora que criou seu gateway, crie um compartilhamento de arquivos para que ele use. Para obter instruções, consulteCriar um compartilhamento de arquivos.

Crie um compartilhamento de arquivos

Nesta seção, você pode encontrar instruções sobre como criar um compartilhamento de arquivos. Você pode criar um compartilhamento de arquivos que pode ser acessado usando o protocolo Network File System (NFS) ou Server Message Block (SMB).

> **Note**
>
> Quando um arquivo é gravado no gateway de arquivos por um cliente NFS ou SMB, o gateway de arquivos carrega os dados do arquivo para o Amazon S3 seguidos de seus metadados (proprietários, carimbos de data/hora e assim por diante). O upload dos dados do arquivo cria um objeto S3 e o upload dos metadados do arquivo atualiza os metadados do objeto S3. Esse processo cria outra versão do objeto, resultando em duas versões de um objeto. Se o Versionamento do S3 estiver habilitado, ambas as versões serão armazenadas. Se você alterar os metadados de um arquivo armazenado no gateway de arquivos, um novo objeto S3 será criado e substituirá o objeto S3 existente. Esse comportamento é diferente de editar um arquivo em um sistema de arquivos, onde a edição de um arquivo não resulta na criação de um novo arquivo. Teste todas as operações de arquivo que você planeja usar comAWSStorage Gateway para que você entenda como cada operação de arquivo interage com o armazenamento do Amazon S3.
>
> Considere cuidadosamente o uso do controle de versão e CRR (Replicação entre regiões) do S3 no Amazon S3 quando você estiver carregando dados do gateway de arquivos. O upload de arquivos do gateway de arquivos para o Amazon S3 quando o controle de versão do S3 está habilitado resulta em pelo menos duas versões de um objeto S3.
>
> Determinados fluxos de trabalho envolvendo arquivos grandes e padrões de gravação de arquivos, como uploads de arquivos que são executados em várias etapas, podem aumentar o número de versões armazenadas de objetos S3. Se o cache do gateway de arquivos precisar liberar espaço devido a altas taxas de gravação de arquivos, várias versões de objeto S3 poderão ser criadas. Esses cenários aumentam o armazenamento S3 se o controle de versão do S3 estiver ativado e aumentam os custos de transferência associados à CRR. Teste todas as operações de arquivos que você planeja usar com o Storage Gateway para entender como cada operação de arquivo interage com o armazenamento do Amazon S3.
>
> O uso do utilitário Rsync com o gateway de arquivos resulta na criação de arquivos temporários no cache e na criação de objetos S3 temporários no Amazon S3. Essa situação resulta em cobranças de exclusão antecipada nas classes de armazenamento S3 Standard — IA (S3 Standard — IA) e S3 Intelligent-Tiering.

Quando você cria um compartilhamento NFS, por padrão, qualquer pessoa que tenha acesso ao servidor NFS pode acessar o compartilhamento de arquivos NFS. Você pode limitar o acesso aos clientes por endereço IP.

Para SMB, você pode ter um dos três modos diferentes de autenticação:

- O compartilhamento de arquivos com acesso ao Microsoft Active Directory (AD). Qualquer usuário do Microsoft AD autenticado tem acesso a esse tipo de compartilhamento de arquivos.
- Um compartilhamento de arquivos SMB com acesso limitado. Somente determinados usuários e grupos que você especifica recebem acesso (por meio de uma lista de permissões). Os usuários e grupos também podem ter o acesso negado (por meio de uma lista de negação).
- Um compartilhamento de arquivos SMB com acesso de convidado. Qualquer pessoa que possa fornecer a senha de convidado obtém acesso ao compartilhamento de arquivos.

> **Note**
>
> Os compartilhamentos de arquivos exportados pelo gateway em compartilhamentos de arquivos NFS são compatíveis com as permissões POSIX. Em compartilhamentos de arquivos SMB, é possível usar listas de controle de acesso (ACLs) para gerenciar as permissões sobre arquivos e pastas no compartilhamento. Para obter mais informações, consulte Usar as ACLs do Microsoft Windows para controlar o acesso a um compartilhamento de arquivos SMB.

Um gateway de arquivo pode hospedar um ou mais compartilhamentos de arquivos de tipos diferentes. Você pode ter vários compartilhamentos de arquivos NFS e SMB em um gateway de arquivos.

> **Important**
>
> Para criar um compartilhamento de arquivos, um gateway de arquivo requer que você ative o AWS Security Token Service (AWS STS). Certifique-se de queAWS STSé ativado noRegião da AWSEm que você está criando o gateway de arquivos. SeAWS STSnão está ativado nissoRegião da AWS, ative-o. Para obter informações sobre como ativar oAWS STS, consulteAtivar e desativar oAWS STSem umRegião da AWSnoAWS Identity and Access ManagementGuia do usuário do.

> **Note**
>
> Você pode usarAWS Key Management Service(AWS KMS) para criptografar objetos que o gateway de arquivos armazena no Amazon S3. Para fazer isso usando o console do Storage Gateway, consulte.Criar um compartilhamento de arquivos NFSouCriar um compartilhamento de arquivos SMB. Também é possível fazer isso usando a API do Storage Gateway API. Para obter instruções, consulteCreateNFSFileShareouCreateSMBFileSharenoAWSReferência da API Storage Gateway.
>
> Por padrão, um gateway de arquivos usa a criptografia no lado do servidor gerenciada com o Amazon S3 (SSE-S3) quando grava dados em um bucket do S3. Se você fizer o SSE-KMS (criptografia no lado do servidor com oAWS KMS— managed keys) a criptografia padrão do bucket do S3, os objetos que um gateway de arquivos armazena são criptografados com o SSE-KMS.
>
> Para criptografar usando o SSE-KMS com sua própria chave do AWS KMS, você deve habilitar a criptografia do SSE-KMS. Ao fazer isso, forneça o nome de recurso da Amazon (ARN) da chave do KMS ao criar o compartilhamento de arquivos. Também é possível atualizar as configurações do KMS para o compartilhamento de arquivos usando a operação de API UpdateNFSFileShare ou UpdateSMBFileShare. Essa atualização se aplica a objetos armazenados nos buckets do Amazon S3 após a atualização.
>
> Se você configurar o gateway de arquivos para usar o SSE-KMS para criptografia, será necessário adicionar manualmentekms:Encrypt,kms:Decrypt,kms:ReEncrypt,kms:GenerateDataKey, ekms:DescribeKeyPermissões para a função do IAM associada ao compartilhamento de arquivos. Para obter mais informações, consulteUsar políticas baseadas em identidade (políticas do IAM) para o Storage Gateway.

Tópicos

Criar um compartilhamento de arquivos NFS

Use o procedimento a seguir para criar um compartilhamento de arquivos Network File System (NFS).

> **Note**
>
> Quando um arquivo é gravado no gateway de arquivos por um cliente NFS, o gateway de arquivos carrega os dados do arquivo para o Amazon S3 seguidos de seus metadados (proprietários, carimbos de data/hora e assim por diante). O upload dos dados do arquivo cria um objeto S3 e o upload dos metadados do arquivo atualiza os metadados do objeto S3. Esse processo cria outra versão do objeto, resultando em duas versões de um objeto. Se o Versionamento do S3 estiver habilitado, ambas as versões serão armazenadas.
> Se você alterar os metadados de um arquivo armazenado no gateway de arquivos, um novo objeto S3 será criado e substituirá o objeto S3 existente. Esse comportamento é diferente de editar um arquivo em um sistema de arquivos, onde a edição de um arquivo não resulta na criação de um novo arquivo. Teste todas as operações de arquivo que você planeja usar comAWSStorage Gateway para que você entenda como cada operação de arquivo interage com o armazenamento do Amazon S3.
> Considere cuidadosamente o uso do controle de versão e CRR (Replicação entre regiões) do S3 no Amazon S3 quando você estiver carregando dados do gateway de arquivos. O upload de arquivos do gateway de arquivos para o Amazon S3 quando o controle de versão do S3 está habilitado resulta em pelo menos duas versões de um objeto S3.
> Determinados fluxos de trabalho envolvendo arquivos grandes e padrões de gravação de arquivos, como uploads de arquivos que são executados em várias etapas, podem aumentar o número de versões armazenadas de objetos S3. Se o cache do gateway de arquivos precisar liberar espaço devido a altas taxas de gravação de arquivos, várias versões de objeto S3 poderão ser criadas. Esses cenários aumentam o armazenamento S3 se o controle de versão do S3 estiver ativado e aumentam os custos de transferência associados à CRR. Teste todas as operações de arquivos que você planeja usar com o Storage Gateway para entender como cada operação de arquivo interage com o armazenamento do Amazon S3.
> O uso do utilitário Rsync com o gateway de arquivos resulta na criação de arquivos temporários no cache e na criação de objetos S3 temporários no Amazon S3. Essa situação resulta em cobranças de exclusão antecipada nas classes de armazenamento S3 Standard — IA (S3 Standard — IA) e S3 Intelligent-Tiering.

Para criar um compartilhamento de arquivos NFS

1. Abrir oAWSConsole Storage Gatewayhttps://console.aws.amazon.com/storagegateway/home/.
2. SelecioneCriar compartilhamento de arquivosPara abrir oConfigurações de compartilhamento de arquivos.

3. para oGateway, escolha o Amazon S3 File Gateway na lista.
4. para oLocal do Amazon S3, siga um destes procedimentos:

   - Para conectar o compartilhamento de arquivos diretamente ao bucket do S3, escolhaO nome do bucket do S3e, em seguida, insira o nome do bucket do S3 e, opcionalmente, um nome de prefixo para objetos criados pelo compartilhamento de arquivos. Seu gateway usa esse bucket para armazenar e recuperar arquivos. Para obter mais informações sobre como criar um novo bucket, consulte.Como criar um bucket do S3?noGuia do usuário do Amazon S3.
   - Para conectar o compartilhamento de arquivos a um bucket do S3 por meio de um ponto de acesso, escolhaUm ponto de acesso do S3e, em seguida, insira o nome do ponto de acesso do S3 e, opcionalmente, um nome de prefixo para objetos criados pelo compartilhamento de arquivos. Sua política de bucket deve ser configurada para delegar o controle de acesso ao ponto de acesso. Para obter mais informações sobre pontos de acesso, consulte.Gerenciamento de acesso a dados com pontos de acesso do Amazon S3eDelegar controle de acesso a pontos de acessonoGuia do usuário do Amazon S3.
   - Para conectar o compartilhamento de arquivos a um bucket do S3 por meio de um alias de ponto de acesso, escolhaAlias de ponto de acesso S3e, em seguida, insira o nome do alias do ponto de acesso do S3 e, opcionalmente, um nome de prefixo para objetos criados pelo compartilhamento de arquivos. Se você escolher essa opção, o gateway de arquivos não poderá criar um novoAWS Identity and Access ManagementPolítica de acesso e função do IAM em seu nome. Você deve selecionar uma função do IAM existente e configurar uma política de acesso naAcesso ao bucket do S3seção que se segue. Para obter mais informações sobre aliases de ponto de acesso, consulte.Usar um alias em estilo de bucket para seu ponto de acessonoGuia do usuário do Amazon S3.

   > **Note**
   >
   > - Se você inserir um nome de prefixo ou optar por se conectar por meio de um alias de ponto de acesso ou ponto de acesso, deverá inserir um nome de compartilhamento de arquivo.
   > - O nome do prefixo deve terminar com uma barra (/).
   > - Depois que o compartilhamento de arquivos for criado, o nome do prefixo não pode ser modificado nem excluído.

- Para obter mais informações sobre como usar nomes de prefixos, consulte.Organizar objetos usando prefixosnoGuia do usuário do Amazon S3.

5. para oRegião da AWS, escolha oRegião da AWSdo bucket do S3.
6. para oNome do compartilhamento de arquivos, insira um nome para o compartilhamento de arquivos. O nome padrão é o nome do bucket do S3 ou o nome do ponto de acesso.

> **Note**
>
> - Se você inseriu um nome de prefixo ou optou por se conectar por meio de um alias de ponto de acesso ou ponto de acesso, deverá inserir um nome de compartilhamento de arquivo.
> - Depois que o compartilhamento de arquivos for criado, o nome do compartilhamento de arquivos não poderá ser excluído.

7. (Opcional) ParaAWS PrivateLinkpara S3, faça o seguinte:

   1. Para configurar o compartilhamento de arquivos para se conectar ao S3 por meio de um endpoint de interface na sua Virtual Private Cloud (VPC) com tecnologiaAWS PrivateLink, escolhaUsar VPC endpoint.
   2. Para identificar o endpoint da interface VPC com o qual você deseja que o compartilhamento de arquivos se conecte, escolha um dos doisID de VPC endpointouNome DNS do endpoint da VPCe, em seguida, forneça as informações necessárias no campo correspondente.

> **Note**
>
> - Essa etapa é necessária se o compartilhamento de arquivos se conectar ao S3 por meio de um ponto de acesso VPC ou por meio de um alias associado a um ponto de acesso da VPC.
> - Conexões de compartilhamento de arquivos usandoAWS PrivateLinknão são compatíveis com gateways FIPS.
> - Para obter informações sobre oAWS PrivateLink, consulteAWS PrivateLinkpara Amazon S3noGuia do usuário do Amazon S3.

8. Em Access objects using (Acessar objetos usando), escolha Network File System (NFS) (Sistema de arquivos de rede (NFS)).
9. Em Audit logs (Logs de auditoria), escolha uma das seguintes opções:

   - Para desativar o registro em log, escolhaDisable logging (Desativar o registro em log)..
   - Para criar um novo log de auditoria, escolhaCriar um novo grupo de logs.
   - Para usar um log de auditoria existente, escolhaUse um grupo de logs existenteE, em seguida, escolha um log de auditoria na lista.

   Para obter mais informações sobre logs de auditoria, consulte Noções básicas sobre registros de auditoria do gateway.
10. para oAtualização automatizada de cache do S3, escolhaDefinir intervalo de atualizaçãoe defina a hora em dias, horas e minutos para atualizar o cache do compartilhamento de arquivos usando Time To Live (TTL). TTL é o período de tempo desde a última atualização. Após o intervalo TTL ter decorrido, acessar o diretório faz com que o gateway de arquivos atualize primeiro o conteúdo desse diretório a partir do bucket do Amazon S3.
11. para oNotificação de upload de arquivos, escolhaTempo de liquidação (segundos)para ser notificado quando um arquivo tiver sido totalmente carregado para o S3 pelo gateway de arquivos. DefinaTempo de liquidaçãoem segundos para controlar o número de segundos a aguardar após o último ponto no tempo que um cliente escreveu em um arquivo antes de gerar um`ObjectUploaded`Notificações. Como os clientes podem fazer muitas gravações pequenas em arquivos, é melhor definir esse parâmetro pelo maior tempo possível para evitar gerar várias notificações para o mesmo arquivo em um pequeno período de tempo. Para obter mais informações, consulte Obtendo notificação de upload de arquivos.

   > **Note**
   >
   > Essa configuração não tem efeito sobre o tempo do upload do objeto para o S3, somente no tempo da notificação.

12. (Opcional) Na seção Add tags (Adicionar tags), insira uma chave e um valor para adicionar tags ao compartilhamento de arquivos. Uma tag é um par de chave/valor que diferencia maiúsculas de minúsculas e ajuda você a gerenciar, filtrar e pesquisar o compartilhamento de arquivos.
13. Escolha Next (Próximo). OConfigurar como os arquivos são armazenados no Amazon S3A página é exibida.

14. para oClasse de armazenamento para novos objetos, escolha uma classe de armazenamento para usar para novos objetos criados no bucket do Amazon S3:

    - Para armazenar seus dados de objetos acessados com frequência de forma redundante em várias zonas de disponibilidade separadas geograficamente, escolhaS3 Standard. Para obter mais informações sobre a classe de armazenamento S3 Standard, consulte.Classes de armazenamento de objetos acessados com frequêncianoGuia do usuário do Amazon Simple Storage Service.
    - Para otimizar os custos de armazenamento movendo automaticamente os dados para o nível de acesso de armazenamento mais econômico, escolhaS3 Intelligent-Tiering. Para obter mais informações sobre a classe de armazenamento S3 Intelligent-Tiering, consulteClasse de armazenamento que otimiza automaticamente objetos muito e pouco acessadosnoGuia do usuário do Amazon Simple Storage Service.
    - Para armazenar seus dados de objetos raramente acessados de forma redundante em várias zonas de disponibilidade separadas geograficamente, escolhaS3 Standard – IA. Para obter mais informações sobre a classe de armazenamento S3 Standard — IA, consulte.Classes de armazenamento de objetos acessados com pouca frequêncianoGuia do usuário do Amazon Simple Storage Service.
    - Para armazenar seus dados de objetos raramente acessados em uma única zona de disponibilidade, escolhaS3 One Zone – IA. Para obter mais informações sobre a classe de armazenamento S3 One Zone — IA, consulte.Classes de armazenamento de objetos acessados com pouca frequêncianoGuia do usuário do Amazon Simple Storage Service.

    Para ajudar a monitorar o faturamento do S3, useAWS Trusted Advisor. Para obter mais informações, consulteFerramentas de monitoramentonoGuia do usuário do Amazon Simple Storage Service.

15. Em Object metadata (Metadados do objeto), escolha os metadados que você deseja usar:

    - Para habilitar a adivinhação do tipo MIME dos objetos enviados com base nas extensões de arquivo, escolhaAcho que o tipo MIME.
    - Para conceder controle total ao proprietário do bucket do S3 que mapeia para o compartilhamento de arquivos NFS, escolhaDê controle total ao proprietário do balde. Para obter mais informações sobre como usar seu compartilhamento de arquivos para acessar objetos em um bucket de propriedade de outra conta, consulteUso de um compartilhamento de arquivos para acesso entre contas.

- Se você estiver usando esse compartilhamento de arquivos em um bucket que requer que o solicitante ou leitor, em vez do proprietário do bucket, pague pelas cobranças de acesso, escolhaHabilitar pagamentos do solicitante. Para obter mais informações, consulte Buckets de pagamento pelo solicitante.

16. para oAcesso ao bucket do S3, escolha oAWS Identity and Access ManagementFunção do (IAM) que você deseja que o gateway de arquivos use. Assim, é possível acessar o bucket do Amazon S3:

    - Para habilitar o gateway de arquivos para criar uma nova função do IAM e uma política de acesso em seu nome, escolhaCriar uma nova função do IAM. Essa opção não estará disponível se o compartilhamento de arquivos se conectar ao Amazon S3 usando um alias de ponto de acesso.
    - Para selecionar uma função do IAM existente e configurar a política de acesso manualmente, escolhaUsar uma função do IAM existente. Você deve usar essa opção se o compartilhamento de arquivos se conectar ao Amazon S3 usando um alias de ponto de acesso. NoIAM role (Função do IAM)Em, insira o nome de recurso da Amazon (ARN) para a função usada para acessar o bucket do. Para obter informações sobre as funções do IAM, consulteFunções do IAMnoAWS Identity and Access ManagementGuia do usuário do.

    Para obter mais informações sobre o acesso ao bucket do S3, consulte Como conceder acesso a um bucket do Amazon S3.

17. para oCriptografia, escolha o tipo de chaves de criptografia a serem usadas para criptografar objetos que o gateway de arquivos armazena no Amazon S3:

    - Para usar a criptografia do lado do servidor gerenciada com o Amazon S3 (SSE-S3), escolhaChaves gerenciadas pelo S3 (SSE-S3).
    - Para usar a criptografia do lado do servidor gerenciada com oAWS Key Management Service(SSE-KMS), escolhaChaves gerenciadas pelo KMS (SSE-KMS). NoChave primária, escolha uma existenteAWS KMS keyou escolhaCriar uma nova chave do KMSPara criar uma nova chave do KMS noAWS Key Management Service(AWS KMS) console do. Para obter mais informações sobreAWS KMS, consulteO que é oAWS Key Management Service?noAWS Key Management ServiceGuia do desenvolvedor.

> **Note**
>
> Para especificar umAWS KMSchave com um alias que não está listado ou para usar umAWS KMSchave de um diferenteConta da AWS, você deverá usar oAWS Command Line Interface(AWS CLI). Para obter mais informações, consulteCreateNFSFileSharenoAWSReferência da API Storage Gateway. Chaves KMS assimétricas não são suportadas.

18. SelecioneProximopara definir as configurações de acesso a arquivos.

Para definir as configurações de acesso a arquivos

1. para oClientes permitidos, especifique se deseja permitir ou restringir o acesso de cada cliente ao compartilhamento de arquivos. Forneça o endereço IP ou a notação CIDR para os clientes que você deseja permitir o acesso. Para obter informações sobre clientes NFS compatíveis, consulte Clientes NFS compatíveis para um gateway de arquivos.
2. para oOpções de montagem, especifique as opções que você desejaNível de squasheExportar como.

   Em Nível de extermínio, escolha uma das seguintes opções:

   - Toda a abóbora: Todo o acesso de usuário é mapeado para o ID de usuário (UID) (65534) e o ID de grupo (GID) (65534).
   - Sem abóbora de raiz: O superusuário remoto (raiz) recebe acesso como raiz.
   - Squash raiz (padrão): O acesso para o superusuário remoto (raiz) é mapeado para o UID (65534) e o GID (65534).

   Em Exportar como, escolha uma das seguintes opções:

   - leitura/gravação
   - Somente leitura

   > **Note**
   >
   > Para compartilhamentos de arquivos montados em um cliente Microsoft Windows, se você escolherSomente leitura, você provavelmente verá uma mensagem de erro. Ela

indica que um erro inesperado está impedindo que você crie a pasta. Você pode ignorar a mensagem.

3. Em Padrões de metadados de arquivo, é possível editar as Permissões de diretório, as Permissões de arquivo, o ID de usuário e o ID de grupo. Para obter mais informações, consulte Edição de padrões de metadados para seu compartilhamento de arquivos NFS.
4. Escolha Next (Próximo).
5. Revise as definições de configuração do compartilhamento de arquivos e escolhaFinish.

   Após a criação do seu compartilhamento de arquivos NFS, você poderá ver as configurações na guia Details (Detalhes) do compartilhamento de arquivos.

Próxima etapa

Monte seu compartilhamento de arquivos NFS no cliente

Criar um compartilhamento de arquivos SMB

Antes de criar um compartilhamento de arquivos Server Message Block (SMB), certifique-se de definir as configurações de segurança SMB no gateway de arquivos. Também é necessário configurar o Microsoft Active Directory (AD) ou o acesso de convidado para a autenticação. O compartilhamento de arquivos oferece apenas um tipo de acesso SMB. Para obter instruções, consulteEditando configurações SMB para um gateway.

> **Note**
>
> Um compartilhamento de arquivos SMB não funciona corretamente, a menos que as portas necessárias estejam abertas no grupo de segurança. Para obter mais informações, consulte Requisitos de porta.

> **Note**
>
> Quando um arquivo é gravado no gateway de arquivos por um cliente SMB, o gateway de arquivos carrega os dados do arquivo para o Amazon S3 seguidos de seus metadados (proprietários, carimbos de data/hora e assim por diante). O upload dos dados do arquivo

cria um objeto S3 e o upload dos metadados do arquivo atualiza os metadados do objeto S3. Esse processo cria outra versão do objeto, resultando em duas versões de um objeto. Se o Versionamento do S3 estiver habilitado, ambas as versões serão armazenadas.
Se você alterar os metadados de um arquivo armazenado no gateway de arquivos, um novo objeto S3 será criado e substituirá o objeto S3 existente. Esse comportamento é diferente de editar um arquivo em um sistema de arquivos, onde a edição de um arquivo não resulta na criação de um novo arquivo. Teste todas as operações de arquivo que você planeja usar comAWSStorage Gateway para que você entenda como cada operação de arquivo interage com o armazenamento do Amazon S3.
Considere cuidadosamente o uso do controle de versão e CRR (Replicação entre regiões) do S3 no Amazon S3 quando você estiver carregando dados do gateway de arquivos. O upload de arquivos do gateway de arquivos para o Amazon S3 quando o controle de versão do S3 está habilitado resulta em pelo menos duas versões de um objeto S3.
Determinados fluxos de trabalho envolvendo arquivos grandes e padrões de gravação de arquivos, como uploads de arquivos que são executados em várias etapas, podem aumentar o número de versões armazenadas de objetos S3. Se o cache do gateway de arquivos precisar liberar espaço devido a altas taxas de gravação de arquivos, várias versões de objeto S3 poderão ser criadas. Esses cenários aumentam o armazenamento S3 se o controle de versão do S3 estiver ativado e aumentam os custos de transferência associados à CRR. Teste todas as operações de arquivos que você planeja usar com o Storage Gateway para entender como cada operação de arquivo interage com o armazenamento do Amazon S3.
O uso do utilitário Rsync com o gateway de arquivos resulta na criação de arquivos temporários no cache e na criação de objetos S3 temporários no Amazon S3. Essa situação resulta em cobranças de exclusão antecipada nas classes de armazenamento S3 Standard — IA (S3 Standard — IA) e S3 Intelligent-Tiering.

Criar um compartilhamento de arquivos SMB

Para criar um compartilhamento de arquivos SMB

1. Abrir oAWSConsole Storage Gatewayhttps://console.aws.amazon.com/storagegateway/home/.
2. SelecioneCriar compartilhamento de arquivosPara abrir oConfigurações de compartilhamento de arquivos.
3. para oGateway, escolha o Amazon S3 File Gateway na lista.
4. para oLocal do Amazon S3, siga um destes procedimentos:

- Para conectar o compartilhamento de arquivos diretamente ao bucket do S3, escolhaO nome do bucket do S3e, em seguida, insira o nome do bucket e, opcionalmente, um nome de prefixo para objetos criados pelo compartilhamento de arquivos. Seu gateway usa esse bucket para armazenar e recuperar arquivos. Para obter mais informações sobre como criar um novo bucket, consulte.Como criar um bucket do S3?noGuia do usuário do Amazon S3.
- Para conectar o compartilhamento de arquivos a um bucket do S3 por meio de um ponto de acesso, escolhaUm ponto de acesso do S3e, em seguida, insira o nome do ponto de acesso do S3 e, opcionalmente, um nome de prefixo para objetos criados pelo compartilhamento de arquivos. Sua política de bucket deve ser configurada para delegar o controle de acesso ao ponto de acesso. Para obter mais informações sobre pontos de acesso, consulte.Gerenciamento de acesso a dados com pontos de acesso do Amazon S3eDelegar controle de acesso a pontos de acessonoGuia do usuário do Amazon S3.
- Para conectar o compartilhamento de arquivos a um bucket do S3 por meio de um alias de ponto de acesso, escolhaAlias de ponto de acesso S3e, em seguida, insira o nome do alias do ponto de acesso do S3 e, opcionalmente, um nome de prefixo para objetos criados pelo compartilhamento de arquivos. Se você escolher essa opção, o gateway de arquivos não poderá criar um novoAWS Identity and Access ManagementPolítica de acesso e função do IAM em seu nome. Você deve selecionar uma função do IAM existente e configurar uma política de acesso naAcesso ao bucket do S3seção que se segue. Para obter mais informações sobre aliases de ponto de acesso, consulte.Usar um alias em estilo de bucket para seu ponto de acessonoGuia do usuário do Amazon S3.

> **Note**
>
> - Se você inserir um nome de prefixo ou optar por se conectar por meio de um alias de ponto de acesso ou ponto de acesso, deverá inserir um nome de compartilhamento de arquivo.
> - O nome do prefixo deve terminar com uma barra (/).
> - Depois que o compartilhamento de arquivos for criado, o nome do prefixo não pode ser modificado nem excluído.
> - Para obter mais informações sobre como usar nomes de prefixos, consulte.Organizar objetos usando prefixosnoGuia do usuário do Amazon S3.

5. para oRegião da AWS, escolha oRegião da AWSdo bucket do S3.

6. para oNome do compartilhamento de arquivos, insira um nome para o compartilhamento de arquivos. O nome padrão é o nome do bucket do S3 ou o nome do ponto de acesso.

> **Note**
>
> - Se você inseriu um nome de prefixo ou optou por se conectar por meio de um alias de ponto de acesso ou ponto de acesso, deverá inserir um nome de compartilhamento de arquivo.
> - Depois que o compartilhamento de arquivos for criado, o nome do compartilhamento de arquivos não poderá ser excluído.

7. (Opcional) ParaAWS PrivateLinkpara S3, faça o seguinte:

   1. Para configurar o compartilhamento de arquivos para se conectar ao S3 por meio de um endpoint de interface na sua Virtual Private Cloud (VPC) com tecnologiaAWS PrivateLink, escolhaUsar VPC endpoint.
   2. Para identificar o endpoint da interface VPC com o qual você deseja que o compartilhamento de arquivos se conecte, escolha um dos doisID de VPC endpointouNome DNS do endpoint da VPCe, em seguida, forneça as informações necessárias no campo correspondente.

> **Note**
>
> - Essa etapa é necessária se o compartilhamento de arquivos se conectar ao S3 por meio de um ponto de acesso VPC ou por meio de um alias associado a um ponto de acesso da VPC.
> - Conexões de compartilhamento de arquivos usandoAWS PrivateLinknão são compatíveis com gateways FIPS.
> - Para obter informações sobre oAWS PrivateLink, consulteAWS PrivateLinkpara Amazon S3noGuia do usuário do Amazon Simple Storage Service.

8. Em Access objects using (Acessar objetos usando), escolha Server Message Block (SMB).
9. Em Audit logs (Logs de auditoria), escolha uma das seguintes opções:

   - Para desativar o registro em log, escolhaDisable logging (Desativar o registro em log)..
   - Para criar um novo log de auditoria, escolhaCriar um novo grupo de logs.

- Para usar um grupo de logs existente, escolhaUse um grupo de logs existenteE, em seguida, escolha um log de auditoria na lista.

Para obter mais informações sobre logs de auditoria, consulte Noções básicas sobre registros de auditoria do gateway.

10. para oAtualização automatizada de cache do S3, escolhaDefinir intervalo de atualizaçãoe, em seguida, defina a hora em dias, horas e minutos para atualizar o cache do compartilhamento de arquivos usando Time To Live (TTL). TTL é o período de tempo desde a última atualização. Após o intervalo TTL ter decorrido, acessar o diretório faz com que o gateway de arquivos atualize primeiro o conteúdo desse diretório a partir do bucket do Amazon S3.
11. para oNotificação de upload de arquivos, escolhaTempo de liquidação (segundos)para ser notificado quando um arquivo tiver sido totalmente carregado para o S3 pelo gateway de arquivos. DefinaTempo de liquidaçãoem segundos para controlar o número de segundos a aguardar após o último ponto no tempo que um cliente escreveu em um arquivo antes de gerar um`ObjectUploaded`Notificações. Como os clientes podem fazer muitas gravações pequenas em arquivos, é melhor definir esse parâmetro pelo maior tempo possível para evitar gerar várias notificações para o mesmo arquivo em um pequeno período de tempo. Para obter mais informações, consulte Obtendo notificação de upload de arquivos.

> **Note**
>
> Essa configuração não tem efeito sobre o tempo do upload do objeto para o S3, somente no tempo da notificação.

12. (Opcional) NoTagsSeção, escolhaAdicionar nova tagE, em seguida, insira uma chave e um valor para adicionar tags ao compartilhamento de arquivos. Uma tag é um par de chave/valor que diferencia maiúsculas de minúsculas e ajuda você a gerenciar, filtrar e pesquisar o compartilhamento de arquivos.
13. Escolha Next (Próximo). OConfigurações de armazenamento do Amazon S3A página é exibida.
14. para oClasse de armazenamento para novos objetos, escolha uma classe de armazenamento para usar para novos objetos criados no bucket do Amazon S3:

    - Para armazenar seus dados de objetos acessados com frequência de forma redundante em várias zonas de disponibilidade separadas geograficamente, escolhaS3 Standard. Para obter mais informações sobre a classe de armazenamento S3 Standard, consulte.Classes de

armazenamento de objetos acessados com frequêncianoGuia do usuário do Amazon Simple Storage Service.

- Para otimizar os custos de armazenamento movendo automaticamente os dados para o nível de acesso de armazenamento mais econômico, escolhaS3 Intelligent-Tiering. Para obter mais informações sobre a classe de armazenamento S3 Intelligent-Tiering, consulteClasse de armazenamento que otimiza automaticamente objetos muito e pouco acessadosnoGuia do usuário do Amazon Simple Storage Service.
- Para armazenar seus dados de objetos raramente acessados de forma redundante em várias zonas de disponibilidade separadas geograficamente, escolhaS3 Standard – IA. Para obter mais informações sobre a classe de armazenamento S3 Standard — IA, consulte.Classes de armazenamento de objetos acessados com pouca frequêncianoGuia do usuário do Amazon Simple Storage Service.
- Para armazenar seus dados de objetos raramente acessados em uma única zona de disponibilidade, escolhaS3 One Zone – IA. Para obter mais informações sobre a classe de armazenamento S3 One Zone — IA, consulte.Classes de armazenamento de objetos acessados com pouca frequêncianoGuia do usuário do Amazon Simple Storage Service.

Para ajudar a monitorar o faturamento do S3, useAWS Trusted Advisor. Para obter mais informações, consulteFerramentas de monitoramentonoGuia do usuário do Amazon Simple Storage Service.

15. Em Object metadata (Metadados do objeto), escolha os metadados que você deseja usar:

    - Para habilitar a adivinhação do tipo MIME dos objetos enviados com base nas extensões de arquivo, escolhaAcho que o tipo MIME.
    - Para conceder controle total ao proprietário do bucket do S3 que mapeia para o compartilhamento de arquivos SMB, escolhaDê controle total ao proprietário do balde. Para obter mais informações sobre como usar seu compartilhamento de arquivos para acessar objetos em um bucket de propriedade de outra conta, consulteUso de um compartilhamento de arquivos para acesso entre contas.
    - Para conceder controle total ao proprietário do bucket do S3 que mapeia para o compartilhamento de arquivos SMB, escolhaHabilitar pagamentos do solicitante. Para obter mais informações, consulte Buckets de pagamento pelo solicitante.

16. para oAcesso ao bucket do S3, escolha oAWS Identity and Access ManagementFunção do (IAM) que você deseja que o gateway de arquivos use. Assim, é possível acessar o bucket do Amazon S3:

- Para habilitar o gateway de arquivos para criar uma nova função do IAM e uma política de acesso em seu nome, escolhaCriar uma nova função do IAM. Essa opção não estará disponível se o compartilhamento de arquivos se conectar ao Amazon S3 usando um alias de ponto de acesso.
- Para selecionar uma função do IAM existente e configurar a política de acesso manualmente, escolhaUsar uma função do IAM existente. Você deve usar essa opção se o compartilhamento de arquivos se conectar ao Amazon S3 usando um alias de ponto de acesso. NoIAM role (Função do IAM)Em, insira o nome de recurso da Amazon (ARN) para a função usada para acessar o bucket do. Para obter informações sobre as funções do IAM, consulteFunções do IAMnoAWS Identity and Access ManagementGuia do usuário do.

Para obter mais informações sobre o acesso ao bucket do S3, consulte Como conceder acesso a um bucket do Amazon S3.

17. para oCriptografia, escolha o tipo de chaves de criptografia a serem usadas para criptografar objetos que o gateway de arquivos armazena no Amazon S3:

    - Para usar a criptografia do lado do servidor gerenciada com o Amazon S3 (SSE-S3), escolhaChaves gerenciadas pelo S3 (SSE-S3).
    - Para usar a criptografia do lado do servidor gerenciada com oAWS Key Management Service(SSE-KMS), escolhaChaves gerenciadas pelo KMS (SSE-KMS). NoChave primária, escolha uma existenteAWS KMS keyou escolhaCriar uma nova chave do KMSPara criar uma nova chave do KMS noAWS Key Management Service(AWS KMS) console do. Para obter mais informações sobreAWS KMS, consulteO que é oAWS Key Management Service?noAWS Key Management ServiceGuia do desenvolvedor.

    > **Note**
    >
    > Para especificar umAWS KMSchave com um alias que não está listado ou para usar umAWS KMSchave de um diferenteConta da AWS, você deverá usar oAWS Command Line Interface(AWS CLI). Para obter mais informações, consulteCreateNFSFileSharenoAWSReferência da API Storage Gateway. Chaves KMS assimétricas não são suportadas.

18. Escolha Next (Próximo). OConfigurações de acesso a arquivosA página é exibida.
19. para oMétodo de autenticação, escolha o método de autenticação que você deseja usar.

- Para usar o Microsoft AD corporativo para acesso autenticado pelo usuário ao compartilhamento de arquivos SMB, escolhaActive Directory. O gateway de arquivos deve estar integrado ao domínio.
- Para fornecer apenas acesso de hóspede, escolhaAcesso aos convidados. Se você selecionar esse método de autenticação, o gateway de arquivos não precisará fazer parte de um domínio do Microsoft AD. Também é possível usar um gateway de arquivos membro do domínio do AD para criar compartilhamentos de arquivos com acesso de convidado. Você deve definir uma senha de convidado para o servidor SMB no campo correspondente.

> **Note**
>
> Ambos os tipos de acesso estão disponíveis ao mesmo tempo.

20. NoConfigurações de compartilhamento SMB, escolha suas configurações.

    Em Exportar como, escolha uma das seguintes opções:

    - Leitura/gravação (o valor padrão)
    - Somente leitura

> **Note**
>
> Para compartilhamentos de arquivos montados em um cliente Microsoft Windows, se você escolherSomente leitura, você provavelmente verá uma mensagem de erro. Ela indica que um erro inesperado está impedindo que você crie a pasta. Você pode ignorar a mensagem.

    Em File/directory access controlled by (Acesso ao arquivo/diretório controlado por), escolha uma das seguintes opções:

    - Para definir permissões refinadas em arquivos e pastas no compartilhamento de arquivos SMB, escolhaLista de controle de acesso do Windows. Para obter mais informações, consulte Usar as ACLs do Microsoft Windows para controlar o acesso a um compartilhamento de arquivos SMB.

- Para usar permissões POSIX para controlar o acesso a arquivos e diretórios armazenados por meio de um compartilhamento de arquivos NFS ou SMB, escolhaPermissões POSIX.

Se o método de autenticação forActive Directory, paraUsuários/grupos administrativos, insira uma lista separada por vírgulas de usuários e grupos do AD. Faça isso se você quiser que o usuário administrador tenha privilégios para atualizar as listas de controle de acesso (ACLs) em todos os arquivos e pastas no compartilhamento de arquivos. Esses usuários e grupos terão direitos de administrador para o compartilhamento de arquivos. Um grupo deve ser prefixado com o@personagem, por exemplo,`@group1`.

para oDiferenciação de letras maiúsculas e minúsculas, escolha uma das seguintes opções:

- Para permitir que o gateway controle a sensibilidade entre maiúsculas e minúsculasEspecificado pelo cliente.
- Para permitir que o cliente controle a sensibilidade entre maiúsculas e minúsculasForce maiúscula.

> **Note**
>
> - Se selecionada, essa configuração se aplica imediatamente a novas conexões de cliente SMB. As conexões de cliente SMB existentes devem se desconectar do compartilhamento de arquivos e reconectar para que a configuração entre em vigor.

para oEnumeração baseada em acesso, escolha uma das seguintes opções:

- Para tornar os arquivos e pastas no compartilhamento visíveis somente para usuários que têm acesso de leitura, escolhaDesabilitado para arquivos e diretórios.
- Para tornar os arquivos e pastas no compartilhamento visíveis para todos os usuários durante a enumeração de diretórios, escolhaAtivado para arquivos e diretórios.

> **Note**
>
> A enumeração baseada em acesso é um sistema que filtra a enumeração de arquivos e pastas em um compartilhamento de arquivos SMB com base nas listas de controle de acesso (ACLs) do compartilhamento.

para oBloqueio oportunista (oplock), escolha uma das seguintes opções:

- Para permitir que o compartilhamento de arquivos use o bloqueio oportunista para otimizar a estratégia de buffer de arquivos, escolhaEnabled (Habilitado). Na maioria dos casos, permitir o bloqueio oportunista melhora o desempenho, especialmente no que diz respeito aos menus de contexto do Windows.
- Para evitar o uso de bloqueio oportunista, escolhaDesabilitado. Se vários clientes Windows em seu ambiente costumam editar os mesmos arquivos simultaneamente, desabilitar o bloqueio oportunista às vezes pode melhorar o desempenho.

> **Note**
>
> Permitir o bloqueio oportunista em compartilhamentos que diferenciam maiúsculas de minúsculas não é recomendado para cargas de trabalho que envolvam acesso a arquivos com o mesmo nome em diferentes casos.

21. (Opcional) NoAcesso ao compartilhamento de arquivos de usuário e grupo, escolha suas configurações.

    para oUsuários e grupos permitidos, escolhaAdicionar usuário permitidoouAdicionar grupo permitidoE insira um usuário ou grupo do AD que pode permitir acesso ao compartilhamento de arquivos. Repita esse processo para permitir quantos usuários e grupos forem necessários.

    para oUsuários e grupos negados, escolhaAdicionar usuário negadoouAdicionar grupo negadoE insira um usuário ou grupo do AD que deve negar o acesso ao compartilhamento de arquivos. Repita esse processo para negar quantos usuários e grupos forem necessários.

> **Note**
>
> OAcesso ao compartilhamento de arquivos de usuário e grupoa seção aparece somente seActive DirectoryÉ selecionado.
> Insira somente o nome do usuário ou grupo do AD. O nome de domínio é inferido pela associação do gateway no AD específico no qual o gateway ingressou.
> Se você não especificar usuários ou grupos permitidos ou negados, qualquer usuário do AD autenticado poderá exportar o compartilhamento de arquivos.

22. Escolha Next (Próximo).
23. Revise as definições de configuração do compartilhamento de arquivos e escolhaFinish.

    Após a criação do compartilhamento de arquivos SMB, você poderá visualizar as configurações na guia Detalhes do compartilhamento de arquivos.

Próxima etapa

Monte seu compartilhamento de arquivos SMB no cliente

Monte e use seu compartilhamento de arquivos

A seguir você pode encontrar instruções sobre como montar seu compartilhamento de arquivos no cliente, como usá-lo, testar seu gateway de arquivo e limpar os recursos conforme necessário. Para obter mais informações sobre clientes de Network File System (NFS) compatíveis, consulte Clientes NFS compatíveis para um gateway de arquivos. Para obter mais informações sobre clientes de Service Message Block (SMB) compatíveis, consulte Clientes SMB compatíveis para um gateway de arquivos.

Você pode encontrar exemplos de comandos para montar o compartilhamento de arquivos no AWS Management Console. Nas seções a seguir, você poderá encontrar detalhes sobre como montar seu compartilhamento de arquivos no cliente, usar seu compartilhamento, testar seu gateway de arquivo e limpar os recursos conforme necessário.

Tópicos

Monte seu compartilhamento de arquivos NFS no cliente

Agora você montar o compartilhamento de arquivos NFS em uma unidade no cliente e mapeá-lo para um bucket do Amazon S3.

Para montar um compartilhamento de arquivos e mapeá-lo para um bucket do Amazon S3

1. Se você estiver usando um cliente Microsoft Windows, recomendamos criar um compartilhamento de arquivos SMB e o acesse usando um cliente SMB já instalado no cliente Windows. Se você usar NFS, ative Serviços para NFS no Windows.
2. Monte seu compartilhamento de arquivos NFS:
    - Para clientes Linux, digite o seguinte comando no prompt de comando.

```
sudo mount -t nfs -o nolock,hard [Your gateway VM IP address]:/[S3 bucket name] [mount path on your client]
```

- Para clientes MacOS, digite o seguinte comando no prompt de comando.

```
sudo mount_nfs -o vers=3,nolock,rwsize=65536,hard -v [Your gateway VM IP address]:/[S3 bucket name] [mount path on your client]
```

- Para clientes Windows, digite o seguinte comando no prompt de comando.

```
mount –o nolock -o mtype=hard [Your gateway VM IP address]:/[S3 bucket name] [Drive letter on your windows client]
```

Por exemplo, suponha que em um cliente Windows seu endereço IP da VM seja 123.123.1.2 e nome do bucket do Amazon S3 sejatest-bucket. Suponha também que você deseja mapear para a unidade T. Nesse caso, o comando tem a seguinte aparência.

```
mount -o nolock -o mtype=hard 123.123.1.2:/test-bucket T:
```

> **Note**
>
> Ao montar compartilhamentos de arquivos, esteja ciente do seguinte:
>
> - Pode acontecer de uma pasta e um objeto existirem em um bucket do Amazon S3 e terem o mesmo nome. Neste caso, se o nome do objeto não contiver uma barra no final, apenas a pasta ficará visível no gateway de arquivos. Por exemplo, se um bucket contiver um objeto chamadotestoutest/E uma pasta chamadatest/test1, onlytest/etest/test1são visíveis em um gateway de arquivos.
> - É provável que você precise montar novamente o compartilhamento de arquivos ao reinicializar seu cliente.
> - Por padrão, o Windows usa uma montagem flexível para montar o compartilhamento NFS. As montagens flexíveis expiram mais facilmente quando há problemas de conexão. É recomendável usar uma montagem de disco rígido porque uma montagem é mais segura e preserva melhor os dados. O comando de montagem flexível omite o switch **`-o mtype=hard`**. O comando de montagem de disco rígido do Windows usa o switch `-o mtype=hard`.
> - Se você estiver usando clientes Windows, verifique suas opções `mount` após a montagem executando o comando `mount` sem opções. A resposta deve confirmar

que o compartilhamento de arquivos foi montado usando as opções mais recentes que você forneceu. Ela também deve confirmar que você não está usando entradas antigas em cache, que levam pelo menos 60 segundos para desaparecer.

Próxima etapa

Teste seu S3 File Gateway

Monte seu compartilhamento de arquivos SMB no cliente

Agora você montar seu compartilhamento de arquivos SMB e mapear para uma unidade acessível por seu cliente. A seção File Gateway (gateway) do console mostra os comandos de montagem compatíveis que você pode usar para clientes SMB. A seguir, você pode encontrar algumas opções adicionais para testar.

Você pode usar vários métodos diferentes para montar compartilhamentos de arquivos SMB, incluindo o seguinte:

- Prompt de comando (`cmdkeyenet use`) — Use o prompt de comando para montar o compartilhamento de arquivos. Armazene suas credenciais com`cmdkeye`, em seguida, monte a unidade com`net use`E inclua o`/persistent:yese/savecred`Alterna se quiser que a conexão permaneça em reinicializações do sistema. Os comandos específicos que você usa serão diferentes dependendo se você deseja montar a unidade para acesso do Microsoft Active Directory (AD) ou acesso de usuário convidado. Os exemplos são fornecidos abaixo.
- Explorador de arquivos (Map Network Drive) — Use o Windows File Explorer para montar seu compartilhamento de arquivos. Defina as configurações para especificar se você deseja que a conexão permaneça nas reinicializações do sistema e solicite credenciais de rede.
- Script do PowerShell — Crie um script PowerShell personalizado para montar seu compartilhamento de arquivos. Dependendo dos parâmetros especificados no script, a conexão pode ser persistente em reinicializações do sistema, e o compartilhamento pode ser visível ou invisível para o sistema operacional enquanto montado.

> **Note**
>
> Se você for um usuário do Microsoft AD, verifique com o administrador para garantir que você tenha acesso ao compartilhamento de arquivos SMB antes de montá-lo no seu sistema local.
>
> Se você for um usuário convidado, certifique-se de que você tem a senha da conta de usuário convidado antes de tentar montar o compartilhamento de arquivos.

Para montar o compartilhamento de arquivos SMB para usuários autorizados do Microsoft AD usando o prompt de comando:

1. Verifique se o usuário do Microsoft AD tem as permissões necessárias para o compartilhamento de arquivos SMB antes de montar o compartilhamento de arquivos no sistema do usuário.
2. Insira o seguinte no prompt de comando para montar o compartilhamento de arquivos:

   ```
   net use WindowsDriveLetter: \\GatewayIPAddress\FileShareName /
   persistent:yes
   ```

Para montar o compartilhamento de arquivos SMB com uma combinação de nome de usuário e senha específica usando o prompt de comando:

1. Certifique-se de que a conta de usuário tenha acesso ao compartilhamento de arquivos SMB antes de montar o compartilhamento de arquivos no sistema.
2. Insira o seguinte no prompt de comando para salvar as credenciais do usuário no Gerenciador de credenciais do Windows:

   ```
   cmdkey /add:GatewayIPAddress /user:DomainName\UserName /pass:Password
   ```
3. Insira o seguinte no prompt de comando para montar o compartilhamento de arquivos:

   ```
   net use WindowsDriveLetter: \\GatewayIPAddress\FileShareName /
   persistent:yes /savecred
   ```

Para montar o compartilhamento de arquivos SMB para usuários convidados usando o prompt de comando:

1. Certifique-se de que você tem a senha da conta de usuário convidado antes de montar o compartilhamento de arquivos.
2. Digite o seguinte no prompt de comando para salvar as credenciais de convidado no Gerenciador de credenciais do Windows:

   ```
   cmdkey /add:GatewayIPAddress /user:DomainName\smbguest /pass:Password
   ```

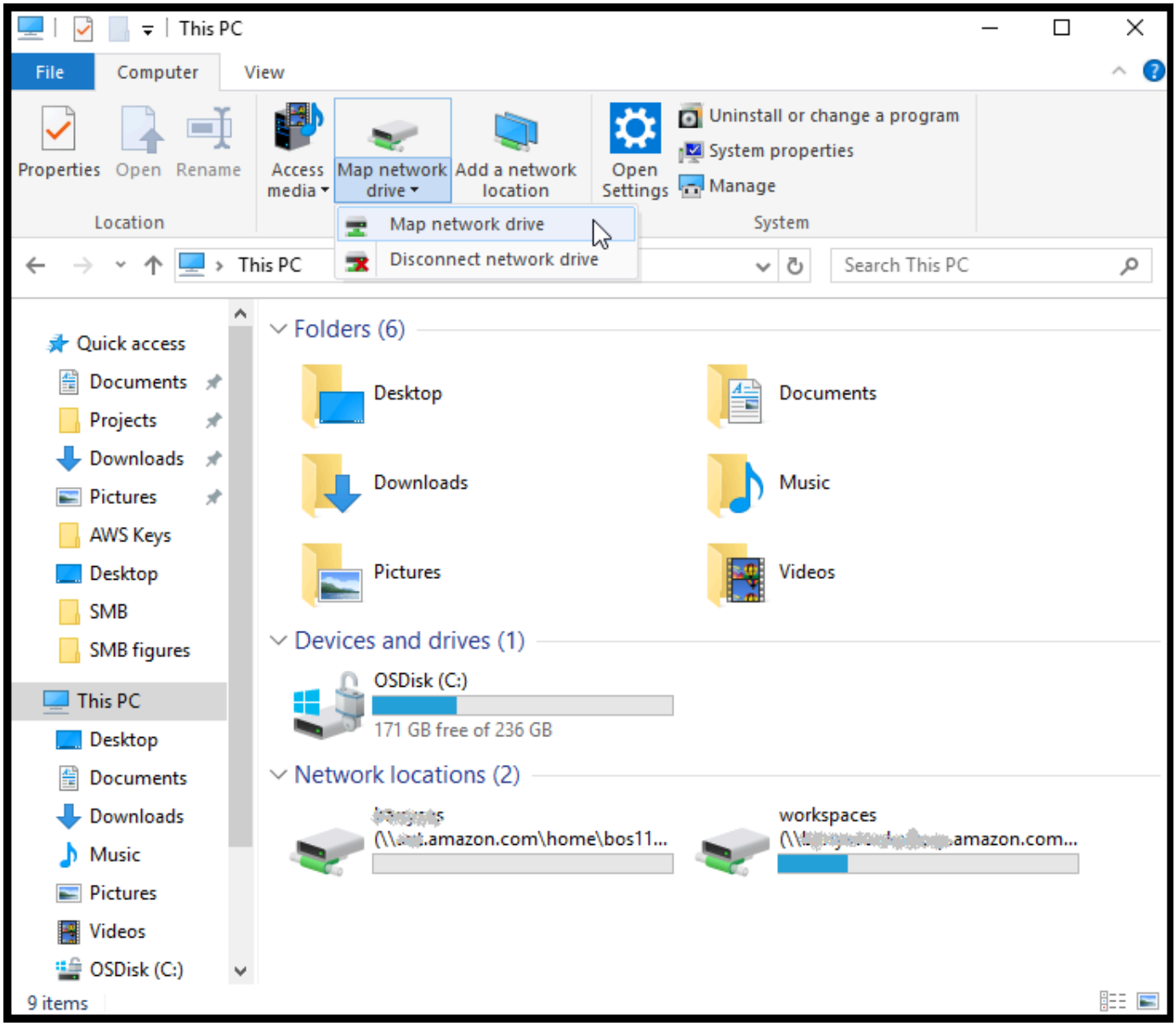
3. Digite o seguinte no prompt de comando.

   ```
   net use WindowsDriveLetter: \\$GatewayIPAddress\$Path /user:$GatewayID\smbguest /persistent:yes /savecred
   ```

> **Note**
>
> Ao montar compartilhamentos de arquivos, esteja ciente do seguinte:
>
> - Pode acontecer de uma pasta e um objeto existirem em um bucket do Amazon S3 e terem o mesmo nome. Neste caso, se o nome do objeto não contiver uma barra no final, apenas a pasta ficará visível no gateway de arquivos. Por exemplo, se um bucket contiver um objeto chamado`testoutest/`E uma pasta chamada`test/test1`, only`test/etest/test1`são visíveis em um gateway de arquivos.
> - A menos que você configure sua conexão de compartilhamento de arquivos para salvar suas credenciais de usuário e persistir nas reinicializações do sistema, talvez seja necessário remontar o compartilhamento de arquivos sempre que reiniciar o sistema cliente.

Para montar um compartilhamento de arquivos SMB usando Windows File Explorer

1. Pressione a tecla Windows e digite **`File Explorer`** na caixa Pesquisa do Windows ou pressione **`Win+E`**.
2. No painel de navegação, escolha Este PC. Em seguida, escolha Mapear unidade de rede para Mapear unidade de rede na guia Computador, como exibido na captura de tela a seguir.



3. Na caixa de diálogo Mapear unidade de rede, escolha uma letra de unidade em Unidade.
4. Para Pasta, digite ***[File Gateway IP]**[SMB File Share Name]*** ou selecione Procurar para escolher seu compartilhamento de arquivos SMB na caixa de diálogo.
5. (Opcional) Selecione Reconectar ao entrar se quiser que seu ponto de montagem persista após reinicializações.
6. (Opcional) Selecione Conectar usando credenciais diferentes se você deseja que um usuário insira o logon do Microsoft AD ou uma conta de usuário e senha de convidado.
7. Escolha Finalizar para concluir o ponto de montagem.

Você pode editar configurações de compartilhamento de arquivos, editar usuários e grupos permitidos e negados e alterar o acesso de convidado com senha no Storage Gateway Management Console. Você também pode atualizar os dados no cache de compartilhamento de arquivos e excluir um compartilhamento de arquivos do console.

Para modificar suas propriedades de compartilhamento de arquivos SMB

1. Abra o console Storage Gateway emhttps://console.aws.amazon.com/storagegateway/home.
2. No painel de navegação, escolha File Shares (Compartilhamentos de arquivos).
3. Na página File Share (Compartilhamento de arquivos), marque a caixa de seleção próxima ao compartilhamento de arquivos SMB que você deseja modificar.
4. Em Ações, escolha a ação desejada:

   - Escolha Edit file share settings (Editar configurações de compartilhamento de arquivos) para modificar o acesso do compartilhamento.
   - Escolha Edit allowed/denied users (Editar usuários permitidos/negados) para adicionar ou excluir usuários e grupos e digite os usuários e grupos permitidos e negados nas caixas Allowed Users (Usuários permitidos), Denied Users (Usuários negados), Allowed Groups (Grupos permitidos) e Denied Groups (Grupos negados). Use os botões Add Entry (Adicionar entrada) para criar novos direitos de acesso e o botão (X) para remover acesso.
5. Ao terminar, escolha Save (Salvar).

   Quando adiciona permissão a usuários e grupos, você cria uma lista de permissões. Sem uma lista de permissões, todos os usuários autenticados do Microsoft AD podem acessar o compartilhamento de arquivos SMB. Todos os usuários e grupos marcados como negados são adicionados a uma lista de negações e não podem acessar o compartilhamento de arquivos SMB. Nos casos em que um usuário ou grupo está na lista de negações e na lista de permissões, a lista de negação tem precedência.

   Você pode habilitar as listas de controle de acesso (ACLs) em seu compartilhamento de arquivos SMB. Para obter informações sobre como habilitar as ACLs, consulte Usar as ACLs do Microsoft Windows para controlar o acesso a um compartilhamento de arquivos SMB.

Próxima etapa

Teste seu S3 File Gateway

Trabalhando com compartilhamentos de arquivos em um bucket com objetos pré-exisiting

Você pode exportar um compartilhamento de arquivos em um bucket do Amazon S3 com objetos criados fora do gateway de arquivos usando NFS ou SMB. Os objetos no bucket criados fora do gateway serão exibidos como arquivos no sistema de arquivos NFS ou SMB quando os clientes do sistema de arquivos os acessarem. Permissões e acesso padrão de Portable Operating System Interface (POSIX) são usados no compartilhamento de arquivos. Quando você grava arquivos de volta em um bucket do Amazon S3, eles assumem as propriedades e os direitos de acesso que você concede a eles.

Você pode fazer upload de objetos em um bucket do S3 a qualquer momento. Para que o compartilhamento de arquivos exiba esses objetos adicionados recentemente como arquivos, é necessário atualizar o bucket do S3. Para obter mais informações, consulte the section called “Atualizar objetos no bucket do Amazon S3”.

> **Note**
>
> Não recomendamos ter vários usuários que gravam em um bucket do Amazon S3. Se você fizer isso, leia a seção “Posso ter vários usuários que gravam em meu bucket do Amazon S3? noPerguntas frequentes sobre Storage Gateway.

Para atribuir padrões de metadados a objetos acessados usando NFS, consulte Editar padrões de metadados no Gerenciando seu Amazon S3 File Gateway.

Para SMB, você pode exportar um compartilhamento usando o Microsoft AD ou acesso de convidado para um bucket do Amazon S3 com objetos pré-existentes. Os objetos exportados por meio de um compartilhamento de arquivos SMB herdam a propriedade e as permissões de POSIX do diretório pai imediatamente acima deles. Para objetos na pasta raiz, listas de controle de acesso (ACL) raiz são herdadas. Para ACL raiz, o proprietário é `smbguest`, as permissões dos arquivos são 666 e os diretórios são 777. Isso se aplica a todas as formas de acesso autenticado (Microsoft AD e convidado)

Teste seu S3 File Gateway

Você pode copiar arquivos e pastas para sua unidade mapeada. O upload dos arquivos para seu bucket do Amazon S3 é feito automaticamente.

Para fazer upload de arquivos de um cliente Windows para o Amazon S3

1. No cliente Windows, navegue até a letra da unidade em que você montou o compartilhamento de arquivos. O nome da unidade é precedido pelo nome do bucket do S3.
2. Copie arquivos ou uma pasta para a unidade.
3. No console de gerenciamento do Amazon S3, navegue até o bucket mapeado. Você deve ver os arquivos e pastas que você copiou no bucket do Amazon S3 que especificou.

   Você pode ver o compartilhamento de arquivos que criou noCompartilhe arquivosGuiano noAWSConsole de gerenciamento de Storage Gateway.

Seu cliente NFS ou SMB pode gravar, ler, excluir, renomear e truncar arquivos.

> **Note**
>
> Os gateways de arquivos não são compatíveis com a criação de links físicos ou simbólicos em um compartilhamento de arquivos.

Lembre-se do seguinte ao trabalhar com gateways de arquivos S3:

- As leituras são atendidas por um cache de leitura. Em outras palavras, se os dados não estiverem disponíveis, serão extraídos do S3 e adicionados ao cache.
- As gravações são enviadas ao S3 por multipart uploads otimizados por meio de um cache de write-back.
- As leituras e gravações são otimizadas para que somente as partes solicitadas ou alteradas sejam transferidas pela rede.
- As exclusões removem os objetos do S3.
- Os diretórios são gerenciados como objetos de pasta no S3, usando a mesma sintaxe que o console do Amazon S3. Você pode renomear os diretórios vazios.
- O desempenho de operações recursivas do sistema de arquivos (por exemplo, `ls -l`) dependerá do número de objetos em seu bucket.

Próxima etapa

Para onde ir agora?

Para onde ir agora?

Nas seções anteriores, você criou e começou a usar um gateway de arquivos, incluindo a montagem de um compartilhamento de arquivos e testar sua configuração.

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

- Para gerenciar seu gateway de arquivos, consulte Gerenciando seu Amazon S3 File Gateway.
- Para otimizar seu gateway de arquivos, consulte Como otimizar o desempenho de um gateway.
- Para solucionar problemas de gateway (consulte Solução de problemas em seu gateway).
- Para saber mais sobre as métricas do Storage Gateway e saber como monitorar o desempenho do gateway (consulte).

Para limpar os recursos dos quais você 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. Se você não pretende continuar usando o gateway, exclua-o. Para obter mais informações, consulte Como excluir seu gateway usando o console do AWS Storage Gateway e como limpar os recursos associados.
2. Exclua a VM do Storage Gateway do host local. Se tiver criado seu gateway em uma Instância do Amazon EC2, encerre a instância.

Como ativar um gateway em uma nuvem privada virtual

É possível criar uma conexão privada entre o dispositivo de software local e a infraestrutura de armazenamento baseada em nuvem. Depois, você pode usar o dispositivo de software para transferir dados para oAWSarmazenamento sem que seu gateway se comunique comAWSServiços de armazenamento pela internet pública. Usando o serviço Amazon VPC, você pode iniciarAWSRecursos em uma rede virtual personalizada. É possível usar uma nuvem privada virtual (VPC) para controlar as configurações de rede, como o intervalo de endereços IP, sub-redes, tabelas de rotas e gateways de rede. Para obter mais informações sobre VPCs, consulteO que é Amazon VPC?noAmazon VPC User Guide.

Para usar um gateway com um VPC endpoint do Storage Gateway VPC, faça o seguinte:

- Use o console da VPC para criar um VPC endpoint para o Storage Gateway e obtenha o ID do VPC endpoint Especifique esse ID de endpoint da VPC ao criar e ativar o gateway.
- Se estiver ativando um gateway de arquivos, crie um VPC endpoint para o Amazon S3. Especifique esse endpoint da VPC ao criar compartilhamentos de arquivos para o gateway.
- Se estiver ativando um gateway de arquivos, instale um proxy HTTP e configure-o no console local da máquina virtual do gateway de arquivos. Você precisa desse proxy para gateways de arquivos no local baseados em hipervisor, como aqueles baseados em VMware, Microsoft HyperV e Linux Kernel-based Virtual Machine (KVM). Nesses casos, você precisa do proxy para habilitar seus endpoints privados do Amazon S3 de fora da VPC. Para obter informações sobre como configurar um proxy HTTP, consulte Configurar um proxy HTTP.

> **Note**
>
> Seu gateway deve estar ativado na mesma região em que o VPC endpoint foi criado. Para o gateway de arquivos, o armazenamento do Amazon S3 configurado para o compartilhamento de arquivos deve estar na mesma região em que você criou o VPC endpoint para o Amazon S3.

Tópicos

- Permitir tráfego para portas necessárias em seu proxy HTTP

Criar um VPC endpoint para o Storage Gateway

Siga estas instruções para criar um VPC endpoint. Se você já tiver um VPC endpoint para o Storage Gateway, poderá usá-lo.

Para criar um VPC endpoint para o Storage Gateway

1. Faça login no AWS Management Console e abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, selecione Endpoints (Endpoints) e Create Endpoint (Criar endpoint).
3. NoCriar endpointPágina, escolhaAWSServiçospeloCategoria 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 Create endpoint (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 seção DNS Names (Nomes DNS), use o primeiro nome DNS que não especifica 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.

> **Important**
>
> Se estiver criando um gateway de arquivos, você também precisará criar um endpoint para o Amazon S3. Siga as mesmas etapas exibidas na seção Para criar um VPC endpoint para o Storage Gateway acima, mas escolha`com.amazonaws.us-east-2.s3`em Nome do serviço em vez disso. Depois, selecione a tabela de rotas à qual você quer que o endpoint do S3 seja associado, em vez de sub-rede/grupo de segurança. Para obter instruções, consulteCriar um endpoint do gateway.

Configurando e configurando um proxy HTTP (somente gateways de arquivos locais)

Se estiver ativando um gateway de arquivos, você precisará instalar um proxy HTTP e configurá-lo no console local da máquina virtual do gateway de arquivos. Esse proxy é necessário para que o gateway de arquivos no local acesse endpoints privados do Amazon S3 de fora da VPC. Se você já tiver um proxy HTTP no Amazon EC2, poderá usá-lo. No entanto, é necessário verificar 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

Se você não tiver um proxy do Amazon EC2, use o procedimento a seguir para configurar um proxy HTTP.

Como configurar um servidor de proxy

1. Inicialize uma AMI Linux do Amazon EC2. Recomendamos usar uma família de instâncias que seja otimizada para rede, como c5n.large.

