Guia do usuário

AWSStorage Gateway

Versão da API 2021-03-31

AWSStorage Gateway: Guia do usuário

Table of Contents

O que é o Amazon FSx File Gateway?

O Storage Gateway oferece soluções de armazenamento de gateway de arquivos, gateway de volume e gateway de fita.

O Amazon FSx File Gateway (FSx File) é um novo tipo de gateway de arquivos que fornece baixa latência e acesso eficiente a compartilhamentos de arquivos do FSx for Windows File Server na nuvem a partir de sua instalação local. Se você mantiver o armazenamento de arquivos local devido aos requisitos de latência ou largura de banda, poderá usar o arquivo FSx para acesso contínuo a compartilhamentos de arquivos do Windows totalmente gerenciados, altamente confiáveis e praticamente ilimitados fornecidos noAWSCloud by FSx for Windows File Server.

Benefícios do uso do Amazon FSx File Gateway

O FSx File fornece os seguintes benefícios:

- Ajuda a eliminar servidores de arquivos locais e consolida todos os dados emAWSPara aproveitar a escala e a economia do armazenamento em nuvem.
- Fornece opções que você pode usar para todas as cargas de trabalho de arquivos, incluindo aquelas que exigem acesso local aos dados da nuvem.
- Aplicativos que precisam permanecer no local agora podem experimentar a mesma baixa latência e alto desempenho que eles têm emAWS, sem taxar suas redes ou afetar as latências experimentadas por seus aplicativos mais exigentes.

Como o Amazon FSx File Gateway funciona

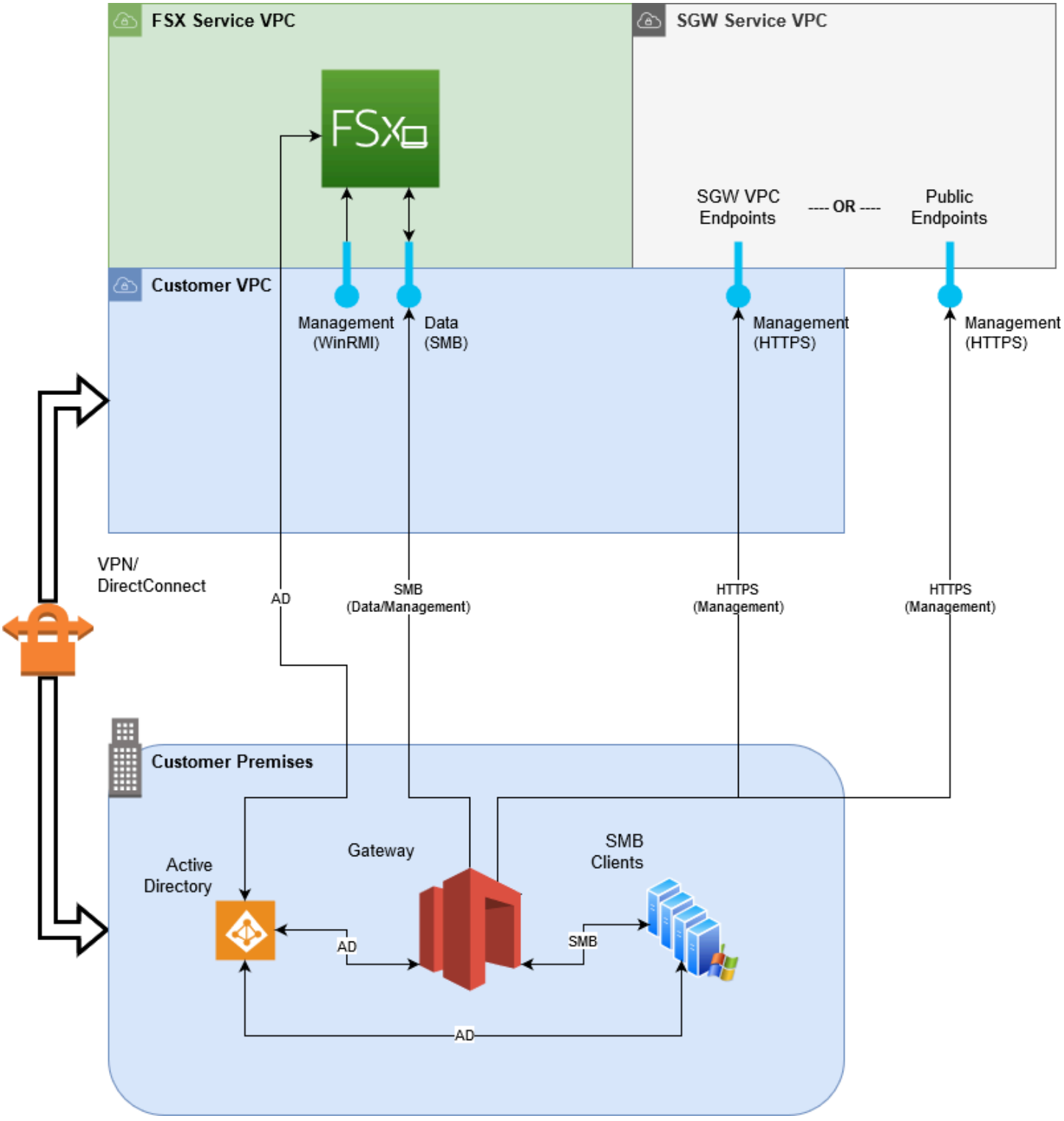
Para usar o Amazon FSx File Gateway (FSx File), é necessário ter pelo menos um sistema de arquivos do Amazon FSx for Windows File Server. Você também deve ter acesso local ao FSx for Windows File Server, seja por meio de uma VPN ou por meio de umAWS Direct ConnectConexão. Para obter mais informações sobre como usar sistemas de arquivos do Amazon FSx, consulteO que é o Amazon FSx for Windows File Server?