2. Use o comando a seguir para instalar o squid: **`sudo yum install squid`**. Isso cria um arquivo de configuração padrão no`/etc/squid/squid.conf`.
3. Substitua o conteúdo desse arquivo de configuração pelo seguinte:

```
#
# Recommended minimum configuration:
#

# Example rule allowing access from your local networks.
# Adapt to list your (internal) IP networks from where browsing
# should be allowed
acl localnet src 10.0.0.0/8             # RFC1918 possible internal network
acl localnet src 172.16.0.0/12       # RFC1918 possible internal network
acl localnet src 192.168.0.0/16    # RFC1918 possible internal network
acl localnet src fc00::/7       # RFC 4193 local private network range
acl localnet src fe80::/10      # RFC 4291 link-local (directly plugged) machines

acl SSL_ports port 443
acl SSL_ports port 1026
acl SSL_ports port 1027
acl SSL_ports port 1028
acl SSL_ports port 1031
acl SSL_ports port 2222
acl CONNECT method CONNECT

#
# Recommended minimum Access Permission configuration:
#
# Deny requests to certain unsafe ports
http_access deny !SSL_ports

# Deny CONNECT to other than secure SSL ports
http_access deny CONNECT !SSL_ports

# Only allow cachemgr access from localhost
http_access allow localhost manager
http_access deny manager

# Example rule allowing access from your local networks.
# Adapt localnet in the ACL section to list your (internal) IP networks
# from where browsing should be allowed
http_access allow localnet
http_access allow localhost
```

```
# And finally deny all other access to this proxy
http_access deny all

# Squid normally listens to port 3128
http_port 3128

# Leave coredumps in the first cache dir
coredump_dir /var/spool/squid

#
# Add any of your own refresh_pattern entries above these.
#
refresh_pattern ^ftp:                    1440       20%        10080
refresh_pattern ^gopher:            1440       0%          1440
refresh_pattern -i (/cgi-bin/|\?) 0             0%          0
refresh_pattern .                              0              20%        4320
```

4. Se você não precisar bloquear o servidor de proxy e não precisar fazer alterações, habilite-o e inicie-o usando os comandos a seguir. Estes comandos iniciarão o servidor na inicialização.

```
sudo chkconfig squid on
sudo service squid start
```

Agora, configure o proxy HTTP para o Storage Gateway para o usá-lo. Ao configurar o gateway para usar um proxy, use a porta padrão 3128 do Squid. O arquivo squid.conf que é gerado abrange as seguintes portas TCP necessárias por padrão:

- TCP 443
- TCP 1026
- TCP 1027
- TCP 1028
- TCP 1031
- TCP 2222

Como usar o console local da VM para configurar o proxy HTTP

1. Faça login no seu console local da VM do gateway: Para obter informações sobre como fazer login, consulte Como fazer login no console local do gateway de arquivo.

2. No menu principal, escolha Configure HTTP proxy (Configurar proxy HTTP).
3. No menu Configuration (Configuração), escolha Configure HTTP proxy (Configurar proxy HTTP).
4. Forneça o nome do host e a porta do servidor de proxy.

Para obter informações detalhadas sobre como configurar um proxy HTTP, consulte Configurar um proxy HTTP.

Permitir tráfego para portas necessárias em seu proxy HTTP

Se você usar um proxy HTTP, certifique-se de permitir tráfego do Storage Gateway para os destinos e as portas listados a seguir.

Quando o Storage Gateway se comunica por meio de endpoints públicos, ele se comunica com os seguintes serviços do Storage Gateway.

```
anon-cp.storagegateway.region.amazonaws.com:443
client-cp.storagegateway.region.amazonaws.com:443
proxy-app.storagegateway.region.amazonaws.com:443
dp-1.storagegateway.region.amazonaws.com:443
storagegateway.region.amazonaws.com:443 (Required for making API calls)
s3.region.amazonaws.com (Required only for File Gateway)
```

> **Important**
>
> Dependendo do gatewayAWSRegião, substitua*região*No endpoint com a string de região correspondente. Por exemplo, se você criar um gateway na região Oeste dos EUA (Oregon), o endpoint será semelhante ao seguinte:`storagegateway.us-west-2.amazonaws.com:443`.

Quando o Storage Gateway se comunica por meio do VPC endpoint, ele se comunica com oAWSServiços por meio de várias portas no VPC endpoint do Storage Gateway VPC e da porta 443 no endpoint privado do Amazon S3.

- Portas TCP no VPC endpoint do Storage Gateway.
  - 443, 1026, 1027, 1028, 1031 e 2222
- Porta TCP no endpoint privado do S3

- 443

Gerenciando seu Amazon S3 File Gateway

A seguir você pode encontrar informações sobre como gerenciar os recursos de seu Amazon S3 File Gateway.

Tópicos

Adicionar um compartilhamento de arquivos

Depois que o gateway de arquivos do S3 estiver ativado e em execução, você poderá adicionar outros compartilhamentos de arquivos e conceder acesso aos buckets do Amazon S3. Buckets que você pode conceder acesso para incluir os buckets em um diferenteConta da AWSDo que seu compartilhamento de arquivos. Para obter informações sobre como adicionar compartilhamento de arquivos, consulte Crie um compartilhamento de arquivos.

Tópicos

Como conceder acesso a um bucket do Amazon S3

Quando você cria um compartilhamento de arquivos, seu gateway de arquivos requer acesso para carregar arquivos no bucket do Amazon S3 e para executar ações em quaisquer pontos de acesso ou pontos de extremidade de nuvem privada virtual (VPC) usados para se conectar ao bucket. Para conceder esse acesso, seu gateway de arquivos assume umAWS Identity and Access Management(IAM) que está associada a uma política do IAM que concede esse acesso.

A função exige essa política do IAM e um relacionamento de confiança do serviço de token de segurança (STS) para ela. A política determina quais ações a função pode realizar. Além disso, o bucket do S3 e todos os pontos de acesso ou pontos de acesso associados devem ter uma política de acesso que permita que a função do IAM os acesse.

Você pode criar a função e a política de acesso sozinho, ou o gateway de arquivos pode criá-las para você. Se o gateway de arquivos criar a política para você, ela terá uma lista de ações do S3. Para obter informações sobre funções e permissões, consulteCriar uma função para delegar permissões a umAWS service (Serviço da AWS)noIAM User Guide.

A política de confiança do exemplo a seguir permite que o gateway de arquivos assuma uma função do IAM.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "storagegateway.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Se você não quiser que o gateway de arquivos crie uma política em seu nome, crie sua própria política e anexe-a ao compartilhamento de arquivos. Para obter mais informações sobre como fazer isso, consulte Crie um compartilhamento de arquivos.

A política de exemplo a seguir permite que o gateway de arquivos realize todas as ações do Amazon S3 listadas na política. A primeira parte da declaração permite que todas as ações listadas sejam

executadas no bucket do S3 chamado `TestBucket`. A segunda parte permite as ações listadas em todos os objetos no `TestBucket`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:GetAccelerateConfiguration",
                "s3:GetBucketLocation",
                "s3:GetBucketVersioning",
                "s3:ListBucket",
                "s3:ListBucketVersions",
                "s3:ListBucketMultipartUploads"
            ],
            "Resource": "arn:aws:s3:::TestBucket",
            "Effect": "Allow"
        },
        {
            "Action": [
                "s3:AbortMultipartUpload",
                "s3:DeleteObject",
                "s3:DeleteObjectVersion",
                "s3:GetObject",
                "s3:GetObjectAcl",
                "s3:GetObjectVersion",
                "s3:ListMultipartUploadParts",
                "s3:PutObject",
                "s3:PutObjectAcl"
            ],
            "Resource": "arn:aws:s3:::TestBucket/*",
            "Effect": "Allow"
        }
    ]
}
```

A política de exemplo a seguir é semelhante à anterior, mas permite que o gateway de arquivos execute ações necessárias para acessar um bucket por meio de um ponto de acesso.

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

```
            "Action": [
                "s3:AbortMultipartUpload",
                "s3:DeleteObject",
                "s3:DeleteObjectVersion",
                "s3:GetObject",
                "s3:GetObjectAcl",
                "s3:GetObjectVersion",
                "s3:ListMultipartUploadParts",
                "s3:PutObject",
                "s3:PutObjectAcl"
            ],
            "Resource": "arn:aws:s3:us-east-1:123456789:accesspoint/
TestAccessPointName/*",
            "Effect": "Allow"
        }
    ]
}
```

> **Note**
>
> Se você precisar conectar o compartilhamento de arquivos a um bucket do S3 por meio de um endpoint VPC, consultePolíticas de endpoint para o Amazon S3noAWS PrivateLinkGuia do usuário do.

Prevenção contra o ataque “Confused deputy” em todos os serviços

O problema confused deputy é um problema de segurança em que uma entidade que não tem permissão para executar uma ação pode coagir uma entidade mais privilegiada a executá-la. Na AWS, a personificação entre serviços pode resultar no problema do confused deputy. A personificação nos serviços pode ocorrer quando um serviço (o serviço de chamada) chama outro serviço (o serviço chamado). O serviço de chamada pode ser manipulado de modo a usar suas permissões para atuar nos recursos de outro cliente de uma forma na qual ele não deveria ter permissão para acessar. Para evitar isso, a AWS fornece ferramentas que ajudam você a proteger seus dados para todos os serviços com entidades principais de serviço que receberam acesso aos recursos em sua conta.

Recomendamos o uso das chaves de contexto de condição global `aws:SourceArn` e `aws:SourceAccount` em políticas de recursos para limitar as permissões que o AWS Storage Gateway concede a outro serviço para o recurso. Se você utilizar ambas as chaves de contexto de

condição global, o valor `aws:SourceAccount` e a conta no valor `aws:SourceArn` deverão utilizar o mesmo ID de conta quando utilizados na mesma instrução de política.

O valor de`aws:SourceArn`deve ser o ARN do Storage Gateway ao qual o compartilhamento de arquivos está associado.

A maneira mais eficaz de se proteger contra o problema confuso do deputado é usar o`aws:SourceArn`chave de contexto de condição global com o ARN completo do recurso. Se você não souber o ARN completo do recurso ou se você estiver especificando vários recursos, use o ARN completo do recurso`aws:SourceArn`chave de condição de contexto global com curingas (*) para as partes desconhecidas do ARN. Por exemplo, `arn:aws:`*`servicename`*`::`*`123456789012`*`:*`.

O exemplo a seguir mostra como você pode usar o`aws:SourceArn`e`aws:SourceAccount`chaves de contexto de condição global no Storage Gateway para evitar o problema confuso do deputado.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "ConfusedDeputyPreventionExamplePolicy",
      "Effect": "Allow",
      "Principal": {
        "Service": "storagegateway.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "123456789012"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:storagegateway:us-east-1:123456789012:gateway/
sgw-712345DA"
        }
      }
    }
  ]
}
```

Uso de um compartilhamento de arquivos para acesso entre contas

Conta entreAcesso é quando uma conta da Amazon Web Services e os usuários dela recebem acesso a recursos que pertencem a outra conta da Amazon Web Services. Com os gateways de arquivos, você pode usar um compartilhamento de arquivos em uma conta da Amazon Web Services

para acessar objetos em um bucket do Amazon S3 que pertence a outra conta da Amazon Web Services.

Para usar um compartilhamento de arquivos de propriedade de uma conta da Amazon Web Services para acessar um bucket do S3 em outra conta da Amazon Web Services

1. Verifique se o proprietário do bucket do S3 concedeu à conta da Amazon Web Services acesso ao bucket do S3 que você precisa acessar e aos objetos desse bucket. Para obter informações sobre como conceder esse acesso, consulteExemplo 2: Proprietário do bucket concedendo permissões de bucket entrenoGuia do usuário do Amazon Simple Storage Service. Para obter uma lista das permissões necessárias, consulte Como conceder acesso a um bucket do Amazon S3.
2. Verifique se a função do IAM usada por seu compartilhamento de arquivos para acessar o bucket do S3 inclui as permissões de operações como `s3:GetObjectAcl` e `s3:PutObjectAcl`. Além disso, certifique-se de que a função do IAM inclui uma política de confiança que permite que a sua conta assuma essa função do IAM. Para um exemplo de uma política de confiança desse tipo, consulte Como conceder acesso a um bucket do Amazon S3.

   Se seu compartilhamento de arquivo usar uma função existente para acessar o bucket do S3, você deve incluir permissões para operações `s3:GetObjectAcl` e `s3:PutObjectAcl`. Uma função também precisa de uma política de confiança que permita à sua conta assumir essa função. Para um exemplo de uma política de confiança desse tipo, consulte Como conceder acesso a um bucket do Amazon S3.
3. Abra o console do Storage Gatewayhttps://console.aws.amazon.com/storagegateway/home.
4. Escolha Give bucket owner full control (Conceder controle total ao proprietário do bucket) nas configurações de Object metadata (Metadados do objeto) da caixa de diálogo Configure file share setting (Definir configurações de compartilhamento de arquivos).

Após criar ou atualizar seu compartilhamento de arquivos para acesso entre contas e montá-lo no local, é altamente recomendável testar sua configuração. Isso pode ser feito indicando o conteúdo do diretório ou gravando arquivos de teste e garantindo que os arquivos sejam exibidos como objetos no bucket do S3.

> **Important**
>
> Certifique-se de configurar as políticas corretamente para conceder o acesso entre contas para a conta usada por seu compartilhamento de arquivos. Se não fizer isso, as atualizações

nos arquivos por meio de aplicativos locais não serão propagadas para o bucket do Amazon S3 com o qual você está trabalhando.

Recursos

Para obter mais informações sobre políticas de acesso e listas de controle de acesso, consulte:

Diretrizes para usar as opções disponíveis de política de acessonoGuia do usuário do Amazon Simple Storage Service

Visão geral da Lista de controle de acesso (ACL)noGuia do usuário do Amazon Simple Storage Service

Excluir um compartilhamento de arquivos

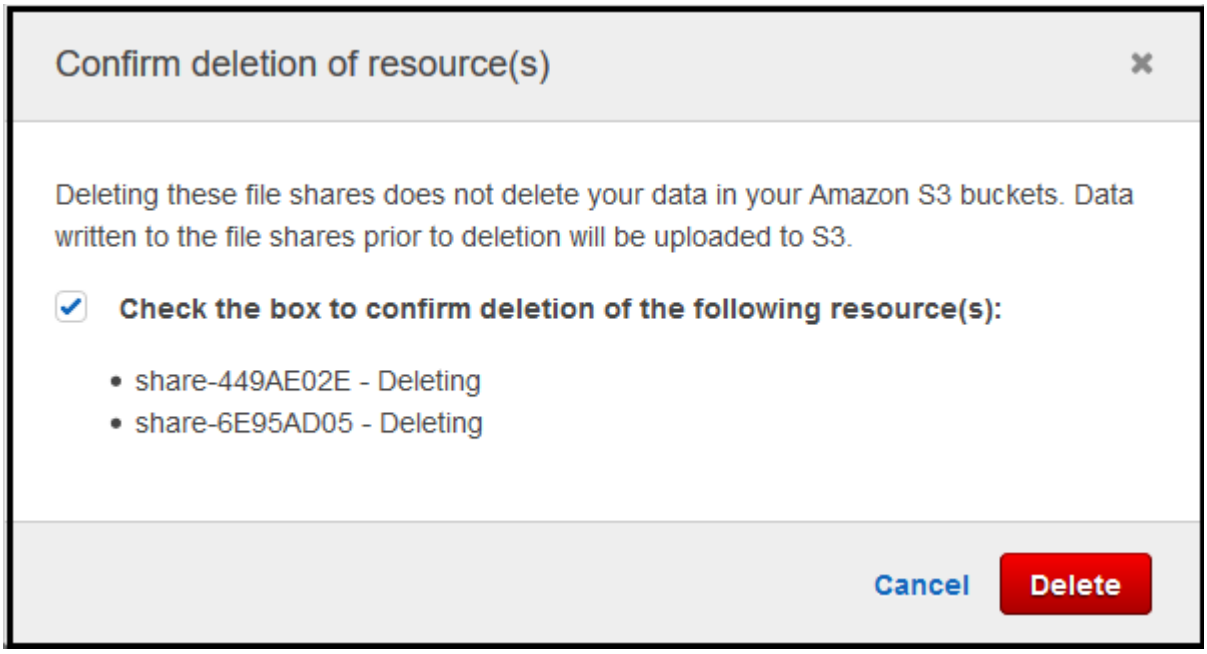
Se você não precisar mais de um compartilhamento de arquivos, poderá excluí-lo por meio do Console do Storage Gateway. Ao excluir um compartilhamento de arquivos, o gateway é desanexado do bucket do Amazon S3 ao qual o compartilhamento de arquivos é mapeado. No entanto, o bucket do S3 e seu conteúdo não são excluídos.

Se seu gateway estiver fazendo upload de dados para um bucket do S3 ao excluir um compartilhamento de arquivos, o processo será concluído somente quando todos os dados tiverem sido carregados. Ele permanecerá no status DELETING até os dados serem completamente carregados.

Se você desejar que seus dados sejam totalmente carregados, use o procedimento Para excluir um compartilhamento de arquivos a seguir. Se você não quiser esperar até que os dados sejam totalmente carregados, consulte o procedimento Para excluir à força um compartilhamento de arquivos posteriormente neste tópico.

Para excluir um compartilhamento de arquivos

1. Abra o console do Storage Gatewayhttps://console.aws.amazon.com/storagegateway/home.
2. Escolha File shares (Compartilhamentos de arquivo) e, em seguida, o compartilhamento de arquivos que você deseja excluir.
3. Para Actions, escolha Delete file share. A caixa de diálogo de confirmação a seguir será exibida.



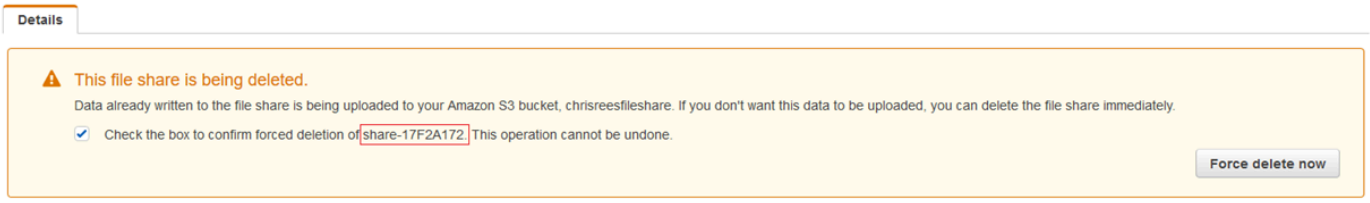
4. Na caixa de diálogo de confirmação, marque a caixa de seleção para o compartilhamento de arquivos ou compartilhamentos que você deseja excluir. Em seguida, escolha Delete.

Em alguns casos, talvez você queira excluir o compartilhamento de arquivos antes que todos os dados gravados em arquivos no compartilhamento de arquivos do NFS (Sistema de arquivos em rede) sejam carregados. Por exemplo, talvez você tenha a intenção de descartar os dados que foram gravados, mas que ainda não foram carregados. Em outro exemplo, o bucket do Amazon S3 ou objetos que revertem o compartilhamento de arquivos podem ter sido excluídos. Isso significa que não é mais possível fazer o carregamento de dados especificados.

Nesses casos, você pode excluir o compartilhamento de arquivos à força usando oAWS Management Consoleou o`DeleteFileShare`Operação da API. Essa operação aborta o processo de carregamento de dados. Quando fizer isso, o compartilhamento de arquivos entrará no status FORCE_DELETING. Para excluir à força um compartilhamento de arquivos do console, consulte o procedimento a seguir.

Para excluir à força um compartilhamento de arquivos

1. Abra o console do Storage Gatewayhttps://console.aws.amazon.com/storagegateway/home.
2. Escolha File shares (Compartilhamentos de arquivos), escolha o compartilhamento de arquivos que você deseja excluir à força e aguarde alguns segundos. A mensagem de exclusão é exibida na guia Detalhes.



> **Note**
>
> Você não pode desfazer a operação de exclusão à força.

3. Na mensagem que aparece na guia Details (Detalhes), verifique o ID do compartilhamento de arquivos que você deseja excluir à força, selecione a caixa de confirmação e escolha Force delete now (Forçar exclusão agora).

Também é possível usar a operação de API DeleteFileShare para excluir à força o compartilhamento de arquivos.

Editar definições para o compartilhamento de arquivos NFS

Você pode editar a classe de armazenamento do bucket do Amazon S3, nome do compartilhamento de arquivos, metadados de objeto, nível de squash, exportação como e configurações de atualização automatizada de cache.

> **Note**
>
> Não é possível editar um compartilhamento de arquivos existente para apontar para um novo bucket ou ponto de acesso, ou para modificar as configurações de endpoint da VPC. Você pode definir essas configurações somente ao criar um novo compartilhamento de arquivos.

Para editar as configurações de compartilhamento de arquivos

1. Abra o console do Storage Gatewayhttps://console.aws.amazon.com/storagegateway/home.
2. Escolha File shares e, em seguida, o compartilhamento de arquivos que deseja atualizar.
3. para oAções, escolhaEditar configurações do compartilhamento.
4. Faça uma ou mais das coisas a seguir:

- (Opcional) ParaNome do compartilhamento de arquivos, insira um novo nome para o compartilhamento de arquivos.
- Em Audit logs (Logs de auditoria), escolha uma das seguintes opções:
  - SelecioneDisable logging (Desativar o registro em log).Para desativar o registro.
  - SelecioneCriar um novo grupo de logsPara criar um novo log de auditoria.
  - SelecioneUsar um grupo de logs existenteE, em seguida, selecione um log de auditoria existente na lista.

  Para obter mais informações sobre logs de auditoria, consulte Noções básicas sobre registros de auditoria do gateway.
- (Opcional) ParaAtualização automatizada de cache do S3, marque a caixa de seleção e defina a hora em dias, horas e minutos para atualizar o cache do compartilhamento de arquivos usando Time To Live (TTL). TTL é o período de tempo desde a última atualização. Após o intervalo TTL ter decorrido, acessar o diretório faz com que o gateway de arquivos atualize primeiro o conteúdo desse diretório a partir do bucket do Amazon S3.
- (Opcional) ParaNotificação de upload de arquivos, escolha a caixa de seleção a ser notificada quando um arquivo tiver sido totalmente carregado para o S3 pelo S3 File Gateway. DefinaTempo de liquidaçãoem segundos para controlar o número de segundos a aguardar após o último ponto no tempo que um cliente escreveu em um arquivo antes de gerar um`ObjectUploaded`Notificações. Como os clientes podem fazer muitas gravações pequenas em arquivos, é melhor definir esse parâmetro pelo maior tempo possível para evitar gerar várias notificações para o mesmo arquivo em um pequeno período de tempo. Para obter mais informações, consulte Obtendo notificação de upload de arquivos.

  > **Note**
  >
  > Essa configuração não tem efeito sobre o tempo do upload do objeto para o S3, somente no tempo da notificação.

- para oClasse de armazenamento para novos objetos, escolha uma classe de armazenamento para usar para novos objetos criados no bucket do Amazon S3:
  - Selecione S3 Standard para armazenar seus dados de objetos acessados com frequência de forma redundante em várias zonas de disponibilidade separadas geograficamente. Para obter mais informações sobre a classe de armazenamento S3 Standard, consulteClasses

de armazenamento de objetos acessados com frequêncianoGuia do usuário do Amazon Simple Storage Service.

- Escolha S3 Intelligent-Tiering para otimizar os custos de armazenamento movendo automaticamente os dados para o nível de acesso de armazenamento mais econômico. Para obter mais informações sobre a classe de armazenamento S3 Intelligent-Tiering, consulteClasse de armazenamento que otimiza automaticamente objetos muito e pouco acessadosnoGuia do usuário do Amazon Simple Storage Service.
- Selecione S3 Standard-IA para armazenar seus dados de objetos raramente acessados de forma redundante em várias zonas de disponibilidade separadas geograficamente. Para obter mais informações sobre a classe de armazenamento S3 Standard — IA, consulteClasses de armazenamento de objetos acessados com pouca frequêncianoGuia do usuário do Amazon Simple Storage Service.
- Selecione S3 One Zone-IA para armazenar seus dados de objetos raramente acessados em uma única zona de disponibilidade. Para obter mais informações sobre a classe de armazenamento S3 One Zone — IA, consulteClasses de armazenamento de objetos acessados com pouca frequêncianoGuia do usuário do Amazon Simple Storage Service.

- Em Object metadata (Metadados do objeto), escolha os metadados que você deseja usar:
  - Escolha a opção Guess MIME type para habilitar a adivinhação do tipo MIME dos objetos enviados com base nas extensões de arquivo.
  - Escolha Give bucket owner full control (Conceder controle total ao proprietário do bucket) para conceder controle total ao proprietário do bucket do S3 que está mapeado no compartilhamento Network File System (NFS) ou Server Message Block (SMB) do arquivo. Para obter mais informações sobre como usar seu compartilhamento de arquivos para acessar objetos em um bucket de propriedade de outra conta, consulte Uso de um compartilhamento de arquivos para acesso entre contas.
  - Escolha Enable requester pays (Habilitar o Pagamento pelo solicitante) se você estiver usando esse compartilhamento de arquivos em um bucket que requer que o solicitante ou o leitor, em vez do proprietário dele, pague pelas cobranças de acesso. Para obter mais informações, consulte Buckets de pagamento pelo solicitante.
- Em Squash level (Nível de compressão), escolha a configuração do nível de compressão que deseja para o compartilhamento de arquivos NFS e, em seguida, escolha Save (Salvar).

> **Note**
>
> Você pode escolher uma configuração do nível de compressão apenas para compartilhamentos de arquivos NFS. Compartilhamentos de arquivos SMB não usam configurações de compressão.

Os valores possíveis são os seguintes:

- Root squash (default) – O acesso para o superusuário remoto (raiz) é mapeado para o UID (65534) e o GID (65534).
- No root squash – O superusuário remoto (raiz) recebe acesso como raiz.
- All squash – Todo o acesso do usuário é mapeado para o UID (65534) e o GID (65534).

O valor padrão para o nível de compressão é Root squash.

- para oExportar como, escolha uma opção para o compartilhamento de arquivos. O valor padrão é Read-write.

> **Note**
>
> Para compartilhamentos de arquivos montados em um cliente Microsoft Windows, se você selecionar Read-only (Somente leitura) para Export as (Exportar como), provavelmente verá uma mensagem de erro. Ela indica que um erro inesperado está impedindo que você crie a pasta. Esse é um problema conhecido no NFS versão 3. Você pode ignorar a mensagem.

5. Escolha Save (Salvar).

Edição de padrões de metadados para seu compartilhamento de arquivos NFS

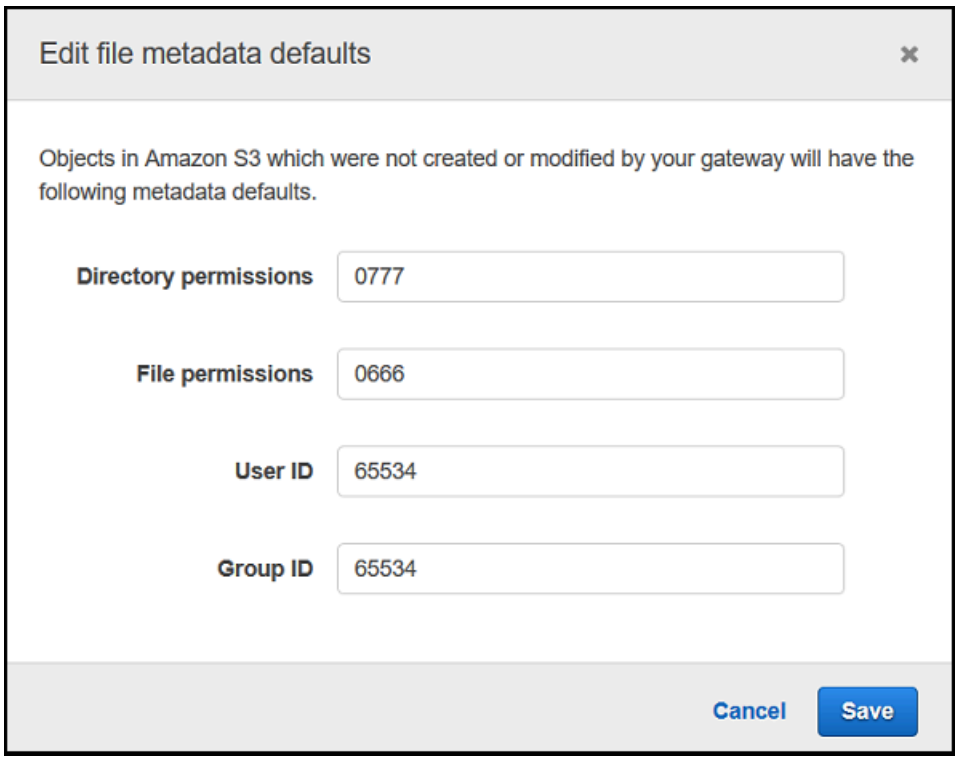
Se você não definir valores de metadados para arquivos ou diretórios no bucket do, o gateway de arquivos do S3 definirá valores de metadados padrão. Esses valores incluem permissões Unix para arquivos e pastas. Você pode editar os padrões de metadados no console do Storage Gateway.

Quando o S3 File Gateway armazena arquivos e pastas no Amazon S3, as permissões de arquivo Unix são armazenadas em metadados de objeto. Quando o gateway de arquivos do S3 descobre objetos que não foram armazenados pelo gateway de arquivos do S3, esses objetos recebem permissões de arquivo Unix padrão. A tabela a seguir descreve as permissões padrão do Unix.

Metadados	Descrição
Permissões de diretório	Modo de diretório do Unix no formato "nnnn". Por exemplo, "0666" representa o modo de acesso para todos os diretórios dentro do compartilhamento de arquivos. O valor padrão é 0777.
Permissões de arquivo	Modo de arquivo do Unix no formato "nnnn". Por exemplo, "0666" representa o modo de arquivo para todos os diretórios dentro do compartilhamento de arquivos. O valor padrão é 0666.
ID de usuário	ID de proprietário padrão de arquivos no compartilhamento de arquivos. O valor padrão é 65534.
ID do grupo	ID de grupo padrão de arquivos no compartil hamento de arquivos. O valor padrão é 65534.

Para editar padrões de metadados

1. Abra o console do Storage Gatewayhttps://console.aws.amazon.com/storagegateway/home.
2. Escolha File shares e, em seguida, o compartilhamento de arquivos que deseja atualizar.
3. Em Actions, escolha Edit file metadata defaults.
4. Na caixa de diálogo Edit file metadata defaults, forneça as informações de metadados e escolha Save.



Edição de configurações de acesso ao compartilhamento de arquivos NFS

Recomendamos alterar as configurações de clientes NFS permitidos de seu compartilhamento de arquivos NFS. Se você não alterar, qualquer cliente em sua rede poderá acessar seu compartilhamento de arquivos.

Para editar as configurações de acesso do NFS

1. Abra o console do Storage Gatewayhttps://console.aws.amazon.com/storagegateway/home.
2. Escolha File shares (Compartilhamentos de arquivo) e, em seguida, o compartilhamento de arquivos NFS que deseja editar.
3. Em Actions (Ações), escolha Edit share access settings (Editar configurações de acesso de compartilhamento).
4. NoEditar clientes permitidos, escolhaAdicionar entrada, forneça o endereço IP ou a notação CIDR para os clientes que você deseja permitir e escolhaSalvar.

Editando configurações SMB para um gateway

As configurações SMB no nível do gateway permitem configurar a estratégia de segurança, autenticação do Active Directory, acesso de convidado, permissões de grupo local e visibilidade de compartilhamento de arquivos para compartilhamentos de arquivos SMB em um gateway.

Para editar as configurações SMB de nível de gateway

1. Abra o console do Storage Gatewayhttps://console.aws.amazon.com/storagegateway/home.
2. SelecioneGateways doEm seguida, escolha o gateway para o qual você deseja editar as configurações de SMB.
3. DoAçõesMenu suspenso, escolhaEditar configurações SMBEm seguida, escolha as configurações que deseja editar.

Consulte os tópicos a seguir para obter mais informações.

Tópicos

- Definindo um nível de segurança para seu gateway
- Usar o Active Directory para autenticar usuários
- Fornecer acesso de convidado ao compartilhamento de arquivos
- Configurar grupos locais para seu gateway
- Configuração da visibilidade do compartilhamento de arquivos

Definindo um nível de segurança para seu gateway

Usando um gateway de arquivos do S3, você pode especificar um nível de segurança para seu gateway. Ao especificar esse nível de segurança, é possível definir se o seu gateway exigirá uma assinatura SMB ou criptografia SMB, ou se você gostaria de habilitar a versão do SMB.

Para configurar os níveis segurança

1. Abra o console do Storage Gatewayhttps://console.aws.amazon.com/storagegateway/home.
2. SelecioneGateways doEm seguida, escolha o gateway para o qual você deseja editar as configurações de SMB.
3. DoAçõesMenu suspenso, escolhaEditar configurações SMBe, depois, escolhaConfigurações de segurança SMB.

4. Em Security level (Nível de segurança), escolha uma das seguintes opções:

> **Note**
>
> Essa configuração é chamada de `SMBSecurityStrategy` na Referência de API. Um nível de segurança mais alto pode afetar o desempenho.

- Impor criptografia— Se você escolher essa opção, o gateway de arquivos do S3 permitirá somente conexões de clientes SMBv3 que tiverem a criptografia habilitada. Essa opção é altamente recomendada para ambientes que trabalham com dados confidenciais. Essa opção funciona com clientes SMB no Microsoft Windows 8, Windows Server 2012 ou mais recentes.
- Impor assinatura— Se você escolher essa opção, o gateway de arquivos do S3 permitirá somente conexões de clientes SMBv2 ou SMBv3 que tiverem a assinatura habilitada. Essa opção funciona com clientes SMB no Microsoft Windows Vista, Windows Server 2008, ou mais recentes.
- Cliente negociado— Se você escolher essa opção, as solicitações serão estabelecidas com base no que for negociado pelo cliente. Essa opção é recomendada quando você quer maximizar a compatibilidade entre diferentes clientes em seu ambiente.

> **Note**
>
> Para gateways ativados antes de 20 de junho de 2019, o nível de segurança padrão é Client negotiated (Negociado pelo cliente).
> Para gateways ativados a partir de 20 de junho de 2019, o nível de segurança padrão é Enforce encryption (Exigir criptografia).

5. Escolha Save (Salvar).

Usar o Active Directory para autenticar usuários

Para usar seu Active Directory corporativo para acesso autenticado de usuário para seu compartilhamento de arquivo SMB, edite as configurações de SMB para seu gateway com suas credenciais de domínio do Microsoft AD. Isso permite que seu gateway ingresse no domínio de seu Active Directory e permite que os membros do domínio acessem o arquivo de compartilhamento SMB.

> **Note**
>
> O uso doAWS Directory Service, você pode criar um serviço de domínio do Active Directory hospedado noNuvem AWS.

Qualquer pessoa que pode fornecer a senha correta obtém acesso de convidado ao arquivo de compartilhamento SMB.

Você também pode habilitar listas de controle de acesso (ACLs) em seu compartilhamento de arquivos SMB. Para obter informações sobre como habilitar as ACLs, consulte Usar as ACLs do Microsoft Windows para controlar o acesso a um compartilhamento de arquivos SMB.

Para habilitar autenticação do Active Directory

1. Abra o console do Storage Gatewayhttps://console.aws.amazon.com/storagegateway/home.
2. SelecioneGateways doEm seguida, escolha o gateway para o qual você deseja editar as configurações de SMB.
3. DoAçõesMenu suspenso, escolhaEditar configurações SMBe, depois, escolhaConfigurações do Active Directory.
4. Para Domain name (Nome de domínio), forneça o domínio onde você queira que o gateway participe. Você pode ingressar em um domínio usando seu endereço IP ou a unidade organizacional. Uma unidade organizacional é uma subdivisão do Active Directory que pode conter usuários, grupos, computadores e outras unidades organizacionais.

   > **Note**
   >
   > Se seu gateway não conseguir entrar em um diretório do Active Directory, tente ingressar com o endereço IP do diretório usando a operação de API JoinDomain.

   > **Note**
   >
   > Active Directory status (Status do Active Directory) mostra Detached (Desanexado) quando um gateway nunca ingressou em um domínio.

5. Forneça o usuário do domínio e a senha do domínio e, em seguida, escolha Save (Salvar).

Uma mensagem na parte superior da seção Gateways do seu console indica que seu gateway foi associado com êxito ao seu domínio do AD.

Para limitar o acesso ao compartilhamento de arquivos específicos de usuários e grupos do AD

1. No console do Storage Gateway, escolha o compartilhamento de arquivos do qual você deseja limitar o acesso.
2. DoAçõesmenu suspenso, escolhaEditar configurações de acesso ao compartilhamento de arquivos.
3. NoAcesso ao compartilhamento de arquivos de usuário e grupoSeção, escolha suas configurações.

   para oUsuários e grupos permitidos, escolhaAdicionar usuário permitidoouAdicionar grupo permitidoE insira um usuário ou grupo do AD que pode permitir o acesso ao compartilhamento de arquivos. Repita esse processo para permitir quantos usuários e grupos forem necessários.

   para oUsuários e grupos negados, escolhaAdicionar usuário negadoouAdicionar grupo negadoE insira um usuário ou grupo do AD que deve negar o acesso ao compartilhamento de arquivos. Repita esse processo para negar quantos usuários e grupos forem necessários.

   > **Note**
   >
   > OAcesso ao compartilhamento de arquivos de usuário e grupoa seção aparece somente seActive DirectoryEstá selecionado.
   > Insira somente o nome do usuário ou grupo do AD. O nome de domínio é inferido pela associação do gateway no AD específico no qual o gateway ingressou.
   > Se você não especificar usuários ou grupos permitidos ou negados, qualquer usuário do AD autenticado poderá exportar o compartilhamento de arquivos.

4. Quando terminar de adicionar as entradas, escolha Save (Salvar).

Fornecer acesso de convidado ao compartilhamento de arquivos

Se você deseja fornecer somente acesso de convidado, o gateway de arquivos do S3 não precisa ser parte de um domínio do Microsoft AD. Você também pode usar um gateway de arquivos do S3 que é um membro de um domínio do AD para criar compartilhamentos de arquivos com acesso

de convidado. Antes de criar um compartilhamento de arquivos usando o acesso de convidado, é preciso alterar a senha padrão.

Para alterar a senha de acesso convidado

1. Abra o console do Storage Gatewayhttps://console.aws.amazon.com/storagegateway/home.
2. SelecioneGateways doEm seguida, escolha o gateway para o qual você deseja editar as configurações de SMB.
3. DoAçõesmenu suspenso, escolhaEditar configurações SMBe, depois, escolhaConfigurações de acesso de convidados.
4. para oSenha de convidados, forneça uma senha e, em seguida, escolhaSalvar.

Configurar grupos locais para seu gateway

As configurações do Grupo Local permitem que você conceda aos usuários ou grupos do Active Directory permissões especiais para os compartilhamentos de arquivos SMB no gateway.

Você pode usar as configurações do Grupo local para atribuir permissões de administrador do gateway. Os administradores do gateway podem usar o snap-in do Console de Gerenciamento Microsoft de Pastas Compartilhadas para forçar o fechamento de arquivos que estão abertos e bloqueados.

> **Note**
>
> Você deve adicionar pelo menos um usuário ou grupo Administrador do Gateway antes de poder ingressar no gateway a um domínio do Active Directory.

Para atribuir administradores de gateway

1. Abra o console do Storage Gatewayhttps://console.aws.amazon.com/storagegateway/home.
2. SelecioneGateways doEm seguida, escolha o gateway para o qual você deseja editar as configurações de SMB.
3. DoAçõesMenu suspenso, escolhaEditar configurações SMBe, depois, escolhaConfigurações do Grupo Local.
4. NoConfigurações do Grupo LocalSeção, escolha suas configurações. Esta seção aparece somente para compartilhamentos de arquivos que usam o Active Directory.

para oAdministradores do gateway, adicione usuários e grupos do Active Directory que você deseja conceder permissões de Administrador do Gateway local. Adicione um usuário ou grupo por linha, incluindo o nome de domínio. Por exemplo, **`corp\Domain Admins`**. Para criar linhas adicionais, escolhaAdicionar novo administrador do gateway.

> **Note**
>
> Editando Gateway Admins desconecta e reconecta todos os compartilhamentos de arquivos SMB.

5. SelecioneSalve as alteraçõese, depois, escolhaProsseguirpara confirmar a mensagem de aviso exibida.

Configuração da visibilidade do compartilhamento de arquivos

A visibilidade do compartilhamento de arquivos controla se os compartilhamentos em um gateway estão visíveis ao listar compartilhamentos aos usuários.

Para definir a visibilidade do compartilhamento de arquivos

1. Abra o console do Storage Gatewayhttps://console.aws.amazon.com/storagegateway/home.
2. SelecioneGateways doEm seguida, escolha o gateway para o qual você deseja editar as configurações de SMB.
3. DoAçõesmenu suspenso, escolhaEditar configurações SMBe, depois, escolhaConfigurações de visibilidade do compartilhamento de arquivos.
4. para oStatus de visibilidade, marque a caixa de seleção para que os compartilhamentos neste gateway apareçam ao listar compartilhamentos aos usuários. Mantenha a caixa de seleção desmarcada para que os compartilhamentos neste gateway não apareçam ao listar compartilhamentos aos usuários.

Editar definições para o compartilhamento de arquivos SMB

Depois de criar um compartilhamento de arquivos SMB, você pode editar a classe de armazenamento do bucket do Amazon S3, metadados de objeto, sensibilidade entre maiúsculas e minúsculas, enumeração baseada em acesso, logs de auditoria, atualização automatizada de cache e as configurações de exportação como para o compartilhamento de arquivos.

> **Note**
>
> Não é possível editar um compartilhamento de arquivos existente para apontar para um novo bucket ou ponto de acesso, ou para modificar as configurações de endpoint da VPC. Você pode definir essas configurações somente ao criar um novo compartilhamento de arquivos.

Como editar as configurações de compartilhamento de arquivos SMB

1. Abra o console do Storage Gatewayhttps://console.aws.amazon.com/storagegateway/home.
2. Escolha File shares e, em seguida, o compartilhamento de arquivos que deseja atualizar.
3. para oAções, escolhaEditar configurações do compartilhamento.
4. Faça uma ou mais das coisas a seguir:

   - (Opcional) ParaNome do compartilhamento de arquivos, insira um novo nome para o compartilhamento de arquivos.
   - Em Audit logs (Logs de auditoria), escolha uma das seguintes opções:
     - SelecioneDisable logging (Desativar o registro em log).Para desativar o registro.
     - SelecioneCriar um novo grupo de logsPara criar um novo log de auditoria.
     - SelecioneUsar um grupo de logs existenteE, em seguida, selecione um log de auditoria existente na lista.

     Para obter mais informações sobre logs de auditoria, consulte Noções básicas sobre registros de auditoria do gateway.
   - (Opcional) ParaAtualização automatizada de cache do S3 após, marque a caixa de seleção e defina a hora em dias, horas e minutos para atualizar o cache do compartilhamento de arquivos usando Time To Live (TTL). TTL é o período de tempo desde a última atualização. Após o intervalo TTL ter decorrido, acessar o diretório faz com que o gateway de arquivos atualize primeiro o conteúdo desse diretório a partir do bucket do Amazon S3.
   - (Opcional) ParaNotificação de upload de arquivos, escolha a caixa de seleção a ser notificada quando um arquivo tiver sido totalmente carregado para o S3 pelo S3 File Gateway. DefinaTempo de liquidaçãoem segundos para controlar o número de segundos a aguardar após o último ponto no tempo que um cliente escreveu em um arquivo antes de gerar um`ObjectUploaded`Notificações. Como os clientes podem fazer muitas gravações pequenas em arquivos, é melhor definir esse parâmetro pelo maior tempo possível para evitar

gerar várias notificações para o mesmo arquivo em um pequeno período de tempo. Para obter mais informações, consulte Obtendo notificação de upload de arquivos.

> **Note**
>
> Essa configuração não tem efeito sobre o tempo do upload do objeto para o S3, somente no tempo da notificação.

- para oClasse de armazenamento para novos objetos, escolha uma classe de armazenamento para usar para novos objetos criados no bucket do Amazon S3:
  - Selecione S3 Standard para armazenar seus dados de objetos acessados com frequência de forma redundante em várias zonas de disponibilidade separadas geograficamente. Para obter mais informações sobre a classe de armazenamento S3 Standard, consulteClasses de armazenamento de objetos acessados com frequêncianoGuia do usuário do Amazon Simple Storage Service.
  - Escolha S3 Intelligent-Tiering para otimizar os custos de armazenamento movendo automaticamente os dados para o nível de acesso de armazenamento mais econômico. Para obter mais informações sobre a classe de armazenamento S3 Intelligent-Tiering, consulteClasse de armazenamento que otimiza automaticamente objetos muito e pouco acessadosnoGuia do usuário do Amazon Simple Storage Service.
  - Selecione S3 Standard-IA para armazenar seus dados de objetos raramente acessados de forma redundante em várias zonas de disponibilidade separadas geograficamente. Para obter mais informações sobre a classe de armazenamento S3 Standard — IA, consulteClasses de armazenamento de objetos acessados com pouca frequêncianoGuia do usuário do Amazon Simple Storage Service.
  - Selecione S3 One Zone-IA para armazenar seus dados de objetos raramente acessados em uma única zona de disponibilidade. Para obter mais informações sobre a classe de armazenamento S3 One Zone — IA, consulteClasses de armazenamento de objetos acessados com pouca frequêncianoGuia do usuário do Amazon Simple Storage Service.
- Em Object metadata (Metadados do objeto), escolha os metadados que você deseja usar:
  - Escolha a opção Guess MIME type para habilitar a adivinhação do tipo MIME dos objetos enviados com base nas extensões de arquivo.
  - Escolha Give bucket owner full control (Conceder controle total ao proprietário do bucket) para conceder controle total ao proprietário do bucket do S3 que está mapeado no compartilhamento Network File System (NFS) ou Server Message Block (SMB) do arquivo. Para obter mais informações sobre como usar o compartilhamento de arquivos

para acessar objetos em um bucket de propriedade de outra conta, consulteUso de um compartilhamento de arquivos para acesso entre contas.

- Escolha Enable requester pays (Habilitar o Pagamento pelo solicitante) se você estiver usando esse compartilhamento de arquivos em um bucket que requer que o solicitante ou o leitor, em vez do proprietário dele, pague pelas cobranças de acesso. Para obter mais informações, consulte Buckets de pagamento pelo solicitante.

- para oExportar como, escolha uma opção para o compartilhamento de arquivos. O valor padrão é Read-write.

> **Note**
>
> Para compartilhamentos de arquivos montados em um cliente Microsoft Windows, se você selecionarSomente leiturapeloExportar como, você provavelmente verá uma mensagem de erro. Ela indica que um erro inesperado está impedindo que você crie a pasta. Esse é um problema conhecido no NFS versão 3. Você pode ignorar a mensagem.

- Em File/directory access controlled by (Acesso ao arquivo/diretório controlado por), escolha uma das seguintes opções:
  - Escolha Windows Access Control List (Lista de controles de acesso do Windows) para definir permissões detalhadas em arquivos e pastas no seu compartilhamento de arquivos SMB. Para obter mais informações, consulte Usar as ACLs do Microsoft Windows para controlar o acesso a um compartilhamento de arquivos SMB.
  - Escolha POSIX permissions (Permissões POSIX) para controlar o acesso a arquivos e diretórios armazenados por meio de um compartilhamento de arquivos NFS ou SMB.

  Se o método de autenticação forActive Directory, paraUsuários/grupos administrativos, insira uma lista separada por vírgulas de usuários e grupos do AD. Você pode fazer isso se quiser que o usuário administrador tenha privilégios para atualizar as ACLs em todos os arquivos e pastas no compartilhamento de arquivos. Esses usuários e grupos terão direitos de administrador para o compartilhamento de arquivos. Um grupo deve ser prefixado com a@personagem, por exemplo,`@group1`.

- para oDiferenciação de letras maiúsculas e minúsculas, marque a caixa de seleção para permitir que o gateway controle a sensibilidade entre maiúsculas e minúsculas ou desmarque a caixa de seleção para permitir que o cliente controle a sensibilidade entre maiúsculas

> **Note**
>
> - Se você estiver marcando essa caixa de seleção, essa configuração se aplica imediatamente a novas conexões de cliente SMB. As conexões de cliente SMB existentes devem se desconectar do compartilhamento de arquivos e reconectar para que a configuração entre em vigor.
> - Se você estiver desmarcando essa caixa de seleção, essa configuração pode fazer com que você perca o acesso a arquivos com nomes que diferem apenas no caso deles.

- para oEnumeração baseada em acesso, marque a caixa de seleção para tornar os arquivos e pastas no compartilhamento visíveis somente para usuários que têm acesso de leitura. Mantenha a caixa de seleção desmarcada para tornar os arquivos e pastas no compartilhamento visíveis para todos os usuários durante a enumeração de diretórios.

> **Note**
>
> A enumeração baseada em acesso é um sistema que filtra a enumeração de arquivos e pastas em um compartilhamento de arquivos SMB com base nas listas de controle de acesso (ACLs) do compartilhamento.

- para oBloqueio oportunista (oplock), escolha uma das seguintes opções:
  - SelecioneEnabled (Habilitado)para permitir que o compartilhamento de arquivos use o bloqueio oportunista para otimizar a estratégia de buffer de arquivos, o que melhora o desempenho na maioria dos casos, particularmente no que diz respeito aos menus de contexto do Windows.
  - SelecioneDesabilitadopara evitar o uso de bloqueio oportunista. Se vários clientes Windows em seu ambiente costumam editar os mesmos arquivos simultaneamente, desabilitar o bloqueio oportunista às vezes pode melhorar o desempenho.

> **Note**
>
> Permitir o bloqueio oportunista em compartilhamentos que diferenciam maiúsculas de minúsculas não é recomendado para cargas de trabalho que envolvam acesso a arquivos com o mesmo nome em diferentes casos.

5. Escolha Save changes (Salvar alterações).

Atualizar objetos no bucket do Amazon S3

Enquanto o cliente NFS ou SMB executa as operações do sistema de arquivos, o gateway mantém um inventário dos objetos no bucket do S3 associados ao compartilhamento de arquivos. Seu gateway usa esse inventário armazenado em cache para reduzir a latência e a frequência das solicitações do S3. Esta operação não importa arquivos para o armazenamento em cache do S3 File Gateway. Ele só atualiza o inventário armazenado em cache para refletir as alterações no inventário dos objetos no bucket do S3.

Para atualizar o bucket do S3 para o compartilhamento de arquivos, você pode usar o console do Storage Gateway, oRefreshCacheoperação na Storage Gateway API ou em umAWS Lambdafunção.

Para atualizar objetos em um bucket do S3 a partir do console

1. Abra o console do Storage Gatewayhttps://console.aws.amazon.com/storagegateway/home.
2. Escolha File shares e, em seguida, o compartilhamento de arquivos associado ao bucket do S3 que você deseja atualizar.
3. Em Actions, escolha Refresh cache.

   O tempo que o processo de atualização leva depende do número de objetos armazenados em cache no gateway e o número de objetos que foram adicionados ou removidos do bucket do S3.

Como atualizar objetos em um bucket do S3 usando umAWS Lambdafunção

1. Identifique o bucket do S3 usado pelo S3 File Gateway.
2. Verifique se oEventoA seção está em branco. Ele é preenchido automaticamente mais tarde.
3. Crie uma função do IAM e permita Relacionamento de confiança para o Lambda`lambda.amazonaws.com`.
4. Use a seguinte política.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "StorageGatewayPermissions",
            "Effect": "Allow",
```

```
            "Action": "storagegateway:RefreshCache",
            "Resource": "*"
        },
        {
            "Sid": "CloudWatchLogsPermissions",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogStream",
                "logs:CreateLogGroup",
                "logs:PutLogEvents"
            ],
            "Resource": "*"
        }
    ]
}
```

5. Crie uma função do Lambda a partir do console do Lambda.
6. Use a seguinte função para sua tarefa do Lambda.

```
import json
import boto3
client = boto3.client('storagegateway')
def lambda_handler(event, context):
    print(event)
    response = client.refresh_cache(
        FileShareARN='arn:aws:storagegateway:ap-southeast-2:672406774878:share/
share-E51FBD9C'
    )
    print(response)
    return 'Your FileShare cache has been refreshed'
```

7. para oFunção de execução, escolha a função do IAM criada por você.
8. Opcional: adicione um gatilho para o Amazon S3 e selecione o eventoObjectCreatedouObjectRemoved.

> **Note**
>
> `RefreshCache`precisa concluir um processo antes de iniciar outro. Quando você cria ou exclui muitos objetos em um bucket, o desempenho pode se degradar. Portanto, recomendamos o uso de gatilhos S3. Em vez disso, use a regra do Amazon CloudWatch descrita a seguir.

9. Crie uma regra do CloudWatch no console do CloudWatch e adicione um agendamento. Geralmente, recomendamos umTaxa fixade 30 minutos. No entanto, você pode usar de 1 a 2 horas em um grande bucket S3.
10. Adicione um novo gatilho para eventos do CloudWatch e escolha a regra que você acabou de criar.
11. Salve sua configuração do Lambda. Escolha Test (Testar).
12. SelecioneS3 COLOCARe personalize o teste de acordo com suas necessidades.
13. O teste deve ser bem-sucedido. Caso contrário, modifique o JSON para seus requisitos e teste novamente.
14. Abra o console do Amazon S3 e verifique se o evento criado e o ARN da função Lambda estão presentes.
15. Faça upload de um objeto para seu bucket do S3 usando o console do Amazon S3 ou oAWS CLI.

    O console do CloudWatch gera uma saída do CloudWatch semelhante à seguinte.

```
{
    u'Records': [
        {u'eventVersion': u'2.0', u'eventTime': u'2018-09-10T01:03:59.217Z',
 u'requestParameters': {u'sourceIPAddress': u'MY-IP-ADDRESS'},
        u's3': {u'configurationId': u'95a51e1c-999f-485a-b994-9f830f84769f',
 u'object': {u'sequencer': u'00549CC2BF34D47AED', u'key': u'new/filename.jpeg'},
        u'bucket': {u'arn': u'arn:aws:s3:::MY-BUCKET', u'name': u'MY-GATEWAY-
NAME', u'ownerIdentity': {u'principalId': u'A3OKNBZ72HVPP9'}}, u's3SchemaVersion':
 u'1.0'},
        u'responseElements': {u'x-amz-id-2':
 u'76tiugjhvjfyriugiug87t890nefevbck0iA3rPU9I/s4NY9uXwtRL75tCyxasgsdgfsq+IhvAg5M=',
 u'x-amz-request-id': u'651C2D4101D31593'},
        u'awsRegion': u'MY-REGION', u'eventName': u'ObjectCreated:PUT',
 u'userIdentity': {u'principalId': u'AWS:AROAI5LQR5JHFHDFHDFHJ:MY-USERNAME'},
 u'eventSource': u'aws:s3'}
    ]
}
```

    A invocação do Lambda fornece uma saída semelhante à seguinte.

```
{
    u'FileShareARN': u'arn:aws:storagegateway:REGION:ACCOUNT-ID:share/MY-SHARE-
ID',
```

```
        'ResponseMetadata': {'RetryAttempts': 0, 'HTTPStatusCode': 200,
 'RequestId': '6663236a-b495-11e8-946a-bf44f413b71f',
            'HTTPHeaders': {'x-amzn-requestid': '6663236a-b495-11e8-946a-
bf44f413b71f', 'date': 'Mon, 10 Sep 2018 01:03:59 GMT',
                'content-length': '90', 'content-type': 'application/x-amz-
json-1.1'
        }
    }
}
```

Seu compartilhamento NFS montado em seu cliente refletirá essa atualização.

> **Note**
>
> Para caches que atualizam a criação ou exclusão de objetos grandes em intervalos grandes com milhões de objetos, as atualizações podem levar horas.

16. Excluir seu objeto manualmente usando o console do Amazon S3 ouAWS CLI.
17. Visualize o compartilhamento NFS montado em seu cliente. Verifique se o objeto desapareceu (porque o cache foi atualizado).
18. Verifique seus registros do CloudWatch para ver o registro de sua exclusão com o evento`ObjectRemoved:Delete`.

```
{
    u'account': u'MY-ACCOUNT-ID', u'region': u'MY-REGION', u'detail': {}, u'detail-
type': u'Scheduled Event', u'source': u'aws.events',
    u'version': u'0', u'time': u'2018-09-10T03:42:06Z', u'id':
 u'6468ef77-4db8-0200-82f0-04e16a8c2bdb',
    u'resources': [u'arn:aws:events:REGION:MY-ACCOUNT-ID:rule/FGw-RefreshCache-CW']
}
```

> **Note**
>
> Para trabalhos cron ou tarefas agendadas, seu evento de log do CloudWatch é`u'detail-type': u'Scheduled Event'`.

A atualização do cache apenas inicia a operação de atualização. Quando a atualização do cache termina, não significa necessariamente que o arquivo de atualização esteja concluída.

Para saber se a operação de atualização do arquivo foi concluída antes de verificar se há novos arquivos no compartilhamento de arquivos do gateway, use a notificação `refresh-complete`. Para fazer isso, inscreva-se para ser notificado por meio de um evento do Amazon CloudWatch quando seuRefreshCachea operação é concluída. Para obter mais informações, consulte Receber notificação sobre operações de arquivo.

Uso do S3 Object Lock com um gateway de arquivos do Amazon S3

O Amazon S3 File Gateway oferece suporte ao acesso a buckets do S3 com o bloqueio de objetos do Amazon S3 habilitado. O bloqueio de objetos do Amazon S3 permite que você armazene objetos usando um modelo “Write Once Read Many” (WORM). Ao usar o bloqueio de objetos do Amazon S3, você pode impedir que um objeto no bucket do S3 seja excluído ou substituído. O Amazon S3 Object Lock funciona em conjunto com o versionamento de objetos para proteger seus dados.

Se você ativar o bloqueio de objetos do Amazon S3, ainda poderá modificar o objeto. Por exemplo, ele pode gravar, excluir ou renomeado por meio de um compartilhamento de arquivos em um gateway de arquivos do S3. Ao modificar um objeto dessa forma, o gateway de arquivos do S3 coloca uma nova versão do objeto sem afetar a versão anterior (ou seja, o objeto bloqueado).

Por exemplo, se você usar o gateway de arquivos do S3 ou a interface SMB para excluir um arquivo e o objeto do S3 correspondente estiver bloqueado, o gateway colocará um marcador de exclusão do S3 como a próxima versão do objeto e deixará a versão do objeto original no lugar. Da mesma forma, se um gateway de arquivos do S3 modificar o conteúdo ou os metadados de um objeto bloqueado, uma nova versão do objeto será carregada com as alterações, mas a versão do objeto bloqueado original permanecerá inalterada.

Para obter mais informações sobre bloqueio de objetos do Amazon S3, consulteBloquear objetos usando o bloqueio de objetos do S3noGuia do usuário do Amazon Simple Storage Service.

Compreendendo o status do compartilhamento

Todo compartilhamento de arquivos tem um status associado que informa rapidamente a respeito da integridade do compartilhamento. NA maior parte do tempo, o status indica que a o compartilhamento de arquivos está funcionando normalmente e que nenhuma ação é necessária de sua parte. Em alguns casos, o status indica um problema com que pode ou não exigir uma ação de sua parte.

Você pode ver o status de compartilhamento de arquivos no console do Storage Gateway. O status do compartilhamento de arquivos é exibido na coluna Status para cada compartilhamento de arquivos de seu gateway. O compartilhamento de arquivos que está funcionando normalmente apresenta o status AVAILABLE.

Na tabela a seguir, você encontrará uma descrição de cada status de compartilhamento de arquivos, e se e quando você deve agir com base no status. Um compartilhamento de arquivos apresenta o status AVAILABLE durante todo o tempo ou na maior parte do tempo em que está em uso.

Status	Significado
AVAILABLE	O compartilhamento de arquivos está configurado corretamente e disponível para uso. O status AVAILABLE é o status de execução normal de um compartilhamento de arquivos.
CREATING	O compartilhamento de arquivos está sendo criado e não está pronto para ser usado. O status CREATING é transitório. Nenhuma ação é necessária. Se o compartilhamento de arquivos não sair desse status, é provável que a VM tenha perdido conexão com oAWS.
UPDATING	A configuração de compartilhamento de arquivos está sendo atualizada. Se um compartilhamento de arquivos não sair desse status, é provável que a VM tenha perdido conexão com oAWS.
DELETING	O compartilhamento de arquivos está sendo excluído. O compartil hamento de arquivos não é excluído até que todos os dados sejam carregados paraAWS. O status DELETING é transitório e nenhuma ação é necessária.
FORCE_DELETING	O compartilhamento de arquivos está sendo excluído à força. O compartilhamento de arquivos é excluído imediatamente e o carregame nto paraAWSé anulado. O status FORCE_DELETING é transitório e nenhuma ação é necessária.
UNAVAILABLE	O compartilhamento de arquivos encontra-se em um estado corrompido. Alguns problemas podem fazer com que o compartilhamento de arquivos fique em estado corrompido. Por exemplo, isso pode ser causado por erros de política de função ou caso o compartilhamento de arquivos mapeie para um bucket do Amazon S3 que não existe. Quando o

Status	Significado
	problema que provocou esse estado corrompido é resolvido, o arquivo volta para o estado AVAILABLE.

Melhores práticas de compartilhamento de arquivos

Nesta seção, você pode encontrar informações sobre as melhores práticas em criação de compartilhamentos de arquivos.

Tópicos

Evitar que vários compartilhamentos de arquivos gravem seu bucket do Amazon S3

Ao criar um compartilhamento de arquivos, é recomendável configurar o bucket do Amazon S3 para que apenas um compartilhamento de arquivos possa gravar nele. Se você configurar o bucket do S3 para que vários compartilhamentos de arquivos possam gravar nele, talvez obtenha resultados imprevisíveis. Para evitar isso, você pode criar uma política de bucket do S3 que negue todas as funções, exceto a função usada para o compartilhamento de arquivos inserir ou excluir objetos no bucket. Em seguida, anexe a política ao bucket do S3.

O exemplo de política a seguir nega todas as funções, exceto a função que criou o bucket para gravar no bucket do S3. As ações `s3:DeleteObject` e `s3:PutObject` são negadas para todas as funções, exceto `"TestUser"`. A política se aplica a todos os objetos no bucket `"arn:aws:s3:::TestBucket/*"`.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"DenyMultiWrite",
         "Effect":"Deny",
         "Principal":"*",
         "Action":[
```

```
            "s3:DeleteObject",
            "s3:PutObject"
         ],
         "Resource":"arn:aws:s3:::TestBucket/*",
         "Condition":{
            "StringNotLike":{
               "aws:userid":"TestUser:*"
            }
         }
      }
   ]
}
```

Permitir que clientes NFS específicos montem seu compartilhamento de arquivos

Recomendamos alterar as configurações de clientes NFS permitidos de seu compartilhamento de arquivos. Do contrário, qualquer cliente em sua rede poderá acessar seu compartilhamento de arquivos. Para obter informações sobre como editar as configurações de clientes NFS, consulte Edição de configurações de acesso ao compartilhamento de arquivos NFS.

Monitorando seu gateway de arquivos

É possível monitorar o gateway de arquivos e os recursos associados noAWS Storage Gatewayusando métricas do Amazon CloudWatch e registros de auditoria de compartilhamento de arquivos. Você também pode usar o CloudWatch Events para ser notificado quando as operações de arquivos forem concluídas. Para obter informações sobre as métricas do tipo de gateway de arquivo, consulte Monitorando seu gateway de arquivos.

Tópicos

Obtendo registros de integridade do gateway de arquivos com grupos de logs do CloudWatch

É possível usar o Amazon CloudWatch Logs para obter informações sobre a integridade do gateway de arquivos e recursos relacionados. É possível usar os logs para monitorar o gateway em busca de erros encontrados. Além disso, é possível usar filtros de assinatura do Amazon CloudWatch para automatizar o processamento das informações de log em tempo real. Para obter mais informações, consulteProcessamento em tempo real de dados de log com assinaturasnoGuia do usuário do Amazon CloudWatch.

Por exemplo, é possível configurar um grupo de logs do CloudWatch para monitorar seu gateway e ser notificado quando o gateway de arquivos falhar ao fazer upload de arquivos em um bucket do Amazon S3. Você pode 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 logs do CloudWatch ao ativar um gateway, consulteConfigurar o Amazon S3 File Gateway. Para obter informações gerais sobre grupos de logs do CloudWatch, consulte.Trabalhar com grupos de logs e fluxos de lognoGuia do usuário do Amazon CloudWatch.

Veja a seguir um exemplo de um erro relatado por um gateway de arquivos.

```
{
    "severity": "ERROR",
    "bucket": "bucket-smb-share2",
    "roleArn": "arn:aws:iam::123456789012:role/my-bucket",
    "source": "share-E1A2B34C",
    "type": "InaccessibleStorageClass",
    "operation": "S3Upload",
    "key": "myFolder/myFile.text",
    "gateway": "sgw-B1D123D4",
    "timestamp": "1565740862516"
}
```

Esse erro significa que o gateway de arquivos não consegue carregar o objeto`myFolder/myFile.text`Para o Amazon S3, pois ele fez a transição da classe de armazenamento Amazon S3 Standard para a classe de armazenamento S3 Glacier Flexieval ou para a classe de armazenamento S3 Glacier Deep Archive.

No log de integridade do gateway anterior, estes itens especificam as informações fornecidas:

- `source: share-E1A2B34C` indica o compartilhamento de arquivos que encontrou esse erro.
- `"type": "InaccessibleStorageClass"` indica o tipo de erro que ocorreu. Nesse caso, esse erro foi encontrado quando o gateway estava tentando fazer upload do objeto especificado no Amazon S3 ou ler do Amazon S3. No entanto, neste caso, o objeto passou para o Amazon S3 Glacier. O valor de `"type"` pode ser qualquer erro que o gateway de arquivos encontre. Para obter uma lista de possíveis erros, consulte Como solucionar problemas do gateway de arquivos.
- `"operation": "S3Upload"`indica que esse erro ocorreu quando o gateway estava tentando fazer upload desse objeto no S3.
- `"key": "myFolder/myFile.text"` indica o objeto que causou a falha.
- `gateway": "sgw-B1D123D4` indica o gateway de arquivos que encontrou esse erro.
- `"timestamp": "1565740862516"`indica a hora em que o erro ocorreu.

Para obter informações sobre como solucionar problemas e corrigir esses tipos de erros, consulte Como solucionar problemas do gateway de arquivos.

Como configurar um grupo de logs do CloudWatch depois que o gateway for ativado

O procedimento a seguir mostra como configurar um grupo de logs do CloudWatch depois que o gateway for ativado.

Como configurar um grupo de logs do CloudWatch para trabalhar com o gateway de arquivos

1. Faça login noAWS Management Consolee abra o console do Storage Gateway emhttps://console.aws.amazon.com/storagegateway/home.
2. No painel de navegação, selecioneGateways doE, em seguida, escolha o gateway para o qual você deseja configurar o grupo de logs do CloudWatch.
3. para oAções, escolhaEdição das informações do gateway. Ou, noDetalhesguia, emRegistros de HealtheNão habilitado, escolhaConfigurar grupo de logspara abrir oEditeCustomerGateWayNameCaixa de diálogo.
4. para oGrupo de logs de integridade do gateway, escolha uma das seguintes opções:

   - Disable logging (Desativar o registro em log).se você não quiser monitorar seu gateway usando grupos de log do CloudWatch.
   - Criar um novo grupo de logsPara criar um novo grupo de logs do CloudWatch.
   - Usar um grupo de logs existentepara usar um grupo de logs do CloudWatch que já existe.

     Escolha um grupo de logs noLista de grupos de logs existentes.
5. Escolha Save changes (Salvar alterações).
6. Para ver os logs de integridade do gateway, faça o seguinte:

   1. No painel de navegação, selecioneGateways doE, em seguida, escolha o gateway para o qual você configurou o grupo de logs do CloudWatch.
   2. Selecione oDetalhesguia e abaixoRegistros de Health, escolhaCloudWatch Logs. ODetalhes do grupo de logsa página é aberta no console do CloudWatch.

Como configurar um grupo de logs do CloudWatch para trabalhar com o gateway de arquivos

1. Faça login noAWS Management Consolee abra o console do Storage Gateway emhttps://console.aws.amazon.com/storagegateway/home.

2. SelecioneGateways doE, em seguida, escolha o gateway para o qual você deseja configurar o grupo de logs do CloudWatch.
3. para oAções, escolhaEdição das informações do gateway. Ou, noDetalhesguia, ao lado deRegistro em log, emNão habilitado, escolhaConfigurar grupo de logspara abrir oEdição das informações do gatewayCaixa de diálogo.
4. para oGrupo de logs de gateway do, escolhaUsar um grupo de logs existenteDepois, escolha o grupo de logs que você deseja usar.

   Se você não tiver um grupo de logs, escolha Create a new log group (Criar um novo grupo de logs) para criar um. Você será direcionado para o console do CloudWatch Logs, onde pode criar o grupo de logs. Se criar um grupo de logs, selecione o botão de atualização para visualizar o novo grupo de logs na lista suspensa.
5. Quando concluir, selecione Save.
6. Para ver os logs do gateway, escolha o gateway e escolha oDetalhesGuia.

Para obter informações sobre como solucionar erros, consulte Como solucionar problemas do gateway de arquivos.

Usar métricas do Amazon CloudWatch

É possível obter dados de monitoramento do gateway de arquivos usando oAWS Management Consoleou a API do CloudWatch. O console exibe uma série de gráficos com base nos dados brutos da API do CloudWatch. A API do CloudWatch também pode ser usada por meio de um dosAWSSDKs daouAPI do Amazon CloudWatchFerramentas. Dependendo das necessidades, você pode preferir usar os gráficos exibidos no console ou recuperados da API.

Independentemente do método usado para trabalhar com métricas, você deve 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 sãoGatewayIdeGatewayName. No console do CloudWatch, você pode usar oGateway Metricsexibir para selecionar dimensões específicas do gateway. Para obter mais informações sobre dimensões, consulte.DimensõesnoGuia do usuário do Amazon CloudWatch.
- O nome da métrica, como ReadBytes.

A tabela a seguir resume os tipos de dados de métrica do Storage Gateway disponíveis para você.

Namespace do Amazon CloudWatch	Dimensão	Descrição
`AWS/StorageGateway`	`GatewayId`, `GatewayName`	Essas dimensões filtram dados de métrica que descrevem aspectos do gateway. É possível identificar um gateway de arquivos com o qual se deve trabalhar especificando as dimensões `GatewayId` e `GatewayName`. Os dados de taxa de transferência e latência de um gateway baseiam-se em todos os compartilhamentos de arquivos no gateway. Os dados são disponibilizados automaticamente em períodos de cinco minutos, sem custo adicional.

Trabalhar com métricas de gateway e de arquivo 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 de uma métrica
- Criar alarmes do CloudWatch

Receber notificação sobre operações de arquivo

O Storage Gateway pode iniciar o CloudWatch Events quando as operações de arquivos forem concluídas:

- Você pode ser notificado quando o gateway terminar o upload assíncrono de seus arquivos do compartilhamento de arquivos para o Amazon S3. Usar a`NotificationPolicy`Para solicitar uma notificação de upload de arquivos. Isso envia uma notificação para cada upload de arquivo

concluído para o Amazon S3. Para obter mais informações, consulte Obtendo notificação de upload de arquivos.

- Você pode ser notificado quando o gateway terminar o upload assíncrono do conjunto de arquivos a partir do compartilhamento de arquivos para o Amazon S3. Usar aNotifyWhenUploadedOperação da API para solicitar uma notificação de upload do conjunto de arquivos em funcionamento. Isso envia uma notificação quando todos os arquivos no conjunto de arquivos em funcionamento tiverem sido carregados no Amazon S3. Para obter mais informações, consulte Como receber a notificação de upload do conjunto de arquivos.
- Você pode ser notificado quando o gateway terminar de atualizar o cache para seu bucket do S3. Quando você invoca oRefreshCachePor meio do console do Storage Gateway ou da API do, assine a notificação quando a operação estiver concluída. Para obter mais informações, consulte Obtendo notificação de cache de atualização.

Quando a operação de arquivo solicitada é concluída, o Storage Gateway envia uma notificação por meio do CloudWatch Events. Você pode configurar o CloudWatch Events para enviar a notificação por meio de destinos de eventos, como o Amazon SNS, o Amazon SQS ou umAWS Lambdafunção. Por exemplo, é possível configurar um destino do Amazon SNS para enviar a notificação aos consumidores do Amazon SNS, como um e-mail ou mensagem de texto. Para obter informações sobre o CloudWatch Events, consulteO que é o CloudWatch Events?

Para configurar a notificação do CloudWatch Events

1. Crie um destino, como um tópico do Amazon SNS ou uma função do Lambda, para invocar quando o evento solicitado no Storage Gateway for acionado.
2. Crie uma regra no console do CloudWatch Events para invocar destinos com base em um evento no Storage Gateway.
3. Na regra, crie um padrão de evento para o tipo de evento. A notificação é acionada quando o evento corresponde a esse padrão de regra.
4. Selecione o destino e defina as configurações.

O exemplo a seguir mostra uma regra que inicia o tipo de evento especificado no gateway e no especificadoAWSRegião : Por exemplo, você pode especificar `Storage Gateway File Upload Event` como o tipo de evento.

```
{
   "source":[
```

```
      "aws.storagegateway"
   ],
   "resources":[
      "arn:aws:storagegateway:AWS Region:account-id
                :gateway/gateway-id"
   ],
   "detail-type":[
      "Event type"
   ]
}
```

Para obter informações sobre como usar o CloudWatch Events para acionar regras, consulteCriar uma regra do CloudWatch Events que é acionada em um eventonoGuia do usuário do Amazon CloudWatch Events.

Obtendo notificação de upload de arquivos

Há dois casos de uso nos quais você pode usar a notificação de upload de arquivos:

- Para automatizar o processamento em nuvem de arquivos que são carregados, você pode chamar o`NotificationPolicy`parâmetro e receba de volta um ID de notificação. A notificação que é acionada quando os arquivos são carregados tem o mesmo ID da notificação retornada pela API. Se você mapear esse ID de notificação para rastrear a lista de arquivos dos quais está fazendo upload, você pode acionar o processamento do arquivo que é carregado noAWSquando o evento com a mesma ID é gerado.
- Para casos de uso de distribuição de conteúdo, é possível ter dois gateways de arquivos mapeados para o mesmo bucket do Amazon S3. O cliente de compartilhamento de arquivos do Gateway1 pode fazer upload de novos arquivos para o Amazon S3, e os arquivos são lidos por clientes de compartilhamento de arquivos no Gateway2. Os arquivos são carregados para o Amazon S3, mas eles não são visíveis no Gateway2, pois este usa versões de arquivos no Amazon S3 que são armazenadas em cache localmente. Para tornar os arquivos visíveis no Gateway2, você pode usar o`NotificationPolicy`Para solicitar que a notificação de upload de arquivos do Gateway1 envie uma notificação para você quando o arquivo de upload estiver concluído. Em seguida, você pode usar o CloudWatch Events para emitir automaticamente umRefreshCacheSolicitação para o compartilhamento de arquivos no Gateway2. Quando oRefreshCachea solicitação está concluída, o novo arquivo está visível no Gateway2.

Example Exemplo: notificação de upload de arquivos

O exemplo a seguir mostra uma notificação de upload de arquivos enviada para você por meio do CloudWatch quando o evento corresponde à regra que você criou. Esta notificação está no formato JSON. Você pode configurar essa notificação para ser entregue à mensagem de destino como texto. O `detail-type` é `Storage Gateway Object Upload Event`.

```
{
    "version": "0",
    "id": "2649b160-d59d-c97f-3f64-8aaa9ea6aed3",
    "detail-type": "Storage Gateway Object Upload Event",
    "source": "aws.storagegateway",
    "account": "123456789012",
    "time": "2020-11-05T12:34:56Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:storagegateway:us-east-1:123456789011:share/share-F123D451",
        "arn:aws:storagegateway:us-east-1:123456789011:gateway/sgw-712345DA",
        "arn:aws:s3:::do-not-delete-bucket"
    ],
    "detail": {
        "object-size": 1024,
        "modification-time": "2020-01-05T12:30:00Z",
        "object-key": "my-file.txt",
        "event-type": "object-upload-complete",
        "prefix": "prefix/",
        "bucket-name": "my-bucket",
    }
}
```

Nomes de campos	Descrição
versão	A versão atual da política do IAM.
id	O ID que identifica a política do IAM.
tipo de detalhe	Uma descrição do evento que acionou a notificação que foi enviada.
source	OAWSO serviço que é a origem da solicitação e da notificação.

Nomes de campos	Descrição
conta	O ID daAWSUma conta na qual a solicitação e a notificação foram geradas.
hora	Quando a solicitação para fazer upload de arquivos no Amazon S3 foi feita.
região	OAWSA região da qual a solicitação e a notificação foram enviadas.
recursos	Os recursos do gateway de armazenamento aos quais a política se aplica.
Object size	O tamanho do objeto em bytes.
Hora de modificação	A hora em que o cliente modificou o arquivo.
Object key	O caminho para o arquivo.
event-type	Os CloudWatch Events que acionaram a notificação.
prefix	O nome do prefixo do bucket do S3.
nome-do-seu-bucket	O nome do bucket do S3.

Como receber a notificação de upload do conjunto de arquivos

Existem dois casos de uso em que você pode usar a notificação de upload do conjunto de arquivos de trabalho:

- Para automatizar o processamento em nuvem de arquivos que são carregados, você pode chamar o`NotifyWhenUploaded`API e receba de volta um ID de notificação. A notificação que é acionada quando o conjunto de arquivos em funcionamento tiver sido carregado tem o mesmo ID da notificação retornada pela API. Se você mapear esse ID de notificação para rastrear a lista de arquivos dos quais está fazendo upload, você pode acionar o processamento do conjunto de arquivos cujo upload será feito noAWSquando o evento com a mesma ID é gerado.

- Para casos de uso de distribuição de conteúdo, é possível ter dois gateways de arquivos mapeados para o mesmo bucket do Amazon S3. O cliente de compartilhamento de arquivos do Gateway1 pode fazer upload de novos arquivos para o Amazon S3, e os arquivos são lidos por clientes de compartilhamento de arquivos no Gateway2. Os arquivos são carregados para o Amazon S3, mas eles não são visíveis no Gateway2, pois este usa versões de arquivos no S3 que são armazenadas em cache localmente. Para tornar os arquivos visíveis no Gateway2, use oNotifyWhenUploadedOperação da API para solicitar que a notificação de upload de arquivos do Gateway1 envie uma notificação para você quando o upload do conjunto de arquivos estiver concluído. Em seguida, você pode usar o CloudWatch Events para emitir automaticamente umRefreshCacheSolicitação para o compartilhamento de arquivos no Gateway2. Quando oRefreshCacheA solicitação está concluída, os novos arquivos são visíveis no Gateway2. Esta operação não importa arquivos para o armazenamento em cache do gateway de arquivos. Ele só atualiza o inventário armazenado em cache para refletir as alterações no inventário dos objetos no bucket do S3.

Example Exemplo — Notificação de upload do conjunto de arquivos de trabalho

O exemplo a seguir mostra uma notificação de upload do conjunto de arquivos em funcionamento enviada para você por meio do CloudWatch quando o evento corresponde à regra que você criou. Esta notificação está no formato JSON. Você pode configurar essa notificação para ser entregue à mensagem de destino como texto. O `detail-type` é `Storage Gateway File Upload Event`.

```
{
    "version": "2012-10-17",
    "id": "2649b160-d59d-c97f-3f64-8aaa9ea6aed3",
    "detail-type": "Storage Gateway Upload Notification Event",
    "source": "aws.storagegateway",
    "account": "123456789012",
    "time": "2017-11-06T21:34:42Z",
    "region": "us-east-2",
    "resources": [
        "arn:aws:storagegateway:us-east-2:123456789011:share/share-F123D451",
        "arn:aws:storagegateway:us-east-2:123456789011:gateway/sgw-712345DA"
    ],
    "detail": {
        "event-type": "upload-complete",
        "notification-id": "11b3106b-a18a-4890-9d47-a1a755ef5e47",
        "request-received": "2018-02-06T21:34:42Z",
        "completed": "2018-02-06T21:34:53Z"
    }
```

```
}
```

Nomes de campos	Descrição
versão	A versão atual da política do IAM.
id	O ID que identifica a política do IAM.
tipo de detalhe	Uma descrição do evento que acionou a notificação que foi enviada.
source	OAWSO serviço que é a origem da solicitação e da notificação.
conta	O ID daAWSUma conta na qual a solicitação e a notificação foram geradas.
hora	Quando a solicitação para fazer upload de arquivos no Amazon S3 foi feita.
região	OAWSA região da qual a solicitação e a notificação foram enviadas.
recursos	Os recursos do Storage Gateway aos quais a política se aplica.
event-type	Os CloudWatch Events que acionaram a notificação.
notification-id	O ID gerado aleatoriamente da notificação que foi enviada. Esse ID está no formato UUID. Esse é o ID da notificação que é retornada quando `NotifyWhenUploaded` é chamado.
request-received	O horário em que o gateway recebeu a solicitação `NotifyWhenUploaded` .

Nomes de campos	Descrição
completed	Quando todos os arquivos no conjunto de trabalho foram carregados no Amazon S3.

Obtendo notificação de cache de atualização

Para o caso de uso de notificação de atualização do cache, é possível ter dois gateways de arquivos mapeando para o mesmo bucket do Amazon S3, e o cliente NFS para Gateway1 faz upload dos novos arquivos para o bucket do S3. Os arquivos são carregados para o Amazon S3, mas eles não são exibidos no Gateway2 enquanto o cache não for atualizado. Isso ocorre porque o Gateway2 usa uma versão armazenada localmente em cache dos arquivos no Amazon S3. Você pode querer fazer algo com os arquivos no Gateway2 quando a atualização do cache é concluída. Arquivos grandes podem demorar para serem exibidos no Gateway2, portanto, você pode optar por notificado quando a atualização do cache for concluída. Você pode solicitar uma notificação de atualização do cache do Gateway2 quando todos os arquivos estiverem visíveis nele.

Example Exemplo: notificação de atualização do cache

O exemplo a seguir mostra uma notificação de atualização do cache enviada pelo CloudWatch quando o evento corresponde à regra que você criou. Esta notificação está no formato JSON. Você pode configurar essa notificação para ser entregue à mensagem de destino como texto. O `detail-type` é `Storage Gateway Refresh Cache Event`.

```
{
    "version": "2012-10-17",
    "id": "2649b160-d59d-c97f-3f64-8aaa9ea6aed3",
    "detail-type": "Storage Gateway Refresh Cache Event",
    "source": "aws.storagegateway",
    "account": "209870788375",
    "time": "2017-11-06T21:34:42Z",
    "region": "us-east-2",
    "resources": [
        "arn:aws:storagegateway:us-east-2:123456789011:share/share-F123D451",
        "arn:aws:storagegateway:us-east-2:123456789011:gateway/sgw-712345DA"
    ],
    "detail": {
        "event-type": "refresh-complete",
        "notification-id": "1c14106b-a18a-4890-9d47-a1a755ef5e47",
```

```
        "started": "2018-02-06T21:34:42Z",
        "completed": "2018-02-06T21:34:53Z",
        "folderList": [
            "/"
        ]
    }
}
```

Nomes de campos	Descrição
versão	A versão atual da política do IAM.
id	O ID que identifica a política do IAM.
tipo de detalhe	Uma descrição do tipo do evento que acionou a notificação que foi enviada.
source	OAWSO serviço que é a origem da solicitação e da notificação.
conta	O ID daAWSUma conta na qual a solicitação e a notificação foram geradas.
hora	O horário em que a solicitação para atualizar os arquivos no conjunto de trabalho foi feita.
região	OAWSA região da qual a solicitação e a notificação foram enviadas.
recursos	Os recursos do Storage Gateway aos quais a política se aplica.
event-type	Os CloudWatch Events que acionaram a notificação.
notification-id	O ID gerado aleatoriamente da notificação que foi enviada. Esse ID está no formato UUID. Esse é o ID da notificação que é retornada quando você chama `RefreshCache` .

Nomes de campos	Descrição
started	quando o gateway recebeu o`RefreshCache` Solicitação e a atualização foi iniciada.
completed	O horário em que a atualização do conjunto de trabalho foi concluída.
folderList	Uma lista separada por vírgulas de caminhos de pastas que foram atualizadas no cache. O padrão é ["/"].

Noções básicas de métricas de gateway

A tabela a seguir descreve métricas do que abrangem gateways de arquivos do S3. Cada gateway tem um conjunto de métricas associado a ele. Algumas métricas específicas do gateway têm o mesmo nome que determinadas métricas específicas ao compartilhamento de arquivos. Essas métricas representam medições do mesmo tipo, mas são mapeadas para o gateway, e não para compartilhamento de arquivos.

Você sempre deve especificar se deseja trabalhar com um gateway ou compartilhamento de arquivos ao trabalhar com métricas específicas. Especificamente, ao trabalhar com métricas do gateway, você deve especificar o`GatewayName`Para o gateway cujos dados métricos você deseja visualizar. Para obter mais informações, consulte Usar métricas do Amazon CloudWatch.

A tabela a seguir descreve as métricas do que você pode usar para obter informações sobre oGateway de arquivos S3s.

Métrica	Descrição
`AvailabilityNotifications`	Essa métrica relata o número de notificações de integridade relacionadas à disponibilidade geradas pelo gateway no período do relatório. Unidades: Contagem
`CacheFileSize`	Essa métrica controla o tamanho dos arquivos no cache do gateway.

Métrica	Descrição
	Use essa métrica com o`Average`estatística para medir o tamanho médio de um arquivo no cache do gateway. Use essa métrica com o`Max`estatística para medir o tamanho máximo de um arquivo no cache do gateway. Unidades: Bytes
`CacheFree`	Essa métrica informa o número de bytes disponíveis no cache do gateway. Unidades: Bytes
`CacheHitPercent`	Porcentagem de operações de leitura do aplicativo do gateway que são feitas pelo cache. A amostra é capturada no final do período do relatório. Quando não há operações de leitura do aplicativo a partir do gateway, esta métrica relata 100%. Unidades: Percentual
`CachePercentDirty`	A porcentagem geral do cache do gateway que não persistiu naAWS. A amostra é capturada no final do período do relatório. Unidades: Percentual
`CachePercentUsed`	A porcentagem geral do armazenamento em cache do gateway usado. A amostra é capturada no final do período do relatório. Unidades: Percentual

Métrica	Descrição
`CacheUsed`	Essa métrica informa o número de bytes usados no cache do gateway. Unidades: Bytes
`CloudBytesDownloaded`	O número total de bytes que o gateway carregou noAWSdurante o período de relatório. Use esta métrica com a estatística `Sum` para medir o throughput e com a estatística `Samples` para medir operações de entrada/saída por segundo (IOPS). Unidades: Bytes
`CloudBytesUploaded`	O número total de bytes que o gateway baixou daAWSdurante o período de relatório. Use essa métrica com a estatística `Sum` para medir a taxa de transferência e com a estatística `Samples` para medir IOPS. Unidades: Bytes
`FilesFailingUpload`	Essa métrica rastreia o número de arquivos que não são carregados noAWS. Esses arquivos gerarão notificações de integridade que contêm mais informações sobre o problema. Use essa métrica com o`Sum`estatística para mostrar o número de arquivos que estão atualmente falhando ao carregar paraAWS. Unidades: Contagem

Métrica	Descrição
`FileSharesUnavailable`	Essa métrica fornece o número de compartil hamentos de arquivos nesses gateways que estão noIndisponívelestado. Se essa métrica informar que qualquer compartilhamento de arquivo não está disponível, é provável que haja um problema com o gateway que pode causar interrupção no fluxo de trabalho. É recomendável criar um alarme para o quando essa métrica informa um valor diferente de zero. Unidades: Contagem
`FilesRenamed`	Essa métrica rastreia o número de arquivos renomeados no período de relatório. Unidades: Contagem
`HealthNotifications`	Essa métrica relata o número de notificações de integridade geradas por esse gateway no período do relatório. Unidades: Contagem
`IoWaitPercent`	Essa métrica relata o percentual de tempo que a CPU está aguardando uma resposta do disco local. Unidades: Percentual
`MemTotalBytes`	Essa métrica relata a quantidade total de memória no gateway. Unidades: Bytes

Métrica	Descrição
`MemUsedBytes`	Essa métrica relata a quantidade de memória usada no gateway. Unidades: Bytes
`NfsSessions`	Essa métrica informa o número de sessões do NFS ativas no gateway. Unidades: Contagem
`RootDiskFreeBytes`	Essa métrica informa o número de bytes disponíveis no disco raiz do gateway. Se essa métrica informar que menos de 20 GB são gratuitos, você deverá aumentar o tamanho do disco raiz. Unidades: Bytes
`S3GetObjectRequestTime`	Essa métrica relata o tempo para que o gateway conclua as solicitações de objeto get do S3. Unidades: Milissegundos
`S3PutObjectRequestTime`	Essa métrica relata o tempo para que o gateway conclua as solicitações de objeto put do S3. Unidades: Milissegundos
`S3UploadPartRequestTime`	Essa métrica relata o tempo para que o gateway conclua as solicitações de peças de upload do S3. Unidades: Milissegundos

Métrica	Descrição
`SmbV1Sessions`	Essa métrica informa o número de sessões do SMBv1 ativas no gateway. Unidades: Contagem
`SmbV2Sessions`	Essa métrica informa o número de sessões do SMBv2 ativas no gateway. Unidades: Contagem
`SmbV3Sessions`	Essa métrica informa o número de sessões do SMBv3 ativas no gateway. Unidades: Contagem
`TotalCacheSize`	Essa métrica informa o tamanho total do cache. Unidades: Bytes
`UserCpuPercent`	Essa métrica relata a porcentagem de tempo gasto no processamento do gateway. Unidades: Percentual

Compreendendo métricas de compartilhamento de arquivos

Você pode encontrar informações a seguir sobre as métricas do Storage Gateway que abrangem compartilhamentos de arquivos. Cada compartilhamento de arquivos tem um conjunto de métricas associado a ele. Algumas métricas específicas ao compartilhamento de arquivos têm o mesmo nome que determinadas métricas específicas ao gateway. Essas métricas representam medições do mesmo tipo, mas são dimensionadas para compartilhamento de arquivos.

Você sempre deve especificar se deseja trabalhar com uma métrica de gateway ou de compartilhamento de arquivos, antes de trabalhar com métricas. Mais especificamente, ao trabalhar com métricas de compartilhamento de arquivos, é necessário especificar `File share ID`, que identifica o compartilhamento de arquivos cujas métricas você tem interesse em visualizar. Para obter mais informações, consulte Usar métricas do Amazon CloudWatch.

A tabela a seguir descreve as métricas do Storage Gateway que você pode usar para obter informações sobre os compartilhamentos de arquivos.

Métrica	Descrição
`CacheHitPercent`	Porcentagem de operações de leitura do aplicativo dos compartilhamentos de arquivos que são feitas pelo cache. A amostra é capturada no final do período do relatório. Quando não há operações de leitura do aplicativo a partir do compartilhamento de arquivos, esta métrica relata 100%. Unidades: Percentual
`CachePercentDirty`	A contribuição do compartilhamento de arquivos para o percentual geral do cache do gateway que não persistiu naAWS. A amostra é capturada no final do período do relatório. Usar a`CachePercentDirty` Métrica do gateway para visualizar o percentual geral do cache do gateway que não persistiu naAWS. Unidades: Percentual
`CachePercentUsed`	A contribuição do compartilhamento de arquivos para o percentual geral de uso do armazenamento em cache do gateway. A amostra é capturada no final do período do relatório. Use a métrica `CachePercentUsed` do gateway para visualizar o percentual geral de uso do cache do gateway de armazenamento. Unidades: Percentual

Métrica	Descrição
`CloudBytesUploaded`	O número total de bytes que o gateway carregou noAWSdurante o período de relatório. Use essa métrica com a estatística `Sum` para medir a taxa de transferência e com a estatísti ca `Samples` para medir IOPS. Unidades: Bytes
`CloudBytesDownloaded`	O número total de bytes que o gateway baixou daAWSdurante o período de relatório. Use esta métrica com a estatística `Sum` para medir o throughput e com a estatística `Samples` para medir operações de entrada/s aída por segundo (IOPS). Unidades: Bytes
`ReadBytes`	O número total de bytes lidos dos aplicativos locais no período do relatório para compartil hamento de arquivos. Use essa métrica com a estatística `Sum` para medir a taxa de transferência e com a estatísti ca `Samples` para medir IOPS. Unidades: Bytes
`WriteBytes`	O número total de bytes gravados nos aplicativ os locais no período do relatório. Use essa métrica com a estatística `Sum` para medir a taxa de transferência e com a estatísti ca `Samples` para medir IOPS. Unidades: Bytes

Noções básicas sobre registros de auditoria do gateway

Os logs de auditoria do Amazon S3 File Gateway (S3 File Gateway) fornecem detalhes sobre o acesso do usuário a arquivos e pastas em um compartilhamento de arquivos. É possível usá-los para monitorar as atividades do usuário e tomar medidas se forem identificados padrões de atividade inadequados.

Operações

A tabela a seguir descreve as operações de acesso ao arquivo de log de auditoria do gateway de arquivos.

Nome de operação	Definição
Ler dados	Leia o conteúdo de um arquivo.
Gravar dados	Altere o conteúdo de um arquivo.
Criar	Crie um novo arquivo ou pasta.
Renomear	Renomeie um arquivo ou pasta existente.
Excluir	Exclua um arquivo ou uma pasta.
Atributos de gravação	Atualize metadados de arquivo ou pasta (ACLs, proprietário, grupo, permissões).

Atributos.

A tabela a seguir descreve atributos de acesso ao arquivo de log de auditoria do S3 File Gateway.

Atributo	Definição
`accessMode`	A configuração de permissão do objeto.
`accountDomain` (Somente SMB)	O domínio do Active Directory (AD) ao qual pertence a conta do cliente.

Atributo	Definição
`accountName` (Somente SMB)	O nome de usuário do Active Directory do cliente.
`bucket`	O nome de um bucket do S3.
`clientGid` (Somente NFS)	O identificador do grupo do usuário que acessa o objeto.
`clientUid` (Somente NFS)	O identificador do usuário que acessa o objeto.
`ctime`	A hora em que o conteúdo ou os metadados do objeto foram modificados, definida pelo cliente.
`groupId`	O identificador do proprietário do grupo do objeto.
`fileSizeInBytes`	O tamanho do arquivo em bytes, definido pelo cliente no momento da criação do arquivo.
`gateway`	O ID do Storage Gateway.
`mtime`	A hora em que o conteúdo do objeto foi modificado, definida pelo cliente.
`newObjectName`	O caminho completo para o novo objeto depois que ele foi renomeado.
`objectName`	O caminho completo para o objeto.
`objectType`	Define se o objeto é um arquivo ou uma pasta.
`operation`	O nome da operação de acesso ao objeto.
`ownerId`	O identificador do proprietário do objeto.
`securityDescriptor` (Somente SMB)	Mostra a lista de controle de acesso discricio nário (DACL) definida em um objeto, no formato SDDL.

Atributo	Definição
`shareName`	O nome do compartilhamento que está sendo acessado.
`source`	O ID do compartilhamento de arquivos que está sendo auditado.
`sourceAddress`	O endereço IP da máquina cliente de compartilhamento de arquivos.
`status`	O status da operação. Somente o êxito é registrado (as falhas são registradas, com a exceção das falhas decorrentes de permissões negadas).
`timestamp`	A hora em que a operação ocorreu com base no timestamp do sistema operacional do gateway.
`version`	A versão do formato do log de auditoria.

Atributos registrados por operação

A tabela a seguir descreve os atributos de log de auditoria do S3 File Gateway registrados em cada operação de acesso a arquivos.

	Ler dados	Gravar dados	Criar pasta	Criar arquivo	Renomear arquivo/pasta	Excluir arquivo/pasta	Atributos de gravação (alterar ACL -Somente SMB)	Atributos de gravação (chown)	Atributos de gravação (chmod)	Atributos de gravação (chgrp)
`access`			X	X					X	

	Ler dados	Gravar dados	Criar pasta	Criar arquivo	Renomea arquivo/ pasta	Excluir arquivo/ pasta	Atributos de gravação (alterar ACL -Somente SMB)	Atributos de gravação (chown)	Atributos de gravação (chmod)	Atributos de gravação (chgrp)
accoun main (Somen SMB)	X	X	X	X	X	X	X	X	X	X
accoun me (Somen SMB)	X	X	X	X	X	X	X	X	X	X
bucket	X	X	X	X	X	X	X	X	X	X
client (Somen NFS)	X	X	X	X	X	X		X	X	X
client (Somen NFS)	X	X	X	X	X	X		X	X	X
ctime			X	X						
groupI			X	X						
fileSi nBytes				X						
gatewa	X	X	X	X	X	X	X	X	X	X

	Ler dados	Gravar dados	Criar pasta	Criar arquivo	Renomea arquivo/ pasta	Excluir arquivo/ pasta	Atributos de gravação (alterar ACL -Somente SMB)	Atributos de gravação (chown)	Atributos de gravação (chmod)	Atributos de gravação (chgrp)
mtime			X	X						
newObjName					X					
objecte	X	X	X	X	X	X	X	X	X	X
objecte	X	X	X	X	X	X	X	X	X	X
operat	X	X	X	X	X	X	X	X	X	X
ownerI			X	X				X		
securiescrip (Somen SMB)							X	X		
shareN	X	X	X	X	X	X	X	X	X	X
source	X	X	X	X	X	X	X	X	X	X
sourceress	X	X	X	X	X	X	X	X	X	X
status	X	X	X	X	X	X	X	X	X	X

	Ler dados	Gravar dados	Criar pasta	Criar arquivo	Renomea arquivo/ pasta	Excluir arquivo/ pasta	Atributos de gravação (alterar ACL -Somente SMB)	Atributos de gravação (chown)	Atributos de gravação (chmod)	Atributos de gravação (chgrp)
timest	X	X	X	X	X	X	X	X	X	X
versic	X	X	X	X	X	X	X	X	X	X

Manutenção de 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.

Tópicos

Desligar a 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 dessa seção seja apresentar como o gateway é iniciado e encerrado por meio do Console de Gerenciamento do Gateway de Armazenamento, 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.

Você pode precisar encerrar ou reiniciar a VM para manutenção; por exemplo, ao aplicar um patch ao hipervisor. Para o gateway de arquivos, basta encerrar a VM. Você não desliga o gateway. Embora o foco dessa seção seja apresentar como o gateway é iniciado e encerrado por meio do Console de Gerenciamento do Gateway de Armazenamento, 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.

- Console local da VM do gateway — consulteComo executar tarefas de manutenção no console local.
- API do Storage Gateway — ConsulteShutdownGateway

Gerenciando 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 do Amazon EC2 usam volumes do Amazon EBS como discos locais.

Tópicos

Decidir a quantidade de armazenamento em disco local

Você decide o número e o tamanho dos discos que deseja alocar para o gateway. O gateway requer o seguinte armazenamento adicional:

Gateways de arquivos exigem pelo menos um disco para usar como cache. 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	Tipo de gateway
Armazenamento em cache	O armazenamento em cache funciona como um armazenamento local duradouro para dados no Amazon S3 ou no sistema de arquivos.	• Gateways de arquivo

> **Note**
>
> 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), você tem a opção de 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 o armazenamento em cache. 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. 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 discos para armazenamento em cache.

Determinando o tamanho do armazenamento em cache a ser alocado

Seu gateway usa armazenamento em cache para fornecer acesso de baixa latência aos dados recém-acessados. O armazenamento em cache funciona como um armazenamento local duradouro para dados no Amazon S3 ou no sistema de arquivos. Para obter mais informações sobre como estimar o tamanho do armazenamento em cache, consulte Gerenciando discos locais para o Storage Gateway.

A princípio, você pode usar essa estimativa para provisionar discos para armazenamento em cache. Depois, você pode usar métricas operacionais do Amazon CloudWatch para monitorar o uso do armazenamento em cache e ampliar o armazenamento conforme a necessidade por meio do console. Para obter informações sobre como usar métricas e configurar de alarmes, consulte Performance.

Adicionar armazenamento em cache

À medida que as necessidades de seu aplicativo mudarem, você poderá aumentar a capacidade de armazenamento em cache do gateway. Você pode ampliar a capacidade de cache do gateway sem interromper as funções existentes do gateway. Ao ampliar a capacidade de armazenamento, você o faz com a VM do gateway ativada.

Important

Ao adicionar cache a um gateway existente, é importante criar novos discos no host (hipervisor ou instância do Amazon EC2). Não altere o tamanho dos discos existentes caso

os discos tenham sido alocados anteriormente como um cache. Não remova os discos de cache que foram alocados como armazenamento em cache.

O procedimento a seguir mostra como configurar ou armazenar em cache o armazenamento em cache para o gateway.

Para adicionar e configurar um armazenamento em cache

1. Provisione um novo disco no host (hipervisor ou instância do Amazon EC2). Para obter informações sobre como provisionar um disco em um hipervisor, consulte o manual do usuário do hipervisor. Configure esse disco como armazenamento em cache.
2. Abra o console Storage Gateway emhttps://console.aws.amazon.com/storagegateway/home.
3. No painel de navegação, selecione Gateways da .
4. No menu Actions, escolha Edit local disks.
5. Na caixa de diálogo Edit local disks (Editar discos locais), identifique os discos provisionados e determine qual você deseja usar como armazenamento em cache.

   Se você não vir seus discos, escolha o botão Refresh.
6. Escolha Save para salvar suas definições de configuração.

Usando armazenamento efêmero com gateways EC2

Esta seção descreve as etapas necessárias para evitar a perda de dados quando você seleciona um disco efêmero para armazenamento em cache do seu gateway.

Os discos efêmeros fornecem armazenamento temporário em nível de bloco para a instância do Amazon EC2. Os discos efêmeros são ideais para armazenamento temporário de dados alterados com frequência, como dados no armazenamento em cache de um gateway. Quando você executar seu gateway com uma imagem de máquina da Amazon EC2 do Amazon para o, e o tipo de instância que você selecionar for compatível com armazenamento temporário, os discos são listados automaticamente e você pode selecionar um deles para armazenar dados do seu gateway em cache. Para obter mais informações, consulteArmazenamento de instâncias do Amazon EC2noGuia do usuário do Amazon EC2 para instâncias do Linux.

As gravações do aplicativo gravadas nos discos são armazenadas no cache de maneira síncrona e, depois, carregadas de modo assíncrono no armazenamento durável no Amazon S3. Se os

dados armazenados temporariamente forem perdidos porque uma instância do Amazon EC2 foi interrompida antes da conclusão do upload dos dados, os dados ainda presentes no cache e não foram carregados para o Amazon S3 podem ser perdidos. Você pode evitar a perda de dados seguindo as seguintes etapas antes de reiniciar ou interromper a instância do EC2 que hospeda seu gateway.

> **Note**
>
> Se você estiver usando o armazenamento temporário e interromper e iniciar o gateway, ele ficará permanentemente offline. Isso acontece porque o disco de armazenamento físico é substituído. Não há solução para esse problema, portanto, você teria que excluir o gateway e ativar um novo em uma nova Instância EC2.

As etapas que compõem o procedimento a seguir são específicas para gateways de arquivos.

Para evitar a perda de dados em gateways de arquivos que usam discos efêmeros

1. Interrompa todos os processos que estão gravando no compartilhamento de arquivos.
2. Inscreva-se para receber notificações do CloudWatch Events. Para obter mais informações, consulte Receber notificação sobre operações de arquivo.
3. Chame oAPI NotifyWhenUploadedPara serem notificados quando os dados gravados até o momento da perda do armazenamento efêmero forem armazenados de forma permanente no Amazon S3.
4. Você vai receber o ID da notificação depois que a API concluir o processo.

   Você pode receber um evento do CloudWatch com o mesmo ID de notificação.
5. Verifique se a métrica de `CachePercentDirty` para seu compartilhamento de arquivos é 0. Isso confirma que todos os seus dados foram gravados no Amazon S3. Para obter informações sobre as métricas de compartilhamento de arquivos, consulte Compreendendo métricas de compartilhamento de arquivos.
6. Agora você pode reiniciar ou interromper o gateway de arquivos sem risco de perda de dados.

Como gerenciar largura de banda para seu gateway de arquivo do Amazon S3

Você pode limitar a taxa de transferência de upload do gateway paraAWSPara controlar a quantidade de largura de banda da rede que o gateway usa. Por padrão, um gateway ativado não tem limites de taxa.

Você pode configurar uma programação de limite de taxa de largura de banda usando oAWS Management Console, umAWSO kit de desenvolvimento de software (SDK) ou oAWS Storage GatewayAPI (consulteUpdateBandWidthRateLimitScheduleno AWSReferência da API do Storage Gateway.). Usando uma programação de limite de taxa de largura de banda, você pode configurar limites para mudar automaticamente ao longo do dia ou da semana. Para obter mais informações, consulte Visualize e edite a programação de limite de taxa de largura de banda para seu gateway usando o console do Storage Gateway.

> **Note**
>
> A configuração de limites e agendamentos de taxa de largura de banda não é suportada no momento para o tipo Amazon FSx File Gateway.

Tópicos

- Visualize e edite a programação de limite de taxa de largura de banda para seu gateway usando o console do Storage Gateway
- Como atualizar limites de taxa de largura de banda do gateway por meio doAWS SDK for Java
- Como atualizar limites de taxa de largura de banda do gateway por meio doAWS SDK for .NET
- Como atualizar limites de taxa de largura de banda do gateway por meio doAWS Tools for Windows PowerShell

Visualize e edite a programação de limite de taxa de largura de banda para seu gateway usando o console do Storage Gateway

Esta seção descreve como visualizar e editar a programação de limite de taxa de largura de banda para o gateway.

Para visualizar e editar a programação dos limites da taxa de largura de banda

1. Abra o console Storage Gateway emhttps://console.aws.amazon.com/storagegateway/home.
2. No painel de navegação à esquerda, escolhaGateways doE em seguida o gateway que você deseja gerenciar.
3. para oAções, escolhaEditar programação limite de taxa de largura de banda.

   A programação atual do limite de taxa de largura de banda do gateway é exibida naEditar programação limite de taxa de largura de banda. Por padrão, um novo gateway não tem limites de taxa de largura de banda definidos.
4. (Opcional) EscolhaAdicionar novo limite de taxa de largura de bandapara adicionar um novo intervalo configurável à programação. Para cada intervalo que você adicionar, insira as seguintes informações:

   - Taxa de upload— Insira o limite de taxa de upload, em megabits por segundo (Mbps). O valor mínimo é de 100 Mbps.
   - Dias da semana— Selecione o dia ou os dias durante cada semana quando você deseja que o intervalo seja aplicado. Você pode aplicar o intervalo nos dias da semana (de segunda a sexta-feira), fins de semana (sábado e domingo), todos os dias da semana ou em um dia específico por semana. Para aplicar o limite de taxa de largura de banda de forma uniforme e constante em todos os dias e em todos os momentos, escolhaSem programação.
   - Horário de início— Insira a hora de início do intervalo de largura de banda, usando o formato HH:MM e o deslocamento do fuso horário do UTC para seu gateway.

     > **Note**
     >
     > Seu intervalo de limite de taxa de largura de banda começa no início do minuto especificado aqui.

   - End Time— Insira a hora de término do intervalo de largura de banda, usando o formato HH:MM e o deslocamento de fuso horário do GMT para seu gateway.

     > **Important**
     >
     > O intervalo de limite de taxa de largura de banda termina no final do minuto especificado aqui. Para agendar um intervalo que termina no final de uma hora, insira**59**.

Para agendar intervalos contínuos consecutivos, fazendo a transição no início da hora, sem interrupção entre os intervalos, insira**59**para o minuto final do primeiro intervalo. Digite**00**para o minuto inicial do intervalo sucessivo.

5. (Opcional) Repita a etapa anterior conforme necessário até que a programação de limite de taxa de largura de banda esteja concluída. Se você precisar excluir um intervalo da sua agenda, escolhaRemover.

> **Important**
>
> Os intervalos de limite de taxa de largura de banda 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. Quando terminar, escolhaSalve as alterações.

Como atualizar limites de taxa de largura de banda do gateway por meio doAWS SDK for Java

Ao atualizar programaticamente os limites de taxa de largura de banda, você pode ajustar esses limites automaticamente ao longo de um período — 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 doAWS 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 Como atualizar limites de taxa de largura de banda do gateway por meio doAWS SDK for Java

O exemplo de código Java a seguir atualiza os limites de taxa de largura de banda de um gateway. Para usar esse código de exemplo, você deve fornecer o endpoint de serviço, o Nome de recurso da Amazon (ARN) para o gateway e o limite de upload. Para uma lista deAWSendpoints de serviço que você pode usar com o Storage Gateway, consulteAWS Storage GatewayEndpoints e cotas donoAWSReferência geral.

```
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.
UpdateBandwidthRateLimitScheduleRequest;
   import com.amazonaws.services.storagegateway.model.
UpdateBandwidthRateLimitScheduleReturn;

   import java.util.Arrays;
   import java.util.Collections;
   import java.util.List;

   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 = 100 * 1024 * 1024;  // Bits per second, minimum 100
Megabits/second

       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, null); // download rate not
supported by S3 File gateways

       }

       private static void UpdateBandwidth(String gatewayArn, long uploadRate, long
downloadRate) {
           try
           {
               BandwidthRateLimit bandwidthRateLimit = new
BandwidthRateLimit(downloadRate, uploadRate);
```

```
                BandwidthRateLimitInterval noScheduleInterval = new
BandwidthRateLimitInterval()
                    .withBandwidthRateLimit(bandwidthRateLimit)
                    .withDaysOfWeek(Arrays.asList(1, 2, 3, 4, 5, 6, 0))
                    .withStartHourOfDay(0)
                    .withStartMinuteOfHour(0)
                    .withEndHourOfDay(23)
                    .withEndMinuteOfHour(59);
                UpdateBandwidthRateLimitScheduleRequest
updateBandwidthRateLimitScheduleRequest =
                    new UpdateBandwidthRateLimitScheduleRequest()
                    .withGatewayARN(gatewayArn)
                    .with
BandwidthRateLimitIntervals(Collections.singletonList(noScheduleInterval));

                UpdateBandwidthRateLimitScheduleReturn
updateBandwidthRateLimitScheuduleResponse =
sgClient.UpdateBandwidthRateLimitSchedule(updateBandwidthRateLimitScheduleRequest);

                String returnGatewayARN =
updateBandwidthRateLimitScheuduleResponse.getGatewayARN();
                System.out.println("Updated the bandwidth rate limits of " +
returnGatewayARN);
                System.out.println("Upload bandwidth limit = " + uploadRate + " bits
per second");
            }
            catch (AmazonClientException ex)
            {
                System.err.println("Error updating gateway bandwith.\n" +
ex.toString());
            }
        }
    }
```

Como atualizar limites de taxa de largura de banda do gateway por meio doAWS SDK for .NET

Ao atualizar programaticamente os limites de taxa de largura de banda, você pode ajustar esses limites automaticamente ao longo de um período — por exemplo, usando tarefas programadas. O exemplo a seguir demonstra como atualizar os limites de taxa de largura de banda de um gateway usando oAWSKit de desenvolvimento de software (SDK) para .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 Como atualizar limites de taxa de largura de banda do gateway por meio doAWS SDK for .NET

O exemplo de código C# a seguir atualiza os limites de taxa de largura de banda de um gateway. Para usar esse código de exemplo, você deve fornecer o endpoint de serviço, o Nome de recurso da Amazon (ARN) para o gateway e o limite de upload. Para uma lista deAWSendpoints de serviço que você pode usar com o Storage Gateway, consulteAWS Storage GatewayEndpoints e cotas donoAWSReferência geral.

```
    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 = 100 * 1024 * 1024;  // Bits per second, minimum
 100 Megabits/second

            public static void Main(string[] args)
            {
                // Create a storage gateway client
                sgConfig = new AmazonStorageGatewayConfig();
                sgConfig.ServiceURL = serviceURL;
                sgClient = new AmazonStorageGatewayClient(sgConfig);
```

```
                UpdateBandwidth(gatewayARN, uploadRate, null);

                Console.WriteLine("\nTo continue, press Enter.");
                Console.Read();
            }

            public static void UpdateBandwidth(string gatewayARN, long uploadRate, long
downloadRate)
            {
                try
                {
                   BandwidthRateLimit bandwidthRateLimit = new
BandwidthRateLimit(downloadRate, uploadRate);
                   BandwidthRateLimitInterval noScheduleInterval = new
BandwidthRateLimitInterval()
                    .withBandwidthRateLimit(bandwidthRateLimit)
                    .withDaysOfWeek(Arrays.asList(1, 2, 3, 4, 5, 6, 0))
                    .withStartHourOfDay(0)
                    .withStartMinuteOfHour(0)
                    .withEndHourOfDay(23)
                    .withEndMinuteOfHour(59);
                  List <BandwidthRateLimitInterval> bandwidthRateLimitIntervals = new
List<BandwidthRateLimitInterval>();
                  bandwidthRateLimitIntervals.Add(noScheduleInterval);
                  UpdateBandwidthRateLimitScheduleRequest
updateBandwidthRateLimitScheduleRequest =
                    new UpdateBandwidthRateLimitScheduleRequest()
                       .withGatewayARN(gatewayARN)
                       .with BandwidthRateLimitIntervals(bandwidthRateLimitIntervals);

                    UpdateBandwidthRateLimitScheduleReturn
updateBandwidthRateLimitScheuduleResponse =
sgClient.UpdateBandwidthRateLimitSchedule(updateBandwidthRateLimitScheduleRequest);
                    String returnGatewayARN =
updateBandwidthRateLimitScheuduleResponse.GatewayARN;
                    Console.WriteLine("Updated the bandwidth rate limits of " +
returnGatewayARN);
                    Console.WriteLine("Upload bandwidth limit = " + uploadRate + " bits
per second");
                }
                catch (AmazonStorageGatewayException ex)
                {
```

```
                    Console.WriteLine("Error updating gateway bandwith.\n" +
ex.ToString());
                }
            }
        }
    }
```

Como atualizar limites de taxa de largura de banda do gateway por meio doAWS Tools for Windows PowerShell

Ao atualizar programaticamente os limites de taxa de largura de banda, você pode ajustar esses limites automaticamente ao longo de um período — 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 doAWS Tools for Windows PowerShell. Para usar o código de exemplo, você deve estar familiarizado com a execução de um script do PowerShell. Para obter mais informações, consulte Conceitos básicos no Guia do usuário do AWS Tools for Windows PowerShell.

Example Como atualizar limites de taxa de largura de banda do gateway por meio doAWS Tools for Windows PowerShell

O exemplo a seguir de script do PowerShell atualiza os limites de taxa de largura de banda de um gateway. Para usar esse script de exemplo, você deve fornecer o nome de recurso da Amazon (ARN) para o gateway e o limite de upload.

```
    <#
    .DESCRIPTION
        Update Gateway bandwidth limits schedule

    .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 = 100 * 1024 * 1024
```

```
   $gatewayARN = "*** provide gateway ARN ***"

   $bandwidthRateLimitInterval = New-Object
Amazon.StorageGateway.Model.BandwidthRateLimitInterval
   $bandwidthRateLimitInterval.StartHourOfDay = 0
   $bandwidthRateLimitInterval.StartMinuteOfHour = 0
   $bandwidthRateLimitInterval.EndHourOfDay = 23
   $bandwidthRateLimitInterval.EndMinuteOfHour = 59
   $bandwidthRateLimitInterval.DaysOfWeek = 0,1,2,3,4,5,6
   $bandwidthRateLimitInterval.AverageUploadRateLimitInBitsPerSec =
$UploadBandwidthRate

   #Update Bandwidth Rate Limits
   Update-SGBandwidthRateLimitSchedule -GatewayARN $gatewayARN `
                                       -BandwidthRateLimitInterval
@($bandwidthRateLimitInterval)

   $schedule =  Get-SGBandwidthRateLimitSchedule -GatewayARN $gatewayARN

   Write-Output("`nGateway: " + $gatewayARN);
   Write-Output("`nNew bandwidth throttle schedule: " +
$schedule.BandwidthRateLimitIntervals.AverageUploadRateLimitInBitsPerSec)
```

Como gerenciar atualizações de gateway por meio do console do AWS Storage Gateway

O Storage Gateway lança periodicamente importantes atualizações de software para o gateway. Você pode aplicar as atualizações manualmente no Console de Gerenciamento do Storage Gateway ou aguardar até que as atualizações sejam aplicadas automaticamente durante a manutenção programada. Embora o Storage Gateway verifique se há atualizações a cada minuto, ele somente entrará em manutenção e será reiniciado se de fato houver atualizações.

As versões do software Gateway incluem regularmente atualizações do sistema operacional e patches de segurança que foram validados porAWS. Essas atualizações geralmente são lançadas a cada seis meses e são aplicadas como parte do processo normal de atualização do gateway durante as janelas de manutenção agendadas.

> **Note**
>
> Você deve tratar o dispositivo Storage Gateway como um dispositivo incorporado gerenciado e não deve tentar acessar ou modificar sua instalação de forma alguma. Tentar instalar ou atualizar quaisquer pacotes de software usando métodos diferentes do mecanismo de atualização de gateway normal (por exemplo, ferramentas SSM ou hipervisor) pode causar mau funcionamento do gateway.

Antes de qualquer atualização ser aplicada ao gateway,AWSO notifica por meio de uma mensagem no console do Storage Gateway e em seuAWS Health Dashboard. Para obter mais informações, consulte AWS Health Dashboard. A VM não será reinicializada, mas o gateway ficará indisponível por um curto período durante a atualização e a reinicialização.

Ao implantar e ativar seu gateway, uma programação de manutenção semanal padrão é definida. Você pode modificar a programação da manutenção a qualquer momento. Quando há atualizações disponíveis, a guia Details (Detalhes) exibe uma mensagem de manutenção. Você pode ver a data e a hora em que a última atualização bem-sucedida foi aplicada ao gateway na guia Details.

Para modificar a programação da manutenção

1. Abra o console do Storage Gateway emhttps://console.aws.amazon.com/storagegateway/home.
2. No menu de navegação, escolha Gateways e selecione o gateway para o qual você deseja modificar a programação de atualizações.
3. Em Actions (Ações), escolha Edit maintenance window (Editar janela de manutenção) para marcar a caixa de diálogo Edit maintenance start time (Editar hora de início da manutenção).
4. Em Schedule (Programação), escolha Weekly (Semanal) ou Monthly (Mensal) para programar as atualizações.
5. Se você escolher Weekly (Semanal), modifique os valores para Day of the week (Dia da semana) e Time (Horário).

   Se você escolher Monthly (Mensal), modifique os valores para Day of the month (Dia do mês) e Time (Horário). Se você escolher essa opção e receber um erro, significa que o gateway está em uma versão mais antiga e ainda não foi atualizado para uma versão mais recente.

> **Note**
>
> O valor máximo que pode ser definido para o dia do mês é 28. Se 28 for selecionado, a hora de início da manutenção será no 28º dia de cada mês.

O horário de início da manutenção será exibido na guia Details (Detalhes) do gateway na próxima vez que você abrir a guia Details (Detalhes).

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.

Tópicos

- Executar tarefas no console local da VM (gateway de arquivo)
- Executando tarefas no console local do Amazon EC2 (gateway de arquivos)
- Acessar o console local do gateway
- Como configurar adaptadores de rede para seu gateway

Executar tarefas no console local da VM (gateway de arquivo)

Para um gateway de arquivo implantado localmente, você pode executar as seguintes tarefas de manutenção usando o console local do host da VM. Essas tarefas são comuns aos hipervisores de VMware, Microsoft Hyper-V e Linux Kernel-based Virtual Machine (KVM).

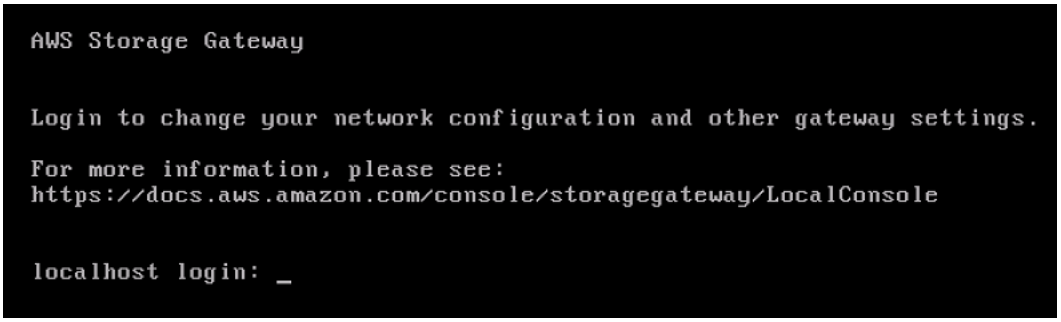
Tópicos

- Como fazer login no console local do gateway de arquivo
- Configurar um proxy HTTP
- Definindo as configurações de rede do gateway
- Testando a conectividade de rede do gateway
- Visualizando o status do recurso do sistema de gateway
- Configurar um servidor NTP (Network Time Protocol) para seu gateway

- Executando comandos de gateway de armazenamento no console local
- Configurar adaptadores de rede para seu gateway

Como fazer login no console local do gateway de arquivo

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, use o nome de usuário padrão e a senha para fazer login. Essas credenciais de login padrão concedem acesso aos menus em que você pode definir configurações de rede do gateway e alterar a senha no console local.AWS Storage GatewayO permite que você defina sua própria senha no console do Storage Gateway, em vez de alterar a senha no console local. Você não precisa saber qual é a senha padrão para definir uma nova senha. Para obter mais informações, consulte Como fazer login no console local do gateway de arquivo.



Para fazer login no console local do gateway

- 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. Isso é feito ao executar o comando `passwd` no menu do console local (item 6 no menu principal). Para obter informações sobre como executar o comando, consulte Executando comandos de gateway de armazenamento no console local. Você também pode definir a senha no console do Storage Gateway. Para obter mais informações, consulte Como fazer login no console local do gateway de arquivo.

Definindo a senha do console local no console do Storage Gateway

Ao fazer login pela primeira vez no console local, faça login na VM com as credenciais padrão. Para todos os tipos de gateways, você usa credenciais padrão. O nome de usuário é `admin` e a senha é `password`.

Recomendamos que você sempre definir 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 Storage Gateway emhttps://console.aws.amazon.com/storagegateway/home.
2. No painel de navegação, selecione Gateways (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 (Definir senha do console local), digite uma nova senha, confirme a senha e escolha Save (Salvar).

   Sua 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.

Configurar um proxy HTTP

Os gateways de arquivos suportam a configuração de um proxy HTTP.

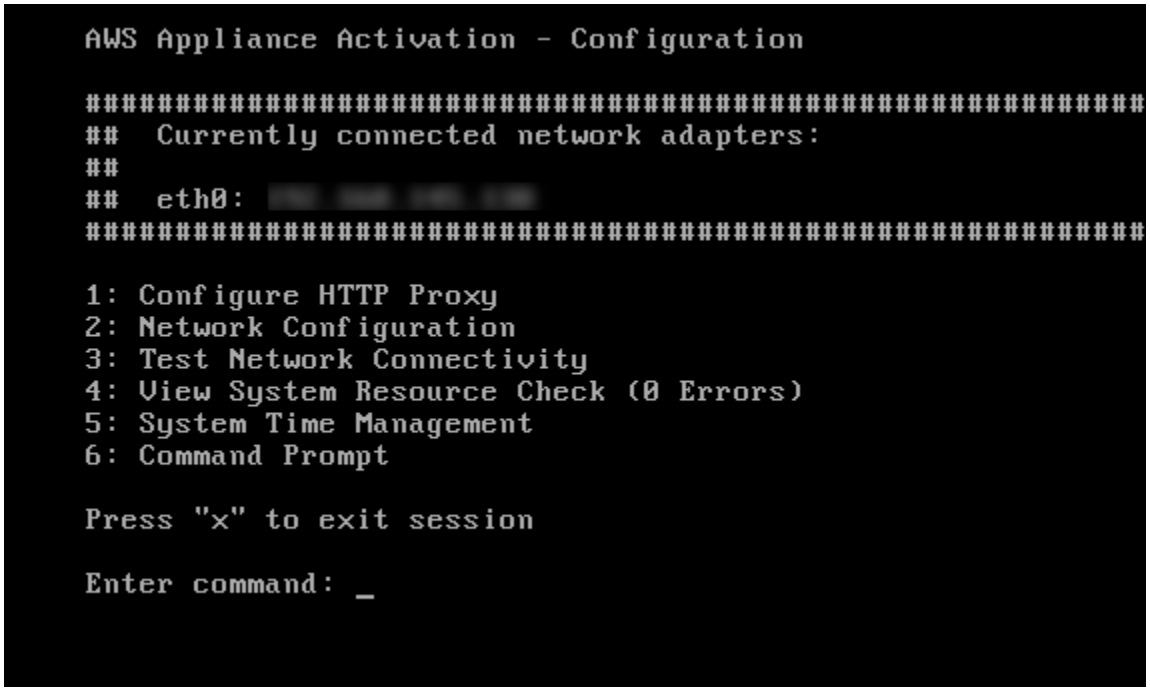
> **Note**
>
> Os gateways de arquivos suportam a somente a configuração de um proxy HTTP.

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

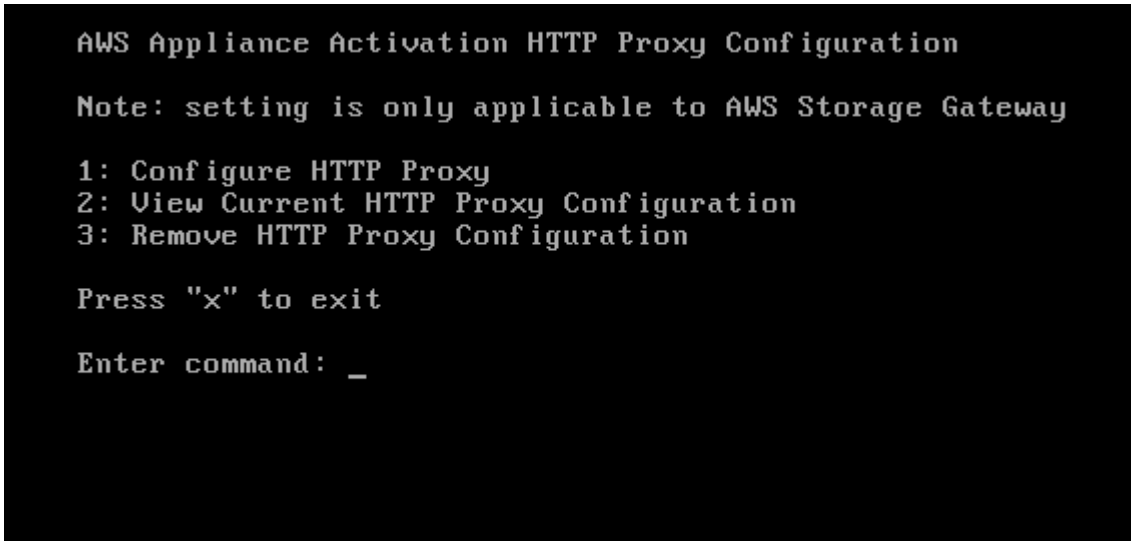
endereço IP e um número de porta para o host que executa o proxy. Depois que você faz isso, o Storage Gateway roteia todosAWSO tráfego de endpoint por meio do servidor de proxy. As comunicações entre o gateway e os endpoints são criptografadas, mesmo quando se usa o proxy HTTP. Para obter informações sobre os requisitos de rede para seu gateway, consulte Requisitos de rede e firewall.

Para configurar um proxy HTTP para um gateway de arquivo

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. NoAWSAtivação do equipamento - Configuraçãomenu principal, insira**1**Para começar a configurar o proxy HTTP.



3. No menu HTTP Proxy Configuration (Configuração de proxy HTTP), digite **1** e forneça o nome do host para o servidor de proxy HTTP.



Você pode configurar outras configurações de HTTP neste menu, como mostrado a seguir.

Para	Faça o seguinte
Configurar um proxy HTTP	Digite **1**. Você precisa fornecer um nome de host e a porta para concluir a configuração.
Visualizar a configuração de proxy HTTP atual	Digite **2**. Se não houver nenhum proxy HTTP 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 HTTP	Digite **3**. A mensagem `HTTP Proxy Configuration Removed` é exibida.

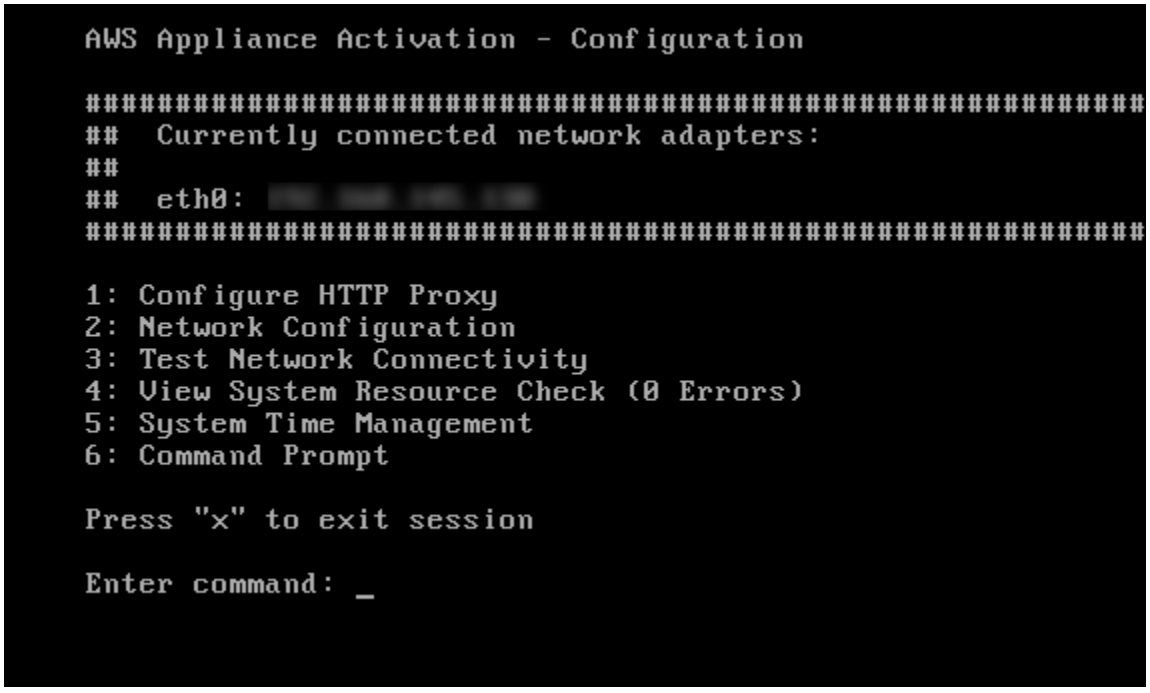
4. Reinicie a VM para aplicar suas configurações de HTTP.