Você baixa e implanta o dispositivo virtual FSx File VMware ou umAWSStorage Gateway Hardware Appliance em seu ambiente local. Depois de implantar o appliance, você ativa o arquivo FSx a partir do console do Storage Gateway ou por meio da Storage Gateway API. Você também pode criar um arquivo FSx usando uma imagem do Amazon Elastic Compute Cloud (Amazon EC2).

Depois que o Amazon FSx File Gateway for ativado e acessar o FSx for Windows File Server, use o console do Storage Gateway para associá-lo ao seu domínio do Microsoft Active Directory. Depois que o gateway ingressar com êxito em um domínio, você usa o console do Storage Gateway para anexar o gateway a um FSx for Windows File Server existente. O FSx for Windows File Server disponibiliza todos os compartilhamentos no servidor como compartilhamentos no Amazon FSx File Gateway. Em seguida, você pode usar um cliente para navegar e se conectar aos compartilhamentos de arquivos no Arquivo FSx que correspondem ao Arquivo FSx selecionado.

Quando os compartilhamentos de arquivos estão conectados, você pode ler e gravar seus arquivos localmente, enquanto se beneficia de todos os recursos disponíveis no FSx for Windows File Server. FSx File mapeia compartilhamentos de arquivos locais e seu conteúdo para compartilhamentos de arquivos armazenados remotamente no FSx for Windows File Server. Há uma correspondência 1:1 entre os arquivos remotos e localmente visíveis e seus compartilhamentos.

O diagrama a seguir fornece uma visão geral da implantação do armazenamento para Storage Gateway.



Observe o seguinte no diagrama:

- AWS Direct Connectou uma VPNé necessário para permitir que o Arquivo FSx acesse o compartilhamento de arquivos do Amazon FSx usando SMB e para permitir que o FSx for Windows File Server entre em seu domínio do Active Directory local.
- Amazon Virtual Private Cloud (Amazon VPC)é necessário para se conectar ao serviço FSx for Windows File Server VPC e ao serviço Storage Gateway VPC usando endpoints privados. O arquivo FSx também pode se conectar aos endpoints públicos.

Você pode usar o Amazon FSx File Gateway em todosAWSRegiões em que o FSx for Windows File Server está disponível.

Configuração do Amazon FSx File Gateway

Esta seção fornece instruções para começar a usar o Amazon FSx File Gateway. Para começar a usá-lo, primeiro registre-se noAWS. Se você estiver usando o pela primeira vez, recomendamos fazer 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 Gerenciamento de Faturamento e Custos da AWS. 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 de grupos a serem adicionadas ao novo usuário do. 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 de

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.