Definindo as configurações de rede do gateway

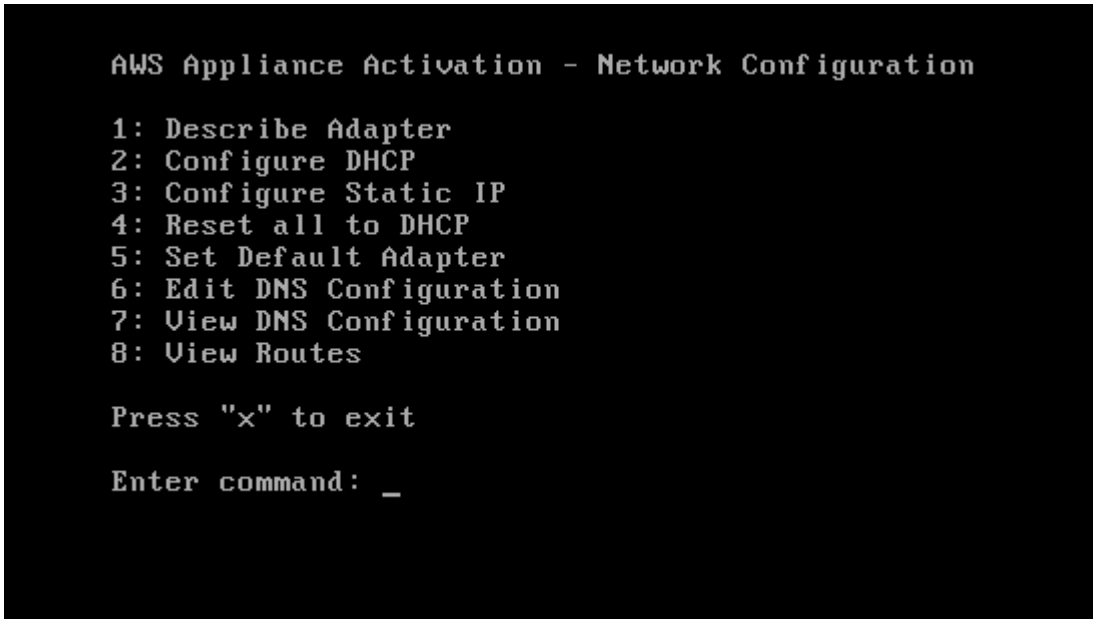
A configuração de rede padrão para o gateway é Dynamic Host Configuration Protocol (DHCP). Com o DHCP, um endereço IP é atribuído automaticamente ao seu gateway. Em alguns casos, pode ser necessário atribuir manualmente o IP do gateway como endereço IP estático, tal como descrito a seguir.

Para configurar seu gateway para usar endereços IP estáticos

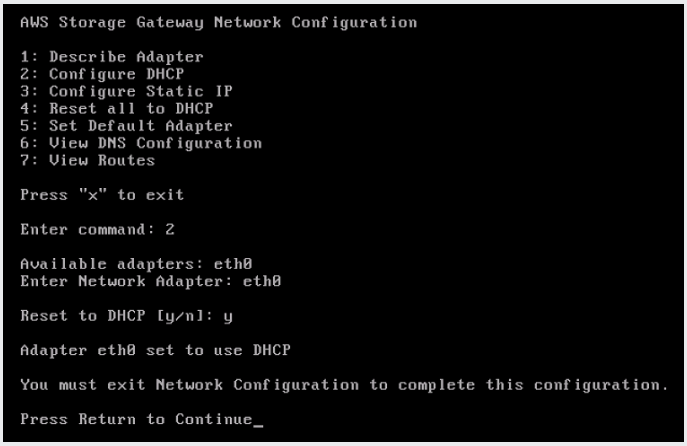
1. Faça login no console local do seu gateway:
   - Para obter mais informações sobre o registro em log no console local do VMware ESXi, consulte Acesso ao console local do gateway com o VMware ESXi.
   - Para obter mais informações sobre o registro em log no console local do Microsoft Hyper-V, consulte 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. NoAWSAtivação do equipamento - Configuraçãomenu principal, insira**2**para começar a configurar sua rede.



3. No menu Network Configuration (Configuração de rede), escolha uma das opções a seguir.


AWS Appliance Activation - Network Configuration
1: Describe Adapter
2: Configure DHCP
3: Configure Static IP
4: Reset all to DHCP
5: Set Default Adapter
6: Edit DNS Configuration
7: View DNS Configuration
8: View Routes
Press "x" to exit
Enter command: _

Para	Faça o seguinte
Obter informações sobre seu adaptador de rede	Digite **1**. Uma lista de nomes de adaptador é exibida e você é então solicitado a digitar um nome de adaptador — por exemplo,**`eth0`**. Se o adaptador especificado estiver em uso, serão exibidas as seguintes informações sobre o adaptador: • O endereço de controle de acesso de mídia (MAC) • IP address • Máscara de rede • Endereço IP do gateway • Status de DHCP habilitado Você pode usar o mesmo nome de adaptador ao configurar um endereço IP estático (opção 3), tal como você define o adaptador de rota padrão do gateway (opção 5).

Para	Faça o seguinte
Configurar o DHCP	Digite **2**. Você é solicitado a configurar a interface de rede para usar o DHCP. 

Para	Faça o seguinte
Configurar um endereço IP estático para gateway	Digite **3**. Você é solicitado a digitar as seguintes informações para configurar um endereço IP estático: • Nome do adaptador de rede • IP address • Máscara de rede • Endereço de gateway padrão • Endereço Domain Name Service (DNS) • Endereço DNS secundário **Important** Se seu 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 obter mais informaçõ es, consulte Desligar a VM do gateway. Se seu gateway usar mais de uma interface de rede, você deverá definir todas as interfaces habilitadas para usar DHCP ou endereços IP estáticos.

Para	Faça o seguinte
	Por exemplo, suponha que a VM do gateway usa duas interfaces configuradas como DHCP. Se você definir posteriormente uma interface para um endereço IP estático, a outra interface será desativada. Para habilitar a interface, nesse caso, você deve configurá-la para um endereço IP estático. 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.
Redefinir todas as configurações de rede do gateway para DHCP	Digite **4**. Todas as interfaces de rede são definidas para usar DHCP. **Important** Se seu 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 obter mais informaçõ es, consulte Desligar a VM do gateway.
Configurar o adaptador de rota padrão do gateway	Digite **5**. Os adaptadores disponíveis para seu gateway são exibidos e você é solicitado a escolher um dos adaptadores — por exemplo,**eth0**.

Para	Faça o seguinte
Editar a configuração de DNS do seu gateway	Digite **6**. Os adaptadores disponíveis dos servidores de DNS primário e secundário são exibidos. O novo endereço IP será solicitado.
Visualizar a configuração de DNS do gateway	Digite **7**. Os adaptadores disponíveis dos servidores de DNS primário e secundário são exibidos. **Note** Para algumas versões do hipervisor VMware, você pode editar a configuração do adaptador neste menu.
Visualizar tabelas de roteamento	Digite **8**. A rota padrão de seu gateway é exibida.

Testando a conectividade de rede do gateway

Você pode usar o console local do gateway para testar a conectividade de rede. Este teste pode ser útil quando estiver solucionando problemas de rede em seu gateway.

Para testar a conectividade de rede do gateway

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. From theAWSAtivação do equipamento - Configuraçãomenu principal, insira o numeral correspondente para selecionarConectividade de rede de teste.

   Se o gateway já tiver sido ativado, o teste de conectividade começa imediatamente. Para gateways que ainda não foram ativados, você deve especificar o tipo de endpoint eRegião da AWSComo descrito nas etapas a seguir.

3. Se o gateway ainda não estiver ativado, insira o numeral correspondente para selecionar o tipo de endpoint para o gateway.
4. Se você selecionou o tipo de endpoint público, insira o numeral correspondente para selecionar oRegião da AWSQue você deseja testar. Para suporteRegiões da AWSe uma lista deAWSendpoints de serviço que você pode usar com o Storage Gateway, consulteAWS Storage GatewayEndpoints e cotas donoAWSReferência geral.

À medida que o teste avança, cada ponto de extremidade exibe[PASSOU]ou[FAILED], indicando o status da conexão da seguinte forma:

Message	Descrição
[PASSED]	Storage Gateway tem conectividade de rede.
[FAILED]	O Storage Gateway não tem conectividade de rede.

Visualizando o status do recurso do sistema de gateway

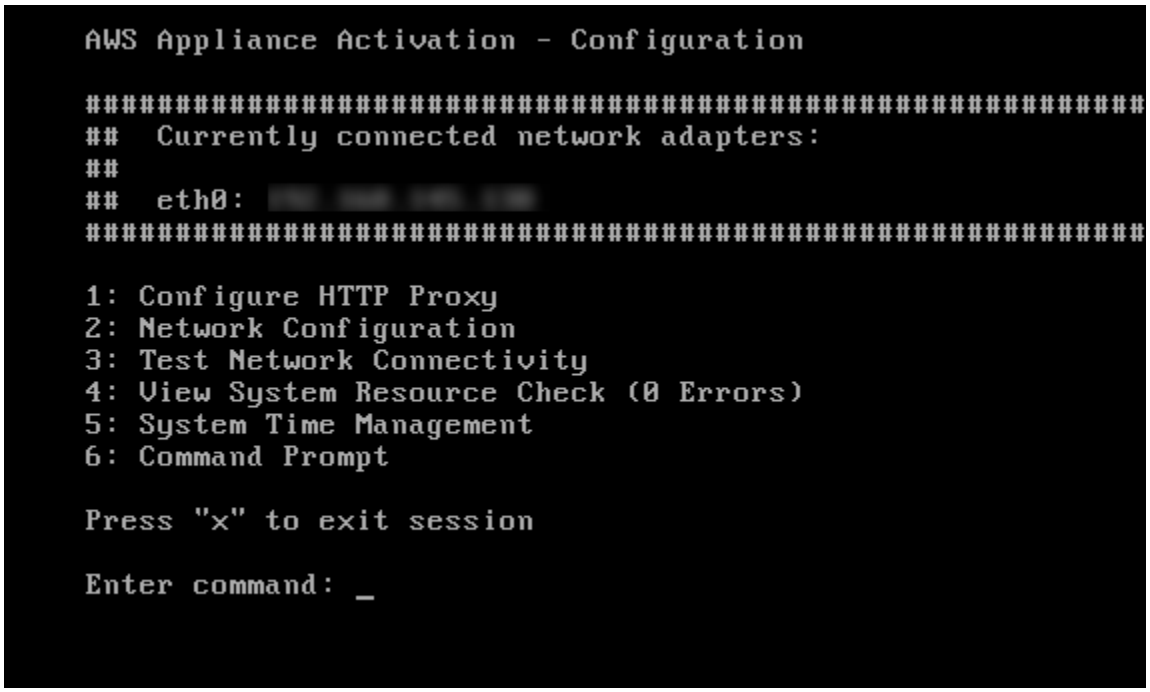
Quando o seu gateway é iniciado, ele verifica os núcleos da CPU virtual, o tamanho do volume raiz e a RAM. Ele determina se esses recursos do sistema são suficientes para seu gateway funcionar corretamente. Você pode visualizar os resultados dessa verificação no console local do gateway.

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. NoAWSAtivação do equipamento - Configuraçãomenu principal, insira**4**Para visualizar os resultados da verificação de recursos do sistema.



O console exibe uma mensagem [OK], [WARNING] ou [FAIL] para cada recurso, tal como descrito na tabela a seguir.

Message	Descrição
[OK]	O recurso passou na verificação de recursos do sistema.
[WARNING]	O recurso não atende aos requisitos recomendados, mas seu gateway poderá continuar funcionando. Seu Storage Gateway

Message	Descrição
	exibe uma mensagem que descreve os resultados da verificação de recursos.
[FAIL]	O recurso não atende aos requisitos mínimos. Seu gateway talvez não funcione corretame nte. Seu Storage Gateway exibe uma mensagem que descreve os resultados da verificação de recursos.

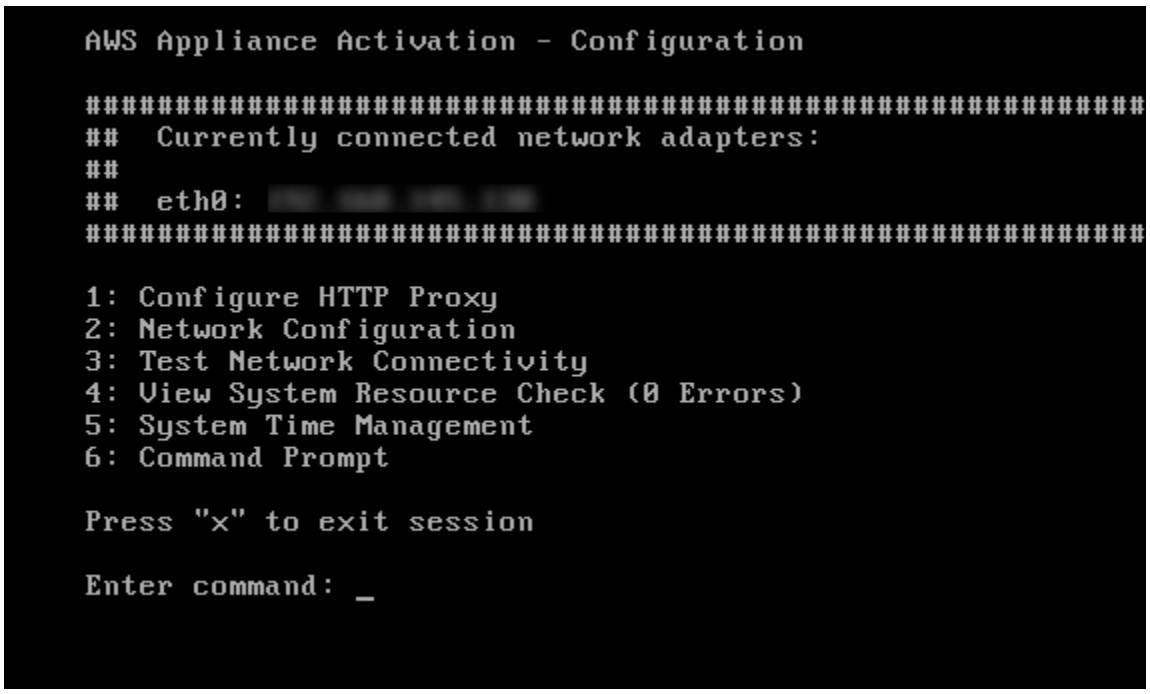
O console também exibe o número de erros e avisos ao lado da opção de menu de verificação de recursos.

Configurar um servidor NTP (Network Time Protocol) para seu gateway

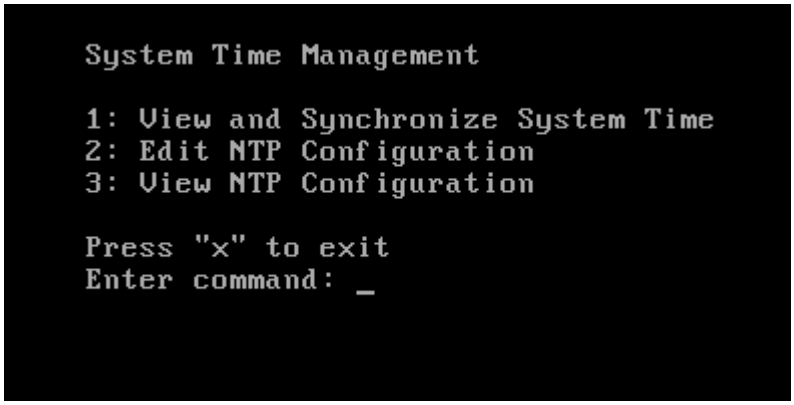
Você pode visualizar e editar as configurações do servidor de protocolo de horário da rede (NTP) e sincronizar o horário da VM em seu gateway com o host do hipervisor para evitar desvios de horário.

Para gerenciar o horário do sistema

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. NoAWSAtivação do equipamento - Configuraçãomenu principal, insira**5**para gerenciar o tempo do sistema.



3. No menu System Time Management (Gestão do horário do sistema) escolha uma das seguintes opções.



Para	Faça o seguinte
Exibir e sincronizar o horário da sua VM com o horário do servidor NTP.	Digite **1**. O horário atual da sua VM é exibida. Seu gateway de arquivo determina a diferença de horário da VM do gateway, e o horário do seu servidor NTP solicita que você sincronize o horário da VM com o do NTP.

Para	Faça o seguinte
	Assim que seu gateway estiver implantado e em execução, em algumas situações o horário da VM do gateway pode apresentar desvios. Por exemplo, imagine que há alguma interrupção prolongada na rede e o host do hipervisor e o gateway não recebem atualizações de horário. Neste caso, 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 obter 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 obter mais informações, consulte Como sincronizar o horário da VM do gateway. Para um gateway implantado na KVM, é possível verificar e sincronizar o tempo da VM usando a interface de linha de comando `virsh` para a KVM.

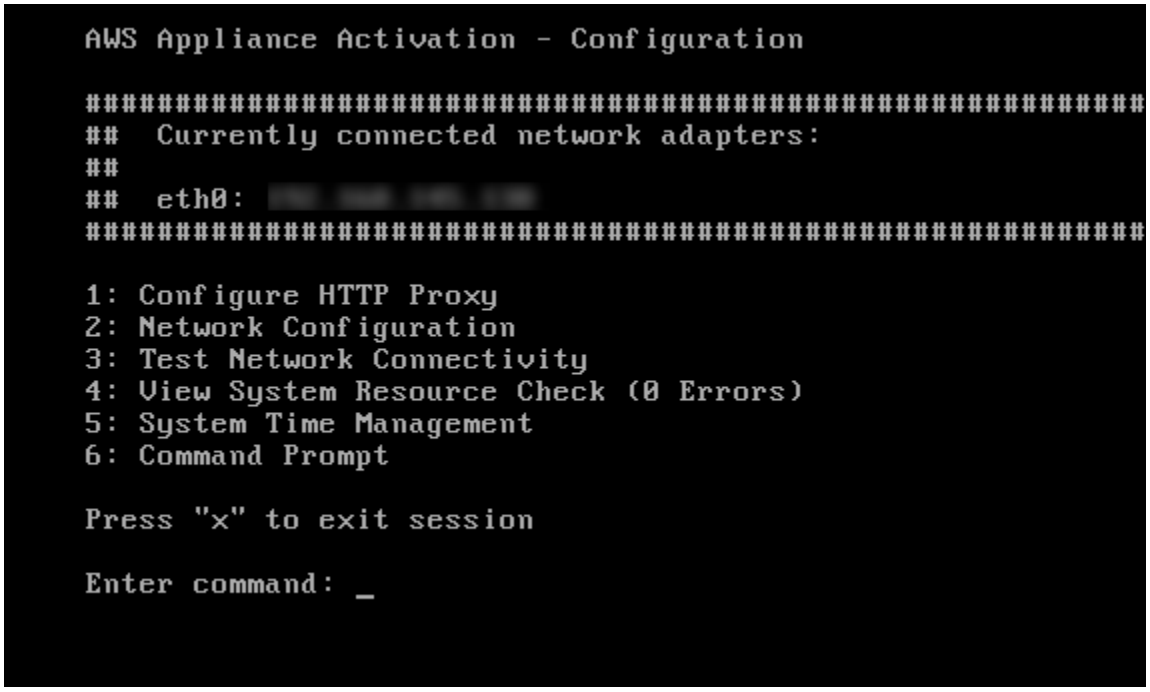
Para	Faça o seguinte
Editar a configuração do seu servidor NTP	Digite **2**. Você é solicitado a fornecer um servidor NTP preferencial e um secundário.
Exibir a configuração do seu servidor NTP	Digite **3**. A configuração do seu servidor NTP é exibida.

Executando comandos de gateway de armazenamento 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, entrar em contato com o Support da Amazon Web Services, e mais.

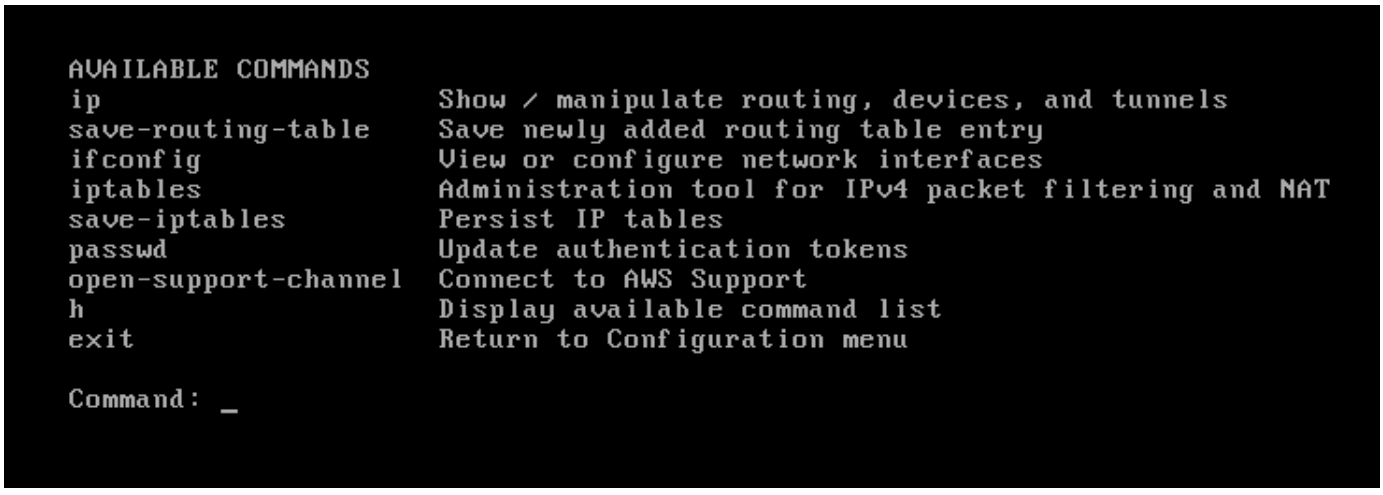
Para executar um comando de configuração ou diagnóstico

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. NoAWSAtivação do equipamento - Configuraçãomenu principal, insira**6**peloPrompt de comando.



3. NoAWSAtivação do equipamento - Prompt de comandoconsole, insira**h**e, em seguida, pressione o botãoRetornechave.

   O console exibe o menu AVAILABLE COMMANDS (COMANDOS DISPONÍVEIS) com a função dos comandos, conforme mostrado na captura de tela a seguir.



4. No prompt de comando, insira o comando que você quer usar e seguir as instruções.

Para obter informações a respeito de um comando, digite o nome do comando no prompt do comando.

Configurar adaptadores de rede para seu gateway

Por padrão, o Storage Gateway é configurado para usar o tipo de adaptador de rede E1000, mas você pode reconfigurar seu gateway para usar o adaptador de rede VMXNET3 (10 GbE). Você também pode 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

Configurar seu 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 adaptador VMXNET3 (10 GbE). Para obter mais informações sobre esse adaptador, consulte o site da VMware.

Para hosts de hipervisor KVM, o Storage Gateway oferece suporte para o uso de `virtio` drivers de dispositivos de rede. O uso do tipo de adaptador de rede E1000 para hosts da KVM não é compatível.

> **Important**
>
> Para selecionar o VMXNET3, o sistema operacional convidado deve ser Other Linux64 (Outro Linux64).

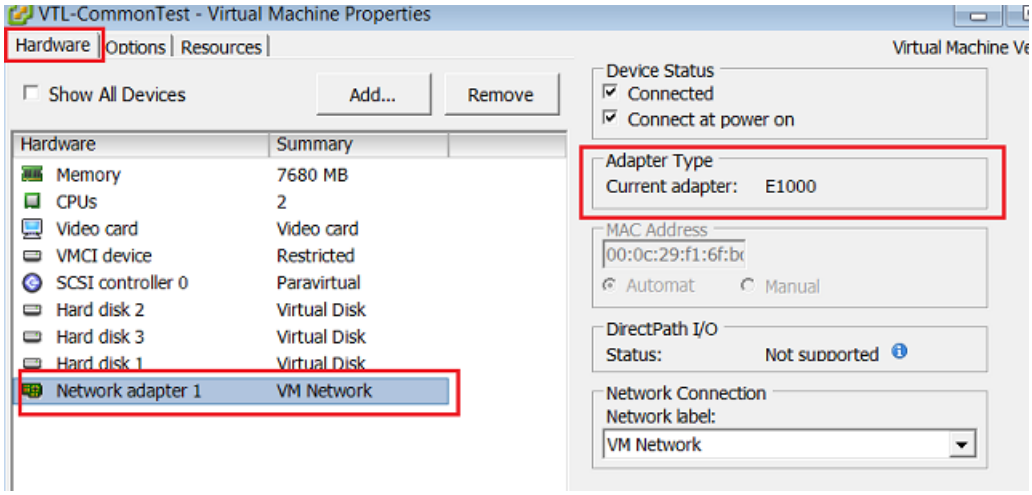
Veja a seguir as etapas executadas para configurar seu gateway para usar o adaptador VMXNET3:

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 Enter (Adaptador). Esse adaptador é substituído 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.

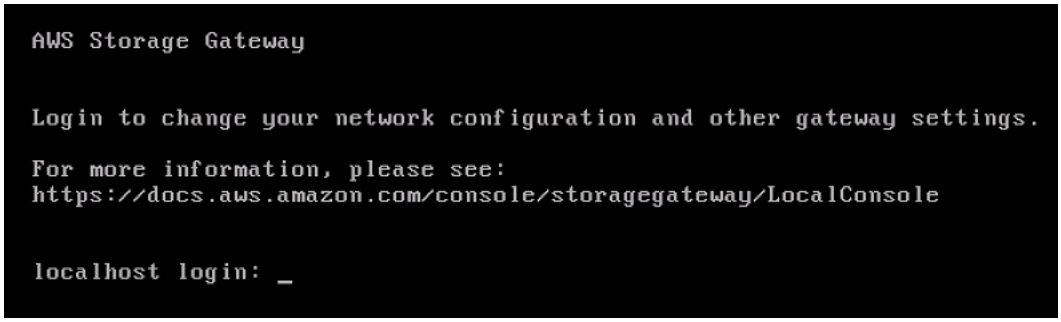
> **Note**
>
> Embora você possa usar simultaneamente os adaptadores de rede E1000 e VMXNET3 em seu gateway, isso não é recomendável porque pode provocar problemas de rede.

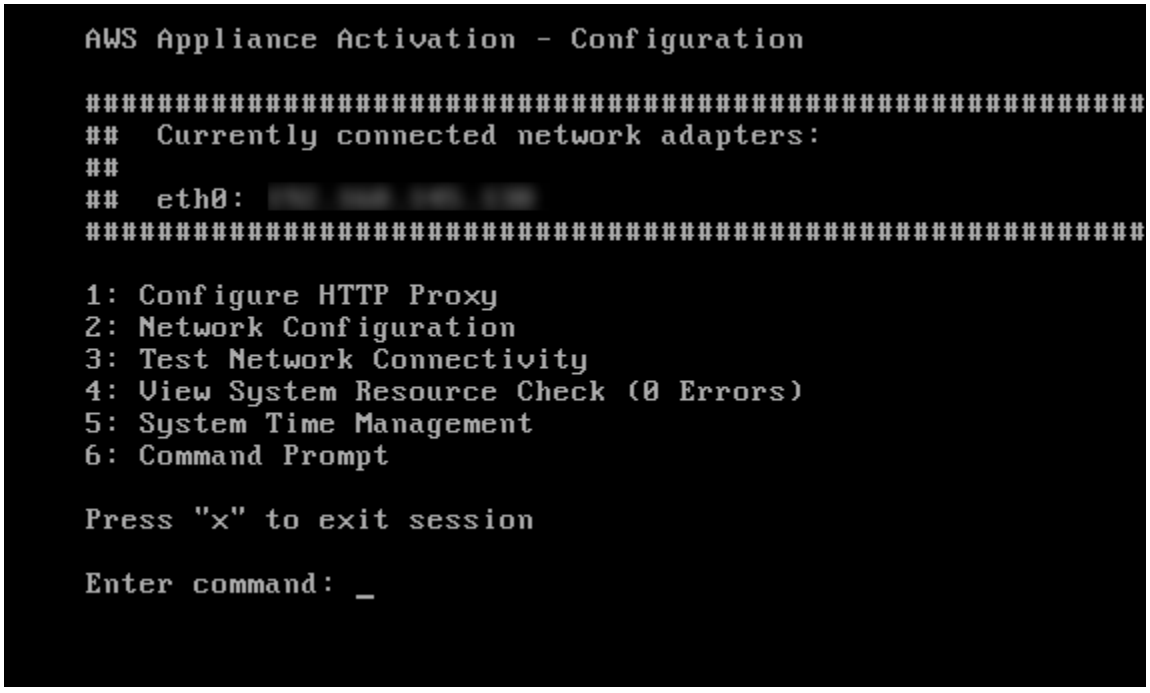
5. Escolha Add para abrir o assistente Add Hardware.
6. Escolha Ethernet Adapter e em seguida Next.
7. No assistente Network Enter, selecione **`VMXNET3`** para Adapter Enter (Adaptador) e escolha Next (Próximo).
8. No assistente Virtual Machine Properties, verifique se na seção Adapter Enter (Adaptador) o campo Current adapter (Adaptador atual) está definido como VMXNET3 e depois selecione OK (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.

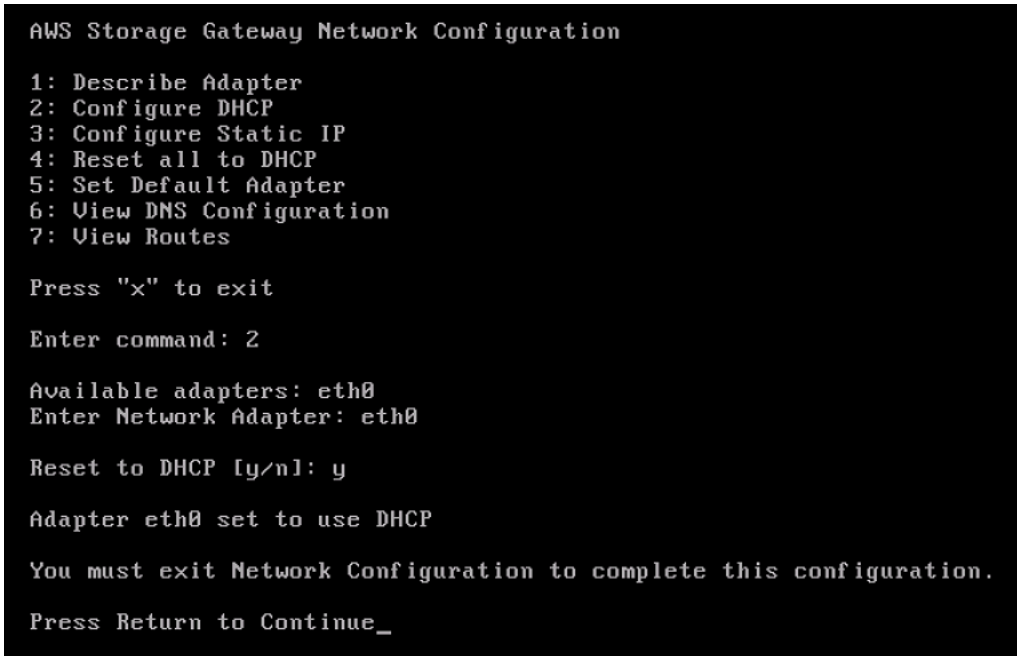
Para configurar o adaptador para a rede

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 do gateway de arquivo.





2. No prompt, digite **2** para selecionar Network Configuration (Configuração de rede) e pressione **Enter** para abrir o menu de configuração de rede.
3. No prompt, digite **4** para selecionar Reset all to DHCP (Redefinir tudo para DHCP) e digite **y** (para "sim") no prompt para redefinir todos os adaptadores para usar o protocolo de configuração dinâmica de hosts (DHCP). Todos os adaptadores disponíveis são configurados para usar DHCP.



Se seu gateway já estiver ativado, você deve encerrá-lo e reiniciá-lo no Console de Gerenciamento do Storage Gateway. 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 Testando a conectividade de rede do gateway.

Executando tarefas no console local do Amazon EC2 (gateway de arquivos)

Algumas tarefas de manutenção exigem que você faça login no console local ao executar um gateway implantado em uma Instância do Amazon EC2. Nesta seção, você pode encontrar informações sobre como fazer login no console local e executar tarefas de manutenção.

Tópicos

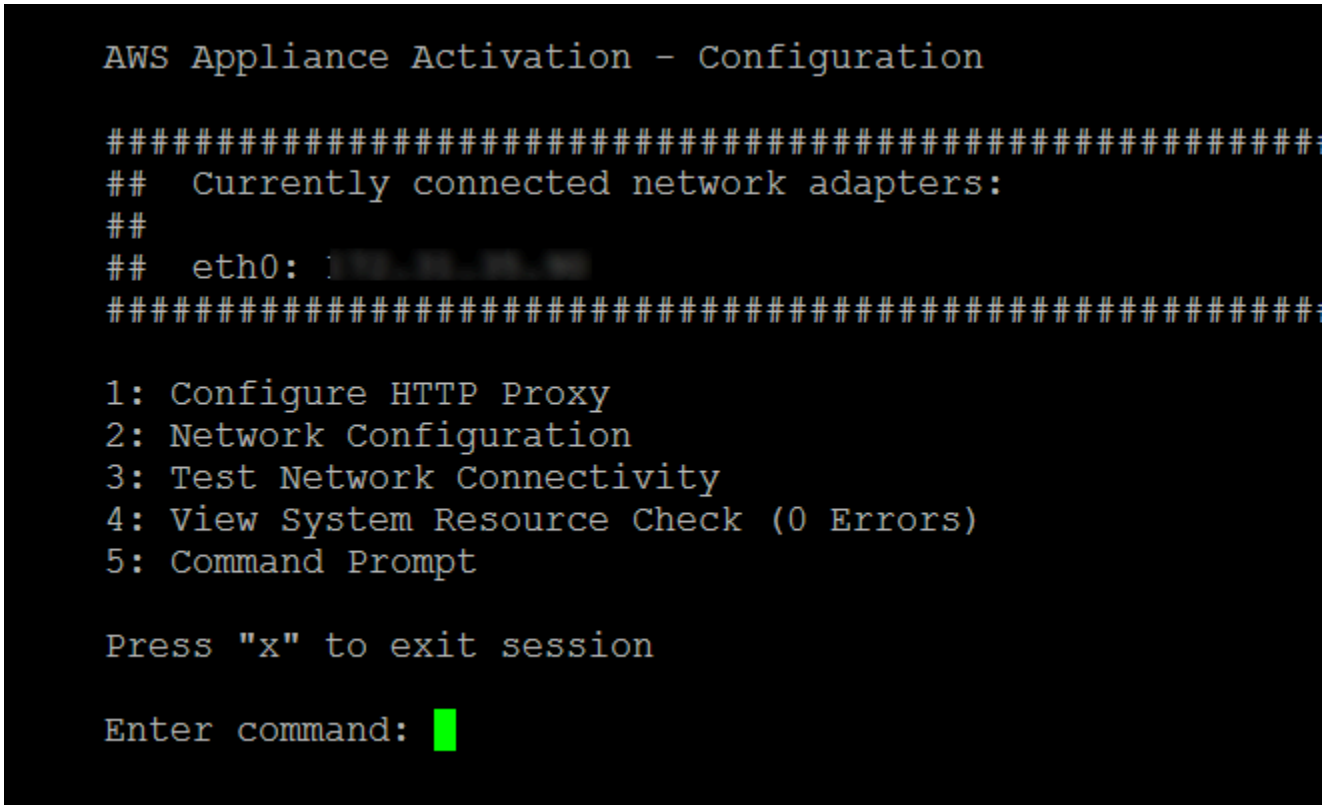
- Fazer login no console local do gateway Amazon EC2
- Roteamento do gateway implantado no EC2 por meio de um proxy HTTP
- Definindo as configurações de rede do gateway
- Testando a conectividade de rede do gateway
- Visualizando o status do recurso do sistema de gateway
- Executando comandos do Storage Gateway no console local

Fazer login no console local do gateway Amazon EC2

Você pode se conectar à sua Instância do Amazon EC2 usando um cliente Secure Shell (SSH). Para obter informações detalhadas, consulteConecte-se à sua instânciaGuia do usuário do Amazon EC2. Para se conectar dessa forma, você precisará do par de chaves SSH que você especificou ao executar sua instância. Para obter mais informações sobre pares de chaves do Amazon EC2, consultePares de chave do Amazon EC2Guia 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, verá oAWSAtivação do equipamento - ConfiguraçãoNo menu principal, como mostrado na captura de tela a seguir.



Para saber mais sobre isso	Consulte este tópico
Configurar um proxy HTTP para seu gateway	Roteamento do gateway implantado no EC2 por meio de um proxy HTTP

Para saber mais sobre isso	Consulte este tópico
Configurar configurações de rede para seu gateway	Testando a conectividade de rede do gateway
Testar a conectividade de rede	Testando a conectividade de rede do gateway
Exibir uma verificação de recursos do sistema	Fazer login no console local do gateway Amazon EC2.
Executar comandos do console do Storage Gateway	Executando comandos do Storage Gateway no console local

Para encerrar o gateway, digite **0**.

Para sair da sessão de configuração, digite **x** para sair do menu.

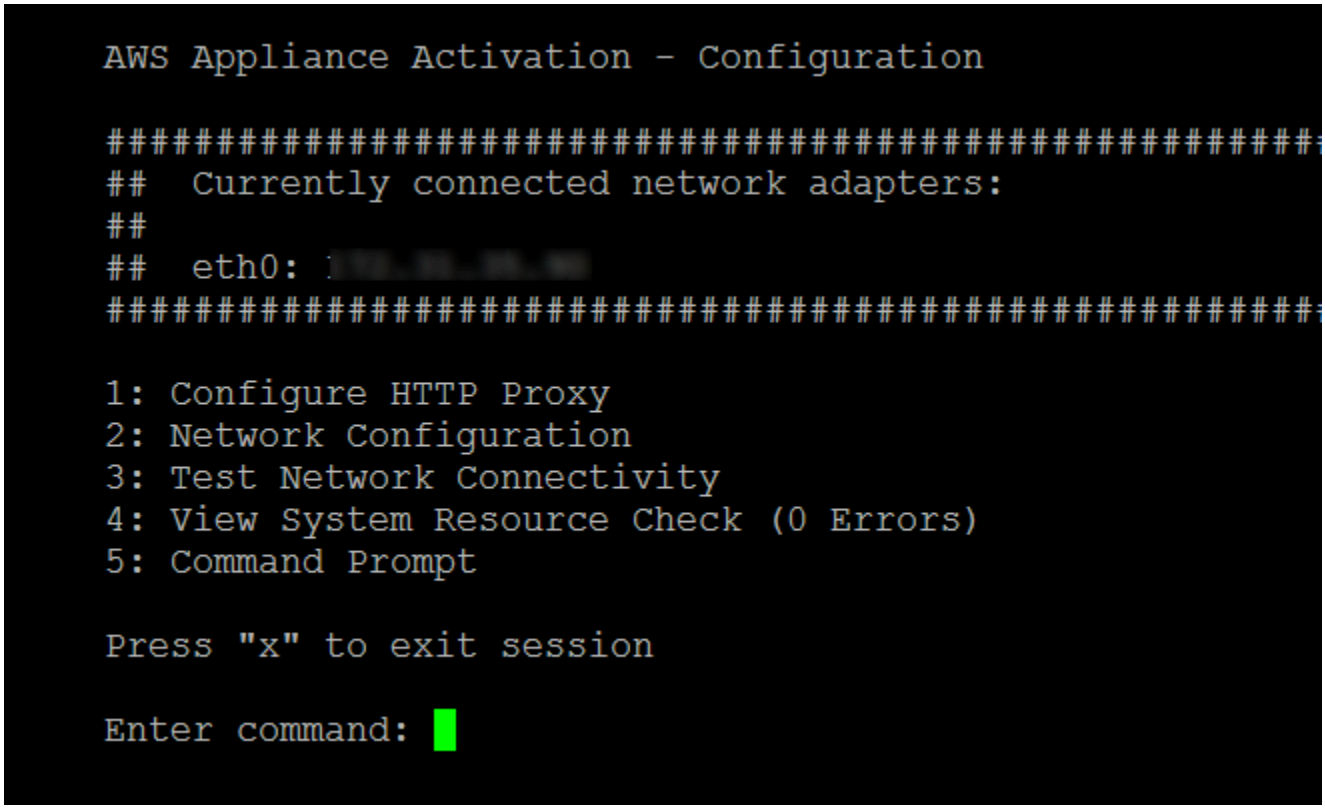
Roteamento do gateway implantado no EC2 por meio de um proxy HTTP

O Storage Gateway é compatível com a configuração de um proxy Secure Socket versão 5 (SOCKS5) entre o gateway implantado no Amazon EC2 eAWS.

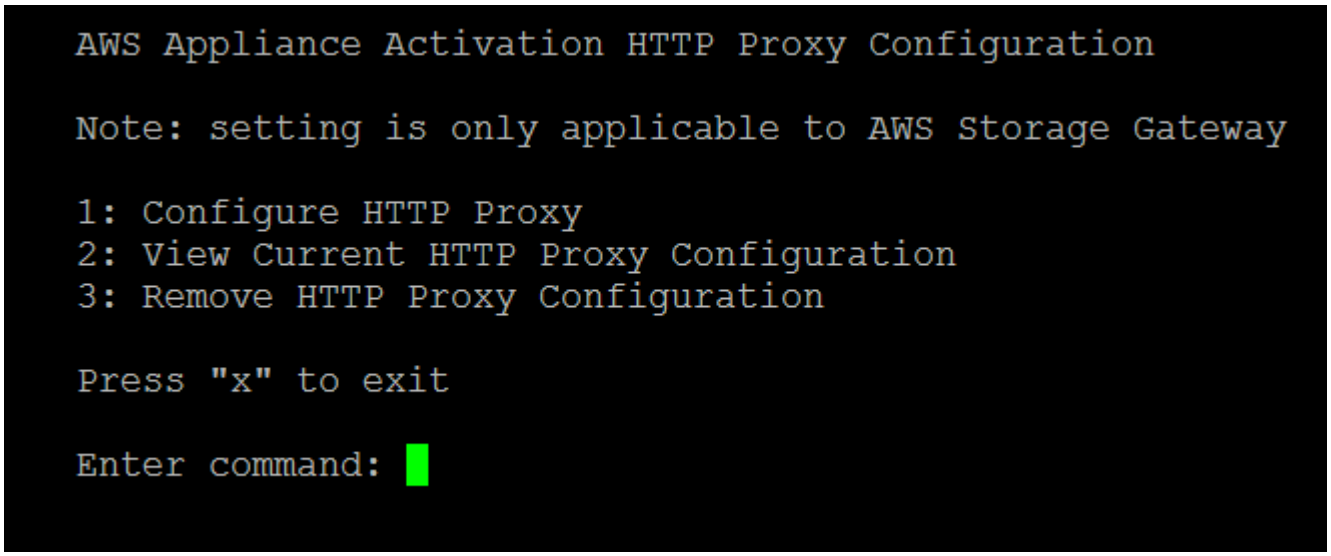
Se seu gateway precisar usar um servidor de proxy para se comunicar com a internet, será preciso definir as configurações de proxy HTTP para esse gateway. Para fazer isso, especifique um endereço IP e um número de porta para o host que executa o proxy. Depois que você faz isso, o Storage Gateway roteia todosAWSO tráfego de endpoint por meio do servidor de 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 Fazer login no console local do gateway Amazon EC2.
2. NoAWSAtivação do equipamento - Configuraçãomenu principal, insira**1**Para começar a configurar o proxy HTTP.



3. Escolha uma das seguintes opções noAWSAtivação do equipamento - ConfiguraçãoConfiguração de proxy HTTPmenu.



Para	Faça o seguinte
Configurar um proxy HTTP	Digite **1**.

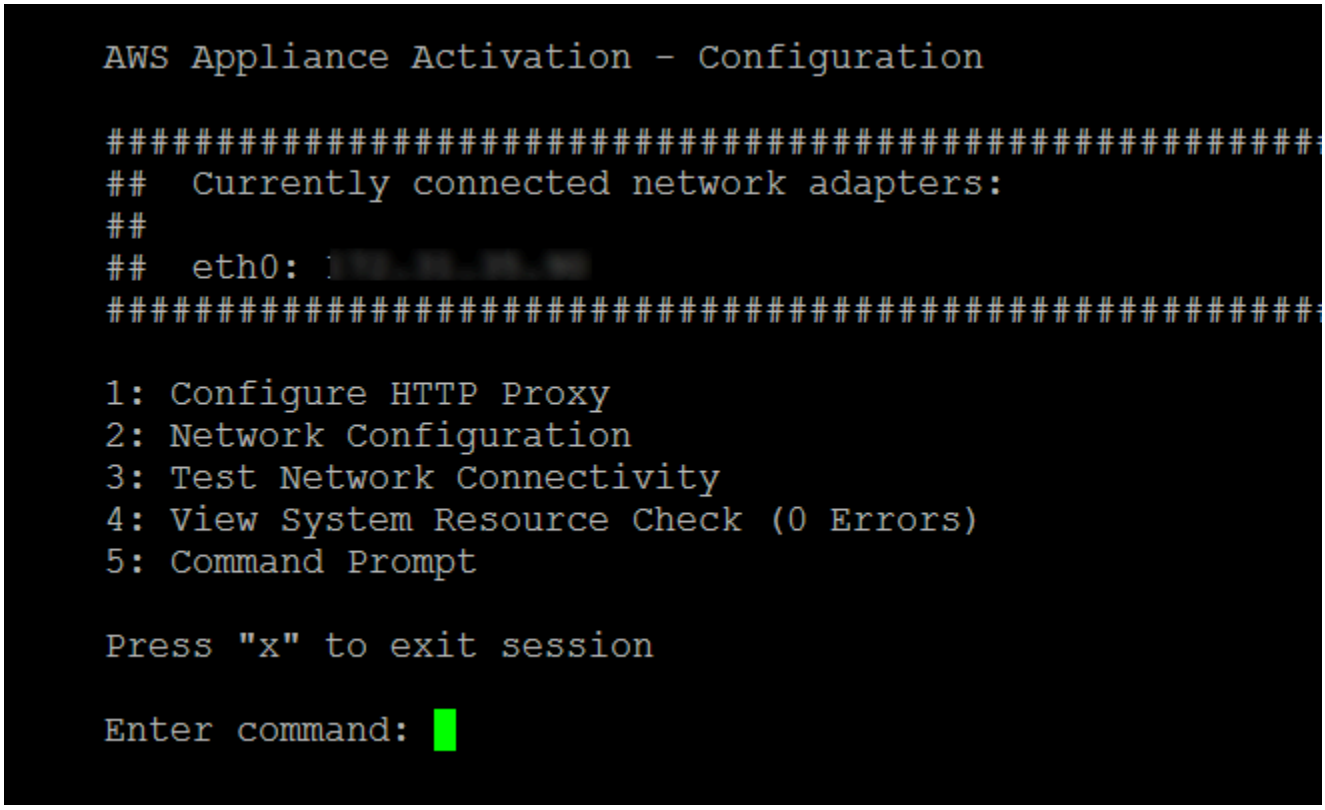
Para	Faça o seguinte
	Você precisa fornecer um nome de host e a porta para concluir a configuração.
Visualizar a configuração de proxy HTTP atual	Digite **2**. Se não houver nenhum proxy HTTP configurado, a mensagem `HTTP Proxy not configured` é exibida. Se houver um proxy HTTP configurado, o nome do host e a porta do proxy serão exibidos.
Remover uma configuração de proxy HTTP	Digite **3**. A mensagem `HTTP Proxy Configuration Removed` é exibida.

Definindo as configurações de rede do gateway

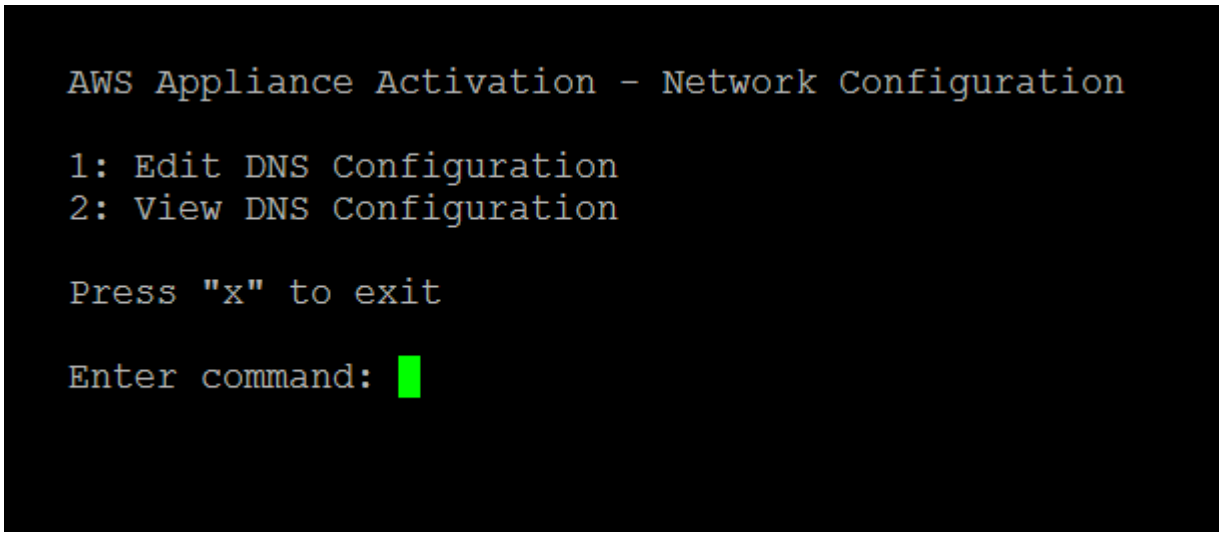
Você pode visualizar e ajustar as configurações do seu servidor de nome de domínio (DNS) através do console local.

Para configurar seu gateway para usar endereços IP estáticos

1. Faça login no console local do gateway. Para obter instruções, consulte Fazer login no console local do gateway Amazon EC2.
2. NoAWSAtivação do equipamento - Configuraçãomenu principal, insira**2**para começar a configurar seu servidor DNS.



3. No menu Network Configuration (Configuração de rede), escolha uma das opções a seguir.



Para	Faça o seguinte
Editar a configuração de DNS do seu gateway	Digite **1**.

Para	Faça o seguinte
	Os adaptadores disponíveis dos servidores de DNS primário e secundário são exibidos. O novo endereço IP será solicitado.
Visualizar a configuração de DNS do gateway	Digite **2**. Os adaptadores disponíveis dos servidores de DNS primário e secundário são exibidos.

Testando a conectividade de rede do gateway

Você pode usar o console local do gateway para testar a conectividade de rede. 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 Fazer login no console local do gateway Amazon EC2.
2. From theAWSAtivação do equipamento - Configuraçãomenu principal, insira o numeral correspondente para selecionarConectividade de rede de teste.

   Se o gateway já tiver sido ativado, o teste de conectividade começa imediatamente. Para gateways que ainda não foram ativados, você deve especificar o tipo de endpoint eRegião da AWSComo descrito nas etapas a seguir.
3. Se o gateway ainda não estiver ativado, insira o numeral correspondente para selecionar o tipo de endpoint para o gateway.
4. Se você selecionou o tipo de endpoint público, insira o numeral correspondente para selecionar oRegião da AWSQue você deseja testar. Para suporteRegiões da AWSe uma lista deAWSendpoints de serviço que você pode usar com o Storage Gateway, consulteAWS Storage GatewayEndpoints e cotas donoAWSReferência geral.

À medida que o teste avança, cada endpoint exibe qualquer[PASSOU]ou[FAILED], indicando o status da conexão da seguinte forma:

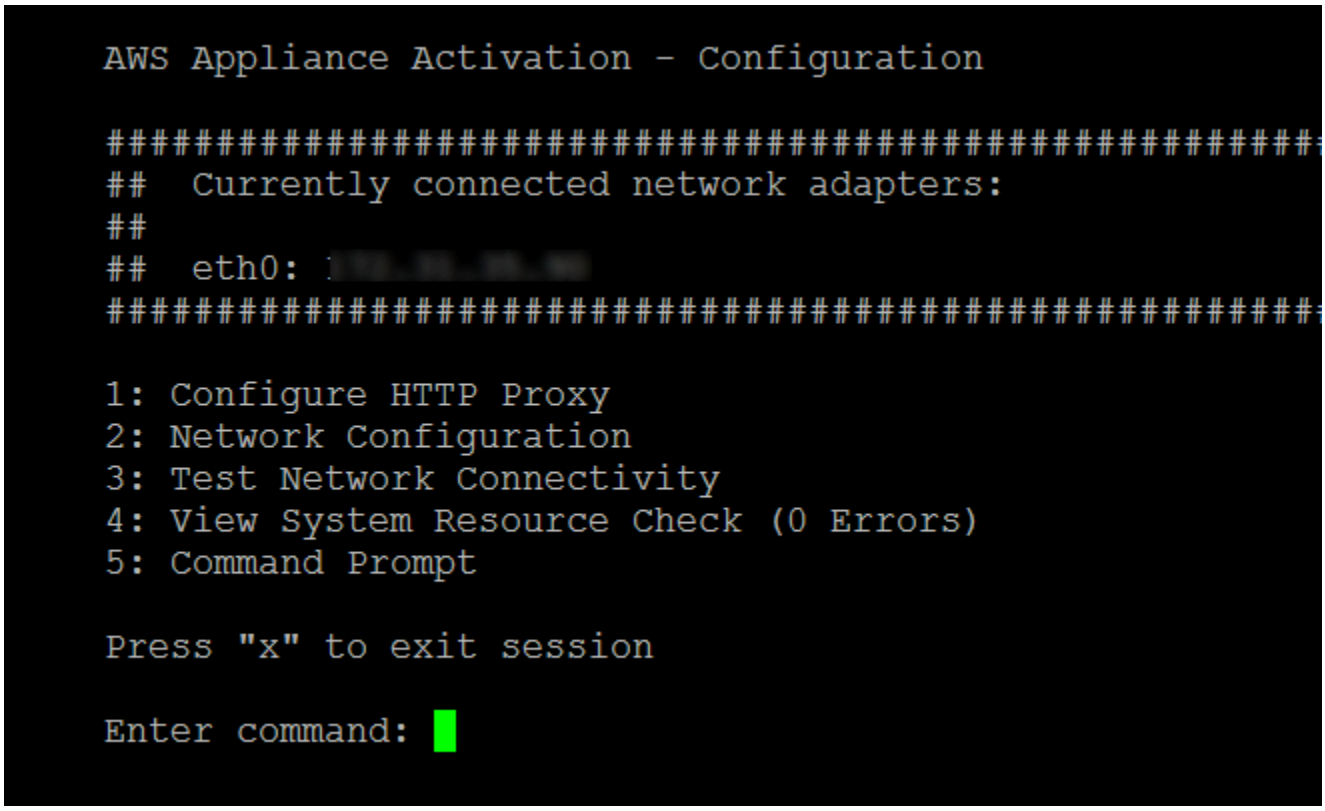
Message	Descrição
[PASSED]	Storage Gateway tem conectividade de rede.
[FAILED]	O Storage Gateway não tem conectividade de rede.

Visualizando o status do recurso do sistema de 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 Fazer login no console local do gateway Amazon EC2.
2. NoConfiguração Storage Gatewaymenu principal, insira**4**Para visualizar os resultados da verificação de recursos do sistema.



O console exibe uma mensagem [OK], [WARNING] ou [FAIL] para cada recurso, tal como descrito na tabela a seguir.

Message	Descrição
[OK]	O recurso passou na verificação de recursos do sistema.
[WARNING]	O recurso não atende aos requisitos recomendados, mas seu gateway poderá continuar funcionando. Seu Storage Gateway exibe uma mensagem que descreve os resultados da verificação de recursos.
[FAIL]	O recurso não atende aos requisitos mínimos. Seu gateway talvez não funcione corretame nte. Seu Storage Gateway exibe uma mensagem que descreve os resultados da verificação de recursos.

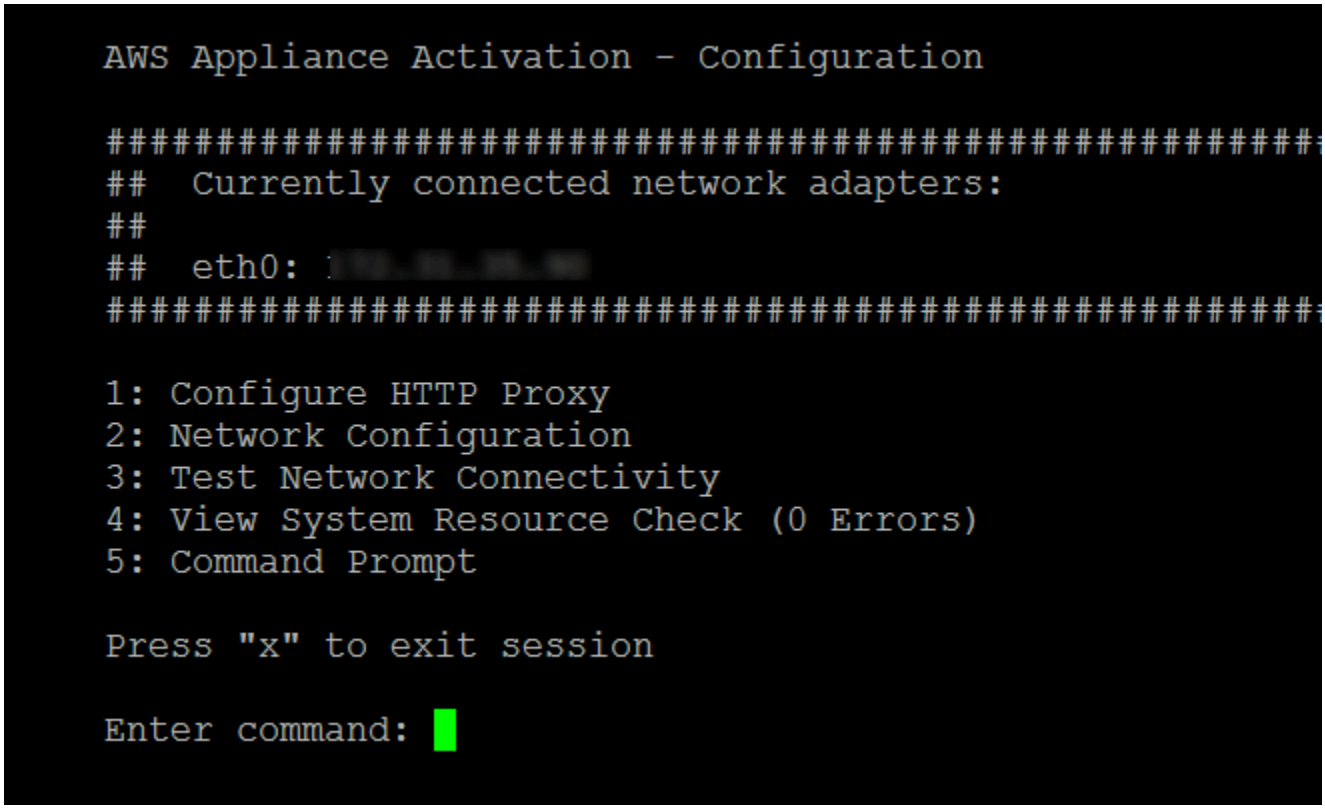
O console também exibe o número de erros e avisos ao lado da opção de menu de verificação de recursos.

Executando comandos do Storage Gateway no console local

O console do AWS Storage Gateway ajuda a oferecer um ambiente seguro para configuração e diagnóstico de problemas em seu gateway. Usando os comandos do console, você pode realizar tarefas de manutenção, como salvar tabelas de roteamento ou entrar em contato com o Support da Amazon Web Services.

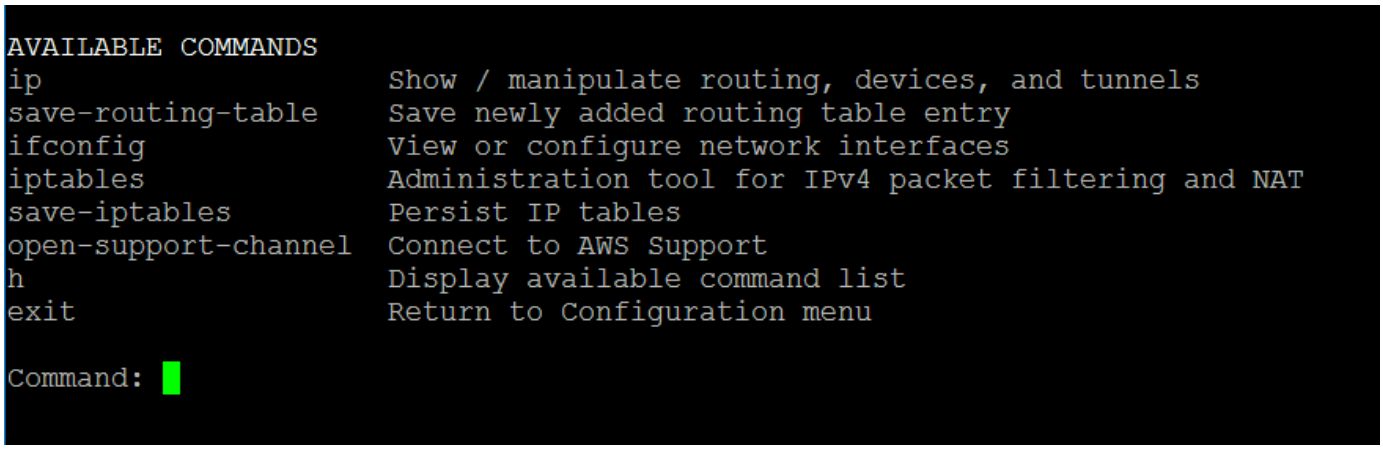
Para executar um comando de configuração ou diagnóstico

1. Faça login no console local do gateway. Para obter instruções, consulte Fazer login no console local do gateway Amazon EC2.
2. NoAWSConfiguração de ativação do dispositivomenu principal, insira**5**peloConsole do gateway.



3. No prompt de comando, digite **h** e pressione a tecla Return (Retornar).

   O console exibe o menu AVAILABLE COMMANDS (COMANDOS DISPONÍVEIS) com os comandos disponíveis. Depois do menu, o prompt do console do gateway é exibido, conforme mostrado na captura de tela a seguir.



4. No prompt de comando, insira o comando que você quer usar e seguir as instruções.

Para obter informações a respeito de um comando, digite o nome do comando no prompt do comando.

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

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.

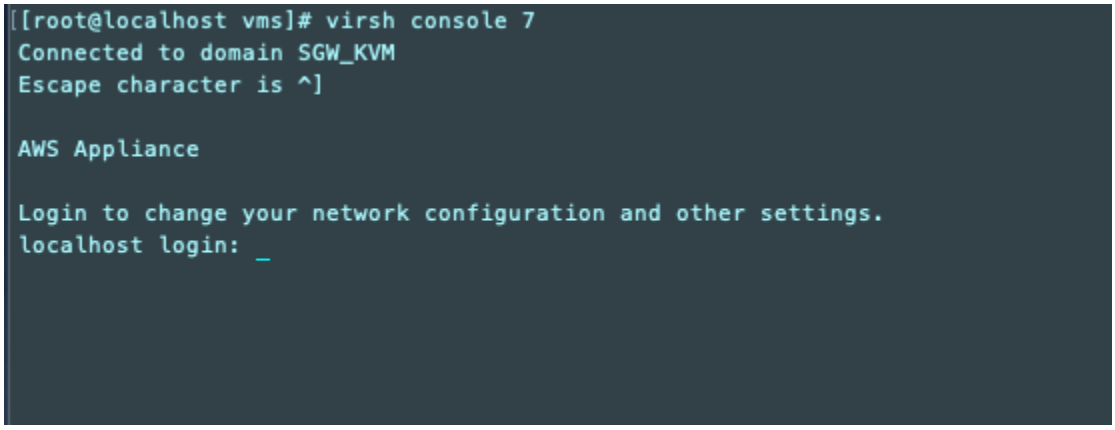
   ```
   # virsh list
   ```

   É possível escolher VMs disponíveis por `Id`.

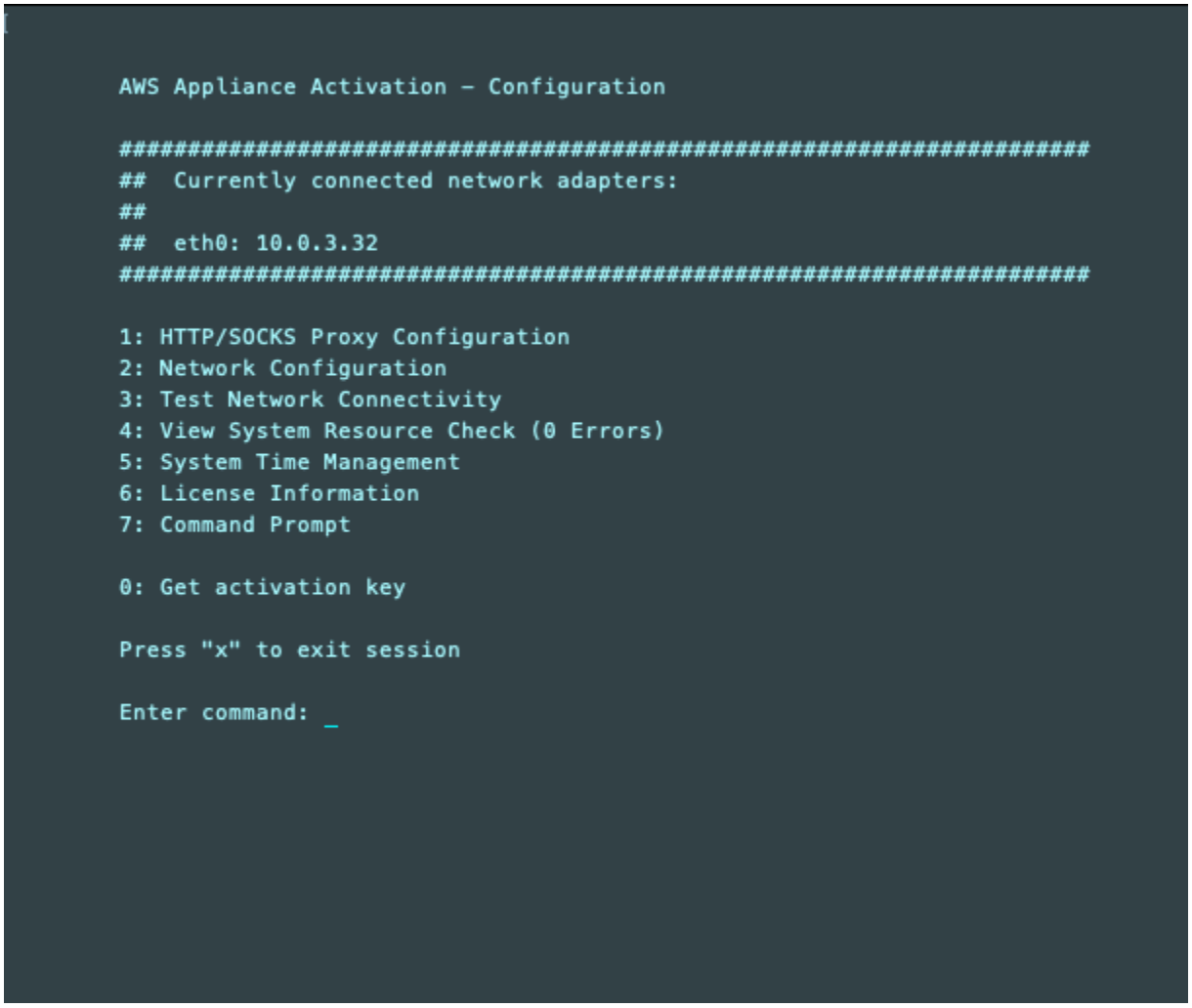
2. Use o comando a seguir para acessar o console local.

   ```
   # virsh console VM_Id
   ```



3. Para obter credenciais padrão para fazer login no console local, consulte Como fazer login no console local do gateway de arquivo.

4. Depois de fazer login, é possível ativar e configurar o gateway.

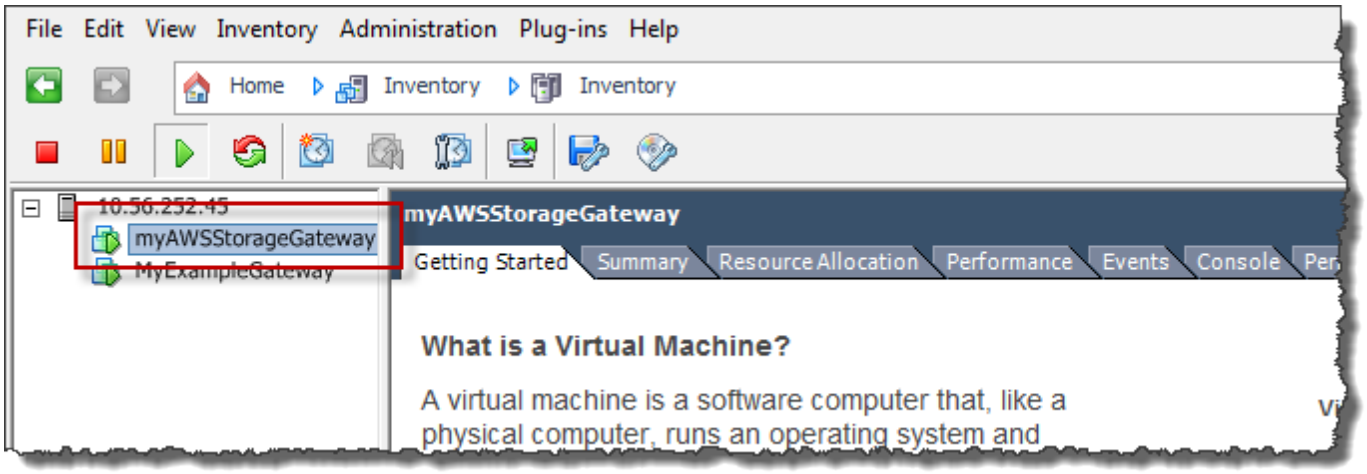


Acesso ao console local do gateway com o VMware ESXi

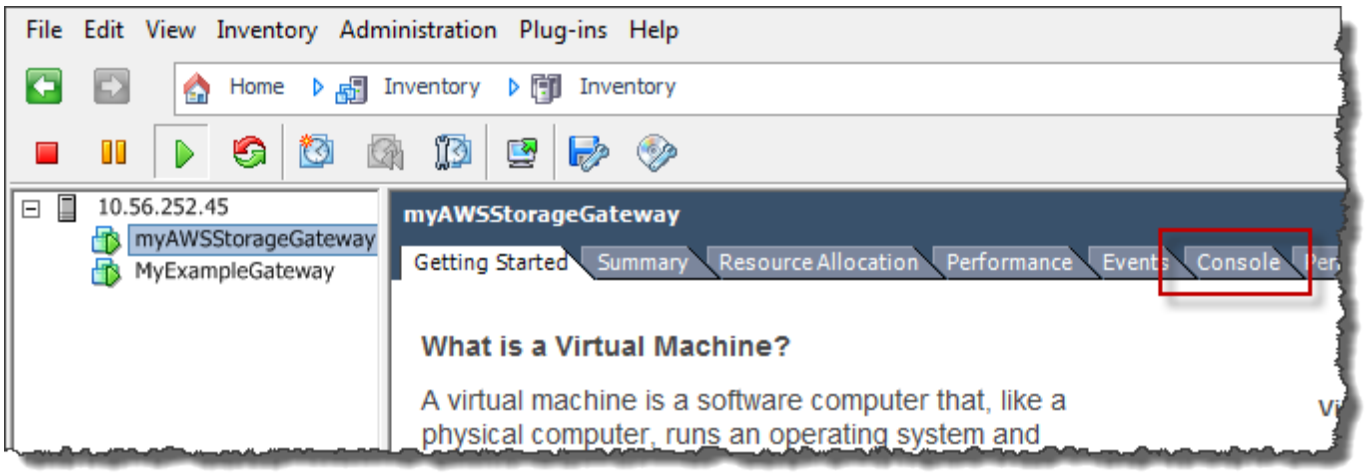
Para acessar o console local de seu gateway com VMware ESXi

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.

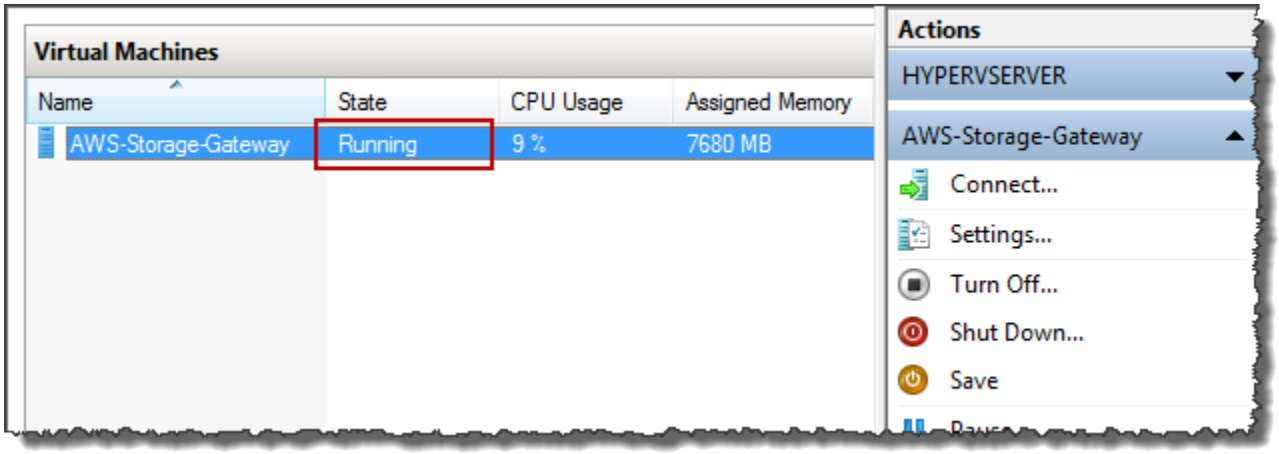
4. Para fazer login usando as credenciais padrão, vá para o procedimento Como fazer login no console local do gateway de arquivo.

Acessar o console local do gateway com o Microsoft Hyper-V

Para acessar o console local do gateway (Microsoft Hyper-V)

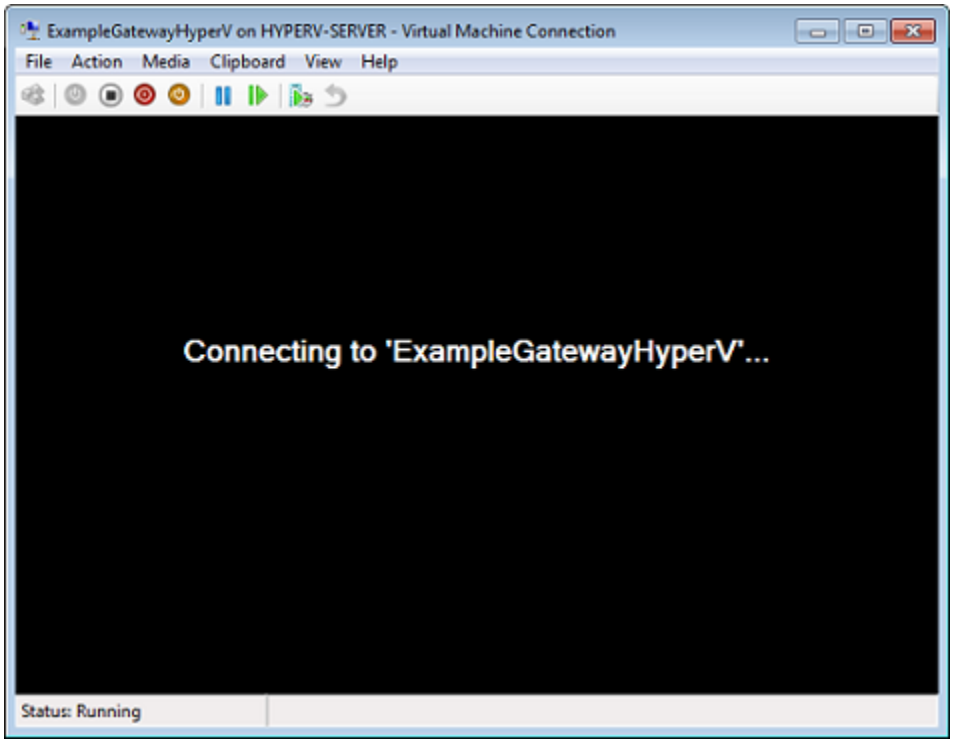
1. Na lista Virtual Machines do Microsoft Hyper-V Manager, selecione a VM de seu gateway.
2. Verifique se o gateway está ativado.

> **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 o nome de usuário e senha fornecidos pelo administrador do hipervisor.



Depois de alguns instantes, a VM estará pronta para você fazer login.

4. Para fazer login usando as credenciais padrão, vá para o procedimento Como fazer login no console local do gateway de arquivo.

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

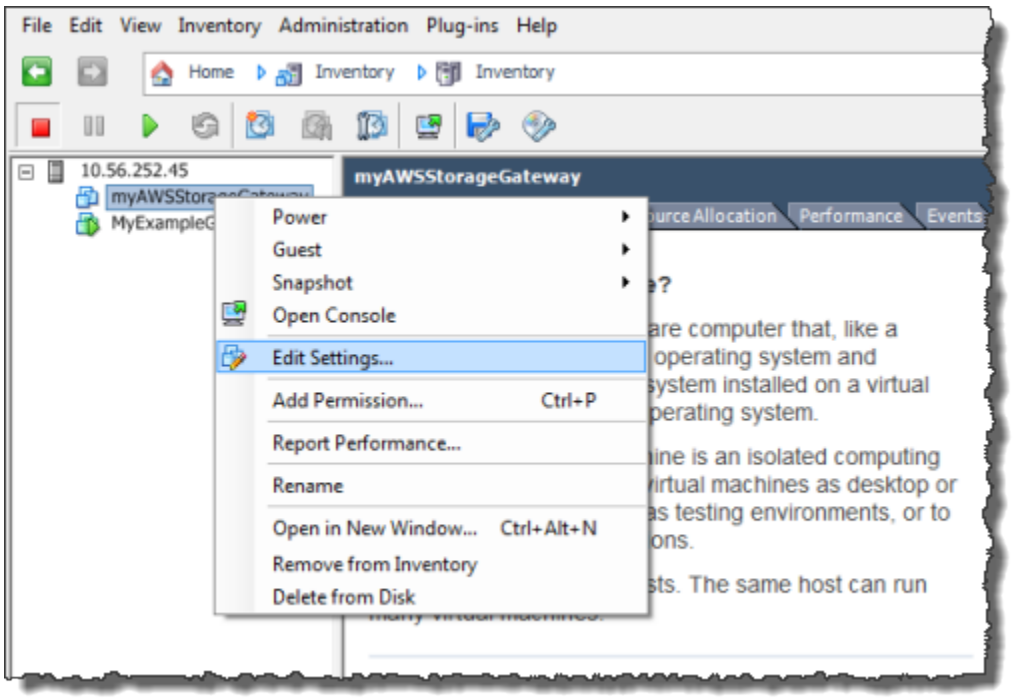
Configuração do Gateway para várias NICs em um host do VMware ESXi

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. O procedimento a seguir mostra como adicionar um adaptador ao VMware ESXi.

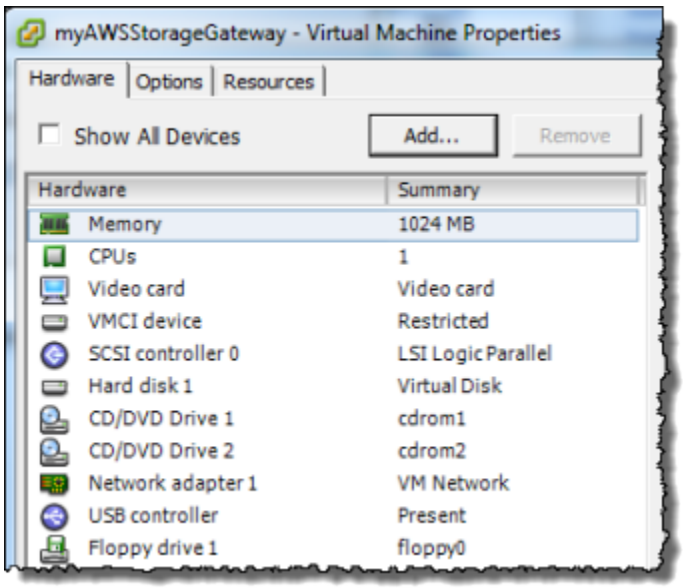
Para configurar um adaptador de rede adicional no host do VMware ESXi para seu gateway

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.

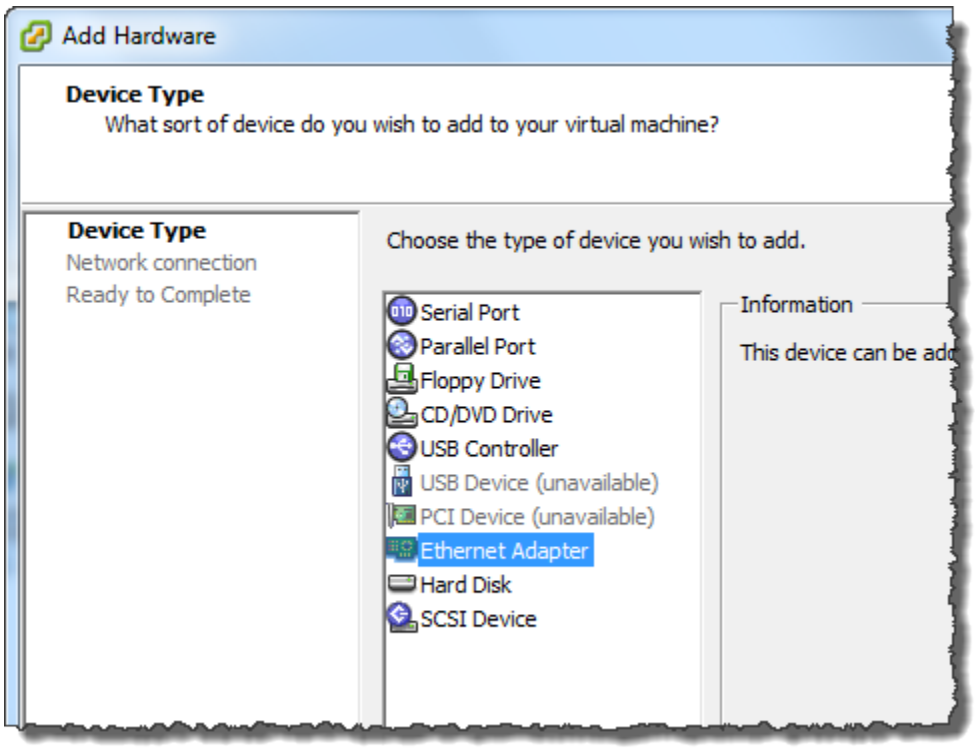


4. Na guia Hardware da caixa de diálogo Propriedades da Máquina Virtual, escolha Adicionar para adicionar um dispositivo.



5. Siga o assistente Add Hardware para adicionar um adaptador de rede.

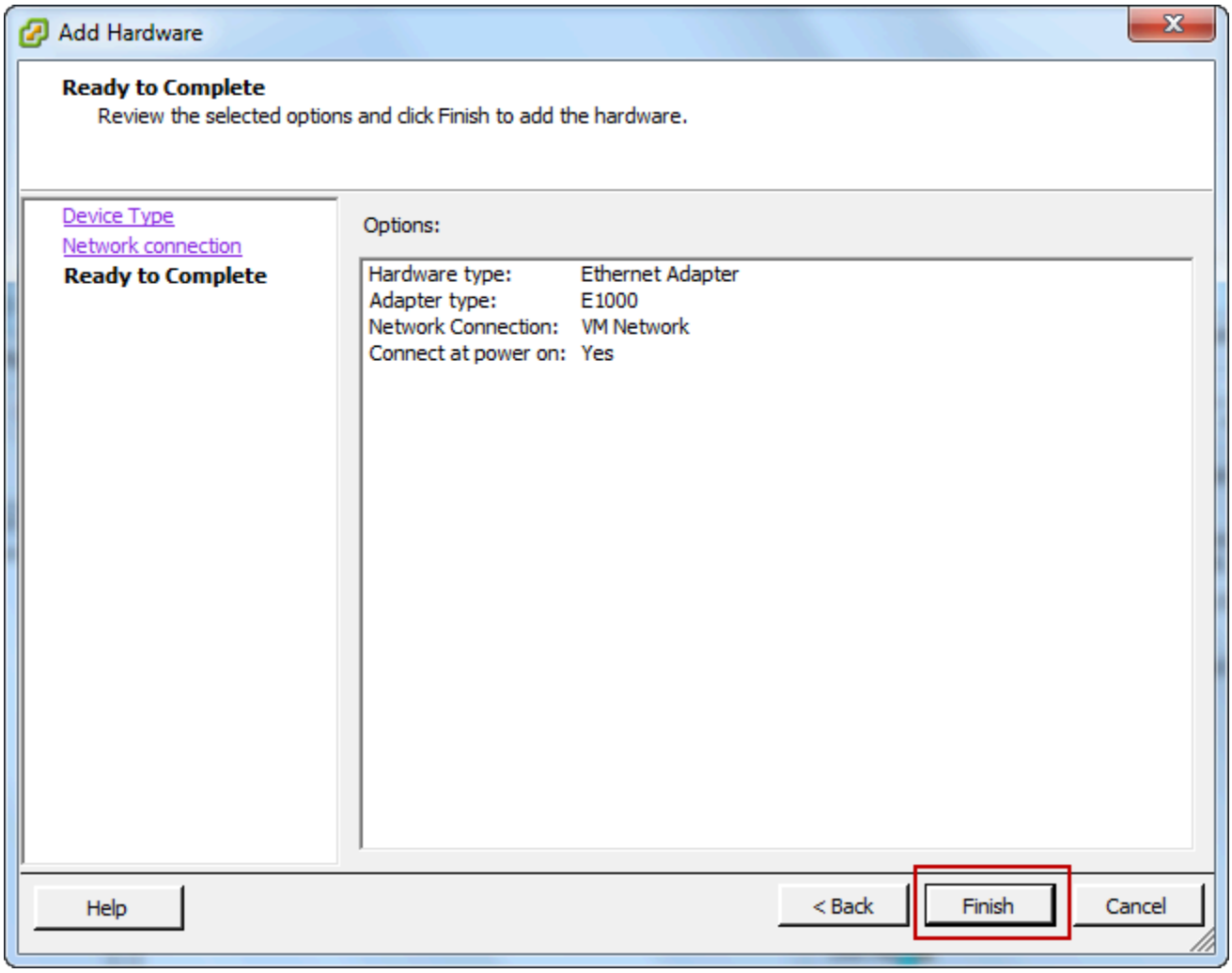
   a. No painel Tipo de Dispositivo, escolha Adaptador Ethernet para adicionar um adaptador e em seguida Seguinte.



   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 E1000 com 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.

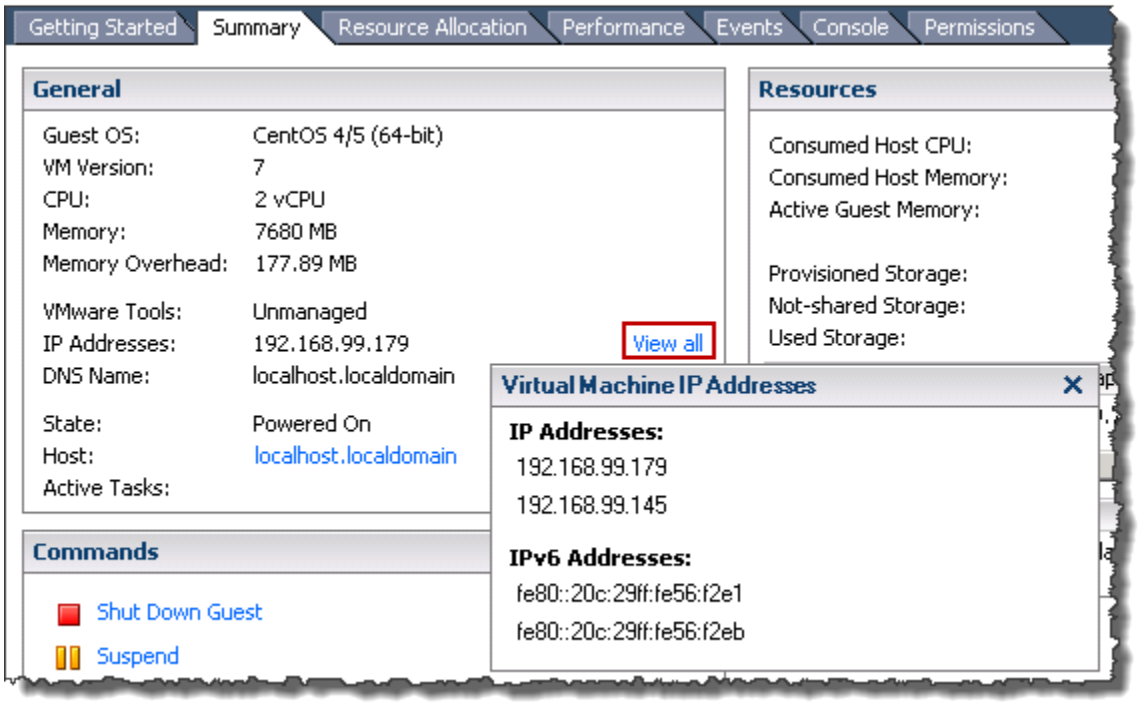
c. No painel Pronto para Completar, reveja as informações e escolha Terminar.



6. Escolha a guia Summary da VM em seguida View All, ao lado da caixa IP Address. A janela Endereço IP da Máquina Virtual exibe todos os endereços IP que você pode usar 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.

A imagem a seguir é somente ilustrativa. Na prática, um dos endereços IP será o endereço por meio do qual o gateway se comunicará com a AWS e o outro será um endereço em uma sub-rede diferente.



7. No console do Storage Gateway, ative o gateway.
8. NoNavegaçãopainel do console do Storage Gateway, escolhaGateways doE em seguida o gateway ao qual você adicionou o adaptador. Confirme se o segundo endereço IP está listado na guia Details.

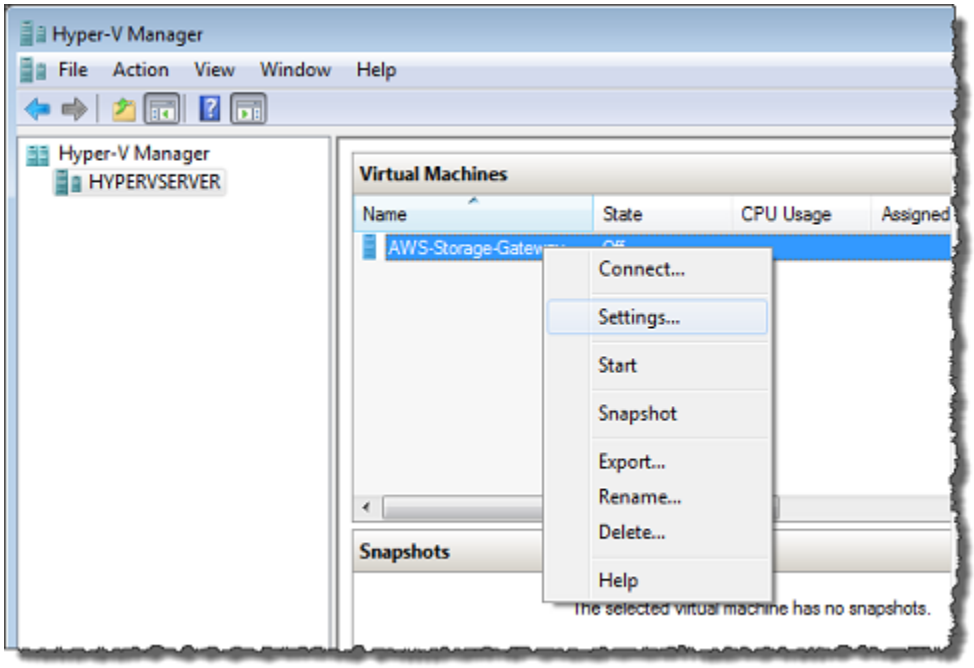
Para obter informações sobre as tarefas do console local comuns ao host do VMware, do Hyper-V e da KVM, consulte Executar tarefas no console local da VM (gateway de arquivo)

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.

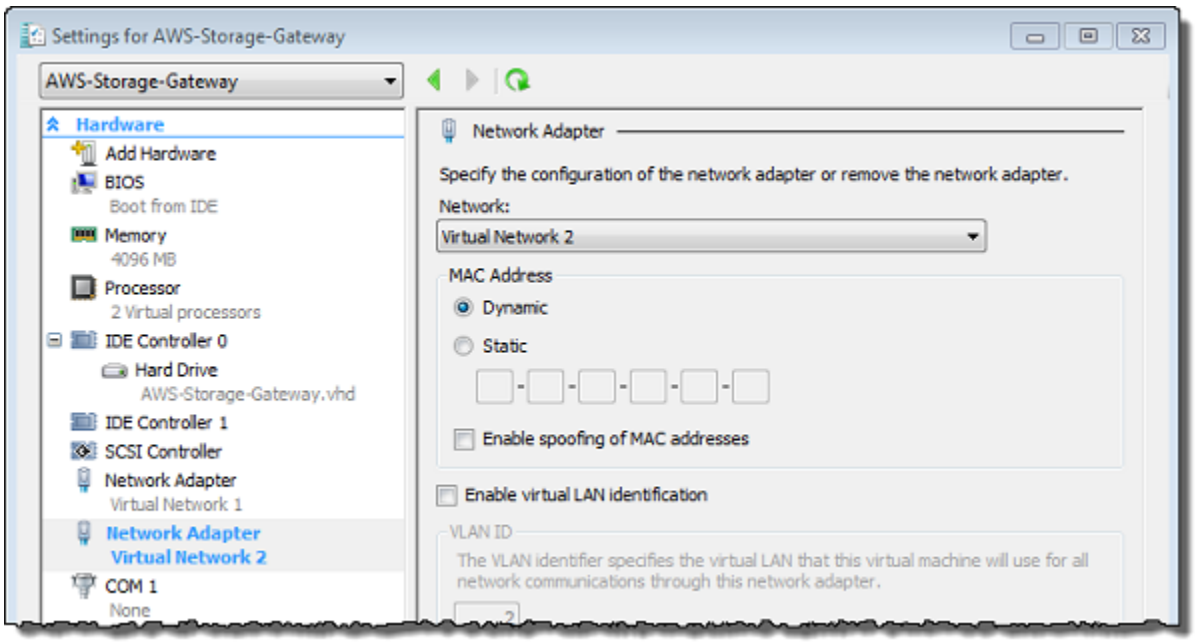
Para configurar um adaptador de rede adicional em um host do Microsoft Hyper-V para seu gateway

1. No console do Storage Gateway, desative o gateway.
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.
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.

Para obter informações sobre as tarefas do console local comuns ao host do VMware, do Hyper-V e da KVM, consulte Executar tarefas no console local da VM (gateway de arquivo)

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.

Assim que excluído, o gateway deixa de ser exibido no Console de Gerenciamento do AWS Storage Gateway e a respectiva conexão com o iniciador iSCSI é encerrada. 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.

Você pode excluir um gateway usando o console do Storage Gateway ou de forma programática. Você pode encontrar informações a seguir sobre como excluir um gateway usando o console do Storage Gateway. Se você deseja excluir seu gateway de forma programática, consulteAWS Storage GatewayReferência de API do.

Tópicos

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 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.

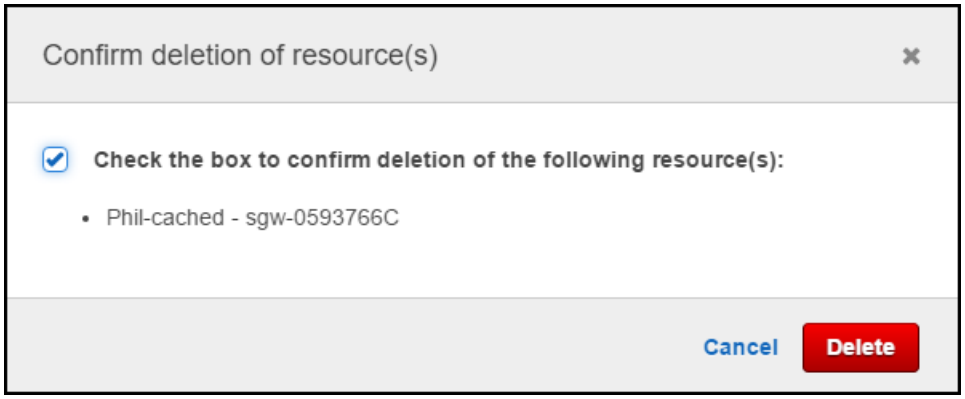
Para excluir um gateway

1. Abra o console Storage Gateway emhttps://console.aws.amazon.com/storagegateway/home.
2. No painel de navegação, escolha Gateways e, em seguida, o gateway que você deseja excluir.
3. Em Actions (Ações), selecione Delete gateway (Excluir gateway).

4.

> **Warning**
>
> Antes de executar essa etapa, verifique se não há nenhum aplicativo gravando no momento nos volumes do gateway. Se excluir o gateway enquanto ele estiver em uso, poderá perder dados.
> Além disso, não é possível recuperar um gateway excluído.

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 que deseja excluir e, em seguida, escolha Delete.



> **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. Você pode optar por remover Instâncias do Amazon EC2 e snapshots do Amazon EBS ao cancelar sua assinatura do Amazon EC2. Se desejar manter sua assinatura do Amazon EC2, poderá 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.

Como remover recursos de um gateway implantado em uma Instância do Amazon EC2

Se desejar excluir um gateway implantado em uma Instância do Amazon EC2, é recomendável limpar oAWSFazer 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 como mostrado emComo excluir um gateway usando o console do Storage Gateway.
2. No console do Amazon EC2, interrompa a instância EC2 se tiver 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 do anexados à instância, se tiver necessidade de usá-los novamente. Para obter mais informações, consulteLimpe a instância e o volumenoGuia do usuário do Amazon EC2 para instâncias do Linux.

Substituindo o File Gateway existente por uma nova instância

Você pode substituir um File Gateway existente por uma nova instância à medida que suas necessidades de dados e desempenho crescem, ou se você receber umAWSNotificação para migrar seu gateway. Talvez seja necessário fazer isso se quiser mover seu gateway para uma plataforma de host melhor ou instâncias mais recentes do Amazon EC2, ou para atualizar o hardware do servidor subjacente.

Existem dois métodos para substituir um File Gateway existente. A tabela a seguir descreve os benefícios e as desvantagens de cada método. Usando essas informações, selecione o método mais adequado para o ambiente de gateway e, em seguida, consulte as etapas do procedimento na seção correspondente abaixo.

	Método 1: Migre disco de cache e Gateway ID para instância de substituição	Método 2: Instância de substituição com disco cache vazio e novo Gateway ID
Dados de disco em cache	Os dados no disco de cache são preservados. Esse método é útil se o gateway tiver um disco de cache grande ou se os aplicativos forem sensíveis ao atraso causado por operações de leitura fora do cache.	Os dados em cache são baixados doAWSnuvem. Esse método é ideal para cargas de trabalho com gravação pesada, se seus aplicativ os puderem tolerar o atraso causado por leituras fora do cache.
Tempo de inatividade	Seu gateway ficará off-line por 1-2 horas durante o processo de migração.	Sem tempo de inatividade. O gateway existente pode ser usado simultaneamente com o gateway de substituição até você optar por excluí-lo . Vários gravadores não são suportados enquanto ambos os gateways estão em uso.

	Método 1: Migre disco de cache e Gateway ID para instância de substituição	Método 2: Instância de substituição com disco cache vazio e novo Gateway ID
ID do gateway	O novo gateway herda o Gateway ID do gateway que ele substitui.	O gateway existente e o gateway de substituição têm IDs de gateway exclusivas e separadas.

> **Note**
>
> Os dados podem ser movidos somente entre gateways do mesmo tipo.

Método 1: Migre disco de cache e Gateway ID para instância de substituição

Para migrar o disco de cache do File Gateway e o ID do gateway para uma instância de substituição:

1. Interrompa todos os aplicativos que estão gravando no gateway de arquivos existente.
2. Verificar se o`CachePercentDirty`Métrica do noMonitoramentoguia para o gateway de arquivos existente é`0`.
3. Desligue o gateway de arquivos existente desligando a máquina virtual host (VM) usando seus controles de hipervisor.

   Para obter mais informações sobre como encerrar uma instância do Amazon EC2, consulteInterromper e iniciar sua instâncianoGuia do usuário do Amazon EC2.

   Para obter mais informações sobre como desligar uma VM KVM, VMware ou Hyper-V, consulte a documentação do hipervisor.
4. Desconecte todos os discos, incluindo o disco raiz, os discos de cache e os discos buffer de upload da VM de gateway antiga.

> **Note**
>
> Anote o ID do volume do disco raiz, bem como o ID do gateway associado a esse disco raiz. Você precisará desanexar esse disco do novo hipervisor de gateway de armazenamento em uma etapa posterior.

Se você estiver usando uma instância do Amazon EC2 como a VM do gateway de arquivos, consulteDesanexar um volume do Amazon EBS de uma instância do WindowsouDesanexar um volume do Amazon EBS de uma instância LinuxnoGuia do usuário do Amazon EC2.

Para obter informações sobre como desanexar discos de uma VM KVM, VMware ou Hyper-V, consulte a documentação do hipervisor.

5. Criar um novoAWSInstância de VM do hipervisor do Storage Gateway, mas não a ative como um gateway. Em uma etapa posterior, essa nova VM assumirá a identidade do gateway antigo.

   Para obter mais informações sobre como criar uma nova VM do Storage Gateway hypervisor, consulteEscolher uma plataforma de hospedagem e fazer download da VM.

   > **Note**
   >
   > Não adicione discos de cache para a nova VM. Essa VM usará os mesmos discos de cache usados pela VM antiga.

6. Configure sua nova VM do Storage Gateway para usar as mesmas configurações de rede que a 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 precisar configurar manualmente um endereço IP estático para a VM do gateway, consulteComo configurar uma rede de gateway.

   Se a VM do gateway precisar usar um proxy Secure Socket versão 5 (SOCKS5) para se conectar à Internet, consulteComo rotear seu gateway local por meio de um proxy.

7. Inicie a nova VM do Storage Gateway.

8. Anexe os discos que você desconectou da VM de gateway antiga à nova VM de gateway. Não desconecte o disco raiz existente da nova VM de gateway.

   > **Note**
   >
   > Para migrar com sucesso, todos os discos devem permanecer inalterados. Alterar o tamanho do disco ou outros valores causa inconsistências nos metadados que impedem a migração bem-sucedida.

9. Inicie o processo de migração do gateway conectando-se à nova VM com um URL que usa o seguinte formato:

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

   Você pode usar o mesmo endereço IP para a nova VM de gateway usada para a VM de gateway antiga. O URL será semelhante ao seguinte exemplo:

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

   Use esse URL de um navegador ou da linha de comando usando cURL.

   Quando a migração do gateway é iniciada com êxito, a seguinte mensagem é exibida:

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

10. Aguarde até que o status do gateway seja exibido comoRunningnoAWSConsole do Storage Gateway. Dependendo da largura de banda disponível, isso pode levar até 10 minutos.
11. Pare a nova VM do Storage Gateway.
12. Desconecte o disco raiz do gateway antigo, cujo ID de volume você anotou anteriormente, do novo gateway.
13. Inicie a nova VM do Storage Gateway.
14. Se o gateway foi associado a um domínio do Active Directory, entre novamente no domínio. Para obter instruções, consulteConfigurar o acesso ao Microsoft Active Directory.

> **Note**
>
> Você deve concluir esta etapa mesmo se o status do gateway de arquivos aparecer comoIngressou.

15. Confirme se seus compartilhamentos estão disponíveis no endereço IP da nova VM de gateway e, em seguida, exclua a VM de gateway antiga.

> **Warning**
>
> Não é possível recuperar um gateway excluído.

Para obter mais informações sobre como excluir uma instância do Amazon EC2, consulteEncerrar a instânciaanoGuia do usuário do Amazon EC2. Para obter mais informações sobre como excluir uma VM KVM, VMware ou Hyper-V, consulte a documentação do hipervisor.

Método 2: Instância de substituição com disco cache vazio e novo Gateway ID

Para configurar uma instância do File Gateway de substituição com o disco de cache vazio e o novo ID do Gateway:

1. Interrompa todos os aplicativos que estão gravando no gateway de arquivos existente. Verificar se o`CachePercentDirty`Métrica do noMonitoramentoGuia é`0`antes de configurar compartilhamentos de arquivos no novo gateway.
2. Usar aAWS Command Line Interface(AWS CLI) para coletar e salvar as informações de configuração sobre o gateway de arquivos e compartilhamentos de arquivos existentes fazendo o seguinte:

   a. Salve as informações de configuração do gateway para o gateway de arquivos.

```
aws storagegateway describe-gateway-information --gateway-arn
 "arn:aws:storagegateway:us-east-2:123456789012:gateway/sgw-12A3456B"
```

Este comando gera um bloco JSON que contém metadados sobre o gateway, como seu nome, interfaces de rede, fuso horário configurado e seu estado (se o gateway está em execução).

b. Salve as configurações do Server Message Block (SMB) do gateway de arquivos.

```
aws storagegateway describe-smb-setting --gateway-arn
 "arn:aws:storagegateway:us-east-2:123456789012:gateway/sgw-12A3456B"
```

Esse comando gera um bloco JSON que contém metadados sobre o compartilhamento de arquivos SMB, como seu nome de domínio, status do Microsoft Active Directory, se a senha do convidado está definida e o tipo de estratégia de segurança.

c. Salve as informações de compartilhamento de arquivos para cada compartilhamento de arquivos SMB e NFS (Network File System) do gateway de arquivos:

- Use o seguinte comando para compartilhamentos de arquivos SMB.

```
aws storagegateway describe-smb-file-shares --file-share-arn-list
 "arn:aws:storagegateway:us-east-2:123456789012:share/share-987A654B"
```

Esse comando gera um bloco JSON que contém metadados sobre o compartilhamento de arquivos NFS, como nome, classe de armazenamento, status, função do IAM Amazon Resource Name (ARN), uma lista de clientes com permissão para acessar o gateway de arquivos e o caminho usado pelo cliente SMB para identificar o ponto de montagem.

- Use o comando a seguir para compartilhamentos de arquivos NFS.

```
aws storagegateway  describe-nfs-file-shares --file-share-arn-list
 "arn:aws:storagegateway:us-east-2:123456789012:share/share-321A978B"
```

Esse comando gera um bloco JSON que contém metadados sobre o compartilhamento de arquivos NFS, como nome, classe de armazenamento, status, ARN de função do IAM, uma lista de clientes com permissão para acessar o gateway de arquivos e o caminho usado pelo cliente NFS para identificar o ponto de montagem.

3. Interrompa o gateway de arquivos existente fazendo o seguinte:

a. Interrompa todos os aplicativos que estão gravando no gateway de arquivos existente. Verificar se o`CachePercentDirty`Métrica do noMonitoramentoGuia é`0`antes de configurar compartilhamentos de arquivos no novo gateway.

b. Interrompa o gateway de arquivos existente desligando a máquina virtual (VM) que está hospedando o gateway.

4. Crie um novo File Gateway.
5. Monte os compartilhamentos de arquivos configurados no gateway antigo.
6. Confirme se o novo gateway está funcionando corretamente e, em seguida, exclua o gateway antigo do console do Storage Gateway.

> **Important**
>
> Antes de excluir um gateway, verifique se não há nenhum aplicativo gravando no momento no cache do gateway de arquivos. Se você excluir um gateway de arquivos enquanto ele estiver em uso, poderá perder dados.

> **Warning**
>
> Não é possível recuperar um gateway excluído.

7. Exclua a antiga máquina virtual de gateway ou a instância do EC2.

Performance

Nesta seção, você encontra informações sobre o desempenho do Storage Gateway.

Tópicos

Orientação de desempenho para gateways de arquivos

Nesta seção, você pode encontrar orientações de configuração para o provisionamento de hardware para seu a VM de gateway de arquivos. Os tipos e tamanhos de instâncias do Amazon EC2 do que estão listados na tabela são exemplos e são fornecidos para referência.

Para obter melhor desempenho, o tamanho do disco de cache deve ser ajustado ao tamanho do conjunto de trabalho ativo. Usar vários discos locais para o cache aumenta o desempenho de gravação ao paralelizar acesso a dados e gera IOPS maior.

Nas tabelas a seguir,cache de acertosAs operações de leitura são leituras dos compartilhamentos de arquivos que são feitas pelo cache. Perda de cacheAs operações de leitura são leituras dos compartilhamentos de arquivos que são feitas pelo Amazon S3.

> **Note**
>
> Não recomendamos o uso do armazenamento temporário. Para obter informações sobre como usar o armazenamento temporário, consulte Usando armazenamento efêmero com gateways EC2.

A seguir estão exemplos de configurações de gateway de arquivos.

Desempenho do S3 File Gateway em clientes Linux

Exemplos de configuração	Protocolo	Taxa de transferência de gravação (tamanhos de arquivo 1 GB)	Throughput de leitura de acertos	Throughput de leitura de falta de
Disco raiz: 80 GB io1, 4.000 IOPS Disco de cache: Cache de 512 GiB, io1, 1.500 IOPS provision adas Desempenho mínimo da rede: 10 Gbps CPU: 16 vCPU | RAM: 32 GB Protocolo NFS recomendado para Linux	NFSv3 - 1 rosca	110 MiB/seg (0,92 Gbps)	590 MiB/seg (4,9 Gbps)	310 MiB/seg (2,6 Gbps)
	NFSv3 - 8 threads	160 MiB/seg (1,3 Gbps)	590 MiB/seg (4,9 Gbps)	335 MiB/seg (2,8 Gbps)
	NFSv4 - 1 rosca	130 MiB/seg (1,1 Gbps)	590 MiB/seg (4,9 Gbps)	295 MiB/seg (2,5 Gbps)
	NFSv4 - 8 threads	160 MiB/seg (1,3 Gbps)	590 MiB/seg (4,9 Gbps)	335 MiB/seg (2,8 Gbps)
	SMBV3 - 1 rosca	115 MiB/seg (1,0 Gbps)	325 MiB/seg (2,7 Gbps)	255 MiB/seg (2,1 Gbps)
	SMBV3 - 8 fios	190 MiB/seg (1,6 Gbps)	590 MiB/seg (4,9 Gbps)	335 MiB/seg (2,8 Gbps)
Dispositivo de hardware do Storage Gateway Desempenho mínimo da rede: 10 Gbps	NFSv3 - 1 rosca	265 MiB/seg (2,2 Gbps)	590 MiB/seg (4,9 Gbps)	310 MiB/seg (2,6 Gbps)
	NFSv3 - 8 threads	385 MiB/seg (3,1 Gbps)	590 MiB/seg (4,9 Gbps)	335 MiB/seg (2,8 Gbps)
	NFSv4 - 1 rosca	310 MiB/seg (2,6 Gbps)	590 MiB/seg (4,9 Gbps)	295 MiB/seg (2,5 Gbps)

Exemplos de configuração	Protocolo	Taxa de transferência de gravação (tamanhos de arquivo 1 GB)	Throughput de leitura de acertos	Throughput de leitura de falta de
	NFSv4 - 8 threads	385 MiB/seg (3,1 Gbps)	590 MiB/seg (4,9 Gbps)	335 MiB/seg (2,8 Gbps)
	SMBV3 - 1 rosca	275 MiB/seg (2,4 Gbps)	325 MiB/seg (2,7 Gbps)	255 MiB/seg (2,1 Gbps)
	SMBV3 - 8 fios	455 MiB/seg (3,8 Gbps)	590 MiB/seg (4,9 Gbps)	335 MiB/seg (2,8 Gbps)
Disco raiz: 80 GB, io1 SSD, 4.000 IOPS Disco cache: discos de cache NVME de 4 x 2 TB Desempenho mínimo da rede: 10 Gbps CPU: 32 vCPU | RAM: 244 GB Protocolo NFS recomendado para Linux	NFSv3 - 1 rosca	300 MiB/s (2,5 Gbps)	590 MiB/seg (4,9 Gbps)	325 MiB/seg (2,7 Gbps)
	NFSv3 - 8 threads	585 MiB/seg (4,9 Gbps)	590 MiB/seg (4,9 Gbps)	580 MiB/seg (4,8 Gbps)
	NFSv4 - 1 rosca	355 MiB/seg (3,0 Gbps)	590 MiB/seg (4,9 Gbps)	340 MiB/seg (2,9 Gbps)
	NFSv4 - 8 threads	575 MiB/seg (4,8 Gbps)	590 MiB/seg (4,9 Gbps)	575 MiB/seg (4,8 Gbps)
	SMBV3 - 1 rosca	230 MiB/seg (1,9 Gbps)	325 MiB/seg (2,7 Gbps)	245 MiB/seg (2,0 Gbps)
	SMBV3 - 8 fios	585 MiB/seg (4,9 Gbps)	590 MiB/seg (4,9 Gbps)	580 MiB/seg (4,8 Gbps)

Desempenho do gateway de arquivos em clientes Windows

Exemplos de configuração	Protocolo	Taxa de transferência de gravação (tamanhos de arquivo 1 GB)	Throughput de leitura de acertos	Throughput de leitura de falta de
Disco raiz: 80, GB io1, 4.000 IOPS Disco de cache: Cache de 512 GiB, io1, 1.500 IOPS provision adas Desempenho mínimo da rede: 10 Gbps CPU: 16 vCPU | RAM: 32 GB Protocolo SMB recomendado para Windows	SMBV3 - 1 rosca	150 MiB/seg (1,3 Gbps)	180 MiB/seg (1,5 Gbps)	20 MiB/seg (0,2 Gbps)
	SMBV3 - 8 fios	190 MiB/seg (1,6 Gbps)	335 MiB/seg (2,8 Gbps)	195 MiB/seg (1,6 Gbps)
	NFSv3 - 1 rosca	95 MiB/seg (0,8 Gbps)	130 MiB/seg (1,1 Gbps)	20 MiB/seg (0,2 Gbps)
	NFSv3 - 8 threads	190 MiB/seg (1,6 Gbps)	330 MiB/seg (2,8 Gbps)	190 MiB/seg (1,6 Gbps)
Dispositivo de hardware do Storage Gateway Desempenho mínimo da rede: 10 Gbps	SMBV3 - 1 rosca	230 MiB/seg (1,9 Gbps)	255 MiB/seg (2,1 Gbps)	20 MiB/seg (0,2 Gbps)
	SMBV3 - 8 fios	835 MiB/seg (7,0 Gbps)	475 MiB/seg (4,0 Gbps)	195 MiB/seg (1,6 Gbps)
	NFSv3 - 1 rosca	135 MiB/seg (1,1 Gbps)	185 MiB/seg (1,6 Gbps)	20 MiB/seg (0,2 Gbps)
	NFSv3 - 8 threads	545 MiB/seg (4,6 Gbps)	470 MiB/seg (4,0 Gbps)	190 MiB/seg (1,6 Gbps)

Exemplos de configuração	Protocolo	Taxa de transferência de gravação (tamanhos de arquivo 1 GB)	Throughput de leitura de acertos	Throughput de leitura de falta de
Disco raiz: 80 GB, io1 SSD, 4.000 IOPS Disco cache: discos de cache NVME de 4 x 2 TB Desempenho mínimo da rede: 10 Gbps CPU: 32 vCPU | RAM: 244 GB Protocolo SMB recomendado para Windows	SMBV3 - 1 rosca	230 MiB/seg (1,9 Gbps)	265 MiB/seg (2,2 Gbps)	30 MiB/seg (0,3 Gbps)
	SMBV3 - 8 fios	835 MiB/seg (7,0 Gbps)	780 MiB/seg (6,5 Gbps)	250 MiB/seg (2,1 Gbps)
	NFSv3 - 1 rosca	135 MiB/seg (1,1. Gbps)	220 MiB/seg (1,8 Gbps)	30 MiB/seg (0,3 Gbps)
	NFSv3 - 8 threads	545 MiB/seg (4,6 Gbps)	570 MiB/seg (4,8 Gbps)	240 MiB/seg (2,0 Gbps)

> **Note**
>
> Seu desempenho pode variar com base na configuração da plataforma de hospedagem e na largura de banda da rede.

Como otimizar o desempenho de um gateway

Você pode encontrar informações a seguir sobre como otimizar o desempenho de um gateway. A orientação para isso fundamenta-se na adição de recursos ao gateway e na adição de recursos ao servidor de aplicativos.

Como adicionar recursos ao seu gateway

Você pode otimizar o desempenho do gateway adicionando recursos ao seu gateway em uma ou mais das seguintes maneiras.

Use discos de desempenho superior

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 obter informações sobre como adicionar discos, consulteAdicionar armazenamento em cache.

Para medir a taxa de transferência, use o`ReadBytes`e`WriteBytes`Métricas com o`Samples`Estatística do Amazon CloudWatch. 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**
>
> Não existem métricas do CloudWatch disponíveis para todos os gateways. Para obter informações sobre métricas de gateway, consulte Monitorando seu gateway de arquivos.

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 os quatro processadores virtuais atribuídos à VM do gateway contam com o suporte de quatro núcleos. 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 seu aplicativo 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.

O Storage Gateway oferece suporte ao uso de 24 CPUs no servidor host do gateway. Você pode usar 24 CPUs para melhorar significativamente o desempenho de seu gateway. Recomendamos a seguinte configuração de gateway para o servidor de host do gateway:

- 24 CPUs.
- 16 GiB de memória RAM reservada para gateways de arquivos
  - 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 16 TiB a 32 TiB
  - 48 GiB de RAM reservada para gateways com tamanho de cache 32 TiB a 64 TiB
- Disco 1 anexado ao controlador paravirtual 1, para ser usado como cache do gateway da seguinte forma:
  - SSD com um controlador NVMe.
- Disco 2 anexado ao controlador paravirtual 1, para ser usado como buffer de upload do gateway da seguinte forma:
  - SSD com um controlador NVMe.
- Disco 3 anexado ao controlador paravirtual 2, 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.

Respalde os discos virtuais com discos físicos separados.

Ao provisionar discos de gateway, é altamente recomendável não provisionar discos locais para armazenamento local 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, pode apresentar um desempenho ruim.

Como adicionar recursos ao seu ambiente de aplicativos

Aumente a largura de banda entre o servidor de aplicativos 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. Você pode usar o`ReadBytes`e`WriteBytes`métricas do gateway para medir a taxa de transferência total 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.

Usar o VMware vSphere High Availability com o Storage Gateway

O Storage Gateway fornece alta disponibilidade no VMware por meio de um conjunto de verificações de integridade no nível do aplicativo 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.

Com essa integração, um gateway implantado em um ambiente VMware no local ou em uma nuvem VMware na AWS recupera automaticamente da maioria das interrupções de serviço. Ele geralmente faz isso em menos de 60 segundos sem perda de dados.

Para usar o VMware HA com o Storage Gateway, siga as etapas listadas a seguir.

Tópicos

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.

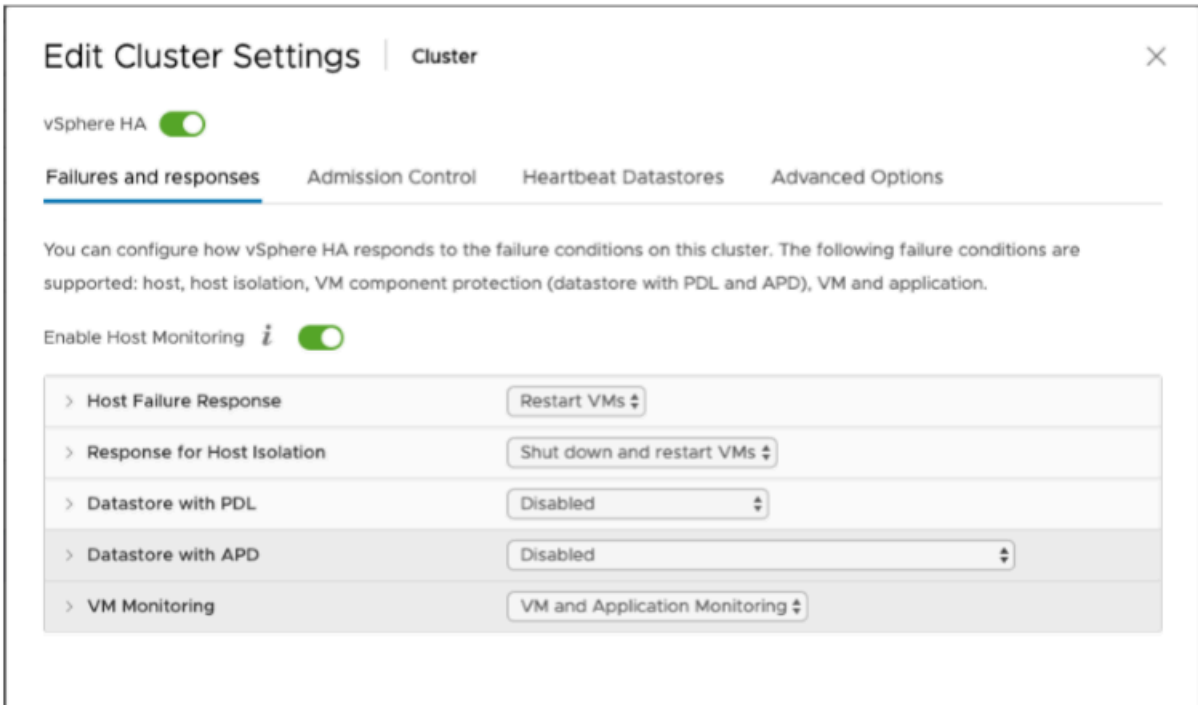
Em seguida, configure o cluster do VMware para funcionar com o Storage Gateway.

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:

   - Proposta à falha do host: VMs Reiniciar VMs
   - Resposta para isolamento do host: Desligar e reiniciar VMs
   - Datastore with PDL: Disabled (Desativado)
   - Datastore with APD: Disabled (Desativado)
   - VM 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 do— Após esse intervalo, a VM é reiniciada se uma pulsação de VM não for recebida.
   - Tempo de atividade mínimo— O cluster aguarda isso muito depois que uma VM começa a monitorar as pulsações das ferramentas de VM.
   - Máximo de redefinições por VM— O cluster reinicia a VM no máximo de vezes que a VM reinicia a VM durante a janela temporal para o máximo de redefinições.
   - Janela de tempo máximo de redefinições— A janela de tempo na qual o máximo de redefinições por VM será contado pelo máximo de redefinições 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.

Fazer download da imagem .ova para o seu tipo de gateway

Use o procedimento a seguir para fazer download da imagem .ova.

Como fazer download da imagem .ova para o seu tipo de gateway

- Faça download da imagem .ova para o seu tipo de gateway de uma das seguintes opções:
  - Gateway de arquivos —

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.

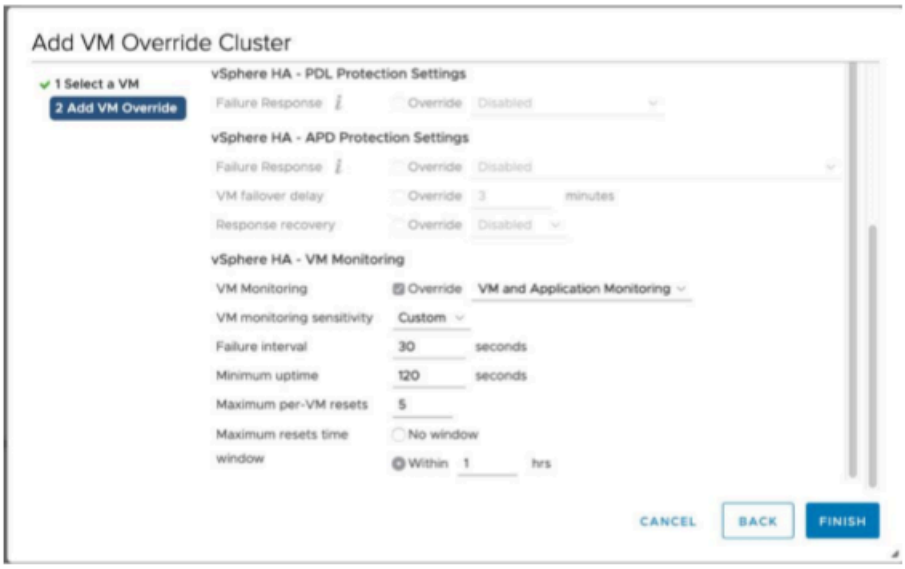
(Opcional) Adicionar opções de substituição para outras VMs no cluster

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

- Escolha as instruções de ativação com base no seu tipo de gateway:
  - Gateway de arquivos —

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 emhttps://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 logs do Amazon CloudWatch. Para obter mais informações, consulte Obtendo registros de integridade do gateway de arquivos com grupos de logs do CloudWatch.

Segurança emAWSStorage Gateway

A segurança da nuvem na AWS é a nossa maior prioridade. Como cliente da AWS, você se contará com um datacenter e uma arquitetura de rede criados para atender aos requisitos das organizações com as maiores exigências de segurança.

A segurança é uma responsabilidade compartilhada entre a AWS e você. O modelo de responsabilidade compartilhada descreve isso como segurança da nuvem e segurança na nuvem:

- Segurança da nuvem: a AWS é responsável pela proteção da infraestrutura que executa produtos da AWS na Nuvem AWS. A AWS também fornece serviços que podem ser usados com segurança. Auditores de terceiros testam e verificam regularmente a eficácia da nossa segurança como parte dos Programas de conformidade da AWS. Para saber mais sobre os programas de conformidade que se aplicam aoAWSStorage GatewayAWSServiços da no escopo pelo programa de conformidade.
- Segurança da nuvem: sua responsabilidade é determinada pelo serviço da AWS que você usa. Você também é responsável por outros fatores, incluindo a confidencialidade de seus dados, os requisitos da sua 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 conformidade. Você também aprende a usar outrosAWSServiços da que ajudam a monitorar e proteger os recursos do Storage Gateway.

Tópicos

Proteção de dados noAWSStorage Gateway

OAWS Modelo de responsabilidade compartilhadaAplica-se à proteção de dados noAWSStorage Gateway Conforme descrito nesse modelo, a AWS é responsável por proteger a infraestrutura global que executa toda a Nuvem AWS. Você é responsável por manter o controle sobre seu conteúdo hospedado nessa infraestrutura. Esse conteúdo inclui as tarefas de configuração e gerenciamento de segurança dos serviços da AWS que você usa. Para obter mais informações sobre a privacidade de dados, consulte as Perguntas frequentes sobre privacidade de dados. Para obter mais informações sobre a proteção de dados na Europa, consulte a postagem do blog AWS Shared Responsibility Model and GDPR no Blog de segurança da AWS.

Para fins de proteção de dados, recomendamos que você proteja as credenciais da conta da Conta da AWS e configure as contas de usuário individuais com o AWS Identity and Access Management (IAM). Dessa maneira, cada usuário receberá apenas as permissões necessárias para cumprir suas obrigações de trabalho. Recomendamos também que você proteja seus dados das seguintes formas:

- Use uma autenticação multifator (MFA) com cada conta.
- Use SSL/TLS para se comunicar com os recursos da AWS. Recomendamos TLS 1.2 ou posterior.
- Configure o registro em log das atividades da API e do usuário com o AWS CloudTrail.
- Use as soluções de criptografia da AWS, juntamente com todos os controles de segurança padrão nos serviços da AWS.
- Use serviços gerenciados de segurança avançada, como o Amazon Macie, que ajuda a localizar e proteger dados pessoais armazenados no Amazon S3.
- Se você precisar de módulos criptográficos validados pelo FIPS 140-2 ao acessar a AWS por meio de uma interface de linha de comando ou uma API, use um endpoint do FIPS. Para obter mais informações sobre endpoints do FIPS, consulte Federal Information Processing Standard (FIPS) 140-2.

É altamente recomendável que você nunca coloque informações de identificação confidenciais, como endereços de e-mail dos seus clientes, em marcações ou campos de formato livre, como um campo Name (Nome). Isso inclui quando você trabalha com o Storage Gateway ou outroAWSserviços usando o console, a API,AWS CLI, ouAWSSDKs. Quaisquer dados inseridos em marcações ou campos de formato livre usados para nomes podem ser usados para logs de cobrança ou diagnóstico. Se você fornecer um URL para um servidor externo, recomendemos fortemente que não sejam incluídas informações de credenciais no URL para validar a solicitação a esse servidor.

Criptografia de dados usandoAWS KMS

O Storage Gateway usa SSL/TLS (Secure Socket Layers/Transport Layer Security) para criptografar dados que são transferidos entre o gateway e o dispositivo de gateway eAWSArmazenamento. Por padrão, o Storage Gateway usa chaves de criptografia gerenciadas pelo Amazon S3 (SSE-S3) no lado do servidor para criptografar todos os dados armazenados no Amazon S3. Você tem a opção de usar a API do Storage Gateway para configurar seu gateway para criptografar dados armazenados na nuvem usando criptografia no lado do servidor comAWS Key Management Service(SSE-KMS) chaves mestras de cliente (CMKs).

> **Important**
>
> Quando você usa umAWS KMSA CMK do para criptografia no lado do servidor, você deve escolher uma CMK simétrica. O Storage Gateway não é compatível com CMKs assimétricas. Para obter mais informações, consulte Como usar chaves simétricas e assimétricas no AWS Key Management Service Guia do desenvolvedor.

Criptografar um compartilhamento de arquivos

Para um compartilhamento de arquivos, você pode configurar seu gateway para criptografar seus objetos com oAWS KMSchaves gerenciadas usando o SSE-KMS. Para obter informações sobre como usar a API Storage Gateway para criptografar dados gravados em um compartilhamento de arquivos, consulteCreateNFSFileSharenoAWS Storage GatewayReferência de API do.

Criptografar um sistema de arquivos

Para obter mais informações, consulteCriptografia de dados no Amazon FSxnoGuia do usuário do Amazon FSx for Windows File Server.

Ao usar o AWS KMS para criptografar seus dados, lembre-se do 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 chamarAWS KMSOperações de API do. Para obter mais informações, consulteUsar políticas do IAM com oAWS KMSnoAWS Key Management ServiceGuia do desenvolvedor.

- Se você excluir ou desativar sua CMK ou revogar o token concedido, não poderá acessar os dados no volume ou fita. Para obter mais informações, consulteExcluir chaves mestras do clientenoAWS Key Management ServiceGuia do desenvolvedor.
- Se você criar um snapshot de um volume criptografado pelo KMS, o snapshot será criptografado. O snapshot herdará 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 oferece suporte à criação de um volume não criptografado a partir 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?

Controle de acesso e autenticação do Storage Gateway

O acesso ao AWS Storage Gateway exige credenciais que a AWS possa usar para autenticar suas solicitações. Essas credenciais devem ter permissões para acessarAWSRecursos, como um gateway, compartilhamento de arquivos, volume ou fita. As seguintes seções fornecem detalhes sobre como você pode usarAWS Identity and Access Management(IAM)E Storage Gateway para ajudar a proteger seus recursos controlando quem pode acessá-los:

- Autenticação
- Controle de acesso

Autenticação

Você pode acessar a AWS como alguns dos seguintes tipos de identidade:

- Conta de usuário root da Conta da AWS: ao criar pela primeira vez uma Conta da AWS, você começa com uma única identidade de login que tem acesso total a todos os recursos e serviços da AWS na conta. Essa identidade é denominada Conta da AWSusuário root da e é acessada pelo login com o endereço de e-mail e a senha que você usou para criar a conta. Recomendamos

que não use o usuário raiz para suas tarefas do dia a dia, nem mesmo as administrativas. Em vez disso, siga as práticas recomendadas para o uso do usuário root somente a fim de criar seu primeiro usuário do IAM. Depois, armazene as credenciais do usuário raiz com segurança e use-as para executar somente algumas tarefas de gerenciamento de contas e de serviços.