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

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.

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.

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

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

Protocolo	Port	Direção	Origem	Destination (Destino)	Como usar
					oAWSendpoint de serviço. Para obter informações 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. A 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	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	Suporte	PermiteSuportePara 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

Para o FSx File Gateway, você deve usar o Microsoft Active Directory para 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 maioriaAWS 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.

O FSx File Gateway requer as portas a seguir.

Protocolo	Port	Direção	Origem	Destination (Destino)	Como usar
UDP NetBIOS	137	Entrada e saída		Microsoft Active Directory	Para se conectar ao Microsoft Active Directory.
UDP NetBIOS	138	Entrada e saída			Para o serviço de datagrama
TCP LDAP	389	Entrada e saída			Para conexão do cliente Directory System Agent (DSA)
Dados TCP v2/v3	445	Saída			Transferência de dados de armazenamento entre o gateway de arquivos e o FSx for Windows File Server

Protocolo	Port	Direção	Origem	Destination (Destino)	Como usar
TCP (HTTPS)	443	Saída		endpoints do serviço Storage Gateway	Controle de gerenciamento — usado para comunicação de uma VM do Storage Gateway para umaAWSendpoint de serviço
TCP HTTPS	443	Saída		Amazon CloudFront	Para ativação do gateway
TCP	443	Saída		Uso de VPC endpoint	Controle de gerenciamento — usado para comunicação de uma VM do Storage Gateway para umaAWSendpoint de serviço.
TCP	1026	Saída			Usado para controlar o tráfego

Protocolo	Port	Direção	Origem	Destination (Destino)	Como usar
TCP	1027	Saída			Usado somente durante a ativação e pode ser fechado
TCP	1028	Saída			Usado para controlar o tráfego
TCP	1031	Saída			Usado apenas para atualizaç ões de software para gateways de arquivos
TCP	2222	Saída			Usado para abrir um canal de suporte para o gateway ao usar endpoints da VPC
TCP (HTTPS)	8080	Entrada			Necessário brevemente para ativação de um dispositivo de hardware

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

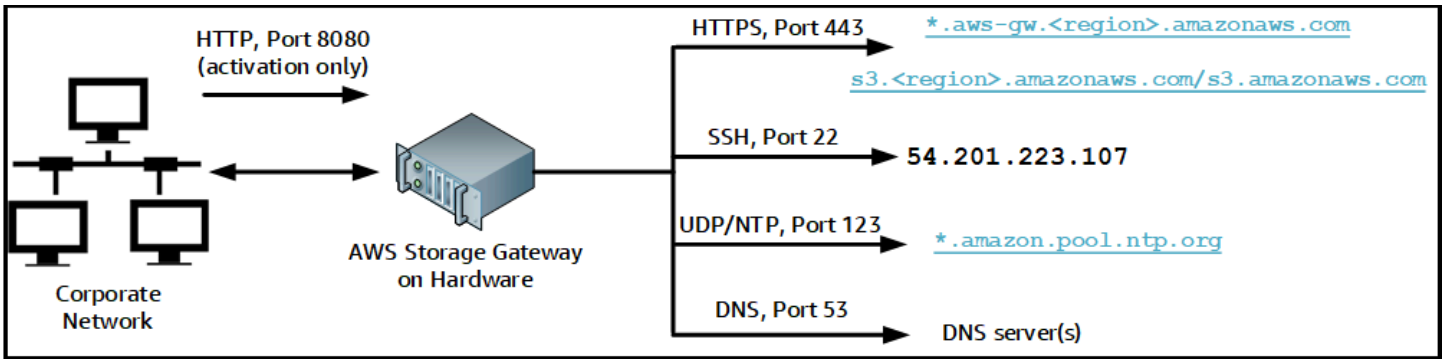
Cada Storage Gateway Hardware Appliance requer os seguintes serviços de rede:

- Acesso à Internet— uma rede sempre disponível de conexão 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.

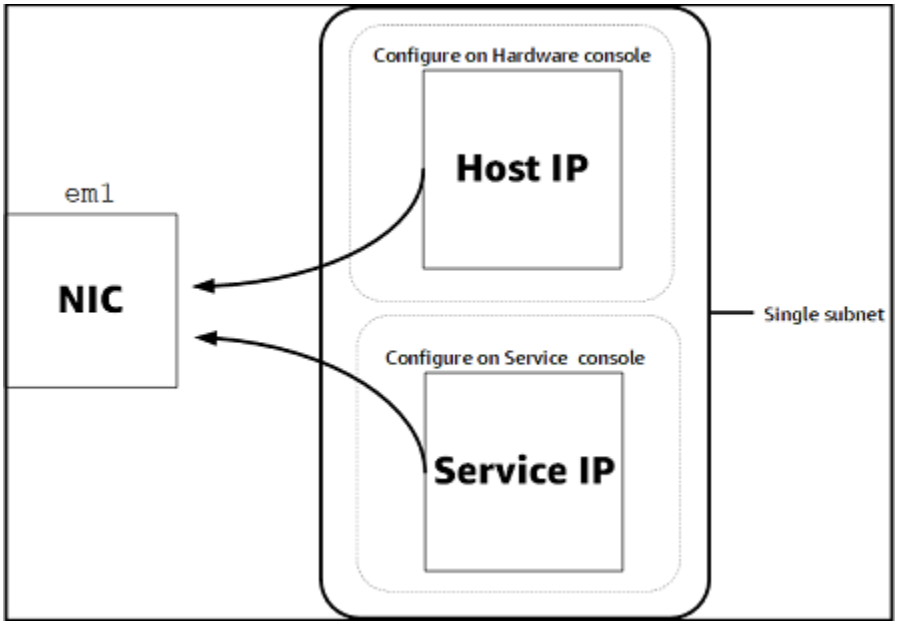
Protocolo	Port	Direção	Origem	Destination (Destino)	Como usar
SSH	22	Saída	Equipamento de hardware	`54.201.223.107`	Canal de suporte
DNS	53	Saída	Equipamento de hardware	Servidores DNS	Resolução de nome
UDP/NTP	123	Saída	Equipamento de hardware	`*.amazon.pool.ntp.org`	Sincronização de horário
HTTPS	443	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 restringir o tráfego de rede, deverá configurar o firewall e o roteador para permitir comunicação externa desses endpoints de serviço para comunicação externaAWS.

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

Veja a seguir o endpoint de serviço requerido 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) (`us-west-2`).

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

Veja a seguir o endpoint do Amazon CloudFront a seguir é 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 do Amazon EC2

DentroAWS Storage Gateway, um security group controla o tráfego para sua instância de gateway do Amazon EC2. Ao configurar um grupo de segurança, recomendamos o seguinte:

- O security group não deve permitir conexões de entrada da Internet externa. Ele deve permitir que apenas instâncias dentro do security group do gateway comuniquem-se com o gateway.

  Se você precisar permitir que as instâncias conectem-se ao gateway de fora desse security group, é recomendável permitir conexões somente na porta 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 Suporte para finalidades de solução de problemas. Para obter mais informações, consulte Você querSuportepara ajudar a solucionar problemas do gateway EC2.

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 Kernel-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 — 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 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.
- Servidor de Terminal do Windows 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 SMB pode gravar, ler, excluir e truncar arquivos. Quando os clientes enviam gravações ao Storage Gateway, ele grava no cache local de maneira síncrona Em seguida, ele grava no Amazon FSx 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 Amazon FSx como cache de leitura.

As gravações e leituras são otimizadas de modo que somente as partes alteradas ou solicitadas sejam transferidas pelo gateway. Exclui arquivos de remoção do Amazon FSx.

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 do Storage Gateway subjacente para simplificar as tarefas de programação. Para obter informações sobre como fazer download de bibliotecas de SDKs, consulte aAWSCentro de desenvolvedores.

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

Regiões do AWS com suporte

O Amazon FSx File Gateway armazena dados de arquivos naAWSRegião em que seu sistema de arquivos Amazon FSx está localizado. Antes de começar a implantar seu gateway, escolha uma região no canto superior direito do console do Storage Gateway.