- Usuário do IAM— UmUsuário do IAMé uma identidade dentro do seuConta da AWSCom permissões personalizadas específicas (por exemplo, permissões para criar um gateway no Storage Gateway). Você pode usar uma senha e um nome do usuário do IAM para fazer login em páginas da Web seguras da AWS como https://console.aws.amazon.com/, AWSFóruns de discussão da ou a AWS SupportCentral de AWS Management Console.

  Além de um nome e senha de usuário, você também pode gerar chaves de acesso para cada usuário. Você pode usar essas chaves ao acessar serviços da AWS de forma programática, seja com um dos vários SDKs ou usando a AWS Command Line Interface (CLI). As ferramentas de SDK e de CLI usam as chaves de acesso para o cadastramento criptográfico da sua solicitação. Se você não utilizar ferramentas da AWS, cadastre a solicitação você mesmo. Suporte Storage GatewaySignature versão 4, um protocolo para autenticar solicitações de API de entrada. Para obter mais informações sobre solicitações de autenticação, consulte Processo de assinatura do Signature Version 4 na Referência geral da AWS.

- Função do IAM: uma função do IAM é uma identidade do IAM que você pode criar em sua conta com permissões específicas. Uma função do IAM é semelhante a um usuário do IAM no sentido de ser uma identidade da AWS com políticas de permissão que determinam o que a identidade pode e não pode fazer na AWS. No entanto, em vez de ser exclusivamente associada a uma pessoa, uma função destina-se a ser assumida por qualquer pessoa que precisar dela. Além disso, uma função não tem credenciais de longo prazo padrão, como uma senha ou chaves de acesso, associadas a ela. Em vez disso, quando você assumir uma função, ela fornecerá credenciais de segurança temporárias para sua sessão de função. As funções do IAM com credenciais temporárias são úteis nas seguintes situações:

  - Acesso de usuário federado: em vez de criar um usuário do IAM, você poderá usar identidades de usuários existentes no AWS Directory Service, em seu diretório de usuários corporativos ou em um provedor de identidades da Web. Estes são conhecidos como usuários federados. A AWS atribui uma função a um usuário federado quando o acesso é solicitado por meio de

um provedor de identidades. Para obter mais informações sobre usuários federados, consulte Usuários federados e funções no Guia do usuário do IAM.

- Acesso ao serviço da AWS: uma função de serviço é uma função do IAM que um serviço assume para realizar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir uma função de serviço do IAM. Para obter mais informações, consulte Criar uma função para delegar permissões a um serviço da AWS no Guia do usuário do IAM.

- Aplicações em execução no Amazon EC2: é possível usar uma função do IAM para gerenciar credenciais temporárias para aplicações em execução em uma instância do EC2 e fazer solicitações da AWS CLI ou da API da AWS. É preferível fazer isso do que armazenar chaves de acesso na instância do EC2. Para atribuir uma função da AWS a uma instância do EC2 e disponibilizá-la para todos os seus aplicativos, crie um perfil de instância que esteja anexado à instância. Um perfil de instância contém a função e permite que programas que estão em execução na instância do EC2 obtenham credenciais temporárias. Para mais informações, consulte Usar uma função do IAM para conceder permissões a aplicações em execução nas instâncias do Amazon EC2 no Guia do usuário do IAM.

Controle de acesso

Você pode ter credenciais válidas para autenticar as solicitações, mas só poderá criar nem acessar os recursos do Storage Gateway. Por exemplo, é preciso ter permissões para criar um gateway no Storage Gateway.

As seções a seguir descrevem como gerenciar permissões para o Storage Gateway. Recomendamos que você leia a visão geral primeiro.

- Visão geral do gerenciamento de permissões de acesso ao Storage Gateway
- Políticas baseadas em identidade (políticas do IAM)

Visão geral do gerenciamento de permissões de acesso ao Storage Gateway

EVERYAWSO recurso da é de propriedade de uma conta da Amazon Web Services, e as permissões para criar ou acessar um recurso são regidas por políticas de permissões. Um administrador de conta pode anexar políticas de permissões a identidades do IAM (ou seja, usuários, grupos e funções), e alguns serviços (como o AWS Lambda) também oferecem suporte à anexação de políticas de permissões a recursos.

> **Note**
>
> Um administrador da conta (ou usuário administrador) é um usuário com privilégios de administrador. Para obter mais informações, consulte Melhores práticas do IAM no Guia do usuário do IAM.

Ao conceder permissões, você decide quem recebe as permissões, os recursos relacionados às permissões concedidas e as ações específicas que deseja permitir nesses recursos.

Tópicos

- Recursos e operações do Storage Gateway
- Entender a propriedade de recursos
- Gerenciar o acesso aos recursos
- Especificar elementos de política: Ações, efeitos, recursos e principais
- Especificar condições em uma política

Recursos e operações do Storage Gateway

No Storage Gateway, o principal recurso é umGateway do. Storage Gateway comporta também os tipos de recurso a seguir: compartilhamento de arquivos, volume, fita virtual, destino iSCSI e dispositivo de biblioteca de fitas virtuais (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 ARN
ARN de gateway	`arn:aws:storagegateway:` *`region`*`:`*`account-id`* `:gateway/` *`gateway-id`*
ARN de compartilhamento de arquivos	`arn:aws:storagegateway:` *`region`*`:`*`account-id`* `:share/`*`share-id`*

> **Note**
>
> Os IDs de recurso do Storage Gateway são maiúsculas Quando você usa esses IDs de recurso com a API do Amazon EC2, o Amazon EC2 espera que estejam em 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.
>
> Os ARNs dos gateways ativados antes de 2 de setembro de 2015 contêm o nome do gateway, em vez de o ID do gateway. Para obter o ARN de seu gateway, use a operação de API `DescribeGatewayInformation`.

Para conceder permissões para operações de API específicas, como criação de uma fita, o Storage Gateway fornece um conjunto de ações de API para você criar e gerenciar esses recursos e sub-recursos. Para obter uma lista de ações de API, consulteAçõesnoAWS Storage GatewayReferência de API do.

Para conceder permissões para operações de API específicas, como criação de uma fita, o Storage Gateway define um conjunto de ações que você pode especificar em uma política de permissões para conceder permissões para operações de API específicas. Uma operação de API pode exigir permissões para mais de uma ação. Para obter uma tabela que mostra todas as ações de API do Storage Gateway e os recursos aos quais elas se aplicam, consultePermissões da API Storage Gateway Referência de ações, recursos e condições.

Entender a propriedade de recursos

UMAproprietário do recursoé a conta da Amazon Web Services que criou o recurso. Ou seja, o proprietário do recurso é a conta da Amazon Web Services doentidade principal(a conta-raiz, um usuário do IAM ou uma função do IAM) que autentica a solicitação que cria o recurso. Os exemplos a seguir ilustram como isso funciona:

- Se você usar as credenciais da conta-raiz da conta da Amazon Web Services para ativar um gateway, a conta da Amazon Web Services será a proprietária do recurso (no Storage Gateway, o recurso é o gateway).
- Se você criar um usuário do IAM na sua conta da Amazon Web Services e conceder permissões ao`ActivateGateway`Para esse usuário, o usuário pode ativar um gateway. No entanto, sua conta da Amazon Web Services, à qual o usuário pertence, é proprietária do recurso de gateway.
- Se você criar uma função do IAM na sua conta da Amazon Web Services com permissões para ativar um gateway, qualquer um capaz de assumir a respectiva função poderá ativar um gateway. Sua conta da Amazon Web Services, à qual a função pertence, é proprietária do recurso de gateway.

Gerenciar o acesso aos recursos

A política de permissões descreve quem tem acesso a quê. A seção a seguir explica as opções disponíveis para a criação das políticas de permissões.

> **Note**
>
> Esta seção aborda o uso do IAM no contexto do Storage Gateway. Não são fornecidas informações detalhadas sobre o serviço IAM. Para obter a documentação completa do IAM, consulteO que é o IAMnoIAM User Guide.Para obter mais informações sobre a sintaxe e as descrições da política do IAM, consulte a Referência de política do AWS IAM no Guia do usuário do IAM.

As políticas anexadas a uma identidade do IAM são conhecidas como políticas baseadas em identidade (políticas do IAM;) e as políticas anexadas a um recurso são conhecidas como políticas baseadas em recurso. O Storage Gateway oferece suporte apenas às políticas baseadas em identidade (políticas do IAM).

Tópicos

- Políticas baseadas em identidade (políticas do IAM)
- Políticas baseadas em recursos

Políticas baseadas em identidade (políticas do IAM)

Você pode anexar as políticas a identidades do IAM. Por exemplo, você pode fazer o seguinte:

- Anexar uma política de permissões a um usuário ou grupo na sua conta— Um administrador da conta pode usar uma política de permissões associada a um usuário para conceder permissões para que ele crie um recurso de Storage Gateway, como um gateway, um volume ou uma fita.
- Anexar uma política de permissões a uma função (grant cross-account permissions): você pode anexar uma política de permissões baseada em identidade a uma função do IAM para conceder permissões entre contas. Por exemplo, o administrador na Conta A pode criar uma função para conceder permissões entre contas a outra conta da Amazon Web Services (por exemplo, Conta B) ou umaAWSserviço da seguinte forma:
  1. Um administrador da Conta A cria uma função do IAM e anexa uma política de permissões à função que concede permissões em recursos da Conta A.
  2. Um administrador da Conta A anexa uma política de confiança à função identificando a Conta B como a entidade principal, que pode assumir a função.
  3. O administrador da conta B pode delegar permissões para assumir a função para todos os usuários na conta B. Isso permite que os usuários na conta B criem ou acessem recursos na conta A. A entidade principal na política de confiança também pode ser uma entidade principal do serviço da AWS se você desejar conceder permissões a um serviço da AWS para assumir a função.

  Para obter mais informações sobre o uso do IAM para delegar permissões, consulte Gerenciamento de acesso no Guia do usuário do IAM.

Veja a seguir um exemplo de política que concede permissões para todas as ações `List*` em todos os recursos. Essa ação é uma ação somente leitura. Por isso, a política não permite que o usuário altere o estado dos recursos.

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

```
        {
            "Sid": "AllowAllListActionsOnAllResources",
            "Effect": "Allow",
            "Action": [
                "storagegateway:List*"
            ],
            "Resource": "*"
        }
    ]
}
```

Para obter mais informações sobre como usar políticas baseadas em identidade com o Storage Gateway, consulteUsar políticas baseadas em identidade (políticas do IAM) para o Storage Gateway. Para obter mais informações sobre usuários, grupos, funções e permissões, consulte Identidades (usuários, grupos e funções) no Guia do usuário do IAM.

Políticas baseadas em recursos

Outros serviços, como Amazon S3, também dão suporte a políticas de permissões baseadas em recursos. Por exemplo: você pode anexar uma política a um bucket do S3 para gerenciar permissões de acesso a esse bucket. O Storage Gateway não é compatível com as políticas baseadas em recursos.

Especificar elementos de política: Ações, efeitos, recursos e principais

Para cada recurso do Storage Gateway (consultePermissões da API Storage Gateway Referência de ações, recursos e condições), o serviço define um conjunto de operações da API (consulteAções). Para conceder permissões a essas operações de API, o Storage Gateway define um conjunto de ações que você pode especificar em uma política. Por exemplo, para o recurso de Storage Gateway, as seguintes ações são definidas:`ActivateGateway`,`DeleteGateway`, e`DescribeGatewayInformation`. Observe que a execução de uma operação de API pode exigir permissões para mais de uma ação.

Estes são os elementos de política mais básicos:

- Recurso – Em uma política, você usa um Amazon Resource Name (ARN – Nome de recurso da Amazon) para identificar o recurso a que a política se aplica. Para os recursos do Storage Gateway, você sempre usa o caractere curinga(*)em políticas do IAM. Para obter mais informações, consulte Recursos e operações do Storage Gateway.

- Ação: você usa palavras-chave de ação para identificar operações de recursos que você deseja permitir ou negar. Por exemplo, dependendo do especificado`Effect`, `ostoragegateway:ActivateGateway`Permite ou nega as permissões de usuário para executar o Storage Gateway`ActivateGateway`operação.
- Efeito - Você especifica o efeito quando o usuário solicita a ação específica, que pode ser permitir ou negar. Se você não conceder (permitir) explicitamente acesso a um recurso, o acesso estará implicitamente negado. Você também pode negar explicitamente o acesso a um recurso, o que pode fazer para ter a certeza de que um usuário não consiga acessá-lo, mesmo que uma política diferente conceda acesso.
- Principal: em políticas baseadas em identidade (políticas do IAM), o usuário ao qual a política é anexada é implicitamente a entidade principal. Para as políticas baseadas em recursos, você especifica quais usuários, contas, serviços ou outras entidades deseja que recebam permissões (aplica-se somente a políticas baseadas em recursos). O Storage Gateway não é compatível com as políticas baseadas em recursos.

Para saber mais sobre a sintaxe e as descrições de políticas do IAM, consulte a Referência de políticas do AWS IAM da no Guia do usuário do IAM.

Para obter uma tabela que mostra todas as ações de API do Storage Gateway, consultePermissões da API Storage Gateway Referência de ações, recursos e condições.

Especificar condições em uma política

Ao conceder permissões, você pode usar a linguagem da política do IAM para especificar as condições sobre quando uma política relativa à concessão de permissões deverá entrar em vigor. Por exemplo, convém que uma política só seja aplicada após uma data específica. Para obter mais informações sobre como especificar condições em uma linguagem de política, consulte Condição no Guia do usuário do IAM.

Para expressar condições, você usa chaves de condição predefinidas. Não há nenhuma chave de condição específica para o Storage Gateway. No entanto, existem chaves de condição em toda a AWS que você pode usar conforme apropriado. Para obter uma lista completa das chaves da AWS, consulte Chaves disponíveis no Guia do usuário do IAM.

Usar políticas baseadas em identidade (políticas do IAM) para o Storage Gateway

Este tópico fornece exemplos de políticas baseadas em identidade em que um administrador de conta pode anexar políticas de permissões a identidades do IAM (ou seja, usuários, grupos e funções).

> **Important**
>
> Recomendamos analisar primeiro os tópicos introdutórios que explicam os conceitos básicos e as opções disponíveis para gerenciar o acesso aos recursos do Storage Gateway. Para obter mais informações, consulte Visão geral do gerenciamento de permissões de acesso ao Storage Gateway.

As seções neste tópico abrangem o seguinte:

- Permissões necessárias para usar o console do Storage Gateway
- AWSpolíticas gerenciadas para Storage Gateway
- Exemplos de política gerenciada pelo cliente

A seguir, um exemplo de uma política de permissões.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowsSpecifiedActionsOnAllGateways",
            "Effect": "Allow",
            "Action": [
                "storagegateway:ActivateGateway",
                "storagegateway:ListGateways"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowsSpecifiedEC2ActionsOnAllGateways",
            "Effect": "Allow",
            "Action": [
```

```
                "ec2:DescribeSnapshots",
                "ec2:DeleteSnapshot"
            ],
            "Resource": "*"
        }
    ]
}
```

A política tem duas declarações (observe os elementos `Action` e `Resource` em ambas as declarações):

- A primeira instrução concede permissões para duas ações de Storage Gateway (`storagegateway:ActivateGatewaystoragegateway:ListGateways`) em um recurso de gateway.

  O caractere curinga (*) significa que essa instrução pode corresponder a qualquer recurso. Nesse caso, a instrução permite que `ostoragegateway:ActivateGatewaystoragegateway:ListGatewaysações` em qualquer gateway. O caractere curinga é usado aqui porque não é possível saber o ID do recurso enquanto o gateway não for criado. Para obter informações sobre como usar um caractere curinga (*) em uma política, consulte Exemplo 2: Permitir acesso somente leitura a um gateway.

  > **Note**
  >
  > Os ARNs identificam exclusivamenteAWSrecursos da AWS. Para obter mais informações, consulte Nomes de recursos da Amazon (ARNs) e namespaces de produtos da AWS na Referência geral da AWS.

  Para restringir permissões para uma ação específica, para gateway apenas, crie uma declaração diferente para essa ação na política e especifique o ID do gateway nessa declaração.

- A segunda declaração concede permissões para as ações `ec2:DescribeSnapshots` e `ec2:DeleteSnapshot`. Essas ações do Amazon Elastic Compute Cloud (Amazon EC2) requerem permissões porque os snapshots gerados no Storage Gateway são armazenados no Amazon Elastic Block Store (Amazon EBS) e gerenciados como recursos do Amazon EC2. Por isso, exigem ações correspondentes do EC2. Para obter mais informações, consulteAçõesnoReferência de APIs do Amazon EC2. Como essas ações do Amazon EC2 não

oferecem suporte a permissões em nível de recurso, a política especifica o caractere curinga (*) como a`Resource`valor em vez de especificar um ARN de gateway.

Para obter uma tabela que mostra todas as ações da API do Storage Gateway e os recursos a que elas se aplicam, consulte[Permissões da API Storage Gateway Referência de ações, recursos e condições](#).

Permissões necessárias para usar o console do Storage Gateway

Para usar o console do Storage Gateway, é necessário conceder permissões somente leitura. Se tiver intenção de descrever snapshots, também precisará conceder permissões para outras ações, tal como mostrado na política de permissões a seguir:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowsSpecifiedEC2ActionOnAllGateways",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeSnapshots"
            ],
            "Resource": "*"
        }
    ]
}
```

Essa permissão adicional é necessária porque os snapshots do Amazon EBS gerados no Storage Gateway são gerenciados como recursos do Amazon EC2.

Para configurar as permissões mínimas necessárias para operar o console do Storage Gateway, consulte[Exemplo 2: Permitir acesso somente leitura a um gateway](#).

AWSpolíticas gerenciadas para Storage Gateway

A Amazon Web Services resolve muitos casos de uso comuns fornecendo políticas autônomas do IAM que são criadas e administradas pela pelo AWS. As políticas gerenciadas concedem permissões necessárias para casos de uso comuns, de maneira que você possa evitar a necessidade de investigar quais permissões são necessárias. Para obter mais informações sobre AWSPolíticas gerenciadas, consulte[AWSpolíticas gerenciadas pela](#)noIAM User Guide.

Os seguintes exemplos deAWSAs políticas gerenciadas da, que é possível associar a usuários na sua conta, são específicas do Storage Gateway:

- AWSStorageGatewayReadOnlyAccess – Concede acesso somente leitura a recursos do AWS Storage Gateway.
- AWSStorageGatewayFullAccess – Concede pleno acesso a recursos do AWS Storage Gateway.

> **Note**
>
> É possível analisar essas políticas de permissões fazendo login no console do IAM e pesquisando políticas específicas.

Além disso, você pode criar políticas do IAM personalizadas para conceder permissões para ações de API do AWS Storage Gateway. Você pode anexar essas políticas personalizadas a usuários ou grupos do IAM que exijam essas permissões.

Exemplos de política gerenciada pelo cliente

Nesta seção, você pode encontrar políticas de usuário de exemplo que concedem permissões para diversas ações do Storage Gateway. Essas políticas funcionam quando você está usandoAWSSDKs e oAWS CLI. Ao usar o console, você precisa conceder permissões adicionais específicas ao console, o que é debatido em Permissões necessárias para usar o console do Storage Gateway.

> **Note**
>
> Todos os exemplos usam a Região do Oeste dos EUA (Oregon) (`us-west-2`) e contêm IDs de conta fictícios.

Tópicos

Exemplo 1: Permitir qualquer ação do Storage Gateway em todos os gateways

A política a seguir permite que um usuário execute todas as ações do Storage Gateway. A política também permite que o usuário execute ações do Amazon EC2 (DescribeSnapshotseDeleteSnapshot) nos snapshots do Amazon EBS gerados a partir do Storage Gateway.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowsAllAWSStorageGatewayActions",
            "Action": [
                "storagegateway:*"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {You can use Windows ACLs only with file shares that are enabled for Active
 Directory.
            "Sid": "AllowsSpecifiedEC2Actions",
            "Action": [
                "ec2:DescribeSnapshots",
                "ec2:DeleteSnapshot"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

Exemplo 2: Permitir acesso somente leitura a um gateway

A política a seguir permite todas as ações `List*` e `Describe*` em todos os recursos. Observe que essas ações são somente leitura. Por isso, a política não permite que o usuário altere o estado de nenhum recurso; ou seja, a política não permite que o usuário execute ações como `DeleteGateway`, `ActivateGateway` e `ShutdownGateway`.

Essa política permite também a ação `DescribeSnapshots` do Amazon EC2. Para obter mais informações, consulteDescribeSnapshotsnoReferência de APIs do Amazon EC2.

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowReadOnlyAccessToAllGateways",
            "Action": [
                "storagegateway:List*",
                "storagegateway:Describe*"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Sid": "AllowsUserToDescribeSnapshotsOnAllGateways",
            "Action": [
                "ec2:DescribeSnapshots"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

Na política anterior, em vez de usar um caractere curinga (*), você pode examinar recursos cobertos pela política para um gateway específico, tal como mostrado no exemplo a seguir. Desse modo, nessa política, essas ações são permitidas apenas no gateway específico.

```
"Resource": [
             "arn:aws:storagegateway:us-west-2:123456789012:gateway/gateway-id/",
             "arn:aws:storagegateway:us-west-2:123456789012:gateway/gateway-id/*"
            ]
```

Em um gateway, você pode restringir ainda mais o escopo do gateway de recursos a apenas volumes, tal como mostrado no exemplo a seguir:

```
"Resource": "arn:aws:storagegateway:us-west-2:123456789012:gateway/gateway-id/volume/
*"
```

Exemplo 3: Permitir acesso a um gateway específico

A política a seguir permite todas as ações em um gateway específico. O usuário não tem permissão para acessar outros gateways que você tenha implantado.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowReadOnlyAccessToAllGateways",
            "Action": [
                "storagegateway:List*",
                "storagegateway:Describe*"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Sid": "AllowsUserToDescribeSnapshotsOnAllGateways",
            "Action": [
                "ec2:DescribeSnapshots"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Sid": "AllowsAllActionsOnSpecificGateway",
            "Action": [
                "storagegateway:*"
            ],
            "Effect": "Allow",
            "Resource": [
                "arn:aws:storagegateway:us-west-2:123456789012:gateway/gateway-id/",
                "arn:aws:storagegateway:us-west-2:123456789012:gateway/gateway-id/*"
            ]
        }
    ]
}
```

A política anterior funcionará se o usuário ao qual a política está anexada usar a API ou umaAWSSDK para acessar o gateway. No entanto, se o usuário for usar o console do Storage Gateway, é também necessário conceder permissões para permitir que o`ListGateways`Ação, conforme mostrado no exemplo a seguir.

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

```
        {
            "Sid": "AllowsAllActionsOnSpecificGateway",
            "Action": [
                "storagegateway:*"
            ],
            "Effect": "Allow",
            "Resource": [
                "arn:aws:storagegateway:us-west-2:123456789012:gateway/gateway-id/",
                "arn:aws:storagegateway:us-west-2:123456789012:gateway/gateway-id/*"
            ]
        },
        {
            "Sid": "AllowsUserToUseAWSConsole",
            "Action": [
                "storagegateway:ListGateways"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

Exemplo 4: Permitir que um usuário acesse um volume específico

A política a seguir permite que um usuário execute todas as ações em um volume específico em um gateway. Como um usuário não tem nenhuma permissão por padrão, a política restringe que o usuário acesse apenas um volume específico.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "GrantsPermissionsToSpecificVolume",
            "Action": [
                "storagegateway:*"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:storagegateway:us-west-2:123456789012:gateway/gateway-
id/volume/volume-id"
        },
        {
            "Sid": "GrantsPermissionsToUseStorageGatewayConsole",
            "Action": [
```

```
                "storagegateway:ListGateways"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

A política anterior funcionará se o usuário ao qual a política está anexada usar a API ou umaAWSSDK para acessar o volume. No entanto, se esse usuário for usar oAWS Storage GatewayConsole, você também deve conceder permissões para permitir que`ListGateways`Ação, conforme mostrado no exemplo a seguir.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "GrantsPermissionsToSpecificVolume",
            "Action": [
                "storagegateway:*"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:storagegateway:us-west-2:123456789012:gateway/gateway-id/volume/volume-id"
        },
        {
            "Sid": "GrantsPermissionsToUseStorageGatewayConsole",
            "Action": [
                "storagegateway:ListGateways"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

Exemplo 5: Permitir todas as ações em gateways com um prefixo específico

A política a seguir autoriza que um usuário execute todas as ações do Storage Gateway em gateways com nomes que começam com`DeptX`. A política permite também o`DescribeSnapshots`A ação do Amazon EC2 é necessária se você quiser descrever snapshots.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowsActionsGatewayWithPrefixDeptX",
            "Action": [
                "storagegateway:*"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:storagegateway:us-west-2:123456789012:gateway/DeptX"
        },
        {
            "Sid": "GrantsPermissionsToSpecifiedAction",
            "Action": [
                "ec2:DescribeSnapshots"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

A política anterior funcionará se o usuário ao qual a política está anexada usar a API ou umaAWSSDK para acessar o gateway. No entanto, se esse usuário planeja usar oAWS Storage GatewayConsole, você deve conceder permissões adicionais, conforme descrito emExemplo 3: Permitir acesso a um gateway específico.

Usar tags para controlar o acesso ao seu gateway e aos recursos do

Para controlar o acesso a ações e recursos do gateway, você pode usar políticas do AWS Identity and Access Management (IAM) baseadas em tags. É possível conceder o controle de duas formas:

1. Controlar o acesso aos recursos do gateway com base nas tags desses recursos.
2. Controlar quais tags podem ser transmitidas em uma condição de solicitação do IAM.

Para obter informações sobre como usar tags para controlar o acesso, consulte Controle do acesso usando tags.

Controlar o acesso com base em tags em um recurso

Para controlar quais ações um usuário ou uma função pode executar em um recurso de gateway, é possível usar tags nesses recursos. Por exemplo, talvez você queira permitir ou negar operações de API específicas em um recurso de gateway de arquivos com base no par de chave/valor da tag no recurso.

O exemplo a seguir permite que um usuário ou uma função execute as ações `ListTagsForResource`, `ListFileShares` e `DescribeNFSFileShares` em todos os recursos. A política será aplicada somente se a tag no recurso tiver sua chave definida como `allowListAndDescribe` e o valor definido como `yes`.

```
{
  "Version": "2012-10-17",
   "Statement": [
      {
          "Effect": "Allow",
                    "Action": [
                        "storagegateway:ListTagsForResource",
                        "storagegateway:ListFileShares",
                        "storagegateway:DescribeNFSFileShares"
                    ],
                    "Resource": "*",
                    "Condition": {
                        "StringEquals": {
                            "aws:ResourceTag/allowListAndDescribe": "yes"
                        }
                    }
      },
      {
          "Effect": "Allow",
          "Action": [
              "storagegateway:*"
          ],
          "Resource": "arn:aws:storagegateway:region:account-id:*/*"
      }
  ]
}
```

Controlar o acesso com base em tags em uma solicitação do IAM

Para controlar o que um usuário do IAM pode fazer um recurso de gateway, é possível usar as condições em uma política do IAM baseada em tags. Por exemplo, você pode criar uma política que permita ou negue a um usuário do IAM a capacidade de executar operações de API específicas com base na tag fornecida na criação do recurso.

No exemplo a seguir, a primeira instrução permitirá que um usuário crie um gateway somente se o par de chave/valor da tag fornecida na criação do gateway for **`Department`** e **`Finance`**. Ao usar a operação da API, você adiciona essa tag à solicitação de ativação.

A segunda instrução permite que o usuário crie um compartilhamento de arquivos Network File System (NFS) ou Server Message Block (SMB) em um gateway somente se o par de chave/valor da tag no gateway corresponder a corresponder a corresponder a corresponder a corresponder a um par de chave/valor da**`Department`**e**`Finance`**. Além disso, o usuário deverá adicionar uma tag ao compartilhamento de arquivos e o par de chave/valor da tag deverá ser **`Department`** e **`Finance`**. Você adiciona tags a um compartilhamento de arquivos ao criar o compartilhamento de arquivos. Não há permissões para as operações `RemoveTagsFromResource` e `AddTagsToResource`, portanto, o usuário não pode executar essas operações no gateway nem no compartilhamento de arquivos.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "storagegateway:ActivateGateway"
         ],
         "Resource":"*",
         "Condition":{
            "StringEquals":{
               "aws:RequestTag/Department":"Finance"
            }
         }
      },
      {
         "Effect":"Allow",
         "Action":[
            "storagegateway:CreateNFSFileShare",
            "storagegateway:CreateSMBFileShare"
```

```
         ],
         "Resource":"*",
         "Condition":{
            "StringEquals":{
               "aws:ResourceTag/Department":"Finance",
               "aws:RequestTag/Department":"Finance"
            }
         }
      }
   ]
}
```

Usar as ACLs do Microsoft Windows para controlar o acesso a um compartilhamento de arquivos SMB

O Amazon S3 File Gateway oferece suporte a dois métodos diferentes para controlar o acesso a arquivos e diretórios armazenados por meio de um compartilhamento de arquivos SMB: Permissões POSIX ou ACLs do Windows.

Nesta seção, você pode encontrar informações sobre como usar listas de controle de acesso (ACLs) do Microsoft Windows em compartilhamentos de arquivos SMB habilitados com o Microsoft Active Directory (AD). Ao usar ACLs do Windows, você pode definir permissões refinadas em arquivos e pastas no seu compartilhamento de arquivos SMB.

Veja a seguir algumas características importantes de ACLs do Windows em compartilhamentos de arquivos SMB:

- As ACLs do Windows são selecionadas por padrão para compartilhamentos de arquivos SMB quando o Gateway de arquivos é associado a um domínio do Active Directory.
- Quando as ACLs são habilitadas, as informações da ACL são mantidas em metadados de objeto do Amazon S3.
- O gateway preserva até 10 ACLs por arquivo ou pasta.
- Quando você usa um compartilhamento de arquivos SMB ativado com ACLs para acessar objetos do S3 criados fora de seu gateway, os objetos herdam as informações das ACLs da pasta pai.
- A ACL raiz padrão para um compartilhamento de arquivos SMB fornece acesso total a todos os usuários, mas você pode alterar as permissões da ACL raiz. É possível usar ACLs raiz para controlar o acesso ao compartilhamento de arquivos. Você pode definir quem pode montar o compartilhamento de arquivos (mapear a unidade) e quais permissões o usuário recebe para os arquivos e as pastas recursivamente no compartilhamento de arquivos. No entanto,

recomendamos que definir essa permissão na pasta de nível superior no bucket do S3 para que sua ACL seja mantida.

Você pode ativar as ACLs do Windows quando cria um novo compartilhamento de arquivos CMB usando a operação de API CreateSMBFileShare. Ou você pode ativar as ACLs do Windows em um compartilhamento de arquivos SMB existente usando a operação de API UpdateSMBFileShare.

Como habilitar ACLs do Windows em um novo compartilhamento de arquivos SMB

Execute as seguintes etapas para habilitar as ACLs do Windows em um novo compartilhamento de arquivos SMB.

Para habilitar as ACLs do Windows ao criar um novo compartilhamento de arquivos SMB

1. Crie um gateway de arquivos se você ainda não tiver um. Para obter mais informações, consulte .
2. Se o gateway não tiver ingressado em um domínio, adicione-o a um domínio. Para obter mais informações, consulte .
3. Crie um compartilhamento de arquivos SMB.
4. Habilite a ACL do Windows no compartilhamento de arquivos no console do Storage Gateway.

   Para usar o console do Storage Gateway, faça o seguinte:

   a. Escolha o compartilhamento de arquivos e selecione Edit file share (Editar o compartilhamento de arquivos).
   b. Para a opção File/directory access controlled by (Acesso a arquivo/diretório controlado por), selecione Windows Access Control List (Lista de controle de acesso do Windows).
5. (Opcional) Adicione um usuário administrador à AdminUsersList, se você quiser que o usuário administrador tenha privilégios para atualizar as ACLs em todos os arquivos e pastas no compartilhamento de arquivos.
6. Atualize as ACLs das pastas pai na pasta raiz. Para fazer isso, use o Explorador de Arquivos do Windows para configurar as ACLs em pastas no compartilhamento de arquivos SMB.

> **Note**
>
> Se você configurar as ACLs na raiz em vez de na pasta pai na raiz, as permissões da ACL não serão mantidas no Amazon S3.

Recomendamos definir ACLs na pasta de nível superior na raiz do seu compartilhamento de arquivos, em vez de definir ACLs diretamente na raiz do compartilhamento de arquivos. Essa abordagem mantém as informações como metadados de objeto no Amazon S3.

7. Habilite a herança conforme apropriado.

> **Note**
>
> Você pode Habilitar a herança para compartilhamentos de arquivos criados após 8 de maio de 2019.

Se você habilitar a herança e atualizar as permissões recursivamente, o Storage Gateway atualizará todos os objetos no bucket do S3. Dependendo do número de objetos no bucket, a atualização pode demorar um pouco para ser concluída.

Como habilitar ACLs do Windows em um compartilhamento de arquivos SMB existente

Execute as seguintes etapas para habilitar ACLs do Windows em um compartilhamento de arquivos SMB existente com permissões POSIX.

Como habilitar as ACLs do Windows em um compartilhamento de arquivos SMB existente usando o console do Storage Gateway

1. Escolha o compartilhamento de arquivos e selecione Edit file share (Editar o compartilhamento de arquivos).
2. Para a opção File/directory access controlled by (Acesso a arquivo/diretório controlado por), selecione Windows Access Control List (Lista de controle de acesso do Windows).
3. Habilite a herança conforme apropriado.

> **Note**
>
> Não recomendamos definir as ACLs no nível raiz porque, se você fizer isso e excluir seu gateway, precisará redefinir as ACLs novamente.

Se você habilitar a herança e atualizar as permissões recursivamente, o Storage Gateway atualizará todos os objetos no bucket do S3. Dependendo do número de objetos no bucket, a atualização pode demorar um pouco para ser concluída.

Limitações de uso de ACLs do Windows

Mantenha os seguintes limites em mente ao usar as ACLs do Windows para controlar o acesso a compartilhamentos de arquivos SMB:

- As ACLs do Windows são compatíveis somente com compartilhamentos de arquivos que são habilitados para o Active Directory ao usar clientes do Windows SMB para acessar os compartilhamentos de arquivos.
- Os gateways de arquivos comportam um máximo de 10 entradas de ACL para cada arquivo e diretório.
- Os gateways de arquivos não oferecem suporte ao`AuditeAlarm`As entradas, que são entradas da lista de controle de acesso do sistema (SACL). Os gateways de arquivos são compatíveis com as entradas `Allow` e `Deny`, que são entradas discricionárias de lista de controle de acesso (DACL).
- As configurações de ACL raiz de compartilhamentos de arquivos SMB estão apenas no gateway, e as configurações são mantidas em atualizações e reinicializações de gateway.

> **Note**
>
> Se você configurar as ACLs na raiz em vez de na pasta pai na raiz, as permissões da ACL não serão mantidas no Amazon S3.

Dadas essas condições, faça o seguinte:

- Se você configurar vários gateways para acessar o mesmo bucket do Amazon S3, configure a ACL raiz em cada um dos gateways para manter as permissões consistentes.
- Se você excluir um compartilhamento de arquivos e recriá-lo no mesmo bucket do Amazon S3, use o mesmo conjunto de ACLs raiz.

Permissões da API Storage Gateway Referência de ações, recursos e condições

Ao configurar o controle de acesso e elaborar políticas de permissões que você pode associar a uma identidade do IAM (políticas baseadas em identidade), use a tabela a seguir como referência. A tabela indica cada operação de API do Storage Gateway, as ações correspondentes às quais você pode conceder permissões para executar a ação e oAWSRecurso para o qual você pode conceder as permissões. Você especifica as ações no campo `Action` da política e o valor do recurso no campo `Resource` da política.

Você pode usarAWSAs chaves de condição em toda a nas suas políticas do Storage Gateway para expressar condições. Para obter uma lista completa das chaves da AWS, consulte Chaves disponíveis no Guia do usuário do IAM.

> **Note**
>
> Para especificar uma ação, use o prefixo `storagegateway:` seguido do nome da operação da API (por exemplo, `storagegateway:ActivateGateway`). Para toda ação do Storage Gateway, você pode especificar um caractere curinga (*) como recurso.

Para obter uma lista de recursos do Storage Gateway com os formatos de ARN, consulteRecursos e operações do Storage Gateway.

A API do Storage Gateway e as permissões necessárias para as ações são as seguintes.

ActivateGateway

Ação/Ações: `storagegateway:ActivateGateway`

Recurso: *

AddCache

Ação/Ações: `storagegateway:AddCache`

Recurso: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*

AddTagsToResource

Ação/Ações: `storagegateway:AddTagsToResource`

Recurso: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

ou

arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/volume/*volume-id*

ou

arn:aws:storagegateway:*region*:*account-id*:tape/*tapebarcode*

AddUploadBuffer

Ação/Ações: storagegateway:AddUploadBuffer

Recurso: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

AddWorkingStorage

Ação/Ações: storagegateway:AddWorkingStorage

Recurso: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

CancelArchival

Ação/Ações: storagegateway:CancelArchival

Recurso: arn:aws:storagegateway:*region*:*account-id*:tape/*tapebarcode*

CancelRetrieval

Ação/Ações: storagegateway:CancelRetrieval

Recurso: arn:aws:storagegateway:*region*:*account-id*:tape/*tapebarcode*

CreateCachediSCSIVolume

Ação/Ações: storagegateway:CreateCachediSCSIVolume

Recurso: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

CreateSnapshot

Ação/Ações: storagegateway:CreateSnapshot

Recurso: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/volume/*volume-id*

CreateSnapshotFromVolumeRecoveryPoint

Ação/Ações: `storagegateway:CreateSnapshotFromVolumeRecoveryPoint`

Recurso: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*`/volume/`*`volume-id`*

CreateStorediSCSIVolume

Ação/Ações: `storagegateway:CreateStorediSCSIVolume`

Recurso: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*

CreateTapes

Ação/Ações: `storagegateway:CreateTapes`

Recurso: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*

DeleteBandwidthRateLimit

Ação/Ações: `storagegateway:DeleteBandwidthRateLimit`

Recurso: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*

DeleteChapCredentials

Ação/Ações: `storagegateway:DeleteChapCredentials`

Recurso: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*`/target/`*`iSCSItarget`*

DeleteGateway

Ação/Ações: `storagegateway:DeleteGateway`

Recurso: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*

DeleteSnapshotSchedule

Ação/Ações: `storagegateway:DeleteSnapshotSchedule`

Recurso: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*`/volume/`*`volume-id`*

DeleteTape

Ação/Ações: `storagegateway:DeleteTape`

Recurso: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

DeleteTapeArchive

Ação/Ações: storagegateway:DeleteTapeArchive

Recurso: *

DeleteVolume

Ação/Ações: storagegateway:DeleteVolume

Recurso: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/volume/*volume-id*

DescribeBandwidthRateLimit

Ação/Ações: storagegateway:DescribeBandwidthRateLimit

Recurso: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

DescribeCache

Ação/Ações: storagegateway:DescribeCache

Recurso: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

DescribeCachediSCSIVolumes

Ação/Ações: storagegateway:DescribeCachediSCSIVolumes

Recurso: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/volume/*volume-id*

DescribeChapCredentials

Ação/Ações: storagegateway:DescribeChapCredentials

Recurso: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/target/*iSCSItarget*

DescribeGatewayInformation

Ação/Ações: storagegateway:DescribeGatewayInformation

Recurso: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

DescribeMaintenanceStartTime

Ação/Ações: `storagegateway:DescribeMaintenanceStartTime`

Recurso: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*

DescribeSnapshotSchedule

Ação/Ações: `storagegateway:DescribeSnapshotSchedule`

Recurso: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*`/volume/`*`volume-id`*

DescribeStorediSCSIVolumes

Ação/Ações: `storagegateway:DescribeStorediSCSIVolumes`

Recurso: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*`/volume/`*`volume-id`*

DescribeTapeArchives

Ação/Ações: `storagegateway:DescribeTapeArchives`

Recurso: *

DescribeTapeRecoveryPoints

Ação/Ações: `storagegateway:DescribeTapeRecoveryPoints`

Recurso: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*

DescribeTapes

Ação/Ações: `storagegateway:DescribeTapes`

Recurso: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*

DescribeUploadBuffer

Ação/Ações: `storagegateway:DescribeUploadBuffer`

Recurso: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*

DescribeVTLDevices

Ação/Ações: `storagegateway:DescribeVTLDevices`

Recurso: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*

DescribeWorkingStorage

Ação/Ações: `storagegateway:DescribeWorkingStorage`

Recurso: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*

DisableGateway

Ação/Ações: `storagegateway:DisableGateway`

Recurso: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*

ListGateways

Ação/Ações: `storagegateway:ListGateways`

Recurso: *

ListLocalDisks

Ação/Ações: `storagegateway:ListLocalDisks`

Recurso: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*

ListTagsForResource

Ação/Ações: `storagegateway:ListTagsForResource`

Recurso: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*

ou

`arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*`/volume/`*`volume-id`*

ou

`arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:tape/`*`tapebarcode`*

ListTapes

Ação/Ações: `storagegateway:ListTapes`

Recurso: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*

ListVolumeInitiators

Ação/Ações: `storagegateway:ListVolumeInitiators`

Recurso: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/volume/*volume-id*

ListVolumeRecoveryPoints

Ação/Ações: storagegateway:ListVolumeRecoveryPoints

Recurso: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

ListVolumes

Ação/Ações: storagegateway:ListVolumes

Recurso: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

RemoveTagsFromResource

Ação/Ações: storagegateway:RemoveTagsFromResource

Recurso: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

ou

arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/volume/*volume-id*

ou

arn:aws:storagegateway:*region*:*account-id*:tape/*tapebarcode*

ResetCache

Ação/Ações: storagegateway:ResetCache

Recurso: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

RetrieveTapeArchive

Ação/Ações: storagegateway:RetrieveTapeArchive

Recurso: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

RetrieveTapeRecoveryPoint

Ação/Ações: storagegateway:RetrieveTapeRecoveryPoint

Recurso: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

ShutdownGateway

Ação/Ações: `storagegateway:ShutdownGateway`

Recurso: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*

StartGateway

Ação/Ações: `storagegateway:StartGateway`

Recurso: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*

UpdateBandwidthRateLimit

Ação/Ações: `storagegateway:UpdateBandwidthRateLimit`

Recurso: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*

UpdateChapCredentials

Ação/Ações: `storagegateway:UpdateChapCredentials`

Recurso: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*`/target/`*`iSCSItarget`*

UpdateGatewayInformation

Ação/Ações: `storagegateway:UpdateGatewayInformation`

Recurso: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*

UpdateGatewaySoftwareNow

Ação/Ações: `storagegateway:UpdateGatewaySoftwareNow`

Recurso: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*

UpdateMaintenanceStartTime

Ação/Ações: `storagegateway:UpdateMaintenanceStartTime`

Recurso: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*

UpdateSnapshotSchedule

Ação/Ações: `storagegateway:UpdateSnapshotSchedule`

Recurso: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*`/volume/`*`volume-id`*

UpdateVTLDeviceType

Ação/Ações: `storagegateway:UpdateVTLDeviceType`

Recurso: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*`/device/`*`vtldevice`*

Tópicos relacionados

- Controle de acesso
- Exemplos de política gerenciada pelo cliente

Usar funções vinculadas ao serviço para Storage Gateway

Use Storage GatewayAWS Identity and Access Management(IAM)Funções vinculadas ao serviço. Uma função vinculada ao serviço é um tipo exclusivo de função do IAM vinculada diretamente ao Storage Gateway. As funções vinculadas a serviços são predefinidas pelo Storage Gateway e incluem todas as permissões que o serviço requer para chamar outrosAWSServiços do em seu nome.

Uma função vinculada ao serviço facilita a configuração do Storage Gateway, já que não é preciso adicionar as permissões necessárias manualmente. O Storage Gateway define as permissões das funções vinculadas ao serviço e, exceto se definido de outra forma, somente o Storage Gateway pode assumir suas funções. As permissões definidas incluem a política de confiança e a política de permissões, e essa política não pode ser anexada a nenhuma outra entidade do IAM.

Para obter informações sobre outros serviços compatíveis com funções vinculadas a serviços, consulte AWS Serviços compatíveis com o IAM e procure os serviços que apresentam Yes (Sim) na coluna Service-Linked Role (Função vinculada a serviço). Escolha um Sim com um link para exibir a documentação da função vinculada a serviço desse serviço.

Permissões de função vinculada ao serviço para o Storage Gateway

O Storage Gateway usa a função vinculada ao serviço chamadaAWSServiceRoleForStorageGateWay— AWSServiceRoleForStorageGateWay.

A função vinculada ao serviço AWSServiceRoleForStorageGateway confia nos seguintes serviços para assumir a função:

- `storagegateway.amazonaws.com`

A política de permissões da função permite que o Storage Gateway conclua as seguintes ações nos recursos especificados:

- Ação: `fsx:ListTagsForResource` em `arn:aws:fsx:*:*:backup/*`

Você deve configurar permissões para permitir que uma entidade do IAM (por exemplo, um usuário, grupo ou função) crie e edite uma função vinculada ao serviço. Para obter mais informações, consulte Service-linked role permissions (Permissões de função vinculada a serviços) no Guia do usuário do IAM.

Criar uma função vinculada ao serviço para o Storage Gateway

Você não precisa criar manualmente uma função vinculada a serviço. Quando você cria um Storage Gateway`AssociateFileSystem`Chamada de API noAWS Management Console, oAWS CLI, ou oAWSO API, Storage Gateway cria a função vinculada ao serviço para você.

> **Important**
>
> Essa função vinculada ao serviço pode aparecer em sua conta se você concluiu uma ação em outro serviço que usa os recursos compatíveis com essa função. Além disso, se você estava usando o serviço Storage Gateway antes de 31 de março de 2021, quando ele começou a oferecer suporte a funções vinculadas a serviços, o Storage Gateway criou a função AWSServiceRoleForStorageGateway na sua conta. Para saber mais, consulte Uma nova função apareceu na minha conta do IAM.

Se você excluir essa função vinculada ao serviço e precisar criá-la novamente, poderá usar esse mesmo processo para recriar a função em sua conta. Quando você cria um Storage Gateway`AssociateFileSystem`A chamada de API do, o Storage Gateway cria a função vinculada ao serviço para você novamente.

Você também pode usar o console do IAM para criar uma função vinculada ao serviço com oAWSServiceRoleForStorageGateWayCaso de uso. Na AWS CLI ou na API do AWS, crie uma

função vinculada ao serviço com o nome de serviço `storagegateway.amazonaws.com`. Para obter mais informações, consulte Criar uma função vinculada ao serviço no Guia do usuário do IAM. Se você excluir essa função vinculada ao serviço, será possível usar esse mesmo processo para criar a função novamente.

Editar uma função vinculada ao serviço para Storage Gateway

O AWS Storage Gateway não permite que você edite a função vinculada ao serviço AWSServiceRoleForStorageGateway. Depois que criar uma função vinculada ao serviço, você não poderá alterar o nome da função, pois várias entidades podem fazer referência a ela. No entanto, você poderá editar a descrição da função usando o IAM. Para obter mais informações, consulte Editar uma função vinculada a serviço no Guia do usuário do IAM.

Excluir uma função vinculada ao serviço do Storage Gateway

O Storage Gateway não exclui automaticamente a função AWSServiceRoleForStorageGateWay. Para excluir a função AWSServiceRoleForStorageGateWay, você precisa invocar a função`iam:DeleteSLR`API. Se não houver recursos de gateway de armazenamento que dependam da função vinculada ao serviço, a exclusão será bem-sucedida, caso contrário, a exclusão falhará. Se você quiser excluir a função vinculada ao serviço, você precisa usar APIs do IAM`iam:DeleteRole`ou`iam:DeleteServiceLinkedRole`. Nesse caso, você precisa usar as APIs do Storage Gateway para primeiro excluir quaisquer gateways ou associações de sistemas de arquivos na conta e, em seguida, excluir a função vinculada ao serviço usando`iam:DeleteRole`ou`iam:DeleteServiceLinkedRole`API. Ao excluir a função vinculada ao serviço usando o IAM, você precisa usar o Storage Gateway`DisassociateFileSystemAssociation`API primeiro para excluir todas as associações de sistema de arquivos na conta. Caso contrário, a operação de exclusão falhará.

> **Note**
>
> Se o serviço Storage Gateway estiver usando a função quando tenta excluir os recursos, a exclusão poderá falhar. Se isso acontecer, espere alguns minutos e tente a operação novamente.

Como excluir recursos do Storage Gateway usados pelo AWSServiceRoleForStorageGateWay

1. Use nosso console de serviço, CLI ou API para fazer uma chamada que limpe os recursos e exclua a função ou use o console, a CLI ou a API do IAM para fazer a exclusão. Nesse caso,

você precisa usar as APIs do Storage Gateway para primeiro excluir quaisquer gateways e associações de sistemas de arquivos na conta.

2. Se você usar o console da IAM, a CLI ou a API, exclua a função vinculada ao serviço usando o IAM`DeleteRole`ou`DeleteServiceLinkedRole`API.

Como excluir manualmente a função vinculada ao serviço usando o IAM

Use o console do IAM, oAWS CLI, ou oAWSAPI do para excluir a função vinculada a serviço AWSServiceRoleForStorageGateWay. Para obter mais informações, consulte Excluir uma função vinculada ao serviço no Guia do usuário do IAM.

Regiões compatíveis com funções vinculadas ao serviço Storage Gateway

O Storage Gateway oferece suporte a funções vinculadas a serviços em todas as regiões em que o serviço está disponível. Para mais informações, consulte Endpoints de serviço da AWS.

O Storage Gateway não oferece suporte a funções vinculadas a serviços em todas as regiões em que o serviço está disponível. Você pode usar a função AWSServiceRoleForStorageGateWay nas regiões a seguir.

Nome da região	Identidade da região	Support no Storage Gateway
Leste dos EUA (Norte da Virgínia)	us-east-1	Sim
Leste dos EUA (Ohio)	us-east-2	Sim
US West (N. California)	us-west-1	Sim
Oeste dos EUA (Oregon)	us-west-2	Sim
Asia Pacific (Mumbai)	ap-south-1	Sim
Asia Pacific (Osaka)	ap-northeast-3	Sim
Ásia-Pacífico (Seul)	ap-northeast-2	Sim
Ásia-Pacífico (Singapura)	ap-southeast-1	Sim
Ásia-Pacífico (Sydney)	ap-southeast-2	Sim

Nome da região	Identidade da região	Support no Storage Gateway
Ásia-Pacífico (Tóquio)	ap-northeast-1	Sim
Canada (Central)	ca-central-1	Sim
Europa (Frankfurt)	eu-central-1	Sim
Europa (Irlanda)	eu-west-1	Sim
Europe (London)	eu-west-2	Sim
Europe (Paris)	eu-west-3	Sim
América do Sul (São Paulo)	sa-east-1	Sim
AWS GovCloud (US)	us-gov-west-2	Sim

Registrar em log e monitorar no AWS Storage Gateway

O Storage Gateway está integrado comAWS CloudTrail, um serviço que fornece um registro das ações executadas por um usuário, uma função ou umAWSserviço no Storage Gateway. O CloudTrail captura todas as chamadas de API para o Storage Gateway como eventos. As chamadas capturadas incluem 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 habilitar a entrega contínua de eventos do CloudTrail a um bucket do Amazon S3, incluindo eventos para o Storage Gateway. Se você não configurar uma trilha, ainda poderá visualizar os eventos mais recentes no console do CloudTrail em Event history (Histórico de eventos). Usando as informações coletadas pelo CloudTrail, é possível determinar a solicitação feita para o 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 sobre o CloudTrail, consulte o AWS CloudTrailGuia do usuário do .

Informações do Storage Gateway no CloudTrail

O CloudTrail é habilitado em sua conta da AWS quando ela é criada. Quando ocorre atividade no Storage Gateway, essa atividade é registrada em um evento do CloudTrail junto com outrosAWSEventos de serviço noHistórico do evento. Você pode visualizar, pesquisar e baixar os

eventos recentes em sua conta da AWS. Para obter mais informações, consulte Como visualizar eventos com o histórico de eventos do CloudTrail.

Para obter um registro contínuo de eventos em seuAWSConta, incluindo eventos do Storage Gateway, crie uma trilha. Uma trilha permite que o CloudTrail entregue arquivos de log a um bucket do Amazon S3. Por padrão, quando você cria uma trilha no console, ela é aplicada a todas as regiões da AWS. A trilha registra em log eventos de todas as regiões na partição da AWS e entrega os arquivos de log para o bucket do Amazon S3 especificado por você. Além disso, você pode configurar outros produtos da AWS para analisar mais profundamente e agir sobre os dados de eventos coletados nos logs do CloudTrail. Para obter mais informações, consulte:

- Visão geral da criação de uma trilha
- CloudTrail Serviços compatíveis e integrações do
- Configuração de notificações do Amazon SNS para o CloudTrail
- Receber arquivos de log do CloudTrail de várias regiões e receber arquivos de log do CloudTrail de várias contas

Todas as ações do Storage Gateway são registradas em log e documentadas noAçõestópico. Por exemplo, as chamadas para as APIs `ActivateGateway`, `ListGateways` e `ShutdownGateway` geram entradas nos arquivos de log do CloudTrail.

Cada entrada de log ou evento contém informações sobre quem gerou a solicitação. As informações de identidade ajudam a determinar:

- Se a solicitação foi feita com credenciais de usuário raiz ou do AWS Identity and Access Management (IAM).
- Se a solicitação foi feita com credenciais de segurança temporárias de uma função ou de um usuário federado.
- Se a solicitação foi feita por outro serviço da AWS.

Para obter mais informações, consulte o Elemento userIdentity do CloudTrail.

Noções básicas sobre as entradas de arquivos de log

Uma trilha é uma configuração que permite a entrega de eventos como arquivos de log a um bucket do Amazon S3 especificado. Os arquivos de log do CloudTrail contêm uma ou mais entradas de log. Um evento representa uma única solicitação de qualquer origem e inclui informações sobre a ação

solicitada, a data e a hora da ação, os parâmetros de solicitação e assim por diante. Os arquivos de log do CloudTrail não são um rastreamento de pilha ordenada de chamadas de API pública. Dessa forma, eles não são exibidos em uma ordem específica.

O exemplo a seguir mostra uma entrada de log do CloudTrail que demonstra a ação .

```
{ "Records": [{
               "eventVersion": "1.02",
               "userIdentity": {
               "type": "IAMUser",
               "principalId": "AIDAII5AUEPBH2M7JTNVC",
               "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": "cloudtrailgatewayvtl",
                                        "gatewayRegion": "us-east-2",
                                        "activationKey": "EHFBX-1NDD0-P0IVU-PI259-
DHK88",
                                        "gatewayType": "VTL"
                                             },
                                             "responseElements": {
                                                                   "gatewayARN":
 "arn:aws:storagegateway:us-east-2:111122223333:gateway/cloudtrailgatewayvtl"
                                             },
                                             "requestID":
 "54BTFGNQI71987UJD2IHTCT8NF1Q8GLLE1QEU3KPGG6F0KSTAUU0",
                                             "eventID": "635f2ea2-7e42-45f0-
bed1-8b17d7b74265",
                                             "eventType": "AwsApiCall",
                                             "apiVersion": "20130630",
                                             "recipientAccountId": "444455556666"
             }]
}
```

O exemplo a seguir mostra uma entrada de log do CloudTrail que demonstra a ação ListGateways.