- Amazon FSx File Gateway — Para suporteAWSRegiões e uma lista deAWSendpoints de serviço que você pode usar com o Amazon FSx File Gateway, consulteEndpoints e cotas do Amazon FSx File GatewaynoAWSReferência geral.
- 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 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 alta performance 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 o 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 do Storage Gateway emhttps://console.aws.amazon.com/storagegateway/homee escolha oAWSRegião na qual você deseja seu dispositivo.
2. SelecioneHardwareNo painel de navegação.
3. SelecioneEquipamento de pedidoe, 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 do 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 compatívelAWSRegiões, consulteRegiões do dispositivo de hardware do StoragenoAWSReferência 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 arquivo ou de fita 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 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 em seu dispositivo de hardware. Para obter mais informações, consulte Configuração de seu gateway.

   Você configura os gateways 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, aumente 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 as 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 do

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 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 paraAWSQue você 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 hardware aoAWS.

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 obter uma lista de compatíveisAWSRegiões, consulteRegiões do dispositivo de hardware do StoragenoAWSReferência 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 umAWSRegião, você verá 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 hardwareSeção, 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 de 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 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 sucesso, 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 de seu gateway

Configuração de seu 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 para seu tipo de gateway. Para obter instruções, consulte Configurar o Amazon FSx 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.

Excluir seu dispositivo de hardware

Depois de ativar o equipamento de hardware em seuAWSConta, talvez você precise movê-lo e ativá-lo 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 seu 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.

   Quando você excluir o dispositivo de hardware, todos os recursos associados ao gateway que está instalado no dispositivo também serão excluídos, 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, verifique se a configuração atende aos pré-requisitos necessários e outros requisitos descritos noConfiguração do Amazon FSx File Gateway.

Tópicos

Etapa 1: Criar um sistema de arquivos do Amazon FSx for Windows File Server

Para criar um Amazon FSx File Gateway noAWS Storage Gateway, o primeiro passo é criar um sistema de arquivos do Amazon FSx for Windows File Server. Se você já criou um sistema de arquivos do Amazon FSx, vá para a próxima etapa,Etapa 2: (Opcional) Criar um Amazon VPC endpoint.

> **Note**
>
> As seguintes limitações se aplicam ao gravar em um sistema de arquivos Amazon FSx a partir de um FSx File Gateway:
>
> - Seu sistema de arquivos Amazon FSx e seu FSx File Gateway devem ser de propriedade do mesmoAWSconta e localizada na mesmaAWSRegião :
> - Cada gateway pode suportar cinco sistemas de arquivos conectados. Ao anexar um sistema de arquivos, o console do Storage Gateway o notifica se o gateway selecionado estiver na capacidade. Nesse caso, você deve escolher um gateway diferente ou desanexar um sistema de arquivos antes de anexar outro.
> - O FSx File Gateway oferece suporte a cotas de armazenamento flexível (emitindo avisos quando os usuários ultrapassam seus limites de dados), mas não suporta cotas rígidas (impondo limites de dados negando acesso de gravação). As cotas flexíveis são suportadas para todos os usuários, exceto o usuário administrador do Amazon FSx. Para

obter mais informações sobre a configuração de cotas de armazenamento, consulteCotas de armazenamentonoGuia do Usuário do Amazon FSx for Windows File Server.

Para criar um sistema de arquivos do FSx for Windows File Server

1. Abrir oAWS Management Consoleemhttps://console.aws.amazon.com/fsx/home/e selecione a região na qual deseja criar seu gateway.
2. Siga as instruções emConceitos básicos do Amazon FSxnoGuia do Usuário do Amazon FSx for Windows File Server.

Etapa 2: (Opcional) Criar um Amazon VPC endpoint

Esta etapa não é necessária quando você está criando um Amazon FSx File Gateway noAWS Storage Gateway. No entanto, recomendamos que você crie um endpoint Virtual Private Cloud (VPC) para Storage Gateway e ative o gateway na VPC. Isso cria uma conexão privada entre a VPC e o Storage Gateway.

Se você já tiver um VPC endpoint para Storage Gateway, pode usá-lo para o FSx File Gateway. Um único endpoint de VPC que pode suportar vários gateways permite que os gateways implantados em sua VPC se conectem à VPC do serviço Storage Gateway. Se você já criou um VPC endpoint para Storage Gateway, vá para a próxima etapa,Etapa 3: Criar e ativar um Amazon FSx File Gateway.

Para criar um Amazon VPC endpoint

1. Abrir oAWS Management Consoleemhttps://console.aws.amazon.com/vpc/home/, e escolha oAWSRegião na qual você deseja criar seu gateway.
2. No painel de navegação à esquerda, escolhaEndpoints doe, depois, escolhaCriar endpoint.
3. NoCriar endpoint, escolhaAWSserviçospeloCategoria de serviço.
4. para oService name (Nome do serviço), procure por`storagegateway`. A Região assumirá como padrão a Região na qual você está conectado — por exemplo,`com.amazonaws.`*`region`*`.storagegateway`. Então, se você estiver conectado ao Leste dos EUA (Ohio), verá`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 oGrupo de segurança, crie um novo security group para usar com sua VPC. Certifique-se de que todas as portas TCP a seguir sejam permitidas no seu grupo de segurança:

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

   > **Note**
   >
   > O gateway usa essas portas para se comunicar de volta ao serviço gerenciado Storage Gateway. Quando você estiver usando um endpoint de VPC, as seguintes portas devem estar abertas para acesso de entrada a partir do endereço IP do gateway.

8. Escolha Create endpoint (Criar endpoint). O estado inicial do endpoint éPendente. Quando o endpoint for criado, anote o ID do VPC endpoint que você acabou de criar.

   > **Note**
   >
   > Recomendamos que você forneça um nome para este endpoint da VPC, por exemplo,**`StorageGatewayEndpoint`**.

9. Quando o endpoint estiver criado, escolhaEndpoints doe, em seguida, escolha o novoVPC endpoint.
10. NoNomes de DNSSeção, use o primeiro nome DNS (Domain Name System) que não especifica uma zona de disponibilidade. Seu nome DNS deve ser semelhante ao seguinte:

    ```
    vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
    east-1.vpce.amazonaws.com
    ```

    > **Note**
    >
    > Esse nome DNS será resolvido para os endereços IP privados de endpoint do Storage Gateway alocados em sua VPC.

11. Revise a lista de portas que devem ser abertas no firewall.

Agora que criou um VPC endpoint, crie seu FSx File Gateway.

Próxima etapa

the section called “Etapa 3: Criar e ativar um gateway FSx File Gateway”

Etapa 3: Criar e ativar um Amazon FSx File Gateway

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

Tópicos

- Configurar um Amazon FSx File Gateway
- Connect seu Amazon FSx File Gateway aoAWS
- Revise as configurações e ative o Amazon FSx File Gateway
- Configurar o Amazon FSx File Gateway

Configurar um Amazon FSx File Gateway

Para configurar um novo FSx File Gateway

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 FSx.
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 deAWSPara 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 escolhida. 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 FSx File Gateway aoAWS

Para conectar um novo FSx File Gateway aoAWS

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

   - Publicly accessible— Seu gateway se comunica comAWSNa internet pública. Se selecionar esta opção, use oEndpoint 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 acessar oAWSPor 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 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 FSx File Gateway

Para ativar um novo FSx File Gateway

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

- Configurar um Amazon FSx File Gateway
- Connect seu Amazon FSx File Gateway aoAWS

Quando terminar, escolhaPróximopara abrir oAnalise e ativeA 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 FSx File Gateway

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

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

   - Configurar um Amazon FSx File Gateway
   - Connect seu Amazon FSx File Gateway aoAWS
   - Revise as configurações e ative o Amazon FSx File Gateway

   Quando terminar, escolhaPróximopara abrir oConfigurar gatewayA página noAWS Storage Gatewayconsole do .
2. NoConfigurar um 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 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 personalizado 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 noGateways doA página doAWS Storage Gatewayconsole do .

Agora que criou seu gateway, é necessário anexar um sistema de arquivos para que ele use. Para obter instruções, consulteAnexar um sistema de arquivos do Amazon FSx for Windows File Server.

Se você não tiver um sistema de arquivos do Amazon FSx existente para anexar, crie um. Para obter instruções, consulteConceitos básicos do Amazon FSx.

Faça as configurações do Active Directory

Nesta etapa, você define as configurações de acesso do Amazon FSx File Gateway no Storage Gateway para ingressar em um Microsoft Active Directory.