```
{
 "Records": [{
               "eventVersion": "1.02",
               "userIdentity": {
                                "type": "IAMUser",
                                "principalId": "AIDAII5AUEPBH2M7JTNVC",
                                "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 ":"
 6U2N42CU37KAO8BG6V1I23FRSJ1Q8GLLE1QEU3KPGG6F0KSTAUU0 ",
                                " eventID ":" f76e5919 - 9362 - 48ff - a7c4 -
 d203a189ec8d ",
                                " eventType ":" AwsApiCall ",
                                " apiVersion ":" 20130630 ",
                                " recipientAccountId ":" 444455556666"
             }]
}
```

Validação de conformidade doAWSStorage Gateway

Auditores de terceiros avaliam a segurança e a conformidade doAWSStorage Gateway como parte de váriosAWSProgramas de conformidade. Eles incluem SOC, PCI, ISO, FedRAMP, HIPAA, MTCS, C5, K-ISMS, ENS High, OSPAR e HITRUST CSF.

Para obter uma lista de serviços da AWS no escopo de programas de conformidade específicos, consulte Serviços da AWS no escopo por programa de conformidade. Para obter informações gerais, consulte Programas de conformidade da AWS.

Você pode fazer download de relatórios de auditoria de terceiros usando o AWS Artifact. Para obter mais informações, consulte Fazer download de relatórios no AWS Artifact.

Sua responsabilidade de conformidade ao usar o Storage Gateway é determinada pela confidencialidade dos dados, pelos objetivos de conformidade da empresa e pelos regulamentos e leis aplicáveis.AWSO fornece os seguintes recursos para ajudar com a conformidade:

- Guias de início rápido de segurança e compatibilidade: estes guias de implantação abordam as considerações de arquitetura e fornecem etapas para implantação de ambientes de linha de base focados em compatibilidade e segurança na AWS.
- Whitepaper Architecting for HIPAA Security and Compliance: este whitepaper descreve como as empresas podem usar a AWS para criar aplicações em conformidade com a HIPAA.
- Recursos de conformidade da AWS: essa coleção de manuais e guias pode ser aplicada a seu setor e local.
- Avaliar recursos com regras no Guia do desenvolvedor do AWS Config: o serviço AWS Config avalia como as configurações de recursos estão em compatibilidade com práticas internas, diretrizes do setor e regulamentos.
- AWS Security Hub: esse serviço da AWS fornece uma visão abrangente do estado de sua segurança na AWS que ajuda você a verificar sua conformidade com padrões e práticas recomendadas de segurança do setor.

Resiliência noAWSStorage Gateway

A infraestrutura global da AWS é criada com base em regiões da AWS e zonas de disponibilidade. As regiões da AWS fornecem várias zonas de disponibilidade separadas e isoladas fisicamente, que são conectadas com baixa latência, altas taxas de transferência e redes altamente redundantes. Com as zonas de disponibilidade, você pode projetar e operar aplicações e bancos de dados que automaticamente executam o failover entre as zonas sem interrupção. As zonas de disponibilidade são mais altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de data center tradicionais.

Para obter mais informações sobre regiões e zonas de disponibilidade da AWS, consulte Infraestrutura global da AWS.

Além doAWSO Storage Gateway oferece vários recursos para ajudar a oferecer suporte às suas necessidades de backup e resiliência de dados:

- 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 obter mais informações, consulteUsar o VMware vSphere High Availability com Storage Gateway.
- Use o AWS Backup para fazer backup de seus volumes. Para obter mais informações, consulteO uso doAWS BackupPara fazer backup de seus volumes.
- Clone seu volume a partir de um ponto de recuperação. Para obter mais informações, consulteComo clonar um volume.
- Arquive fitas virtuais no Amazon S3 Glacier. Para obter mais informações, consulteComo arquivar fitas virtuais.

Segurança da infraestrutura noAWSStorage Gateway

Como um serviço gerenciado,AWSO Storage Gateway é protegido peloAWSProcedimentos de segurança de rede global da descritos noAmazon Web Services: Visão geral dos processos de segurançaWhitepaper.

Você usaAWSAs chamadas de API publicadas pela para acessar o Storage Gateway pela rede. Os clientes devem oferecer suporte a Transport Layer Security (TLS) 1.0 ou posterior. Recomendamos TLS 1.2 ou posterior. Os clientes também devem ter suporte a conjuntos de criptografia com perfect forward secrecy (PFS) como Ephemeral Diffie-Hellman (DHE) ou Ephemeral Elliptic Curve Diffie-Hellman (ECDHE). A maioria dos sistemas modernos como Java 7 e versões posteriores oferece suporte a esses modos.

Além disso, as solicitações devem ser assinadas usando um ID da chave de acesso e uma chave de acesso secreta associada a uma entidade principal do IAM. Ou você pode usar o AWS Security Token Service (AWS STS) para gerar credenciais de segurança temporárias para assinar solicitações.

Práticas recomendadas de segurança para o Storage Gateway

AWSO Storage Gateway fornece uma série de recursos de segurança a serem considerados no desenvolvimento e na implementação das suas próprias políticas de segurança. As melhores práticas a seguir são diretrizes gerais e não representam uma solução completa de segurança. Como essas práticas recomendadas podem não ser adequadas ou suficientes no seu

ambiente, trate-as como considerações úteis em vez de requisitos. Para obter mais informações, consulteAWSMelhores práticas de segurança.

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 Amazon S3 File Gateway. As informações sobre solução de problemas em volumes aplicam-se ao tipo de gateway de volume. As informações sobre solução de problemas em fitas aplicam-se ao tipo de gateway de fita. As informações sobre solução de problemas no gateway se aplicam ao uso de métricas do CloudWatch. As informações de solução de problemas de alta disponibilidade abrangem gateways executados na plataforma VMware vSphere High Availability (HA).

Tópicos

Como solucionar problemas no gateway no local

Você encontrará informações a seguir sobre problemas comuns que podem ocorrer ao trabalhar com gateways locais e como ativar os problemas comuns que podem ocorrer ao trabalhar com gateways locais e como ativarAWS SupportPara ajudar a solucionar problemas do 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.	Use o cliente do hipervisor para se conectar ao host e encontrar o endereço IP do gateway. • 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. Se você ainda estiver tendo dificuldade para encontrar o endereço IP do gateway: • 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.	• Conceda permissão às portas apropriadas para seu gateway. • Se você usar um firewall ou router para filtrar ou limitar o tráfego de rede, deverá configurar o firewall e o roteador para permitir comunicação externa desses endpoints de serviçoAWS. Para obter mais informações sobre requisitos de rede e firewall, consulte Requisitos de rede e firewall.
A ativação do gateway falha quando você clica noProssiga para ativaçãono Storage Gateway Management Console.	• 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 Testando a conectividade de rede do gateway. • 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 sincroniz

Problema	Medida a ser tomada
	ação de horário de hosts e VMs de hipervisor, consulte Configurar um servidor NTP (Network Time Protocol) para seu gateway. • Depois que executar essas etapas, poderá realizar novamente a implantação de gateway usando o console do Storage Gateway e oConfigurar e ativar o gatewayassistente. • 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 obter mais informações, consulte Requisitos de configuração do gateway.
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.	

Problema	Medida a ser tomada
Você precisa melhorar a largura de banda entre o gateway eAWS.	É possível melhorar a largura de banda entre o gateway e a AWS configurando a conexão de Internet com a AWS em um adaptador de rede (NIC) separado daquele que você usa para conectar os aplicativos e a VM do gateway. Essa abordagem é útil se você tiver uma conexão com a AWS com alta largura de banda e desejar evitar a contenção de largura de banda, especialmente durante a restauração de snapshots. Para necessidades de carga de trabalho de alto rendimento, você pode usarAWS Direct ConnectPara estabelecer uma conexão de rede dedicada entre o gateway local eAWS. Para medir a largura de banda da conexão de seu gateway com a AWS, use as métricas `CloudBytesDownloaded` e `CloudBytesUploaded` do gateway. Para saber mais sobre esse assunto, consulte Performance. Ao melhorar a conectividade com a Internet, você ajuda a evitar que o buffer de upload se esgote.

Problema	Medida a ser tomada

A taxa de transferência de ou para seu gateway cai para zero.	• NoGatewayNa guia 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 Microsoft Hyper-V Manager). Se você encontrar alguma incompatibilidade, reinicie seu gateway no console do Storage Gateway, tal como mostrado emDesligar a VM do gateway. Após o reinício, os endereços noEndereços IPlista no console do Storage GatewayGatewayDeve correspon der aos endereços IP de seu gateway, que determinados no cliente do hipervisor client.
	  • 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 gateway com a AWS, tal como descrito em Testando a conectividade de rede do gateway.
	• Verifique a configuração do adaptador de rede do gateway e confirme se todas as interfaces que você queria que estivesse m habilitadas para o gateway estão habilitadas. Para visualiza r a configuração do adaptador de rede de seu gateway, siga as instruções em Configurar adaptadores de rede para seu gateway e selecione a opção para visualizar a configuração de rede do gateway.
	
	É possível visualizar a taxa de transferência para e do gateway por meio do console do Amazon CloudWatch. Para obter mais informações sobre como medir a taxa de transferência entre o gateway e a AWS, consulte Performance.

Você está tendo problemas para importar (implanta r) o Storage Gateway no Microsoft Hyper-V.	Consulte Como solucionar problemas de configuração do Microsoft Hyper-V, que examina alguns dos problemas comuns na implantaç ão de um gateway no Microsoft Hyper-V.

Problema	Medida a ser tomada
Você recebe uma mensagem dizendo: “Os dados que foram gravados no volume do gateway não são armazenados com segurança noAWS“.	Você receberá essa mensagem se a VM do gateway foi criada a partir de um clone ou snapshot de outra VM do gateway. Se esse não for o caso, entre em contato comAWS Support.

HabilitarAWS Supportpara ajudar a solucionar problemas do gateway hospedado no local

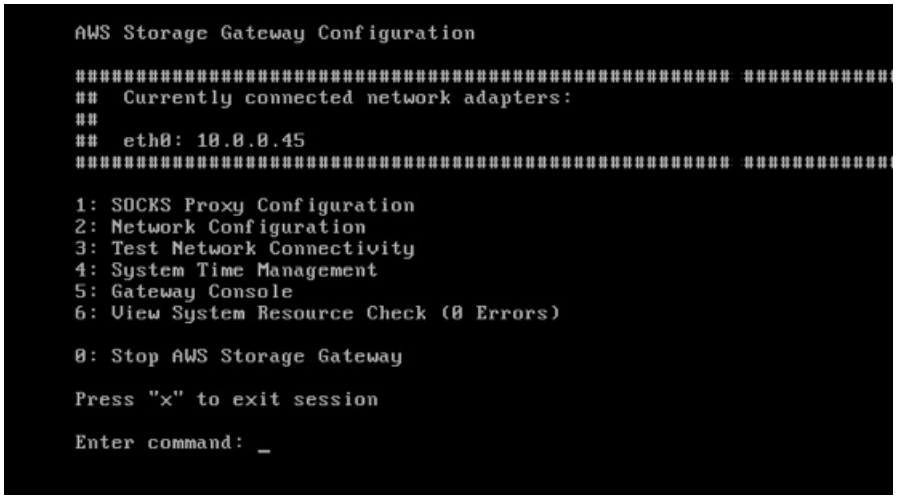
O Storage Gateway fornece um console local que você pode usar para executar várias tarefas de manutenção, incluindo a ativaçãoAWS SupportPara acessar o gateway para ajudá-lo a solucionar problemas de gateway. Por padrão,AWS SupportO acesso ao seu gateway está desativado. Esse acesso é ativado por meio do console local do host. Para darAWS SupportPara acessar o gateway, primeiro faça login no console local do host, navegue até o console do gateway de armazenamento e conecte-se ao servidor do suporte.

Para habilitar oAWS SupportAcesso ao seu gateway

1. Faça login no console local do host.

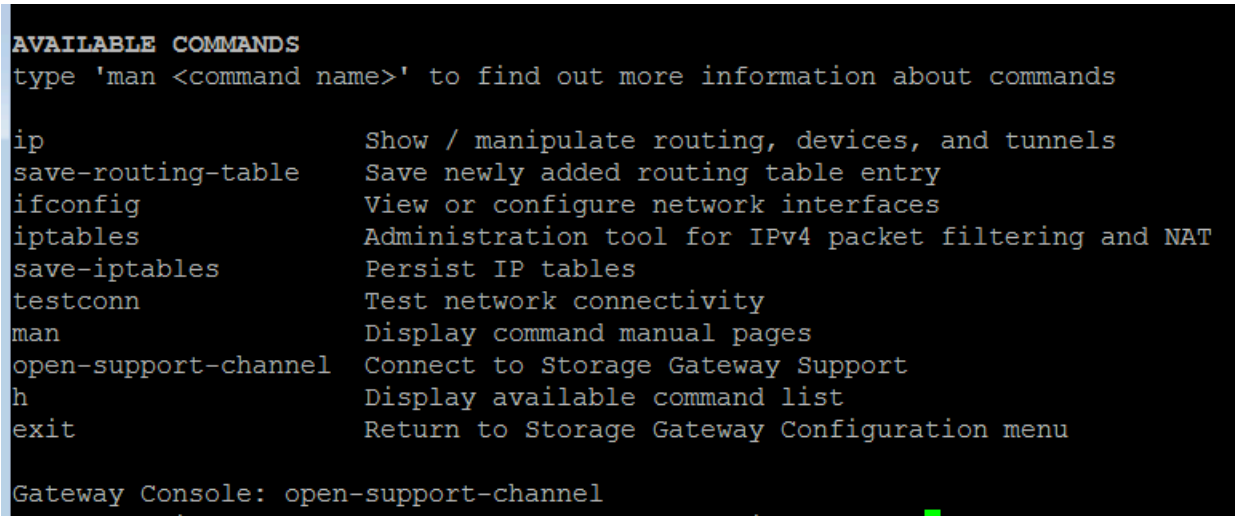
   - VMware ESXi: para obter mais informações, consulteAcesso ao console local do gateway com o VMware ESXi.
   - Microsoft Hyper-V — Para obter mais informações, consulteAcessar o console local do gateway com o Microsoft Hyper-V.

   O console local tem a seguinte aparência.



2. No prompt, insira**5**para abrir oAWS SupportConsole de canal.
3. Insira **h** para abrir a janela AVAILABLE COMMANDS (Comandos disponíveis).
4. Execute um destes procedimentos:

   - Se o gateway estiver usando um endpoint público, noCOMANDOS DISPONÍVEISjanela, insira**`open-support-channel`**para se conectar ao suporte ao cliente para o Storage Gateway. Permita a porta TCP 22 para que você possa abrir um canal de suporte paraAWS. 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 VPC endpoint ou o endereço IP para se conectar ao suporte ao cliente do Storage Gateway. Permita a porta TCP 22 para que você possa abrir um canal de suporte paraAWS. Quando se conectar ao suporte ao cliente, o Storage Gateway atribuirá a você um número de suporte. Anote seu número de suporte.



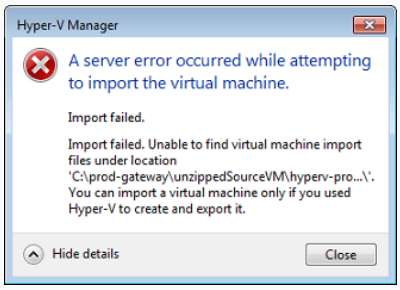
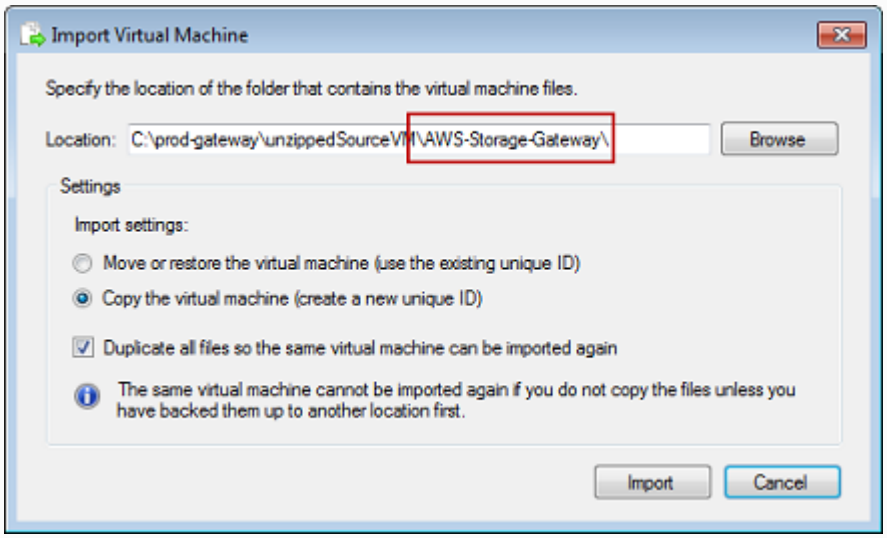
> **Note**
>
> O número do canal não é um número de porta de Transmission Control Protocol/User Datagram Protocol (TCP/UDP). Na verdade, o gateway faz uma conexão Secure Shell (SSH) (TCP 22) com os servidores do Storage Gateway e providencia o canal de suporte para a conexão.

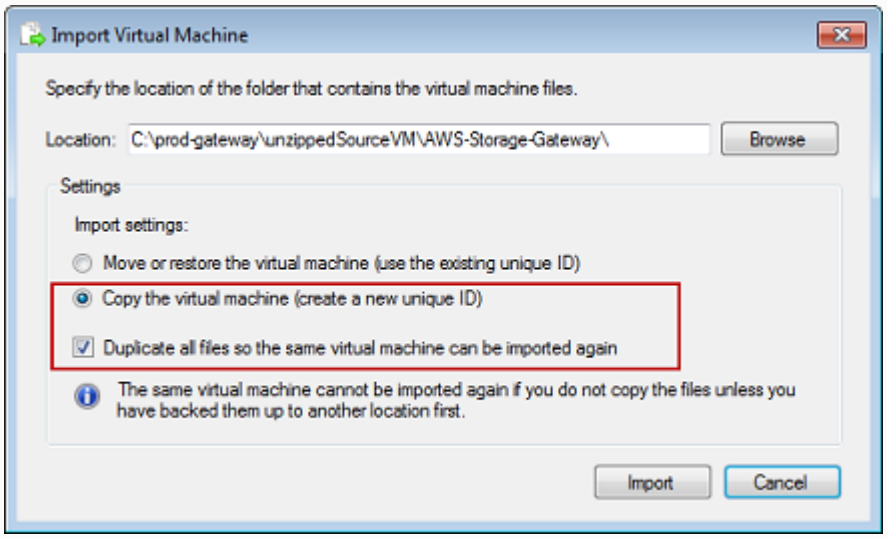
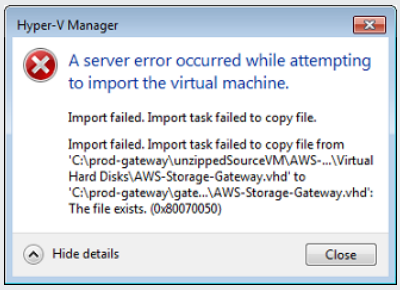
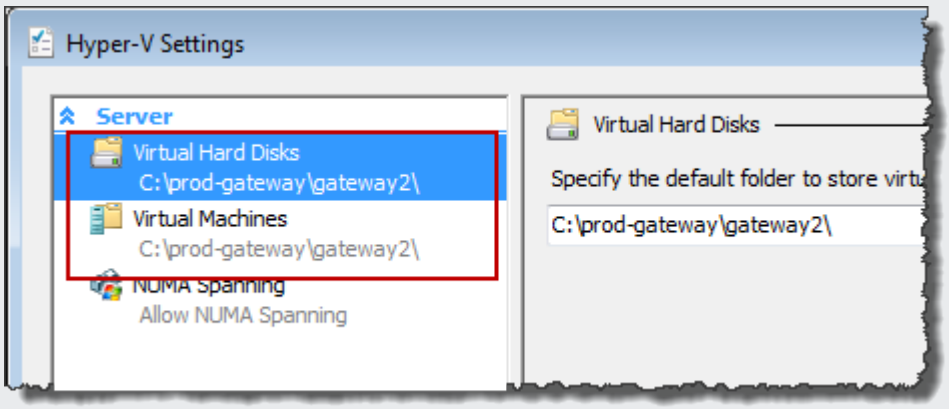
5. Depois que o canal de suporte for estabelecido, forneça o número de serviço de suporte aoAWS SupportentãoAWS Supportpode fornecer assistência para solução de problemas.
6. Quando a sessão de suporte for concluída, insira **q** para finalizá-la. Não feche a sessão até que o Amazon Web Services Support notifique você de que a sessão de suporte está concluída.
7. Digite**`exit`**Para encerrar a sessão do console Storage Gateway.
8. Siga as instruções para sair do console local.

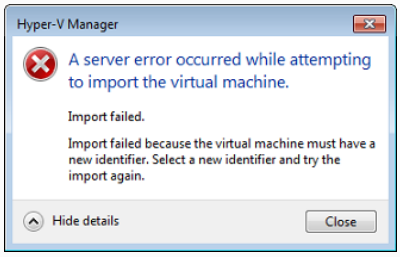
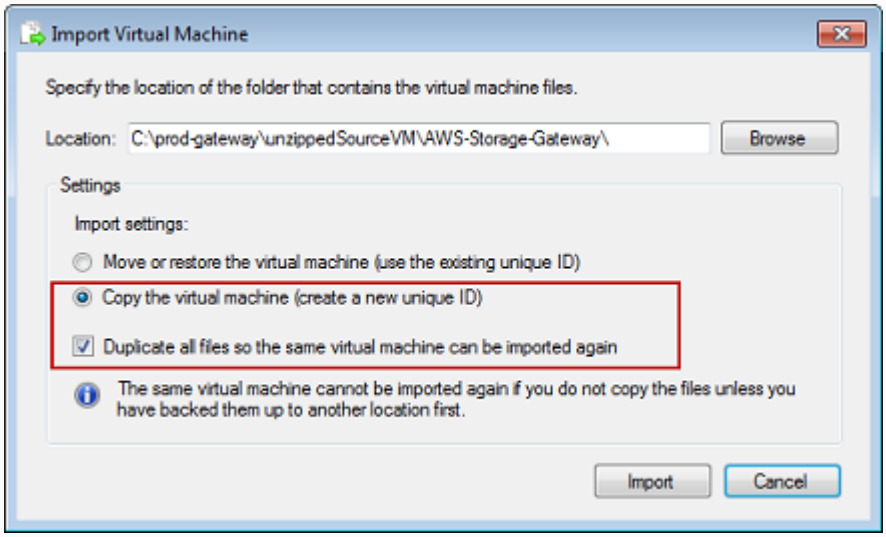
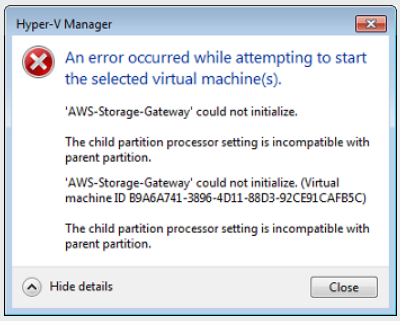
Como solucionar problemas de configuração do Microsoft Hyper-V

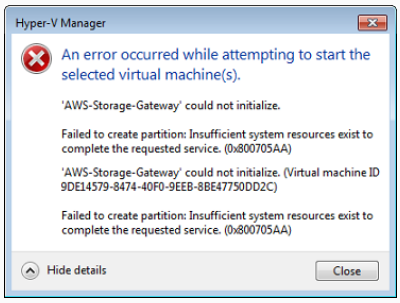
A tabela a seguir lista problemas comuns que você pode encontrar ao implantar o Storage Gateway na plataforma Microsoft Hyper-V.

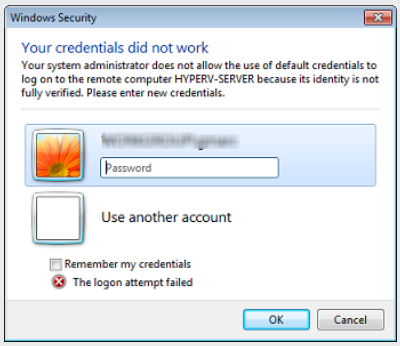
Problema	Medida a ser tomada
Você tenta importar um gateway e recebe a	Esse erro pode ocorrer pelos seguintes motivos:

Problema	Medida a ser tomada
mensagem de erro: “Falha na importação. Unable to find virtual machine import file under location...". 	• 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: “A importação falhou. 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
Você tenta importar um gateway e recebe uma mensagem de erro: “A importação falhou. Import failed because the virtual machine must have a new identifier. Select a new identifier and try the import again". 	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. 
Você tenta iniciar uma VM do gateway e recebe a mensagem de erro "The child partition processor setting is incompatible with parent partition". 	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. Para obter mais informações sobre os requisitos do Storage Gateway, consulteRequisitos de configuração do gateway.

Problema	Medida a ser tomada
Você tenta iniciar uma VM de um gateway e recebe a mensagem de erro “Failed to create partition: Existem recursos insuficientes para concluir o serviço solicitado.” 	Esse erro provavelmente é provocado por uma discrepância de RAM, entre a RAM necessária ao gateway e a RAM disponível no host. Para obter mais informações sobre os requisitos do Storage Gateway, consulteRequisitos de configuração do gateway.
Os snapshots e as atualizações de software do gateway estão ocorrendo em momentos levemente diferentes do que o previsto.	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 obter mais informações, consulte Configurar um servidor NTP (Network Time Protocol) para seu gateway.
É necessário colocar os arquivos descompactados do Storage Gateway do Microsoft Hyper-V no sistema de arquivos do host.	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 `hyperv-server` , você poderá usar o seguinte caminho UNC `\\hyperv-server\c$` , que pressupõe que o nome `hyperv-server` pode ser resolvido ou é definido em seu arquivo de hosts locais.

Problema	Medida a ser tomada
Você será solicitado a fornecer credenciais ao se conectar ao hipervisor. 	Adicione suas credenciais de usuário como administrador local para o host do hipervisor usando a ferramenta Sconfig.cmd.

Solução de problemas do 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 local e um gateway implantado no Amazon EC2, consulteImplantar um gateway de arquivos em um host do Amazon EC2.

Para obter informações sobre como usar o armazenamento temporário, consulte Usando armazenamento efêmero com gateways EC2.

Tópicos

- A ativação do gateway não ocorreu após alguns instantes
- Você não consegue localizar a instância do gateway do EC2 na lista de instâncias
- Você querAWS Supportpara ajudar a solucionar problemas do gateway EC2

A ativação do gateway não ocorreu após alguns instantes

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 do grupo de segurança, consulteAdicionar uma regra de security groupnoGuia do usuário do Amazon EC2 para instâncias do Linux.

- A instância do gateway está marcada como em execução. No console do Amazon EC2, oEstadoO valor para a instância deve ser RUNNING.
- Certifique-se de que o tipo de instância do Amazon EC2 atende aos requisitos mínimos, conforme descrito emRequisitos de armazenamento.

Depois de corrigir o problema, tente ativar o gateway novamente. Para isso, abra o console Storage Gateway, escolhaImplantar um novo gateway no Amazon EC2e insira novamente o endereço IP da instância.

Você não consegue localizar 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. Instâncias baseadas na AMI do Storage Gateway devem iniciar com o texto**`aws-storage-gateway-ami`**.
- Se tiver várias instâncias baseadas na AMI do Storage Gateway AMI, verifique o horário de execução da instância para localizar a instância correta.

Você querAWS Supportpara ajudar a solucionar problemas do gateway EC2

O Storage Gateway fornece um console local que você pode usar para executar várias tarefas de manutenção, incluindo a ativaçãoAWS SupportPara acessar o gateway para ajudá-lo a solucionar problemas de gateway. Por padrão,AWS SupportO acesso ao seu gateway está desativado. Esse acesso é habilitado por meio do console local do Amazon EC2. Você faz login no console local do Amazon EC2 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 security groups e como adicionar regras a eles, consulteGrupos de segurança do Amazon EC2noGuia do usuário do Amazon EC2.

Para deixarAWS SupportConecte-se ao seu gateway, primeiro faça login no console local da Instância do Amazon EC2 do, navegue até o console do gateway de armazenamento e ofereça acesso.

Para habilitar oAWS SupportAcesso a um gateway implantado em uma instância do Amazon EC2

1. Faça login no console local da Instância do Amazon EC2. Para obter instruções, vá paraConecte-se à sua instânciaGuia 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*CHAVE PRIVADA*é o`.pem`O contém o certificado privado do key pair do EC2 que você usou para executar a Instância do Amazon EC2. Para obter mais informações, consulteRecuperar a chave pública para seu par de chavesnoGuia do usuário do Amazon EC2.
   >
   > O*INSTANCE-PUBLIC-DNS-NAME*É o nome Domain Name System (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 no botãoDescriçãoGuia do.

2. No prompt, insira**6 - Command Prompt**para abrir oAWS SupportConsole de canal.
3. Insira **h** para abrir a janela AVAILABLE COMMANDS (Comandos disponíveis).
4. Execute um destes procedimentos:

   - Se o gateway estiver usando um endpoint público, noCOMANDOS DISPONÍVEISjanela, insira**open-support-channel**para se conectar ao suporte ao cliente para o Storage Gateway. Permita a porta TCP 22 para que você possa abrir um canal de suporte paraAWS. 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 VPC endpoint ou o endereço IP para se conectar ao suporte ao cliente do Storage Gateway. Permita a porta TCP 22 para que você possa abrir um canal de suporte paraAWS. 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 o número de serviço de suporte aoAWS SupportentãoAWS Supportpode fornecer assistência para solução de problemas.
6. Quando a sessão de suporte for concluída, insira **`q`** para finalizá-la. Não feche a sessão até que o Amazon Web Services Support notifique você de que a sessão de suporte está concluída.
7. Digite**`exit`**Para encerrar o console Storage Gateway.
8. Siga os menus do console para sair da instância do Storage Gateway.

Como solucionar problemas do dispositivo de hardware de

Os tópicos a seguir discutem os problemas que você pode encontrar com o dispositivo de hardware do Storage Gateway e sugestões sobre como solucioná-los.

Você não pode 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 você executa uma redefinição de fábrica?

Se precisar executar uma redefinição de fábrica no seu dispositivo, entre em contato com a equipe de hardware do Storage Gateway para obter Support do, como descrito na seção sobre suporte a seguir.

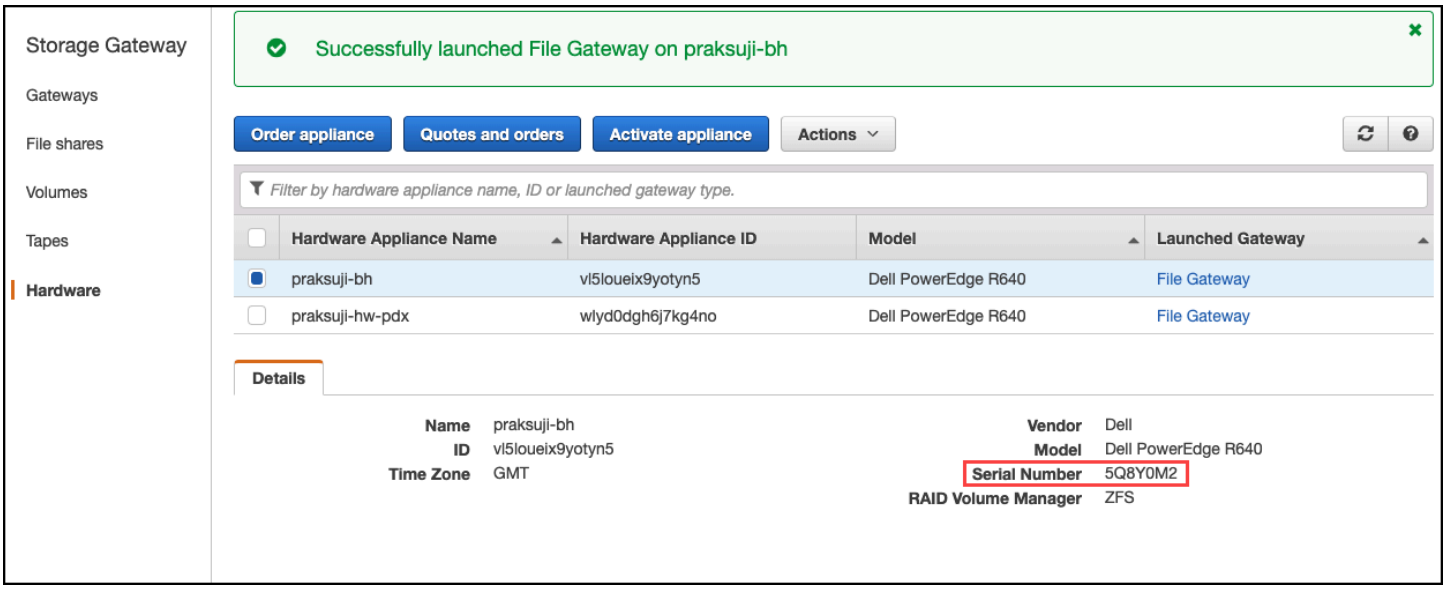
Onde você obtém o suporte Dell iDRAC?

O servidor Dell PowerEdge R640 vem com a interface de gerenciamento do Dell iDRAC. Recomendamos o seguinte:

- Se você usar a interface de gerenciamento do iDRAC, altere a senha padrão. Para obter mais informações sobre as credenciais do iDRAC, consulteDell PowerEdge - Qual é o nome de usuário e senha padrão do iDRAC?.
- Confira se o firmware está atualizado para evitar violações de segurança.
- 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 equipamento de hardware

Para localizar o número de série do equipamento de hardware, acesse aHardwareNo console Storage Gateway, conforme mostrado a seguir.



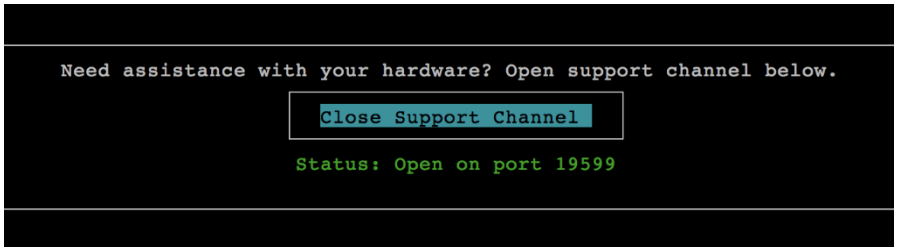
Onde obter suporte ao equipamento de hardware

Para contatar o suporte do Storage Gateway Hardware Appliance,AWS Support.

OAWS SupportA equipe pode solicitar 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 paraAWS

1. Abra o console de hardware.
2. Escolha Open Support Channel (Abrir canal de suporte), como mostrado a seguir.



   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 paraAWS Support.

Como solucionar problemas do gateway de arquivos

É possível configurar o gateway de arquivos com um grupo de logs do Amazon CloudWatch ao executar o VMware vSphere High Availability (HA). Se fizer isso, você receberá notificações sobre o status de integridade do gateway de arquivos e sobre erros que o gateway de arquivos encontra. Você pode encontrar informações sobre essas notificações de erros e de integridade no CloudWatch Logs.

Nas seções a seguir, é possível encontrar informações que podem ajudar a entender a causa de cada erro e notificação de integridade e como corrigir problemas.

Tópicos

- Erros: InaccessibleStorageClass
- Erros: S3Accessnegado

- Erros: InvalidObjectState
- Erros: ObjectMissing
- : Notification Reinicializar
- : Notification HardReboot
- : Notification HealthCheckFailure
- : Notification AvailabilityMonitorTest
- Erros: RoleTrustRelationshipInvalid
- Solução de problemas com métricas do CloudWatch

Erros: InaccessibleStorageClass

Você pode obter um`InaccessibleStorageClass`Erro quando um objeto é movido para fora da classe de armazenamento Amazon S3 Standard.

Aqui, geralmente o gateway de arquivos encontra o erro quando tenta fazer upload do objeto especificado no bucket do S3 ou ler o objeto do bucket do S3. Com esse erro, geralmente o objeto foi movido para o Amazon S3 Glacier e está na classe de armazenamento S3 Glacier ou S3 Glacier Deep Archive.

Para resolver um erro InaccessibleStorageClass

- Mova o objeto da classe de armazenamento S3 Glacier ou S3 Glacier Deep Archive de volta para o S3.

  Se você mover o objeto para o bucket do S3 para corrigir um erro de upload, acabará sendo feito upload do arquivo. Se você mover o objeto para o bucket do S3 para corrigir um erro de leitura, o cliente SMB ou NFS do gateway de arquivos poderá, então, ler o arquivo.

Erros: S3Accessnegado

Você pode obter um`S3AccessDenied`Erro para o acesso ao bucket do Amazon S3 de um compartilhamento de arquivosAWS Identity and Access Management(IAM) da função do. Nesse caso, a função do IAM de acesso a bucket do S3 especificada por`roleArn`No erro não permite a operação envolvida. A operação não é permitida devido às permissões para os objetos no diretório especificado pelo prefixo do Amazon S3.

Para resolver um erro S3AccessDenied

- Modifique a política de acesso do Amazon S3 que está anexada a`roleArn`No log de integridade do gateway de arquivos para permitir permissões para a operação do Amazon S3. Verifique se a política de acesso concede permissão para a operação que causou o erro. Além disso, conceda permissão para o diretório especificado no log para `prefix`. Para obter informações sobre as permissões do Amazon S3, consulteEspecificar permissões em uma políticaemGuia do usuário do Amazon Simple Storage Service.

  Essas operações podem fazer com que ocorra um erro `S3AccessDenied`.

  - `S3HeadObject`
  - `S3GetObject`
  - `S3ListObjects`
  - `S3DeleteObject`
  - `S3PutObject`

Erros: InvalidObjectState

Você pode obter um`InvalidObjectState`Erro quando um gravador diferente do gateway de arquivos determinado modifica o arquivo especificado no bucket do S3 estabelecido. Como resultado, o estado do arquivo para o gateway de arquivos não corresponde ao seu estado no Amazon S3. Todos os uploads subsequentes do arquivo para o Amazon S3 ou as recuperações do arquivo do Amazon S3 falharão.

Para resolver um erro InvalidObjectState

Se a operação que modifica o arquivo for`S3Upload`ou`S3GetObject`, faça o seguinte:

1. Salve a cópia mais recente do arquivo no sistema de arquivos local do cliente SMB ou NFS (você precisa dessa cópia de arquivo na etapa 4). Se a versão do arquivo no Amazon S3 for a mais recente, faça download dessa versão. É possível fazer isso usando o AWS Management Console ou a AWS CLI.
2. Exclua o arquivo no Amazon S3 usando oAWS Management ConsoleouAWS CLI.
3. Exclua o arquivo do gateway de arquivos usando o cliente SMB ou NFS.
4. Copie a versão mais recente do arquivo que você salvou na etapa 1 para o Amazon S3 usando o cliente SMB ou NFS. Faça isso por meio do gateway de arquivos.

Erros: ObjectMissing

Você pode obter um`ObjectMissing`Erro quando um gravador diferente do gateway de arquivos determinado exclui o arquivo especificado do bucket do S3. Todos os uploads subsequentes no Amazon S3 ou as recuperações do Amazon S3 para o objeto falharão.

Para resolver um erro ObjectMissing

Se a operação que modifica o arquivo for`S3Upload`ou`S3GetObject`, faça o seguinte:

1. Salve a cópia mais recente do arquivo no sistema de arquivos local do cliente SMB ou NFS (você precisa dessa cópia de arquivo na etapa 3).
2. Exclua o arquivo do gateway de arquivos usando o cliente SMB ou NFS.
3. Copie a versão mais recente do arquivo que você salvou na etapa 1 usando o cliente SMB ou NFS. Faça isso por meio do gateway de arquivos.

: Notification 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 de gerenciamento do VM Hypervisor ou o console do Storage Gateway. Também é possível reiniciar usando o software de gateway durante o ciclo de manutenção do gateway.

Se a hora da reinicialização estiver dentro de 10 minutos da hora de início da manutenção configurada do gateway, essa reinicialização 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.

: Notification 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 Monitoramento de aplicativos do vSphere High Availability pode acionar esse evento.

Quando o gateway for executado nesse ambiente, verifique a presença da notificação `HealthCheckFailure` e consulte o log de eventos do VMware da VM.

: Notification 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.

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 contatoAWS Support.

: Notification AvailabilityMonitorTest

Você recebe um`AvailabilityMonitorTest`notificação quando vocêexecutar um testedoMonitoramento de disponibilidade e aplicativosSistema em gateways em execução em uma plataforma do VMware vSphere HA.

Erros: RoleTrustRelationshipInvalid

Você recebe esse erro quando a função do IAM para um compartilhamento de arquivos tem uma relação de confiança do IAM configurada incorretamente (isto é, a função do IAM não confia no principal do Storage Gateway chamado`storagegateway.amazonaws.com`). Como resultado, o gateway de arquivos não poderia obter as credenciais para executar nenhuma operação no bucket do S3 que ofereça suporte ao compartilhamento de arquivos.

Para resolver um erro RoleTrustRelationshipInvalid

- Use o console do IAM ou a API do IAM para incluir`storagegateway.amazonaws.com`Como um principal que é confiável pelo IAMrole do compartilhamento de arquivos. Para obter informações sobre a função do IAM, consulteTutorial: delegar acesso atravésAWSContas usando funções do IAM.

Solução de problemas com métricas do CloudWatch

Você pode encontrar informações a seguir sobre ações para solucionar problemas no uso de métricas do Amazon CloudWatch com o Storage Gateway.

Tópicos

Seu gateway reage lentamente ao navegar em diretórios

Se o gateway de arquivos reage lentamente ao executar olscomandos ou navegar diretórios, verifique `oIndexFetcheIndexEviction`Métricas do CloudWatch:

- Se `oIndexFetch`métrica é maior que 0 quando você executa um`ls`Comando ou navegar por diretórios, o gateway de arquivos foi iniciado sem informações sobre o conteúdo do diretório afetado e precisou acessar o Amazon S3. Os esforços subsequentes para listar o conteúdo desse diretório deverão ocorrer com mais rapidez.
- Se `oIndexEviction`A métrica é maior que 0, significa que o gateway de arquivos atingiu o limite do que pode gerenciar em seu cache no momento. Nesse caso, o gateway de arquivos precisa liberar espaço de armazenamento do diretório menos acessado recentemente para listar um novo diretório. Se isso ocorrer com frequência e houver um impacto no desempenho, entre em contatoAWS Support.

  Discutir comAWS SupportO conteúdo do bucket do S3 relacionado e as recomendações para melhorar o desempenho com base no seu caso de uso.

Seu gateway não está respondendo

Se o gateway de arquivos não estiver respondendo, faça o seguinte:

- Se essa foi uma reinicialização atual ou uma atualização de software, verifique a métrica `IOWaitPercent`. Essa métrica mostra a porcentagem de tempo que a CPU fica ociosa quando há uma solicitação de E/S de disco pendente. Em alguns casos, isso pode ser alto (10 ou mais) e pode ter aumentado depois que o servidor foi reinicializado ou atualizado. Nesses casos, o gateway de arquivos pode ser afunilado por um disco raiz lento à medida que recria o cache de índice para RAM. É possível resolver esse problema usando um disco físico mais rápido para o disco raiz.
- Se o`MemUsedBytes`métrica é quase igual ou quase a mesma que a`MemTotalBytes`Em seguida, o gateway de arquivos está ficando sem RAM disponível. Verifique se o gateway de arquivos tem pelo menos a RAM mínima necessária. Se já tiver, considere adicionar mais RAM ao gateway de arquivos com base na carga de trabalho e no caso de uso.

  Se o compartilhamento de arquivos for SMB, o problema também pode ser devido ao número de clientes SMB conectados ao compartilhamento de arquivos. Para ver o número de clientes conectados em determinado momento, verifique a métrica `SMBV(1/2/3)Sessions`. Se houver muitos clientes conectados, talvez seja necessário adicionar mais RAM ao gateway de arquivos.

Se o gateway estiver transferindo dados lentamente para o Amazon S3

Se o gateway de arquivos estiver transferindo dados lentamente para o Amazon S3, faça o seguinte:

- Se o`CachePercentDirty`A métrica é 80 ou mais, o gateway de arquivos está gravando dados mais rapidamente no disco do que pode fazer upload de dados no Amazon S3. Considere aumentar a largura de banda para upload do gateway de arquivos, adicionar um ou mais discos de cache ou desacelerar as gravações do cliente.
- Se o`CachePercentDirty`métrica é baixa, verifique o`IoWaitPercent`Métrica do. Se`IoWaitPercent`É maior que 10, o gateway de arquivos pode ser afunilado pela velocidade do disco de cache local. Recomendamos discos de unidade de estado sólido (SSD) local para o cache, de preferência NVM Express (NVMe). Se esses discos não estiverem disponíveis, tente usar vários discos de cache de discos físicos separados para melhorar o desempenho.
- Se`S3PutObjectRequestTime`,`S3UploadPartRequestTime`, ou`S3GetObjectRequestTime`são altos, pode haver um gargalo na rede. Tente analisar sua rede para verificar se o gateway tem a largura de banda esperada.

Seu gateway está realizando mais operações do Amazon S3 do que o esperado

Se o gateway de arquivos estiver executando mais operações do Amazon S3 do que o esperado, verifique a`FilesRenamed`Métrica do. As operações de renomeação são caras para serem executadas no Amazon S3. Otimize seu fluxo de trabalho para minimizar o número de operações de renomeação.

Você não vê arquivos em seu bucket do Amazon S3

Se você notar que os arquivos no gateway não estão refletidos no bucket do Amazon S3, verifique a`FilesFailingUpload`Métrica do. Se a métrica informar que alguns arquivos estão falhando no upload, verifique suas notificações de integridade. Quando os arquivos falham ao carregar, o gateway gera uma notificação de integridade contendo mais detalhes sobre o problema.

Seu trabalho de backup do gateway falhará ou há erros ao gravar no gateway

Se o trabalho de backup do gateway de arquivos falhar ou houver erros ao gravar no gateway de arquivos, faça o seguinte:

- Se o`CachePercentDirty`A métrica é 90% ou mais, o gateway de arquivos não consegue aceitar novas gravações em disco porque não há espaço disponível suficiente no disco de cache. Para ver a rapidez com que o gateway de arquivos está fazendo upload no Amazon FSx ou no Amazon S3, visualize a`CloudBytesUploaded`Métrica do. Compare essa métrica com o`WriteBytes`, que mostra a rapidez com que o cliente está gravando arquivos no gateway de arquivos. Se o gateway de arquivos estiver gravando mais rápido do que pode fazer upload no Amazon FSx ou Amazon S3, adicione mais discos de cache para cobrir, no mínimo, o tamanho do trabalho de backup. Ou aumente a largura de banda de upload.
- Se um trabalho de backup falhar, mas o`CachePercentDirty`A métrica é inferior a 80%, o gateway de arquivos pode estar atingindo um tempo limite de sessão no lado do cliente. Para SMB, é possível aumentar esse tempo limite usando o comando `Set-SmbClientConfiguration -SessionTimeout 300` do PowerShell. A execução desse comando define o tempo limite para 300 segundos.

  Para o NFS, verifique se o cliente está montado usando uma montagem rígida em vez de uma montagem flexível.

Como solucionar problemas de compartilhamento de arquivos

Você pode encontrar informações a seguir sobre as ações a adotar se enfrentar problemas inesperados em um compartilhamento de arquivos.

Tópicos

Seu compartilhamento de arquivos está preso no status CREATING

Quando o compartilhamento de arquivos está sendo criado, o status é CREATING. O status muda para AVAILABLE depois que o compartilhamento de arquivos é criado. Se o compartilhamento de arquivos ficar paralisado no status CREATING, faça o seguinte:

1. Abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Verifique se o bucket do S3 para o qual você mapeia seu compartilhamento de arquivos existe. Se o bucket não existir, crie-o. Depois que você cria o bucket, o status do compartilhamento de arquivos muda para AVAILABLE. Para obter informações sobre como criar um bucket do S3, consulteCriar um bucketnoGuia do usuário do Amazon Simple Storage Service.

3. Verifique se o nome do bucket está de acordo com as regras de nomenclatura de bucket no Amazon S3. Para obter mais informações, consulte as Regras para nomear buckets no Manual do usuário do Amazon Simple Storage Service.
4. Verifique se a função do IAM usada para acessar o bucket do S3 tem as permissões corretas e se o bucket do S3 está listado como um recurso na política do IAM. Para obter mais informações, consulte Como conceder acesso a um bucket do Amazon S3.

Não é possível criar um compartilhamento de arquivos

1. Se não conseguir criar um compartilhamento de arquivos porque o compartilhamento está paralisado no CREATING, verifique se o bucket do S3 para o qual você mapeia seu compartilhamento de arquivos existe. Para obter informações sobre como fazer isso, consulte o tópico precedente, Seu compartilhamento de arquivos está preso no status CREATING.
2. Se o bucket do S3 existir, verifique seAWS Security Token ServiceÉ habilitado na região em que você está criando o compartilhamento de arquivos. Se não houver um token de segurança habilitado, você deve habilitá-lo. Para obter informações sobre como ativar um token usandoAWS Security Token Service, consulteAtivar e desativarAWSSTS em umAWSRegiãonoIAM User Guide.

Compartilhamentos de arquivos SMB não permitem vários métodos de acesso diferentes

Os compartilhamentos de arquivo SMB possuem as seguintes restrições:

1. Quando o mesmo cliente tenta montar um compartilhamento de arquivos SMB com acesso de convidado e do Active Directory, a seguinte mensagem de erro é exibida: `Multiple connections to a server or shared resource by the same user, using more than one user name, are not allowed. Disconnect all previous connections to the server or shared resource and try again.`
2. Um usuário do Windows não pode permanecer conectado a dois compartilhamentos de arquivos SMB com acesso de convidado, e pode ser desconectado quando uma nova conexão com acesso de convidado é estabelecida.
3. Um cliente Windows não pode montar um compartilhamento de arquivos SMB com acesso de convidado e um do Active Directory exportado pelo mesmo gateway.

Vários compartilhamentos de arquivos não podem gravar no bucket do S3 mapeado

Não é recomendável configurar o bucket do S3 para permitir que vários compartilhamentos de arquivos gravem nele. Esse procedimento pode provocar resultados imprevisíveis.

Em vez disso, é recomendável permitir que apenas um compartilhamento de arquivos grave em cada bucket do S3. Você cria uma política de bucket para permitir que apenas a função associada ao compartilhamento de arquivos grave no bucket. Para obter mais informações, consulte Melhores práticas de compartilhamento de arquivos.

Não é possível fazer upload de arquivos no bucket do S3

Se não conseguir fazer upload de arquivos no bucket do S3, faça o seguinte:

1. Certifique-se de que você concedeu o acesso necessário para o gateway de arquivos do Amazon S3 fazer upload de arquivos no bucket do S3. Para obter mais informações, consulte Como conceder acesso a um bucket do Amazon S3.
2. Verifique se a função que criou o bucket tem permissão para gravar no bucket do S3. Para obter mais informações, consulte Melhores práticas de compartilhamento de arquivos.
3. Se o gateway de arquivos usar o SSE-KMS para criptografia, certifique-se de que a função do IAM associada ao compartilhamento de arquivos incluakms:Encrypt,kms:Decrypt,kms:Reencrypt,kms:GenerateDataKey, ekms:DescribeKeypermissões. Para obter mais informações, consulteUsar políticas baseadas em identidade (políticas do IAM) para o Storage Gateway.

Não é possível alterar a criptografia padrão para usar o SSE-KMS para criptografar objetos armazenados no meu bucket do S3

Se você alterar a criptografia padrão e fizer SSE-KMS (criptografia no lado do servidor comAWS KMS—managed keys) o padrão do bucket do S3, os objetos armazenados pelo Amazon S3 File Gateway no bucket não são criptografados com o SSE-KMS. Por padrão, um gateway de arquivos do S3 usa a criptografia no lado do servidor gerenciada com o Amazon S3 (SSE-S3) quando grava dados em um bucket do S3. Alterar o padrão não altera automaticamente a criptografia.

Para alterar a criptografia e usar o SSE-KMS com sua própria chave AWS KMS, você deve habilitar a criptografia do SSE-KMS. Para fazer isso, forneça o nome de recurso da Amazon (ARN) da chave

do KMS ao criar o compartilhamento de arquivos. Você também pode atualizar as configurações do KMS para seu compartilhamento de arquivos usando a operação de API `UpdateNFSFileShare` ou `UpdateSMBFileShare`. Essa atualização se aplica a objetos armazenados nos buckets do S3 após a atualização. Para obter mais informações, consulte Criptografia de dados usandoAWS KMS.

As alterações feitas diretamente em um bucket do S3 com controle de versão de objeto ativado podem afetar o que você vê no compartilhamento de arquivos

Se o bucket do S3 tiver objetos gravados nele por outro cliente, sua visualização do bucket do S3 pode não estar atualizado como resultado do versionamento de objetos do bucket do S3. Você deve sempre atualizar seu cache antes de examinar arquivos de interesse.

Versionamento de objeto é um recurso de bucket do S3 opcional que ajuda a proteger dados ao armazenar múltiplas cópias do objeto de mesmo nome. Cada cópia tem um valor de ID separado, por exemplo`file1.jpg`:`ID="xxx"`e`file1.jpg`: `ID="yyy"`. O número de objetos com nomes idênticos e suas vidas são controlados por políticas de ciclo de vida do Amazon S3. Para obter mais detalhes sobre esses conceitos do Amazon S3, consulteUsar o versionamentoeGerenciamento do ciclo de vida de objetosnoGuia do desenvolvedor do Amazon S3.

Quando você exclui um objeto versionado, esse objeto será sinalizado com um marcador de exclusão, mas retido. Somente um proprietário do bucket do S3 pode excluir permanentemente um objeto com o controle de versão habilitado.

No gateway de arquivos do S3, os arquivos mostrados são as versões mais recentes dos objetos em um bucket do S3 no momento em que o objeto foi buscado ou que o cache foi atualizado. Os gateways de arquivos S3 ignoram quaisquer versões mais antigas ou quaisquer objetos marcados para exclusão. Ao ler um arquivo, você lê os dados da versão mais recente. Quando você gravar um arquivo em seu compartilhamento de arquivos, o S3 File Gateway cria uma nova versão de um objeto nomeado com suas alterações, e essa versão se torna a versão mais recente.

Seu gateway de arquivos do S3 continua a ler a versão anterior, e as atualizações que você faz são baseadas na versão anterior caso uma nova versão deva ser adicionada ao bucket do S3 fora do seu aplicativo. Para ler a versão mais recente de um objeto, use a ação de API do RefreshCache ou atualize a partir do console, como descrito em Atualizar objetos no bucket do Amazon S3.

> **Important**
>
> Não recomendamos que objetos ou arquivos sejam gravados no bucket do S3 File Gateway S3 de fora do compartilhamento de arquivos.

Ao gravar em um bucket do S3 com o controle de versão de objeto ativado, o Amazon S3 File Gateway pode criar várias versões de um objeto S3

Com o controle de versão de objeto ativado, você pode ter várias versões de um objeto criado no Amazon S3 em cada atualização de um arquivo do seu cliente NFS ou SMB. Aqui estão os cenários que podem resultar em várias versões de um objeto sendo criado no bucket do S3:

- Quando um arquivo é modificado no Amazon S3 File Gateway por um cliente NFS ou SMB depois de ter sido carregado para o Amazon S3, o S3 File Gateway carrega os dados novos ou modificados em vez de fazer upload do arquivo inteiro. A modificação do arquivo resulta em uma nova versão do objeto do Amazon S3 sendo criada.
- Quando um arquivo é gravado no S3 File Gateway por um cliente NFS ou SMB, o S3 File Gateway carrega os dados do arquivo para o Amazon S3 seguidos de seus metadados (proprietários, carimbos de data/hora, etc.). O upload dos dados do arquivo cria um objeto do Amazon S3 e o upload dos metadados do arquivo atualiza os metadados do objeto do Amazon S3. Esse processo cria outra versão do objeto, resultando em duas versões de um objeto.
- Quando o S3 File Gateway está carregando arquivos maiores, talvez seja necessário fazer upload de blocos menores do arquivo antes que o cliente termine de gravar no gateway de arquivos. Alguns motivos para isso incluem liberar espaço em cache ou uma alta taxa de gravações em um arquivo. Isso pode resultar em várias versões de um objeto no bucket do S3.

Você deve monitorar o bucket do S3 para determinar quantas versões de um objeto existem antes de configurar políticas de ciclo de vida para mover objetos para diferentes classes de armazenamento. Você deve configurar a expiração do ciclo de vida para versões anteriores para minimizar o número de versões que você tem para um objeto no bucket do S3. O uso de replicação de mesma região (SRR) ou CRR (replicação entre regiões) entre buckets do S3 aumentará o armazenamento usado. Para obter mais informações sobre replicação, consulteReplicação.

> **Important**
>
> Não configure a replicação entre buckets do S3 até entender quanto armazenamento está sendo usado quando o controle de versão de objeto estiver ativado.

O uso de buckets do S3 versionados pode aumentar significativamente a quantidade de armazenamento no Amazon S3, pois cada modificação em um arquivo cria uma nova versão do objeto S3. Por padrão, o Amazon S3 continua a armazenar todas essas versões, a não ser que você crie especificamente uma política para substituir esse comportamento e limitar o número de versões que são mantidas. Se você observar uso de armazenamento grande incomum com versionamento de objetos habilitado, verifique se você tem políticas de armazenamento definidas adequadamente. Um aumento no número de respostas de `HTTP 503-slow down` para solicitações de navegador também pode ser o resultado de problemas com o versionamento de objetos.

Se você ativar o versionamento de objetos após a instalação de um gateway de arquivos do S3, todos os objetos exclusivos serão retidos (`ID="NULL"`) e você pode vê-los todos no sistema de arquivos. Novas versões de objetos recebem um ID exclusivo (versões mais antigas são retidas). Com base no carimbo de data e hora do objeto, apenas o objeto versionado mais recentemente é visualizável no sistema do arquivo NFS.

Depois de habilitar o versionamento de objetos, o bucket do S3 não pode ser retornado para um estado não versionado. Você pode, contudo, suspender o versionamento. Quando você suspender o versionamento, um novo objeto recebe um ID. Se o mesmo objeto nomeado existe com um valor de `ID="NULL"`, a versão mais antiga será substituída. No entanto, qualquer versão que contém um ID que não é `NULL` é retida. Os carimbos de data e hora identificam o novo objeto como o atual, e é aquele que aparece no sistema de arquivos NFS.

As alterações em um bucket do S3 não são refletidas no Storage Gateway

O Storage Gateway atualiza o cache de compartilhamento de arquivos automaticamente quando você grava arquivos no cache localmente usando o compartilhamento de arquivos. No entanto, o Storage Gateway não atualiza automaticamente o cache quando você carrega um arquivo diretamente para o Amazon S3. Ao fazer isso, você deve executar um`RefreshCache`para ver as alterações no compartilhamento de arquivos. Se você tiver mais de um compartilhamento de arquivos, deverá executar a`RefreshCache`operação em cada compartilhamento de arquivos.

Você pode atualizar o cache usando o console do Storage Gateway e oAWS Command Line Interface(AWS CLI):

- Para atualizar o cache usando o console do Storage Gateway, consulte Atualizando objetos no bucket do Amazon S3.
- Para atualizar o cache usando oAWS CLI:
  1. Execute o comandoaws storagegateway list-file-shares
  2. Copie o número de recurso da Amazon (ARN) do compartilhamento de arquivos com o cache que você deseja atualizar.
  3. Execute arefresh-cacheComando com seu ARN como o valor para--file-share-arn:

     ```
     aws storagegateway refresh-cache --file-share-arn
     arn:aws:storagegateway:eu-west-1:12345678910:share/share-FFDEE12
     ```

Para automatizar oRefreshCacheoperação, consulteComo posso automatizar a operação RefreshCache no Storage Gateway?

As permissões de ACL não estão funcionando conforme o esperado

Se as permissões da lista de controle de acesso (ACL) não estiverem funcionando conforme esperado com o compartilhamento de arquivos SMB, você pode executar um teste.

Para fazer isso, primeiro teste as permissões em um servidor de arquivos do Microsoft Windows ou um compartilhamento de arquivos do Windows local. Em seguida, compare o comportamento com o compartilhamento de arquivos do gateway.

O desempenho do gateway diminuiu depois que você executou uma operação recursiva

Em alguns casos, você pode executar uma operação recursiva, como renomear um diretório ou habilitar a herança para uma ACL, e forçar para baixo na árvore. Se você fizer isso, o gateway de arquivos do S3 aplicará recursivamente a operação a todos os objetos no compartilhamento de arquivos.

Por exemplo, suponha que você aplique a herança a objetos existentes em um bucket do S3. O gateway de arquivos S3 aplica recursivamente a herança a todos os objetos no bucket. Essas operações podem causar queda de desempenho do gateway.

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

Notificação de Health

Quando você executa o gateway no VMware vSphere HA, todos os gateways produzem as notificações de integridade a seguir para o grupo de logs do Amazon CloudWatch configurado. Essas notificações entram em um fluxo de log chamado `AvailabilityMonitor`.

Tópicos

: Notification 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 de gerenciamento do VM Hypervisor 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.

: Notification 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 Monitoramento de aplicativos do vSphere High Availability 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.

: Notification 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 contatoAWS Support.

: Notification AvailabilityMonitorTest

Para um gateway no VMware vSphere HA, você pode obter um`AvailabilityMonitorTest`notificação quando vocêexecutar um testedoMonitoramento de disponibilidade e aplicativossistema no VMware.

Métricas

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 o grupo de logs do CloudWatch configurado para obter detalhes sobre os eventos.

Melhores práticas para recuperar seus dados

Ainda que isso seja raro, o gateway pode enfrentar uma falha irrecuperável. 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 AMI (Amazon Machine Image) do EC2 da Amazon. Se a VM do gateway apresentar problemas, ative um novo gateway e recupere seus dados para esse gateway usando as instruções a seguir.

Tópicos

Recuperando de um desligamento inesperado de 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 Testando a conectividade de rede do gateway.
- 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.

Recuperando seus dados de um disco cache com defeito

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.

Para obter informações detalhadas, consulte Recuperando seus dados de um disco cache com defeito.

Recuperar dados de um datacenter inacessível

Se seu gateway ou data center torna-se inacessível por algum motivo, você pode recuperar seus dados em um outro gateway em outro datacenter ou recuperar um gateway hospedado em uma instância 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 arquivos em um datacenter inacessível

Para o gateway de arquivos, você pode mapear um novo compartilhamento de arquivos para o bucket do Amazon S3 que contém os dados que você deseja recuperar.

1. Crie e ative um novo gateway de arquivos em um host do Amazon EC2. Para obter mais informações, consulte Implantar um gateway de arquivos em um host do Amazon EC2.

2. Crie um novo compartilhamento de arquivos no gateway do EC2 que você criou. Para obter mais informações, consulteCriar um compartilhamento de arquivos.
3. Monte o compartilhamento de arquivos no seu cliente e mapeie-o para o bucket do S3 que contém os dados que você deseja recuperar. Para obter mais informações, consulteMonte e use seu compartilhamento de arquivos.

Mais recursos Storage Gateway

Nesta seção, você encontra informações sobreAWSE software, ferramentas e recursos de terceiros que podem ajudar você a configurar ou gerenciar seu gateway e também sobre as cotas do Storage Gateway.

Tópicos

Configuração do host

Tópicos

Como configurar o VMware for Storage Gateway

Ao configurar o VMware for 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
- Como usar o Storage Gateway com a Alta Disponibilidade

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).

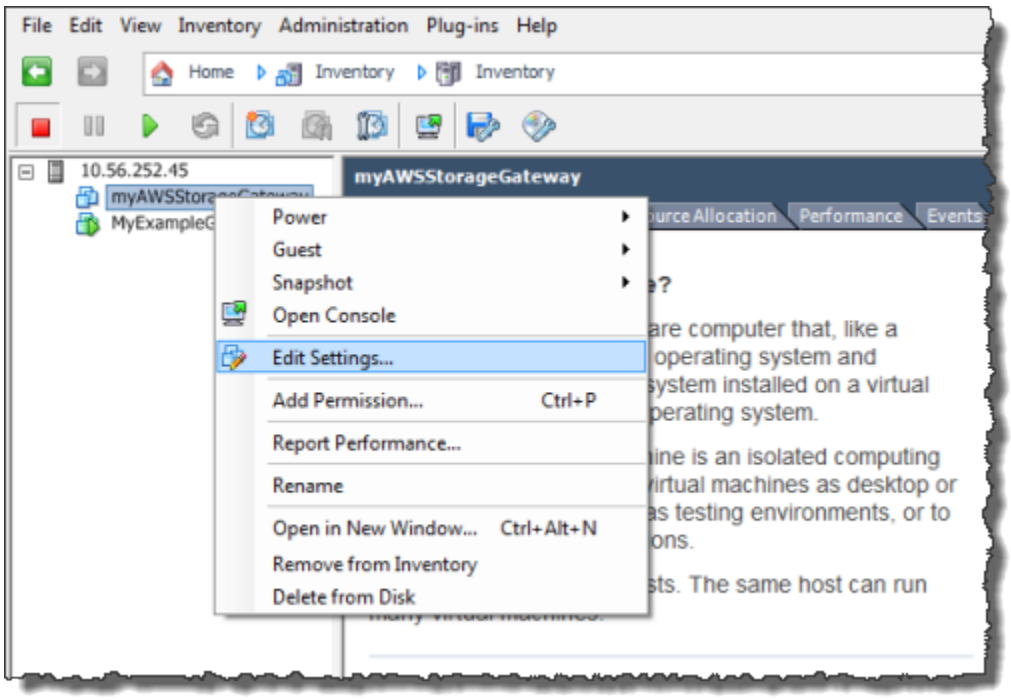
> **Important**
>
> É necessário sincronizar o tempo da VM com o tempo do host para conseguir ativar o gateway.

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.

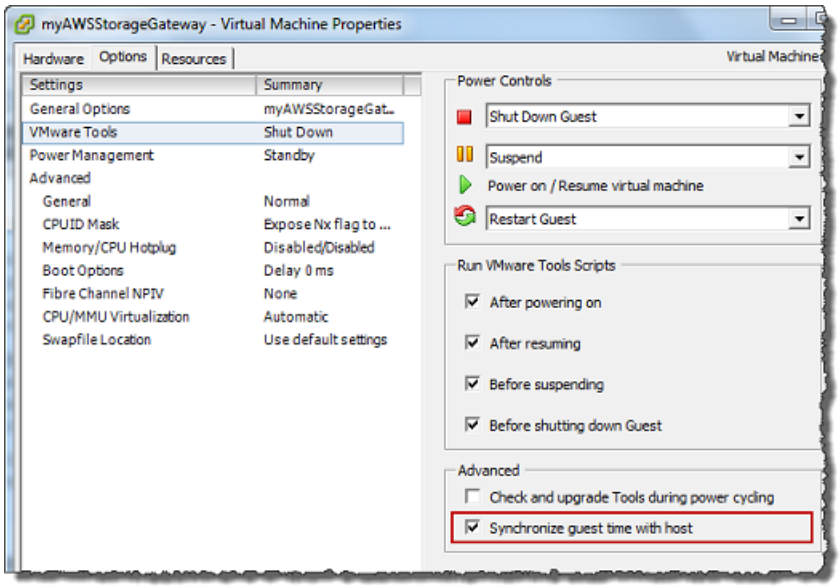
      A caixa de diálogo Virtual Machine Properties é aberta.



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.



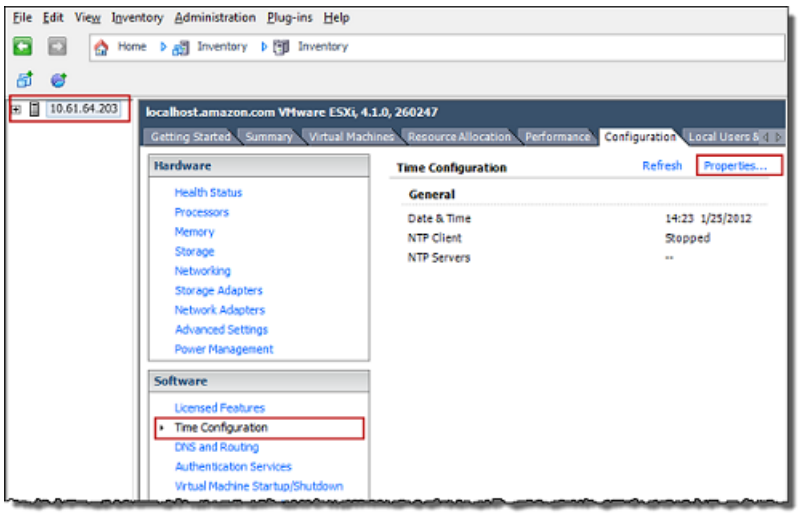
2. Configure o tempo do host.

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.

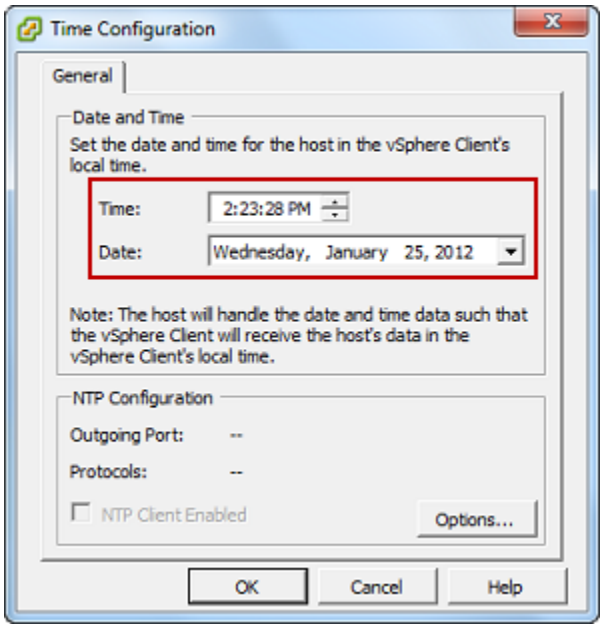
a. No cliente VMware vSphere, selecione o nó do host vSphere no painel esquerdo e escolha a guia Configuration.

b. Selecione Time Configuration no painel Software e escolha o link Properties.

   A caixa de diálogo Time Configuration é exibida.

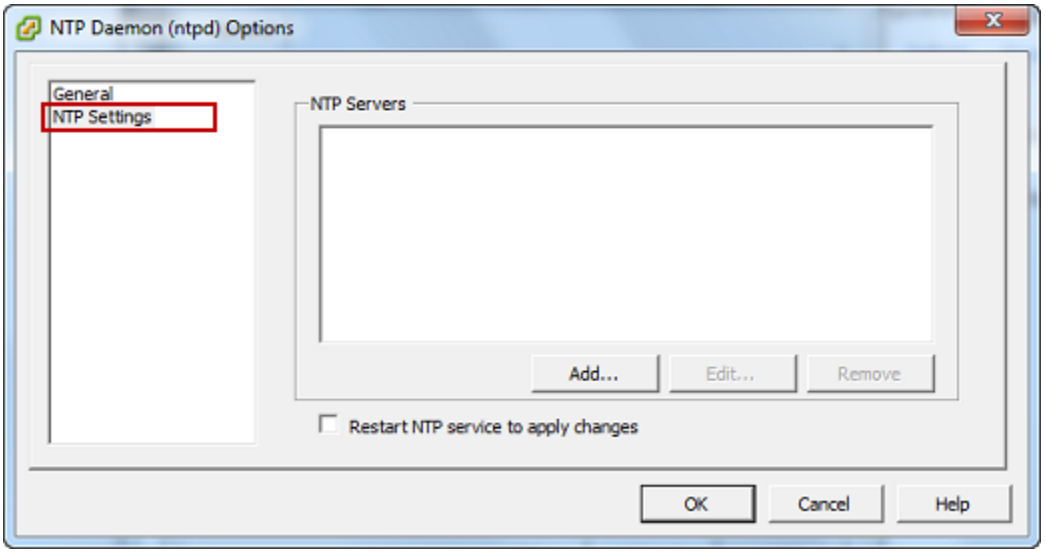


c. No painel Date and Time, defina a data e hora.



d. Configure o host para sincronizar seu tempo automaticamente com um servidor NTP.

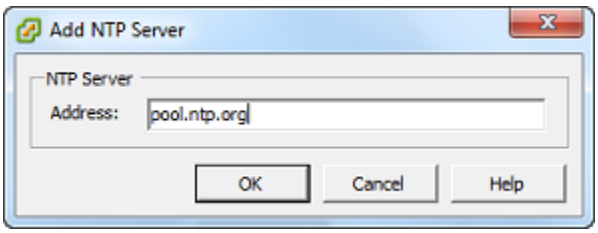
   i. Escolha Options na caixa de diálogo Time Configuration e, na caixa de diálogo NTP Daemon (ntpd) Options, escolha NTP Settings, no painel esquerdo.



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.

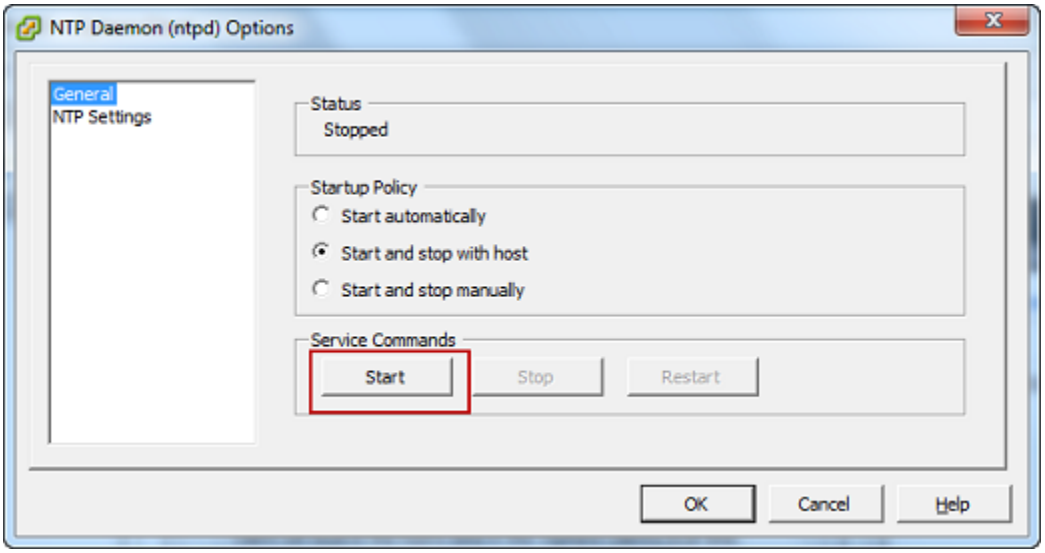
Você pode usar `pool.ntp.org`, conforme mostrado no exemplo a seguir.



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.

Como usar o Storage Gateway com a Alta Disponibilidade

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, consulteVMware HA: Conceitos e práticas recomendadasNo site da VMware.

Para usar o Storage Gateway com o VMware HA, é recomendável fazer o seguinte:

- Implante o VMware ESX`.ova`Pacote 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.
- 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

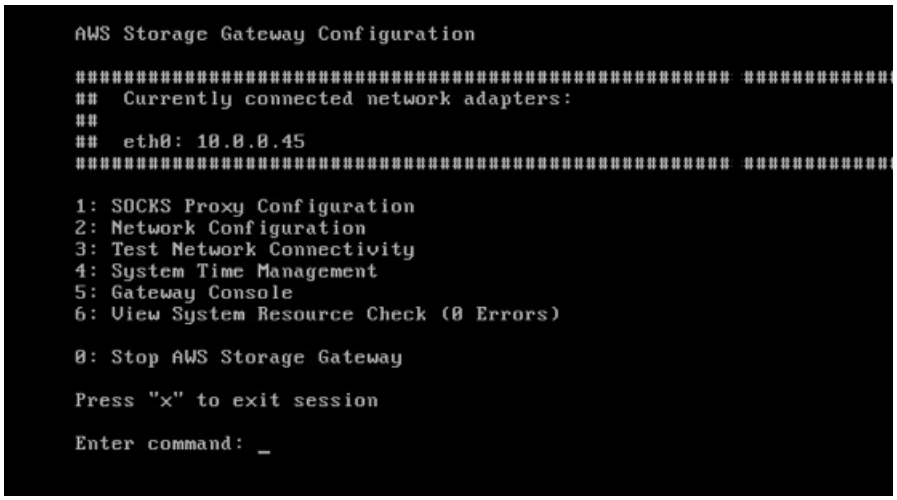
Para um gateway implantado no VMware ESXi, configurar o horário do host do hipervisor e sincronizar o horário da VM com o host é suficiente para evitar desvios de horário. Para obter mais informações, consulte Como sincronizar o tempo da VM com o tempo do host. Para um gateway implantado no Microsoft 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)

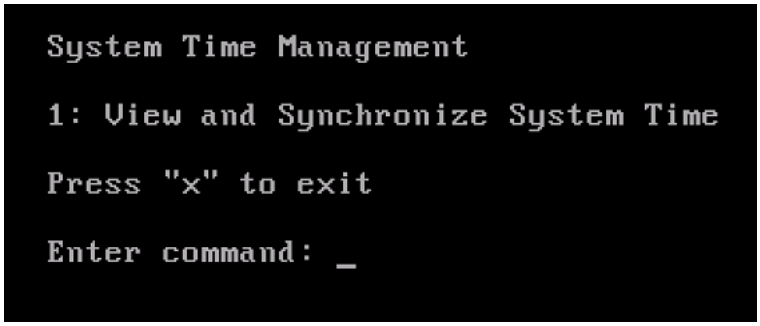
1. Faça login no console local do seu gateway:

   - 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. NoConfiguração Storage GatewayMenu principal, insira**4**peloGerenciamento do horário do sistema.



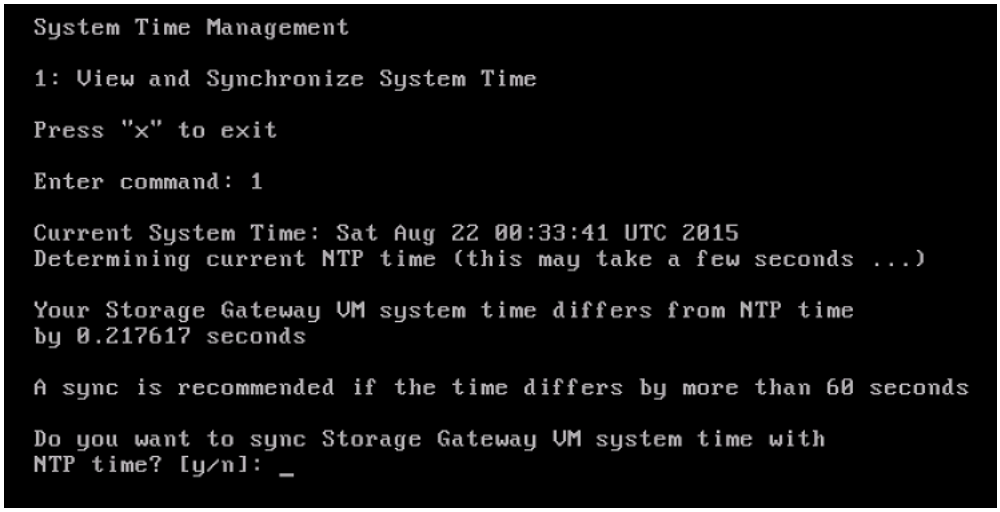
3. No menu System Time Management (Gestão do horário do sistema), digite **1** para View and Synchronize System Time (Exibir e sincronizar o horário do sistema).



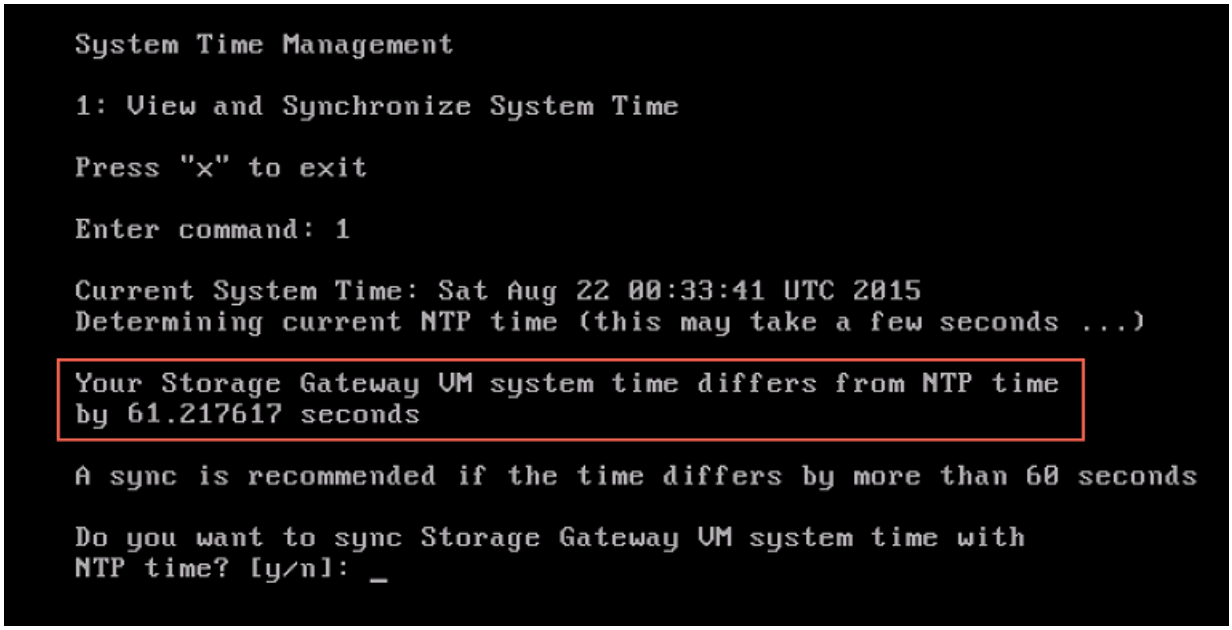
4. Se o resultado indicar que você deve sincronizar o horário de suas VMs com o horário do NTP, digite **y**. Caso contrário, digite **n**.

   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.



   A captura de tela a seguir mostra uma VM que requer sincronização de horário.



Implantar um gateway de arquivos em um host do Amazon EC2

É possível implantar e ativar um gateway de arquivos em uma instância do Amazon Elastic Compute Cloud (Amazon EC2). A imagem de máquina da Amazon (AMI) do gateway de arquivos está disponível como uma AMI de comunidade.

Para implantar um gateway em uma Instância do Amazon EC2

1. Na página Select host platform, escolha Amazon EC2.
2. Escolha Launch instance para iniciar uma AMI do EC2 no gateway de armazenamento. Você será redirecionado para o console do Amazon EC2, onde poderá escolher um tipo de instância.
3. NoEtapa 2: Escolha um tipo de instânciaNa página, escolha a configuração de hardware da instância. O Storage Gateway é compatível com os tipos de instância que atendem a determinados requisitos mínimos É recomendável começar com o tipo de instância m4.xlarge, que atende aos requisitos mínimos para o gateway funcionar corretamente. Para obter mais informações, consulte Requisitos de hardware para VMs locais.

   Você pode redimensionar sua instância depois de executá-la, se necessário. Para obter mais informações, consulteRedimensionar sua instâncianoGuia do usuário do Amazon EC2 para instâncias do Linux.

> **Note**
>
> Alguns tipos de instância, particularmente de i3 do EC2, usam discos SSD NVMe. Isso pode gerar problemas ao iniciar ou interromper o gateway de arquivos; por exemplo, você pode perder dados do cache. Monitorar o`CachePercentDirty`Métrica do Amazon CloudWatch, e só inicie ou interrompa o sistema quando esse parâmetro for`0`. Para saber mais sobre métricas de monitoramento para seu gateway, consulteMétricas e dimensões do Storage Gatewayna documentação do CloudWatch. Para obter mais informações sobre os requisitos dos tipos de instância do Amazon EC2, consultethe section called “Requisitos para os tipos de instância do Amazon EC2”.

4. Selecione Next (Próximo): Configurar os detalhes da instância.
5. NoEtapa 3: Configurar os detalhes da instânciaPágina, escolha um valor paraAtribuir IP público automaticamente. Se não quiser que a sua instância possa ser acessada pela Internet pública, verifique se a opção Auto-assign Public IP (Atribuir IP público automaticamente) está definida como Enable (Ativar). Se não quiser que a sua instância possa ser acessada pela Internet, selecione Auto-assign Public IP (Atribuir IP público automaticamente) como Disable (Desativar).
6. para oIAM role (Função do IAM), escolha oAWS Identity and Access ManagementFunção do (IAM) que você deseja usar para seu gateway.
7. Selecione Next (Próximo): Add Storage.
8. NoEtapa 4: Add StoragePágina, selecioneAdicionar novo volumePara adicionar armazenamento à instância do gateway de arquivos. Você precisa de pelo menos um volume do Amazon EBS para configurar para armazenamento em cache.

   Tamanhos de disco recomendados: Cache (mínimo) 150 GiB e cache (máximo) 64 TiB
9. NoEtapa 5: Adicionar tagsNa página, você pode adicionar uma tag opcional à instância do. Depois, selecione Next (Próximo): Configurar o grupo de segurança.
10. NoEtapa 6: Configurar o grupo de segurançaPágina, adicione regras de firewall para um tráfego específico alcançar sua instância. Você pode criar um novo security group ou escolher um security group existente.

> **Important**
>
> Além da ativação do Storage Gateway e das portas NFS do Secure Shell (SSH), os clientes NFS requerem outras portas de acesso. Para obter informações detalhadas, consulte Requisitos de rede e firewall.

11. Escolha Review and Launch para rever sua configuração.
12. NoEtapa 7: Revisar o lançamento da instânciaPágina, selecioneExecutar.
13. Na caixa de diálogo Select an existing key pair or create a new key pair, escolha Choose an existing key pair e selecione um par de chaves que você tenha criado durante a configuração. Quando estiver pronto, escolha a caixa de confirmação e em seguida Launch Instances.

    Uma página de confirmação informa que a instância está sendo executada.
14. Selecione Visualizar instâncias para fechar a página de confirmação e voltar ao console. Na tela Instances, você pode visualizar o status de sua instância. Demora um pouco para iniciar uma instância. Ao executar uma instância, seu estado inicial é pending. Assim que a instância é iniciada, seu estado é alterado para running (em execução) e ela recebe um nome DNS público.
15. Selecione sua instância, anote o endereço IP público noDescriçãotag e retorne aoConectar-se aoAWSno console do Storage Gateway para continuar a configuração do gateway.

É possível determinar o ID da AMI para iniciar um gateway de arquivos usando o console do Storage Gateway ou consultando oAWS Systems ManagerStorage de parâmetros.

Para determinar o ID da AMI

1. Faça login noAWS Management Consolee abra o console do Storage Gateway emhttps://console.aws.amazon.com/storagegateway/home.
2. Selecione Create gateway (Criar gateway), File gateway (Gateway do arquivo) e Next (Próximo).
3. Na página Choose host platform, escolha Amazon EC2.
4. SelecioneExecutar instânciaPara iniciar a AMI do EC2 do Storage Gateway. Você será redirecionado para a página da AMI da comunidade do EC2, na qual poderá ver o ID da AMI doAWSRegião na URL.

   Ou você pode consultar o repositório de parâmetros do Systems Manager. Você pode usar oAWS CLIou Storage Gateway API para consultar o parâmetro público Systems Manager no

namespace/aws/service/storagegateway/ami/FILE_S3/latest. Por exemplo, usar o seguinte comando da CLI retorna o ID da AMI atual noAWSRegião :