Para configurar as configurações do Active Directory

1. No console do Storage Gateway, escolhaAnexar sistema de arquivos FSx.
2. NoConfirmar gatewayNa lista de gateways, escolha o Amazon FSx File Gateway que você deseja usar.

   Se você não tiver um gateway, será necessário criar um. Verifique se o gateway pode resolver o nome do Controlador de Domínio Active Directory. Para obter mais informações, consulte Pré-requisitos necessários.
3. Insira os valores para oConfigurações do Active Directory:

   > **Note**
   >
   > Se seu gateway já estiver associado a um domínio, você não precisará ingressar novamente. Vá para o próximo passo.

   - para oNome de domínio, Insira o nome de domínio do Active Directory que você deseja usar.
   - para oUsuário de domínio, Insira um nome de usuário para o Active Directory.
   - para oSenha do domínio, Insira a senha do usuário do domínio.

     > **Note**
     >
     > Sua conta deve ser capaz de integrar um servidor a um domínio.

   - para oUnidade organizacional - opcional, você pode especificar uma unidade organizacional à qual o Active Directory pertence.
   - Insira um valor paraControlador (es) de domínio - opcional.
4. SelecionePróximopara abrir oAnexar o sistema de arquivos FSx.

Próxima etapa

Anexar um sistema de arquivos do Amazon FSx for Windows File Server

Anexar um sistema de arquivos do Amazon FSx for Windows File Server

O próximo passo é anexar um sistema de arquivos Amazon FSx ao gateway. Quando você anexa um sistema de arquivos Amazon FSx, todos os compartilhamentos de arquivos no sistema de arquivos são disponibilizados para o Amazon FSx File Gateway (FSx File) para você montar.

> **Note**
>
> As limitações a seguir se aplicam ao gravar em um sistema de arquivos do Amazon FSx a partir do Amazon FSx File Gateway:
>
> - Seu sistema de arquivos Amazon FSx e seu arquivo FSx devem ser de propriedade do mesmoConta da AWSe localizado no mesmoRegião da AWS.
> - Cada gateway pode oferecer suporte a até cinco sistemas de arquivos conectados. Quando você está anexando um sistema de arquivos, o console do Storage Gateway o notifica se o gateway selecionado está na capacidade. Nesse caso, você deve escolher um gateway diferente ou desanexar um sistema de arquivos antes de anexar outro.
> - O FSx File suporta cotas de armazenamento flexível (que avisam quando os usuários ultrapassam seus limites de dados), mas não suportam cotas rígidas (que impõem limites de dados negando acesso de gravação). As cotas flexíveis são suportadas para todos os usuários, exceto o usuário administrador do Amazon FSx. Para obter mais informações sobre a configuração de cotas de armazenamento, consulteCotas de armazenamentono Guia do usuário do Amazon FSx.

Para anexar um sistema de arquivos Amazon FSx

1. No console do Storage Gateway, noSistemas de arquivos FSx >Anexar sistema de arquivos do FSx, preencha os seguintes campos noConfigurações do sistema de arquivos do FSxseção :
   - para oNome do sistema de arquivos do FSx, escolha o sistema de arquivos que deseja anexar na lista suspensa.
   - para oEndereço IP do endpoint local, insira o endereço IP do gateway que os clientes usarão para procurar compartilhamentos de arquivos no sistema de arquivos FSx.

> **Note**
>
> - Se você planeja anexar apenas um sistema de arquivos ao gateway, poderá deixar esse campo em branco para disponibilizar compartilhamentos no sistema de arquivos em todos os endereços IP do gateway. Se você planeja anexar vários sistemas de arquivos, é necessário especificar um endereço IP para cada um deles.
> - Se você anexar um sistema de arquivos sem um endereço IP e precisar anexar outro sistema de arquivos posteriormente, será necessário desanexar o primeiro sistema de arquivos e reanexá-lo com um endereço IP.
> - Para gateways do Amazon EC2, você pode especificar o endereço IP privado da instância do EC2, a menos que ele já esteja em uso por um sistema de arquivos diferente. Nesse caso, você deve adicionar um novo endereço privado ao gateway e, em seguida, reiniciá-lo. Para obter mais informações, consulteVários endereços IPnoGuia do usuário do Amazon EC2.
> - Para gateways locais, você pode especificar o endereço IP da interface de rede primária (estática ou DHCP), a menos que já esteja em uso por um sistema de arquivos diferente. Nesse caso, você deve fornecer um endereço IP diferente da mesma sub-rede que a interface principal, que será disponibilizada como um IP virtual. Não use um endereço IP atribuído a nenhuma interface de rede que não seja a principal.