```
aws --region us-east-2 ssm get-parameter --name /aws/service/storagegateway/ami/
FILE_S3/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/
FILE_S3/latest",
        "Name": "/aws/service/storagegateway/ami/FILE_S3/latest",
        "Value": "ami-123c45dd67d891000"
    }
}
```

Como obter a chave de ativação para seu gateway

Para obter uma chave de ativação do gateway, faça uma solicitação da web à VM do gateway, e ela retornará um redirecionamento que contém a chave de ativação. Essa chave de ativação é repassada como um dos parâmetros para a ação de API `ActivateGateway` a fim de especificar a configuração do gateway. Para obter mais informações, consulteActivateGatewaynoReferência da Storage Gateway.

A solicitação feita para a VM do gateway contém oAWSRegião na qual a ativação ocorre. O URL 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`*.

Tópicos

- AWS CLI
- Linux (bash/zsh)
- Microsoft Windows PowerShell

AWS CLI

Caso ainda não tenha feito isso, você deve instalar e configurar a AWS CLI. Para fazer isso, siga estas instruções no Guia do usuário do AWS Command Line Interface:

- Instalar oAWS Command Line Interface
- Configurar aAWS Command Line Interface

O exemplo a seguir mostra como usar oAWS CLIPara buscar a resposta HTTP, analisar cabeçalhos HTTP e obter a chave de ativação.

```
wget 'ec2_instance_ip_address/?activationRegion=eu-west-2' 2>&1 | \
grep -i location | \
grep -i key | \
cut -d'=' -f2 |\
cut -d'&' -f1
```

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 "$activation_region" ]]; then
    echo "Usage: get-activation-key ip_address activation_region"
    return 1
  fi
  if redirect_url=$(curl -f -s -S -w '%{redirect_url}' "http://$ip_address/?
activationRegion=$activation_region"); 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
  )
  PROCESS {
    $request = Invoke-WebRequest -UseBasicParsing -Uri "http://$IpAddress/?
activationRegion=$ActivationRegion" -MaximumRedirection 0 -ErrorAction SilentlyContinue
    if ($request) {
      $activationKeyParam = $request.Headers.Location | Select-String -Pattern
 "activationKey=([A-Z0-9-]+)"
      $activationKeyParam.Matches.Value.Split("=")[1]
    }
  }
}
```

O uso doAWS Direct ConnectCom Storage Gateway

AWS Direct ConnectO vincula sua rede interna à Nuvem Amazon Web Services. Ao usarAWS Direct ConnectCom o Storage Gateway, é possível criar uma conexão para necessidade de cargas de trabalho com alta taxa de transferência, fornecendo uma conexão de rede dedicada entre o gateway local eAWS.

O Storage Gateway usa endpoints públicos. Com umAWS Direct ConnectAo mesmo tempo, é possível criar uma interface virtual pública para permitir roteamento de tráfego 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 no mesmoAWSRegião como oAWS Direct Connectlocalização, ou pode estar em um diferenteAWSRegião :

A ilustração a seguir mostra um exemplo de comoAWS Direct Connectfunciona com o Storage Gateway.

O procedimento a seguir pressupõe que você tenha criado um gateway operacional.

Para usarAWS Direct ConnectCom Storage Gateway

1. Crie e estabeleça umAWS Direct ConnectConexão do entre seu datacenter local e seu endpoint do Storage Gateway. Para obter mais informações sobre como criar uma conexão, consulteConceitos básicos doAWS Direct ConnectnoAWS Direct ConnectGuia do usuário do .
2. Connect seu dispositivo Storage Gateway local àAWS Direct Connectroteador.
3. Crie uma interface virtual pública e configure seu roteador local de forma adequada. Para obter mais informações, consulteComo criar uma interface virtualnoAWS Direct ConnectGuia do usuário do .

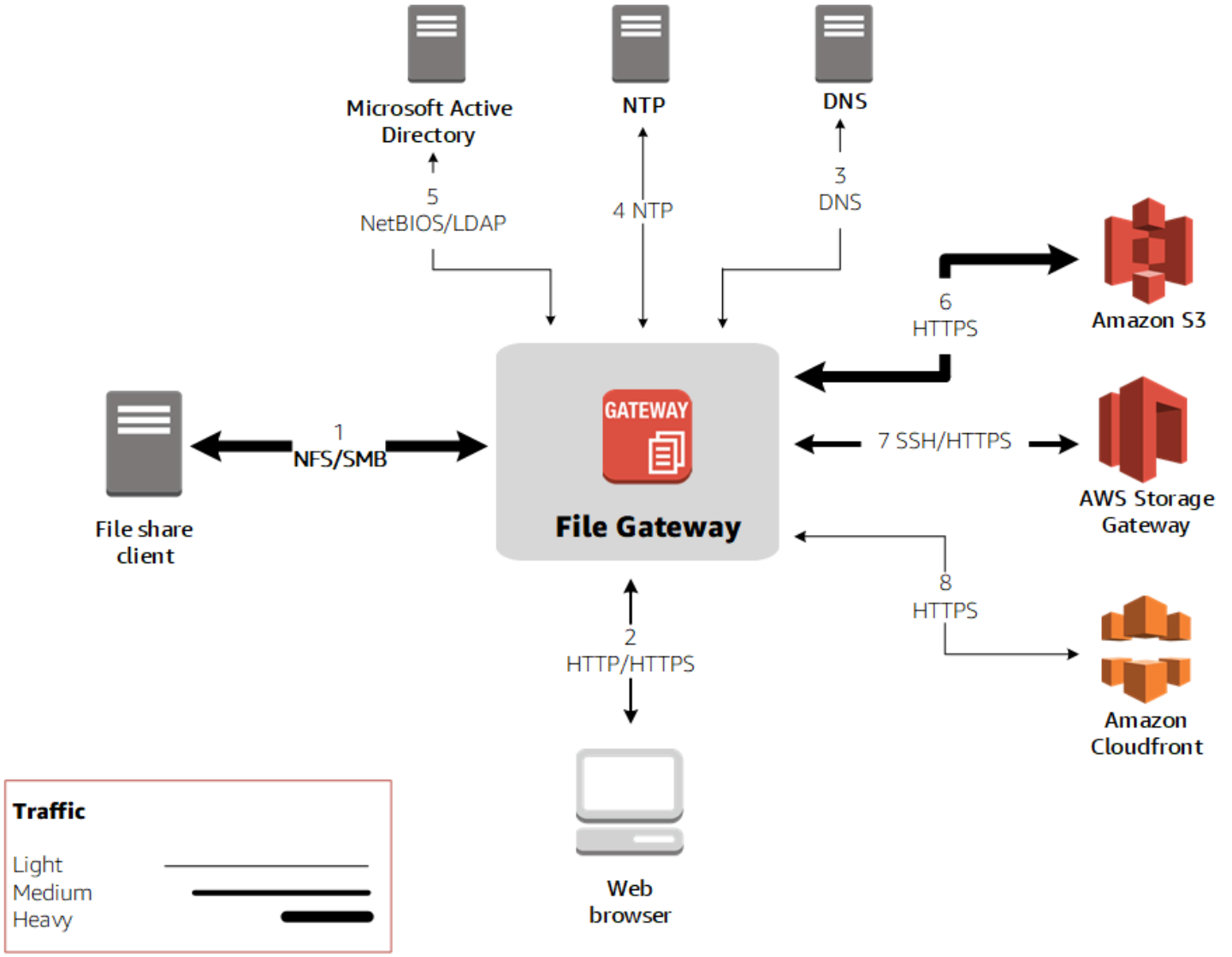
Para obter detalhes sobreAWS Direct Connectconsulte O que é oAWS Direct Connect?noAWS Direct ConnectGuia do usuário do.

Requisitos de porta

O Storage Gateway requer as portas a seguir para ser operado. Algumas portas são comuns e necessárias a todos os tipos de gateway. Outras portas são necessárias por tipos de gateway específicos. Nesta seção, você pode encontrar uma ilustração das portas necessárias e uma lista dessas portas por cada tipo de gateway.

Gateways de Arquivo

A ilustração a seguir mostra as portas a serem abertas para a operação dos gateways de arquivo.



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

No	Para	Protocolo	Port	Como usar	
VM Storage Gateway	Amazon Web Services	Transmission Control Protocol (TCP)	443 (HTTPS)	Para a comunicação entre a VM do Storage GatewayAW Sendpoint de serviço. Para obter	

No	Para	Protocolo	Port	Como usar	
				informaçõ es sobre endpoints de serviço, consulte Permitir acesso ao AWS Storage Gateway por meio de firewalls e roteadores.	

No	Para	Protocolo	Port	Como usar
Seu navegador da web	VM Storage Gateway	TCP	80 (HTTP)	Por sistemas locais para obter a chave de ativação do Storage Gateway. A porta 80 só é usada durante a ativação de um dispositivo Storage Gateway. A VM do 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 console de gerenciamento do Storage Gateway,

No	Para	Protocolo	Port	Como usar	
				o host pelo qual se conecta ao console deverá ter acesso à porta 80 do gateway.	
VM 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.	

No	Para	Protocolo	Port	Como usar	
VM Storage Gateway	Amazon Web Services	TCP	22 (Canal de suporte)	Permite que o Support da Amazon Web Services tenha acesso ao gateway para ajudar 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.	

No	Para	Protocolo	Port	Como usar
VM Storage Gateway	Servidor de Network Time Protocol (NTP)	UDP	123 (NTP)	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: • 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 para ativação.

A tabela a seguir lista as portas que devem ser abertas para um gateway de arquivos usando o protocolo de Network File System (NFS) ou de Server Message Block (SMB). Essas regras de porta são parte de sua definição de security group.

Ru	Elemento de rede	Tipo de compartilhamento de arquivo	Protocolo	Port	Entra	Saída	Obrigaio?	Observações
1	Cliente de compartilhamento de arquivo	NFS	Dados TCP/UDP	111	✓	✓	✓	Transferência de dados de compartilhamento de arquivo (apenas para NFS)
			NFS de TCP/UDP	2049	✓	✓	✓	Transferência de dados de compartilhamento de arquivo (apenas para NFS)
			NFSv3 de TCP/UDP	2004	✓	✓	✓	Transferência de dados de compartilhamento de arquivo (apenas para NFS)
		SMB	SMBv2 de TCP/UDP	139	✓	✓	✓	Serviço de sessão de transferência de dados de compartilhamento de arquivo (apenas para SMB); substitui portas 137-139 por

Ru	Elemento de rede	Tipo de compartilhamento de arquivo	Protocolo	Port	Entra	Saída	Obrigatório?	Observações
								Microsoft Windows NT e posterior
			SMBv3 de TCP/UDP	445	✓	✓	✓	Serviço de sessão de transferência de dados de compartilhamento de arquivo (apenas para SMB); substitui portas 137-139 por Microsoft Windows NT e posterior
2	Navegador da web	NFS e SMB	TCP HTTP	80	✓	✓	✓	Console de Gerenciamento da Amazon Web Services (somente ativação)
			TCP HTTPS	443	✓	✓	✓	Console de Gerenciamento da Amazon Web Services (todas as outras operações)
3	DNS	NFS e SMB	TCP/UDP DNS	53	✓	✓	✓	Resolução de nome de IP
4	NTP	NFS e SMB	UDP NTP	123	✓	✓	✓	Serviço de sincronização da hora

Ru	Elemento de rede	Tipo de compartilhamento de arquivo	Protocolo	Port	Entra	Saída	Obrigatório?	Observações
5	Microsoft Active Directory	SMB	NetBIOS UDP	137	✓	✓	✓	Nome do serviço (não usado para NFS)
			NetBIOS UDP	138	✓	✓	✓	Serviço de datagrama
			TCP LDAP	389	✓	✓		Directory System Agent (DSA); conexão do cliente
			TCP LDAPS	636	✓	✓		LDAPS — Lightweight Directory Access Protocol (LDAP) sobre Secure Socket Layer (SSL)
6	Amazon S3	NFS e SMB	Dados HTTPS	443	✓	✓	✓	Transferência de dados de armazenamento
7	Storage Gateway	NFS e SMB	TCP SSH	22	✓	✓	✓	Canal de suporte
			TCP HTTPS	443	✓	✓	✓	Controle de gerenciamento
8	Amazon CloudFront	NFS e SMB	TCP HTTPS	443	✓	✓	✓	Para ativação

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, você também pode obter o endereço IP da Instância do Amazon EC2 no Console de Gerenciamento do Amazon EC2. 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 EC2. Obtenha então o endereço IP na parte superior da página do console. Para obter instruções, consulte .

É também possível obter o endereço IP no Console de Gerenciamento do Amazon EC2. 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 digite 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 digite o endereço IP elástico.
4. Depois que 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.

Noções Storage Gateway recursos e IDs de recurso

No Storage Gateway, o recurso principal é umGateway doMas outros tipos de recursos incluem:volume,fita virtual,Destino iSCSI, edispositivo 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 de Nome de região da Amazon (ARN)
ARN de gateway	`arn:aws:storagegateway:` *`region`*`:`*`account-id`* `:gateway/` *`gateway-id`*
ARN de compartilhamento de arquivos	`arn:aws:storagegateway:` *`region`*`:`*`account-id`* `:share/`*`share-id`*
ARN de volume	`arn:aws:storagegateway:` *`region`*`:`*`account-id`* `:gateway/` *`gateway-id`* `/volume/`*`volume-id`*
ARN de fita	`arn:aws:storagegateway:` *`region`*`:`*`account-id`* `:tape/`*`tapebarcode`*
ARN de destino (destino iSCSI)	`arn:aws:storagegateway:` *`region`*`:`*`account-id`* `:gateway/` *`gateway-id`* `/target/`*`iSCSItarget`*
ARN de dispositivo de VTL	`arn:aws:storagegateway:` *`region`*`:`*`account-id`* `:gateway/` *`gateway-id`* `/device/`*`vtldevice`*

O Storage Gateway do também é compatível com o uso de Instâncias EC2 e volumes e snapshots do EBS. Esses recursos 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 recurso do Storage Gateway aparecem em maiúscula. Entretanto, quando você usa esses IDs de recurso com a API do Amazon EC2, o Amazon EC2 espera que os IDs de recurso estejam em 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.

> **Important**
>
> Os IDs dos volumes do Storage Gateway e snapshots do Amazon EBS criados em volumes de gateway estão mudando para um formato mais longo. A partir de dezembro de 2016, todos os novos volumes e snapshots começaram a ser criados com string de 17 caracteres. A partir de abril de 2016, você poderá usar os IDs mais longos para testar os sistemas com o novo formato. Para obter mais informações, consulte IDs mais longos para recursos do EC2 e do EBS.
>
> Por exemplo, um volume ARN com o formato de ID de volume mais longo é semelhante ao seguinte: `arn:aws:storagegateway:us-west-2:111122223333:gateway/sgw-12A3456B/volume/vol-1122AABBCCDDEEFFG`.
>
> Um ID de snapshot com o formato de ID mais longo é semelhante ao seguinte: `snap-78e226633445566ee`.
>
> Para obter mais informações, consulteAnúncio: IDs de snapshot e volumes mais longos do Storage Gateway a serem lançados em 2016.

Como atribuir tags a recursos Storage Gateway

No Storage Gateway, você pode 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, você pode 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.

Para o gateway de arquivos, você pode usar tags para controlar o acesso a recursos. Para obter informações sobre como fazer isso, consulte Usar tags para controlar o acesso ao seu gateway e aos recursos do.

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:`. Este prefixo está reservado paraAWSUso do.
- Os caracteres válidos para a propriedade da chave são letras e números UTF-8, espaço e os caracteres especiais + - = . _ : / e @.

Como trabalhar com tags

Você pode trabalhar com tags usando o console do Storage Gateway, a Storage Gateway API ou oInterface da linha de comando (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 emhttps://console.aws.amazon.com/storagegateway/home.
2. No painel de navegação, escolha o recurso o qual você deseja atribui 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 emhttps://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. Selecione 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 emhttps://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.

Consulte também

Usar tags para controlar o acesso ao seu gateway e aos recursos do

Trabalhando com componentes de código aberto paraAWS Storage Gateway

Nesta seção, você pode encontrar informações sobre ferramentas e licenças de terceiros dos quais dependemos para oferecer a funcionalidade do Storage Gateway.

Tópicos

Componentes de código aberto para Storage Gateway

Várias ferramentas e licenças de terceiros são usadas para fornecer funcionalidade para gateway de volume, gateway de fita e Amazon S3 File Gateway.

Use os links a seguir para fazer download do código-fonte de determinados componentes de software de código aberto incluídos com oAWS Storage GatewaySoftware:

- Para gateways implantados no VMware ESXi:Arquivo sources.tar
- Para gateways implantados no Microsoft Hyper-V:Arquivo sources_hyperv.tar
- Para gateways implantados na Máquina virtual baseada em Kernel (KVM) do Linux:Arquivo sources_KVM.tar

Esse produto inclui software desenvolvido pelo projeto OpenSSL para uso no OpenSSL Toolkit (http://www.openssl.org/). Para obter as licenças relevantes para todas as ferramentas de terceiros dependentes, consulteLicenças de terceiros.

Componentes de código aberto para o Amazon S3 File Gateway

Várias ferramentas e licenças de terceiros são usadas para fornecer a funcionalidade do Amazon S3 File Gateway (S3 File Gateway).

Use os links a seguir para baixar o código-fonte de determinados componentes de software de código aberto incluídos com o software S3 File Gateway:

- Para o Amazon S3 File Gateway:sgw-file-s3-open-source.tgz

Esse produto inclui software desenvolvido pelo projeto OpenSSL para uso no OpenSSL Toolkit (http://www.openssl.org/). Para obter as licenças relevantes para todas as ferramentas de terceiros dependentes, consulteLicenças de terceiros.

Cotas

Cotas para compartilhamentos de arquivos

A tabela a seguir relaciona as cotas para compartilhamentos de arquivos.

Descrição	Gateway de arquivos
Número máximo de compartilhamentos de arquivos por bucket do Amazon S3. Existe uma mapeamento individualizado entre um compartilhamento de arquivo e um bucket do S3.	1
Número máximo de compartilhamentos de arquivos por gateway	10
Tamanho máximo de um único arquivo, que é o tamanho máximo de um objeto específico no Amazon S3 **Note** Se você gravar um arquivo superior a 5 TB, obterá a mensagem de erro "file too large" ("arquivo muito grande") e será feito upload somente dos primeiros 5 TB do arquivo.	5 TB
Tamanho máximo de caminho **Note** Os clientes não podem criar um caminho que exceda esse comprimento, e isso ao fazer isso um erro ocorre. Esse limite se aplica a ambos os	1024 bytes

Descrição	Gateway de arquivos
protocolos suportados com gateways de arquivos NFS e SMB.	

Tamanhos de discos locais 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)	Outros discos locais necessários
S3 File Gateway	150 GiB	64 TiB	—

> **Note**
>
> Você pode configurar uma ou mais unidades locais para seu cache até a capacidade máxima.
> Ao adicionar cache a um gateway existente, é importante criar novos discos no host (hipervisor ou Instância do Amazon EC2). Não altere o tamanho dos discos existentes caso os discos tenham sido alocados anteriormente como cache.

Uso de classes de armazenamento

O Storage Gateway é compatível com o Amazon S3 Standard, Amazon S3 Standard-Infrequente Access, Amazon S3 One Zone-Infrequente Access, Amazon S3 Intelligent-Tiering e S3 Glacier. Para obter mais informações sobre classes de armazenamento, consulteClasses de armazenamento do Amazon S3noGuia do usuário do Amazon Simple Storage Service.

Tópicos

- Usando classes de armazenamento com um gateway de arquivos
- Como usar a classe de armazenamento GLACIER com gateway de arquivos

Usando classes de armazenamento com um gateway de arquivos

Ao criar ou atualizar um compartilhamento de arquivos, você tem a opção de selecionar uma classe de storage para seus objetos. Você pode escolher a classe de armazenamento Amazon S3 Standard ou qualquer uma das classes de armazenamento S3 Standard — IA, S3 One Zone-IA ou S3 Intelligent-Tiering. Os objetos armazenados em qualquer uma dessas classes de armazenamento podem ser passados para GLACIER usando uma política de ciclo de vida

Classe de armazenamento do Amazon S3	Considerações
Padrão	Selecione Standard (Padrão) para armazenar seus arquivos acessados com frequência de forma redundante em várias zonas de disponibilidade separadas geograficamente. Esta é a classe de armazenamento padrão. Para obter mais detalhes, consulte Definição de preços do Amazon S3.
S3 Intelligent-Tiering	Escolha Intelligent-Tiering para otimizar os custos de armazenamento movendo automaticamente os dados para o nível de acesso de armazenamento mais econômico. Os objetos armazenados na classe de armazenamento Intelligent-Tiering podem incorrer em cobranças adicionais pela substituição, exclusão, solicitação ou transição de objetos entre classes de armazenamento dentro de 30 dias. Há uma duração mínima de armazenamento de 30 dias, e os objetos excluídos antes de 30 dias incorrem em uma cobrança proporcional igual à taxa de armazenamento para os dias restantes. Considere a frequência com que esses objetos mudam, por quanto tempo você planeja manter esses objetos e com que frequência você precisa acessá-los. Objetos menores que

Classe de armazenamento do Amazon S3	Considerações
	128 KB não estão qualificados para divisão automática na classe de armazenamento Intelligent-Tiering. Esses objetos são cobrados de acordo com as taxas do nível de acesso frequente e as taxas de exclusão antecipada se aplicam. O S3 Intelligent-Tiering agora oferece suporte a uma camada de acesso a arquivamento e um nível de acesso profundo ao arquivamento. O S3 Intelligent-Tiering move os objetos que não foram acessados durante 90 dias para o nível de Acesso de arquivamento e depois de 180 dias sem serem acessados para o nível de Acesso de arquivamento profundo. Sempre que um objeto em uma das camadas de acesso ao arquivamento é restaurado, o objeto se move para a camada Acesso Frequente em poucas horas e estará pronto para ser recuperado. Isso cria erros de tempo limite para usuários ou aplicativos que tentam acessar arquivos por meio de um compartilhamento de arquivos se o objeto só existir em uma das duas camadas de arquivamento. Não use os níveis de arquivamento com S3 Intelligent-Tiering se seus aplicativos estiverem acessando arquivos por meio dos compartilhamentos de arquivos apresentados pelo gateway de arquivos. Quando operações de arquivo que atualizam metadados (como proprietário, carimbo de data/hora, permissões e ACLs) são executadas em relação a arquivos gerenciados pelo gateway de arquivos, o objeto existente é

Classe de armazenamento do Amazon S3	Considerações
	excluído e uma nova versão do objeto é criada nesta classe de armazenamento do Amazon S3. Você deve validar como as operações de arquivos afetam a criação de objetos antes de usar essa classe de armazenamento em produção, pois as taxas de exclusão antecipad a se aplicam. Para obter mais detalhes, consulte Definição de preços do Amazon S3.

Classe de armazenamento do Amazon S3	Considerações
S3 Standard – IA	Selecione Standard-IA para armazenar seus arquivos raramente acessados de forma redundante em várias zonas de disponibilidade separadas geograficamente. Os objetos armazenados na classe de armazenamento Standard-IA podem incorrer em cobranças adicionais pela substituição, exclusão, solicitação, recuperação ou transição de objetos entre classes de armazenamento dentro de 30 dias. Há uma duração mínima de armazenamento de 30 dias. Objetos excluídos antes de 30 dias incorrem em uma cobrança proporcional igual à cobrança de armazenam ento para os dias restantes. Considere a frequência com que esses objetos mudam, por quanto tempo você planeja manter esses objetos e com que frequência você precisa acessá-los. Objetos menores que 128 KB são cobrados por 128 KB e taxas de exclusão antecipada se aplicam. Quando operações de arquivo que atualizam metadados (como proprietário, carimbo de data/hora, permissões e ACLs) são executada s em relação a arquivos gerenciados pelo gateway de arquivos, o objeto existente é excluído e uma nova versão do objeto é criada nesta classe de armazenamento do Amazon S3. Você deve validar como as operações de arquivos afetam a criação de objetos antes de usar essa classe de armazenamento em produção, pois as taxas de exclusão antecipad a se aplicam. Para obter mais detalhes, consulte Definição de preços do Amazon S3.

Classe de armazenamento do Amazon S3	Considerações
S3 One Zone – IA	Selecione One Zone-IA para armazenar seus arquivos acessados com pouca frequência em uma única zona de disponibilidade. Os objetos armazenados na classe de armazenamento One Zone-IA podem incorrer em cobranças adicionais pela substituição, exclusão, solicitação, recuperação ou transição de objetos entre classes de armazenam ento dentro de 30 dias. Há uma duração mínima de armazenamento de 30 dias, e os objetos excluídos antes de 30 dias incorrem em uma cobrança proporcional igual à taxa de armazenamento para os dias restantes. Considere a frequência com que esses objetos mudam, por quanto tempo você planeja manter esses objetos e com que frequência você precisa acessá-los. Objetos menores que 128 KB são cobrados por 128 KB e taxas de exclusão antecipada se aplicam. Quando operações de arquivo que atualizam metadados (como proprietário, carimbo de data/hora, permissões e ACLs) são executada s em relação a arquivos gerenciados pelo gateway de arquivos, o objeto existente é excluído e uma nova versão do objeto é criada nesta classe de armazenamento do Amazon S3. Você deve validar como as operações de arquivos afetam a criação de objetos antes de usar essa classe de armazenamento em produção, pois as taxas de exclusão antecipad a se aplicam. Para obter mais detalhes, consulte Definição de preços do Amazon S3.

Embora você possa gravar objetos diretamente de um compartilhamento de arquivos para o S3-Padrão-IA, S3-One-IA ou S3 Intelligent-Tiering zona de classe de storage, recomendamos que você use uma política de ciclo de vida para transferir esses objetos em vez de gravar diretamente do compartilhamento de arquivos, especialmente se você está esperando para atualizar ou excluir o objeto dentro de 30 dias após o arquivamento. Para obter informações sobre a política de ciclo de vida, consulteGerenciamento do ciclo de vida de objetos.

Como usar a classe de armazenamento GLACIER com gateway de arquivos

Se você transferir um arquivo para o S3 Glacier através das políticas de ciclo de vida do Amazon S3 e o arquivo é visível para o compartilhamento de arquivos clientes por meio do cache, você obtém os erros de I/O quando atualizar o arquivo. Recomendamos que você configure o CloudWatch Events para receber notificações quando ocorrer esses erros de I/O e usar a notificação para executar uma ação. Por exemplo, é possível restaurar o objeto arquivado para o Amazon S3. Depois que o objeto é restaurado para o S3, os clientes de compartilhamento de arquivos podem acessá-los e atualizá-los com êxito por meio do compartilhamento de arquivos.

Para obter informações sobre como restaurar objetos, consulteRestaurar objetos arquivadosnoGuia do usuário do Amazon Simple Storage Service.

Referência de API para Storage Gateway

Além de usar o console, você pode usar a API do AWS Storage Gateway para configurar e gerenciar programaticamente seus gateways. Esta seção descreve as operações do AWS Storage Gateway solicitação de assinatura para autenticação e tratamento de erros. Para obter mais informações sobre as regiões e os endpoints disponíveis para Storage Gateway, consulteAWS Storage GatewayEndpoints e cotas donoAWSReferência geral.

> **Note**
>
> Você também pode usar oAWSSDKs ao desenvolver aplicativos com Storage Gateway. OAWSOs SDKs para Java, .NET e PHP encapsulam a API do Storage Gateway subjacente, simplificando as tarefas de programação. Para obter informações sobre como fazer download de bibliotecas de SDKs, consulte Bibliotecas de códigos de exemplo.

Tópicos

AWS Storage GatewayCabeçalhos de solicitação requeridos

Esta seção descreve os cabeçalhos requeridos que você deve enviar em cada solicitação POST paraAWS 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 operação ActivateGateway.

```
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 paraAWS Storage Gateway. Os cabeçalhos mostrados a seguir que começam com “x-amz” sãoAWS-cabeçalhos específicos. Todos os outros cabeçalhos listados são cabeçalhos comuns usados em transações HTTP.

Cabeçalho	Descrição
`Authorization`	O cabeçalho de autorização contém várias informações sobre a solicitação que permitemAWS Storage GatewayPara determinar 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): `Authorization: AWS4-HMAC_SHA456 Credentials= YourAccessKey /yyymmdd/region/storagegateway/aws4_request, SignedHeaders=content-type;host;x-amz-date;x-amz-target, Signature= CalculatedSignature` Na sintaxe anterior, você especifica YourAccessKey, o ano, o mês e o dia (yyyymmdd), a região e CalculatedSignature. O formato do cabeçalho de autorização é determinado pelos requisitos doAWSProcesso de assinatura V4. Os detalhes da assinatura são discutidos no tópico Solicitações de assinatura.
`Content-Type`	Usar `oapplication/x-amz-json-1.1` Como tipo de conteúdo para todas as solicitações paraAWS Storage Gateway. `Content-Type: application/x-amz-json-1.1`

Cabeçalho	Descrição
`Host`	Use o cabeçalho do host para especificar oAWS Storage Gatewayen dpoint para onde você envia sua solicitação. Por exemplo,`storagegateway.us-east-2.amazonaws.com` É o endpoint da região Leste dos EUA (Ohio). Para obter mais informações sobre os endpoints disponíveis paraAWS Storage Gateway, consulteAWS Storage GatewayEndpoints e cotas donoAWSReferência geral. `Host: storagegateway. region.amazonaws.com`
`x-amz-date`	Você deve fornecer o time stamp no cabeçalho HTTP `Date` ou no cabeçalho `x-amz-date` da AWS. (Algumas bibliotecas de cliente HTTP não permitem a definição do cabeçalho `Date`.) Quando um`x-amz-date` O cabeçalho está presente, oAWS Storage Gatewayig norar qualquer`Date`cabeçalho durante a autenticação da solicitação. O formato `x-amz-date` deve ser o formato básico ISO8601, no formato YYYYMMDD'T'HHMMSS'Z'. Quando forem usados os cabeçalhos `Date` e `x-amz-date` , o formato do cabeçalho de data não precisa ser o ISO8601. `x-amz-date: YYYYMMDD'T'HHMMSS'Z'`
`x-amz-target`	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. `x-amz-target: StorageGateway_ APIversion .operationName` O valor operationName (por exemplo, "ActivateGateway") pode ser encontrado na lista de API, Referência de API para Storage Gateway.

Solicitações de assinatura

O Storage Gateway requer a autenticação de toda solicitação enviada 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 solicitação. Do contrário, a solicitação é rejeitada.

O Storage Gateway suporta autenticação usandoAWSSignature versão 4. 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. Usar uma forma canônica é necessário porque o Storage Gateway usa a mesma forma canônica quando recalcula uma assinatura para comparar com a enviada por você.

- 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: Criar 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
92c0effa6f9224ac752ca179a04cecbede3038b0959666a8160ab452c9e51b3e
```

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: Criar 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 for usada a chave de acesso secreta, wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY, 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 para 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 oferece informações de referência sobre erros do AWS Storage Gateway. 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 de operação `ActivationKeyInvalid` é retornado somente pela API ActivateGateway.

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 exceções de API do AWS Storage Gateway. Quando uma operação do AWS Storage Gateway retorna uma resposta de erro, o corpo da resposta contém uma das exceções a seguir. 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
`IncompleteSignatureException`	A assinatura especificada está incompleta.	400 solicitação inválida
`InternalFailure`	O processamento da solicitação falhou por algum erro ou alguma exceção ou falha desconhecida.	500 Internal Server Error
`InternalServerError`	Uma das mensagens de código de erro de operação em Códigos de erro de operação.	500 Internal Server Error
`InvalidAction`	A ação ou operação solicitada é inválida.	400 solicitação inválida
`InvalidClientTokenId`	O certificado X.509 ouAWSO ID da chave de acesso da fornecido não existe em nossos registros.	403 proibido

Exceção	Message	Código de status HTTP
`InvalidGatewayRequestException`	Uma das mensagens de código de erro de operação em Códigos de erro de operação.	400 solicitação inválida
`InvalidSignatureException`	A assinatura da solicitação que calculamos não corresponde à assinatura que você forneceu. Verificar oAWSChave de acesso e método de assinatura.	400 solicitação inválida
`MissingAction`	Está faltando um parâmetro de ação ou operação na solicitação.	400 solicitação inválida
`MissingAuthenticationToken`	A solicitação deve conter um válido (registrado)AWSID de chave de acesso ou certificado X.509.	403 proibido
`RequestExpired`	A solicitação ultrapassa data de expiração ou a data de solicitação (ambas com acréscimo de 15 minutos) ou a data de solicitação ultrapassa 15 minutes no futuro.	400 solicitação inválida
`SerializationException`	Ocorreu um erro durante a serialização. Verifique se a carga JSON está bem formada.	400 solicitação inválida
`ServiceUnavailable`	Falha na solicitação devido a um erro temporário do servidor.	503 Service Unavailable (503 Serviço não disponível)
`SubscriptionRequiredException`	OAWSO ID da chave de acesso da precisa de uma assinatura do 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 operação do AWS Storage Gateway 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
`BandwidthThrottleScheduleNotFound`	Não foi possível encontrar a limitação de largura de banda.	DeleteBandwidthRateLimit
`CannotExportSnapshot`	Não é possível exportar o snapshot especificado.	CreateCachediSCSIVolume CreateStorediSCSIVolume
`InitiatorNotFound`	Não foi possível encontrar o iniciador especificado.	DeleteChapCredentials
`DiskAlreadyAllocated`	O disco especificado já está alocado.	AddCache AddUploadBuffer AddWorkingStorage CreateStorediSCSIVolume
`DiskDoesNotExist`	O disco especificado não existe.	AddCache AddUploadBuffer AddWorkingStorage CreateStorediSCSIVolume
`DiskSizeNotGigAligned`	O disco especificado não está alinhado em gigabyte.	CreateStorediSCSIVolume
`DiskSizeGreaterThanVolumeMaxSize`	O tamanho do disco é superior ao tamanho máximo de volume.	CreateStorediSCSIVolume

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.	CreateStorediSCSIVolume
`DuplicateCertificateInfo`	As informações de certificado especificadas estão duplicadas.	ActivateGateway
FileSystemAssociationEndpointConfigurationConflict	A configuração de endpoint existente da File System Association entra em conflito com a configuração especificada.	AssociateFilesystem
FileSystemAssociationEndPointTipaddresSalreadyInUse	O endereço IP do endpoint especificado já está em uso.	AssociateFilesystem
FileSystemAssociationEndPointTipAddressausente	O endereço IP do endpoint da associação do sistema de arquivos está ausente.	AssociateFilesystem
FileSystemAssociationNotFound	Não foi encontrada a associação do sistema de arquivos especificado.	UpdateFilesystemAssociation DisassociateFilesystem DescribeFilesystemAssociations
FileSystem NotFound	O sistema de arquivos especificado não foi encontrado.	AssociateFilesystem

Código de erro de operação	Message	Operações que retornam esse código de erro
`GatewayInternalError`	Ocorreu um erro interno no gateway.	AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateStorediSCSIVolume CreateSnapshotFromVolumeRecoveryPoint DeleteBandwidthRateLimit DeleteChapCredentials DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes 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 CreateCachediSCSIVolume CreateSnapshot CreateStorediSCSIVolume CreateSnapshotFromVolumeRecoveryPoint DeleteBandwidthRateLimit DeleteChapCredentials DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes 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 especific ado não foi encontrado.	AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRec overyPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteGateway DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes 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 CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes 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 CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteGateway DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes

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 inválidos.	ActivateGateway AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteGateway DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes

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 é inválido.	CreateStorediSCSIVolume

Código de erro de operação	Message	Operações que retornam esse código de erro
`MaximumVolumeCount Exceeded`	A contagem máxima de volume foi excedida.	CreateCachediSCSIVolume CreateStorediSCSIVolume DescribeCachediSCSIVolumes DescribeStorediSCSIVolumes
`NetworkConfigurati onChanged`	A configuração de rede do gateway mudou.	CreateCachediSCSIVolume CreateStorediSCSIVolume

Código de erro de operação	Message	Operações que retornam esse código de erro
`NotSupported`	A operação especific ada não é comportada.	ActivateGateway AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRec overyPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteGateway DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes

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.	CreateCachediSCSIVolume CreateStorediSCSIVolume

Código de erro de operação	Message	Operações que retornam esse código de erro
`StagingAreaFull`	A área de preparação está cheia.	CreateCachediSCSIVolume CreateStorediSCSIVolume
`TargetAlreadyExists`	O destino especificado já existe.	CreateCachediSCSIVolume CreateStorediSCSIVolume
`TargetInvalid`	O destino especificado é inválido.	CreateCachediSCSIVolume CreateStorediSCSIVolume DeleteChapCredentials DescribeChapCredentials UpdateChapCredentials
`TargetNotFound`	O destino especificado não foi encontrado.	CreateCachediSCSIVolume CreateStorediSCSIVolume DeleteChapCredentials DescribeChapCredentials DeleteVolume UpdateChapCredentials

Código de erro de operação	Message	Operações que retornam esse código de erro
`UnsupportedOperationForGatewayType`	A operação especificada não é válida para o tipo de gateway.	AddCache AddWorkingStorage CreateCachediSCSIVolume CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteSnapshotSchedule DescribeCache DescribeCachediSCSIVolumes DescribeStorediSCSIVolumes DescribeUploadBuffer DescribeWorkingStorage ListVolumeRecoveryPoints
`VolumeAlreadyExists`	O volume especificado já existe.	CreateCachediSCSIVolume CreateStorediSCSIVolume
`VolumeIdInvalid`	O volume especificado é inválido.	DeleteVolume
`VolumeInUse`	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 DescribeCachediSCSIVolumes DescribeSnapshotSchedule DescribeStorediSCSIVolumes UpdateSnapshotSchedule
`VolumeNotReady`	O volume especificado não está pronto.	CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint

Respostas de erro

Quando existe um erro, as informações no cabeçalho da resposta contêm:

- Content-Type: application/x-amz-json-1.1
- 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.

Type: String

error

Contém detalhes de erro específicos à API. Em erros genéricos (isto é, não específicos a nenhuma API), essa informação não é mostrada.

Type: Coleta

errorCode

Um dos códigos de erro de operação .

Type: String

errorDetails

Esse campo não é usado na versão atual da API.

Type: String

mensagem

Uma das mensagens de código de erro de operação em .

Type: 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 de ARN de 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 corresponde 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 ver uma lista das operações do Storage Gateway, consulteAçõesnoAWS Storage GatewayReferência de API do.

Histórico de documentos doAWSStorage Gateway

- Versão da API: 30/06/2013
- Atualização de documentação mais recente: 12 de outubro de 2021

A tabela a seguir descreve as alterações importantes em cada versão doAWSGuia do Usuário Storage GatewayDepois de abril de 2018. Para receber notificações sobre atualizações dessa documentação, você pode se inscrever em um feed RSS.

update-history-change	update-history-description	update-history-date
Procedimentos de criação de gateway	O procedimento para criar um novo gateway foi atualizado para refletir as alterações no console do Storage Gateway. Para obter mais informaçõ es, consulteCriar e ativar um Amazon S3 File Gateway.	12 de outubro de 2021
Support para arquivos de fechamento forçado em compartilhamentos de arquivos SMB	Agora você pode usar as configurações do Grupo local para atribuir permissões de administrador do gateway. Os administradores do gateway podem usar o snap-in do Console de Gerenciam ento Microsoft de Pastas Compartilhadas para forçar o fechamento de arquivos que estão abertos e bloqueado s em compartilhamentos de arquivos SMB. Para obter mais informações, consulteConfigure Grupos Locais para seu gateway.	12 de outubro de 2021

Suporte ao log de auditoria para compartilhamentos de arquivos NFS	Agora, é possível configura r compartilhamentos de arquivos NFS para gerar logs de auditoria que fornecem detalhes sobre o acesso do usuário a arquivos e pastas em um compartilhamento de arquivos. É possível usar esses logs para monitorar as atividades do usuário e tomar medidas se forem identific ados padrões de atividade inadequados. Para obter mais informações, consulteNoções básicas sobre registros de auditoria do gateway.	12 de outubro de 2021
Suporte a alias de ponto de acesso	Os compartilhamentos de arquivos do gateway de arquivos agora podem se conectar ao armazenam ento do Amazon S3 usando aliases de ponto de acesso no estilo bucket. Para obter mais informações, consulteCrie um compartilhamento de arquivos.	12 de outubro de 2021

Suporte a ponto de acesso e endpoint VPC	Os compartilhamentos de arquivos do gateway de arquivos agora podem se conectar a buckets do S3 por meio de pontos de acesso ou endpoints de interface em sua VPC com tecnologiaAWS PrivateLink. Para obter mais informações, consulteCrie um compartilhamento de arquivos.	7 de julho de 2021
Suporte de bloqueio oportunista	Os compartilhamentos de arquivos do gateway de arquivos agora podem usar o bloqueio oportunista para otimizar sua estratégia de buffer de arquivos, o que melhora o desempenho na maioria dos casos, especialmente no que diz respeito aos menus de contexto do Windows. Para obter mais informações, consulteCrie um compartilhamento de arquivos SMB.	7 de julho de 2021
Conformidade com FedRAMP	O Storage Gateway agora está em conformidade com o FedRAMP. Para obter mais informações, consulteValidação de conformidade para Storage Gateway.	24 de novembro de 2020

Limitação de largura de banda baseada em agendamento	Agora o Storage Gateway oferece suporte à limitação de largura de banda baseada em programação para gateways de fita e volume. Para obter mais informaçõ es, consulteAgendamento da limitação da largura de banda usando o console do Storage Gateway.	9 de novembro de 2020
Notificação de upload de arquivos para gateway de arquivos	O gateway de arquivos agora fornece notificação de upload de arquivos, que o notifica quando um arquivo foi totalmente carregado para o Amazon S3 pelo gateway de arquivos. Para obter mais informações, consulteObtendo notificação de upload de arquivos.	9 de novembro de 2020
Enumeração baseada em acesso para gateway de arquivos	O gateway de arquivos agora fornece enumeração baseada em acesso, que filtra a enumeração de arquivos e pastas em um compartil hamento de arquivos SMB com base nas ACLs do compartilhamento. Para obter mais informações, consulteCriar um compartil hamento de arquivos SMB.	9 de novembro de 2020

Migração de gateway de	O gateway de arquivos agora fornece um processo documentado para substituir um gateway de arquivos existente por um novo gateway de arquivos. Para obter mais informações, consulteSubstituindo um gateway de arquivos por um novo gateway de arquivos.	30 de outubro de 2020
Desempenho de leitura de cache frio do gateway de arquivos 4x aumento	O Storage Gateway aumentou o desempenho de leitura de cache frio 4x. Para obter mais informações, consulteOrientação de desempenho para gateways de arquivos.	31 de agosto de 2020
Solicite o equipamento de hardware por meio do console	Agora você pode solicitar o equipamento de hardware por meio doAWSConsole Storage Gateway Para obter mais informações, consulteUsar o Dispositivo Storage Gateway.	12 de agosto de 2020

Support para endpoints do Federal Information Processing Standard (FIPS - Padrão federal de processamento de informações)AWSRegiões da	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, consulteAWSEndpoints e cotas do Storage GatewaynoAWSReferência geral.	31 de julho de 2020

Support para vários compartilhamentos de arquivos anexados a um único bucket do Amazon S3	O gateway de arquivos agora oferece suporte à criação de vários compartilhamentos de arquivos para um único bucket do S3 e a sincronização do cache local do gateway de arquivos com um bucket com base na frequência de acesso ao diretório. Você pode limitar o número de buckets necessários para gerenciar os compartilhamentos de arquivos criados no gateway de arquivos. Você pode definir vários prefixos do S3 para um bucket do S3 e mapear um único prefixo S3 para um único compartilhamento de arquivos de gateway. Você também pode definir nomes de compartilhamento de arquivos de gateway para serem independentes do nome do bucket para se adequar à convenção de nomenclatura de compartilhamento de arquivos local. Para obter mais informações, consulteCriar um compartilhamento de arquivos NFSouCriar um compartilhamento de arquivos SMB.	7 de julho de 2020

Armazenamento em cache local do gateway de arquivos 4x aumento	O Storage Gateway agora oferece suporte a um cache local de até 64 TB para gateway de arquivos, melhorando o desempenho de aplicativos locais, fornecend o acesso de baixa latência a conjuntos de dados de trabalho maiores. Para obter mais informações, consulteTamanhos de discos locais recomendados para seu gatewaynoGuia do Usuário Storage Gateway.	7 de julho de 2020
Veja os alarmes do Amazon CloudWatch no console do Storage Gateway	Agora, é possível visualizar os alarmes do CloudWatch no console do Storage Gateway. Para obter mais informações, consulteEntendendo alarmes do CloudWatch.	29 de maio de 2020

Suporte para endpoints do Federal Information Processing Standard (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 arquivos, consulte Escolher um endpoint de serviço. Para escolher um endpoint de FIPS para um gateway de volumes, consulte Escolher um endpoint de serviço. Para escolher um endpoint de FIPS para um gateway de fitas, consulte Escolher um endpoint de serviço.	22 de maio de 2020
NovoAWSRegiões da	Agora o Storage Gateway está disponível nas regiões África (Cidade do Cabo) e Europa (Milão). Para obter mais informaçõ es, consulteAWSEndpoi nts e cotas do Storage GatewaynoAWSReferência geral.	7 de maio de 2020

Suporte à classe de armazenamento S3 Intelligent-Tiering	Agora o Storage Gateway oferece suporte à 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, consulteClasse de armazenamento que otimiza automaticamente objetos muito e pouco acessadosnoGuia do usuário do Amazon Simple Storage Service.	30 de abril de 2020
NovoAWSRegião	O Storage Gateway agora está disponível noAWSRegião GovCloud (Leste dos EUA). Para obter mais informações, consulteAWSEndpoints e cotas do Storage GatewaynoAWSReferência geral.	12 de março de 2020

Suporte para hipervisor de Linux Kernel-based Virtual Machine (KVM)	Agora o Storage Gateway oferece a possibilidade de implantar um gateway local na plataforma de virtualiz ação da KVM. Os gateways implantados na KVM têm todos as mesmas funcional idades e recursos que os gateways locais existentes. Para obter mais informaçõ es, consulteHipervisores compatíveis e requisitos de hostnoGuia do Usuário Storage Gateway.	4 de fevereiro de 2020
Suporte para o VMware vSphere High Availability	Agora o Storage Gateway oferece suporte para alta disponibilidade no VMware para ajudar a proteger as cargas de trabalho de armazenamento contra falhas de hardware, hipervisor ou rede. Para obter mais informações, consulteUsar o VMware vSphere High Availability com o Storage GatewaynoGuia do Usuário Storage Gateway. Esta versão também inclui melhorias de desempenho. Para obter mais informações, consulteDesempenhonoGuia do Usuário Storage Gateway.	20 de novembro de 2019

NovoRegião da AWSGateway de fita	Agora o gateway de fita está disponível na região América do Sul (São Paulo). Para obter mais informaçõ es, consulteAWSEndpoi nts e cotas do Storage GatewaynoAWSReferência geral.	24 de setembro de 2019
Support ao Amazon CloudWatch Logs	Agora, é possível configura r gateways de arquivos com os grupos de logs do Amazon CloudWatch para receber notificações sobre erros e sobre a integridade do gateway e seus recursos. Para obter mais informações, consulteReceber notificações sobre erros e sobre Health do gateway com os grupos de logs do Amazon CloudWatc hnoGuia do usuário Storage Gateway.	4 de setembro de 2019
NovoRegião da AWS	Agora o Storage Gateway está disponível na região Ásia-Pacífico (Hong Kong). Para obter mais informaçõ es, consulteAWSEndpoi nts e cotas do Storage GatewaynoAWSReferência geral.	14 de agosto de 2019

NovoRegião da AWS	Agora o Storage Gateway está disponível na região do Oriente Médio (Bahrein) . Para obter mais informaçõ es, consulteAWSEndpoi nts e cotas do Storage GatewaynoAWSReferência geral.	29 de julho de 2019
Suporte para 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 infraestr utura de armazenamento baseada em nuvem. Para obter mais informações, consulte Ativar um gateway em uma nuvem privada virtual.	20 de junho de 2019
O compartilhamento de arquivos SMB oferece suporte para ACLs do Microsoft Windows	Para gateways de arquivos, agora você pode usar listas de controle de acesso (ACLs) do Microsoft Windows para controlar o acesso aos compartilhamentos 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

O gateway de arquivos oferece suporte à autorização com base em tag	O gateway de arquivos agora oferece suporte à autorizaç ão com base em tag. Você pode controlar o acesso aos recursos do gateway de arquivos com base nas tags desses recursos. Também é possível controlar o acesso com base nas tags que podem ser transmiti das em uma condição de solicitação do IAM. Para obter mais informações, consulte Controlar o acesso aos recursos do gateway de arquivos.	4 de março de 2019
Disponibilidade de hardware do Storage Gateway na Europa	Agora o dispositivo de hardware do Storage Gateway está disponível na Europa. Para obter mais informaçõ es, consulteAWSRegiões do dispositivo de hardware do StoragenoAWSReferência geral. Além disso, agora você pode aumentar o armazenam ento utilizável no dispositi vo de hardware do Storage Gateway de 5 TB para 12 TB e substituir a placa de rede de cobre instalada 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

Support para dispositivo de hardware do Storage Gateway	O dispositivo de hardware do Storage Gateway pré-instalado em um servidor de terceiros. Você pode gerenciar o dispositivo do AWS Management Console. O dispositivo pode hospedar arquivo, fita e gateways de volume. Para obter mais informações, consulteUsar o Dispositivo Storage Gateway.	18 de setembro de 2018
Suporte para protocolo de Server Message Block (SMB)	Os gateways de arquivos acrescentaram suporte ao protocolo de Server Message Block (SMB) para compartil hamentos de arquivos. Para obter mais informações, consulte Como criar um compartilhamento de arquivos.	20 de junho de 2018

Atualizações anteriores

A tabela a seguir descreve as alterações importantes em cada versão doAWSGuia do Usuário Storage GatewayAntes de maio de 2018.

Alteração	Descrição	Alterado em
Support à classe de armazenam ento S3 One Zone-IA	Para gateways de arquivos, agora você pode escolher o S3 One Zone-IA como a classe de armazenamento padrão para os compartilhamentos de arquivos. Usar essa classe de armazenamento permite que você armazene seus dados de objetos em uma única zona de disponibilidade do Amazon S3. Para obter mais informações, consulte Crie um compartilhamento de arquivos.	4 de abril de 2018

Alteração	Descrição	Alterado em
Novo Região da AWS	Agora o gateway de fita está disponível na região Ásia-Pacífico (Cingapura). Para obter informações detalhadas, consulte Regiões do AWS com suporte.	3 de abril de 2018
Support para notificação de atualização de cache, pagamento pelo solicitante e ACLs padrão para buckets do Amazon S3	Com os gateways de arquivos, você pode enviar notificações quando terminam de atualizar o cache para seu bucket do Amazon S3. Para obter mais informações, consulteArquivo RefreshCache.htmlnoReferência do Storage Gateway. Para gateways de arquivo, você pode especificar que o solicitante ou leitor paga as cobranças de acesso ao invés do proprietário do bucket. Com os gateways de arquivo, você pode ativar conceder controle total ao proprietário do bucket do S3 que mapeia para o compartilhamento de arquivos NFS. Para obter mais informações, consulte Crie um compartilhamento de arquivos.	1º de março de 2018
Novo Região da AWS	Agora o Storage Gateway está disponível na região Europa (Paris). Para obter informações detalhadas, consulte Regiões do AWS com suporte.	18 de dezembro de 2017
Suporte para notificação de upload de arquivos e adivinhação do tipo MIME	Agora, os gateways de arquivos enviam notificações quando todos os arquivos gravados no seu compartilhamento de arquivos NFS são carregados no Amazon S3. Para obter mais informações, consulteNotifyWhenUploadednoReferência do Storage Gateway. Agora, os gateways de arquivos permitem adivinhar o tipo MIME dos objetos carregados com base nas extensões de arquivo. Para obter mais informações, consulte Crie um compartilhamento de arquivos.	21 de novembro de 2017

Alteração	Descrição	Alterado em
Compatibilidade com o VMware ESXi Hypervisor versão 6.5	AWSAgora o Storage Gateway oferece suporte para VMware ESXi Hypervisor versão 6.5. Além das versões 4.1, 5.0, 5.1, 5.5 e 6.0. Para obter mais informações, consulte Hipervisores compatíveis e requisitos de host.	13 de setembro de 2017
Suporte para gateway de arquivos no hipervisor do Microsoft Hyper-V	Agora você pode 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
Novo Região da AWS	Agora o Storage Gateway está disponível na região Ásia-Pacífico (Mumbai). Para obter informações detalhadas, consulte Regiões do AWS com suporte.	02 de maio de 2017
Atualizações nas configurações de compartilhamento de arquivos Compatibilidade com atualização de cache para 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 compartil hamento de arquivos. Para obter mais informações, consulte Crie um 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 na referência da API.	28 de março de 2017

Alteração	Descrição	Alterado em
Suporte para gateways de arquivos no Amazon EC2	AWSAgora o Storage Gateway oferece a possibilidade de implantar um gateway de arquivos no Amazon EC2. Você pode iniciar um gateway de arquivos no Amazon EC2 usando o Storage Gateway Amazon Machine Image (AMI) do, agora disponível como uma comunidade AMI. Para obter informações sobre como criar um gateway de arquivos e implantá-lo em uma Instância EC2, consulte Criar e ativar um Amazon S3 File Gateway. Para obter informações sobre como iniciar uma AMI de gateway de arquivos, consulte Implantar um gateway de arquivos em um host do Amazon EC2. Além disso, agora o gateway de arquivos oferece suporte à configuração de proxy HTTP. Para obter mais informações, consulte Roteamento do gateway implantado no EC2 por meio de um proxy HTTP.	08 de fevereiro de 2017
Novo Região da AWS	Agora o Storage Gateway está disponível na região Europa (Londres). Para obter informações detalhadas, consulte Regiões do AWS com suporte.	13 de dezembro de 2016
Novo Região da AWS	Agora o Storage Gateway está disponível na região Canadá (Central). Para obter informações detalhadas, consulte Regiões do AWS com suporte.	08 de dezembro de 2016
Suporte para gateway de arquivos	Além dos gateways de volumes e do gateway de fita, agora o Storage Gateway oferece 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

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.