2. NoConfigurações da conta de serviço, informe o nome de usuário e a senha associados ao sistema de arquivos do Amazon FSx.

> **Note**
>
> Esse usuário deve ser membro do grupo Operadores de Backup do serviço Active Directory associado aos seus sistemas de arquivos Amazon FSx ou ter permissões equivalentes.

> **Important**
>
> Para garantir permissões suficientes a arquivos, pastas e metadados de arquivos, recomendamos tornar esse usuário um membro do grupo de administradores do sistema de arquivos.

Se você estiver usandoAWS Directory ServiceNo Microsoft Active Directory com Amazon FSx for Windows File Server, o usuário deve ser um membro doAWSGrupo de Administradores delegados de FSx do.
Se você estiver usando um Active Directory autogerenciado com o Amazon FSx for Windows File Server, o usuário deverá ser membro de um dos dois grupos: os administradores de domínio ou o grupo de administradores de sistema de arquivos delegados personalizados que você especificou para a administração do sistema de arquivos quando você criou o sistema de arquivos.
Para obter mais informações, consulteDelegando privilégios à sua conta de serviço Amazon FSxnoGuia do usuário do Amazon FSx for Windows File Server.

3. NoRegistros de auditoriaSeção, escolhaGrupos de logs existentese escolha o log que você deseja usar para monitorar o acesso ao seu sistema de arquivos Amazon FSx. Você pode criar um novo. Se você não quiser monitorar o sistema, escolhaDisable logging (Desativar o registro em log)..
4. para oConfiguração de atualização de cache automatizada, se você quiser que seu cache seja atualizado automaticamente, escolhaDefinir intervalo de atualizaçãoe especifique um intervalo entre 5 minutos e 30 dias.
5. (Opcional) NoTagsSeção, escolhaAdicionar nova tagpara adicionar uma ou mais chaves e um valor para marcar suas configurações.
6. SelecionePróximoe revise as configurações. Para alterar as configurações, você pode escolherEditeEm cada seção.
7. Quando terminar, escolha Concluir.

Próxima etapa

Monte e use seu compartilhamento de arquivos

Monte e use seu compartilhamento de arquivos

Antes de montar o compartilhamento de arquivos no cliente, aguarde que o status do sistema de arquivos Amazon FSx mude paraDisponível. Depois que o compartilhamento de arquivos for montado, você poderá começar a usar o Amazon FSx File Gateway (FSx File).

Tópicos

Monte seu compartilhamento de arquivos SMB no seu cliente

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

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

- O`net use`command — Não é preservado em reinicializações do sistema, a menos que você use o`/persistent:(yes:no)`Alternância.
- O`cmdkey`Utilitário de linha de comando — Cria uma conexão persistente para um compartilhamento de arquivos SMB montado que permanece após uma reinicialização.
- Uma unidade de rede mapeada no File Explorer — Configura o compartilhamento de arquivos montados no login de reconexão e para exigir que você insira suas credenciais de rede.
- Script do PowerShell — Pode ser persistente e pode ser visível ou invisível para o sistema operacional enquanto montado.

> **Note**
>
> Se você for um usuário do Microsoft Active Directory, verifique com o administrador para garantir que você tenha acesso ao compartilhamento de arquivos SMB antes de montá-lo no seu sistema local.
> O Amazon FSx File Gateway não suporta bloqueio SMB ou atributos estendidos SMB.

Para montar um compartilhamento de arquivos SMB para usuários do Active Directory usando o comando de uso de rede

1. Certifique-se de que você tem acesso ao compartilhamento de arquivos SMB antes de montar o compartilhamento de arquivos no seu sistema local.
2. Para clientes do Microsoft Active Directory, digite o seguinte comando no prompt de comando:

   ```
   net use [WindowsDriveLetter]: \\[Gateway IP Address]\[Name of the share on the FSx file system]
   ```

Para montar um compartilhamento de arquivos SMB no Windows usando CmdKey

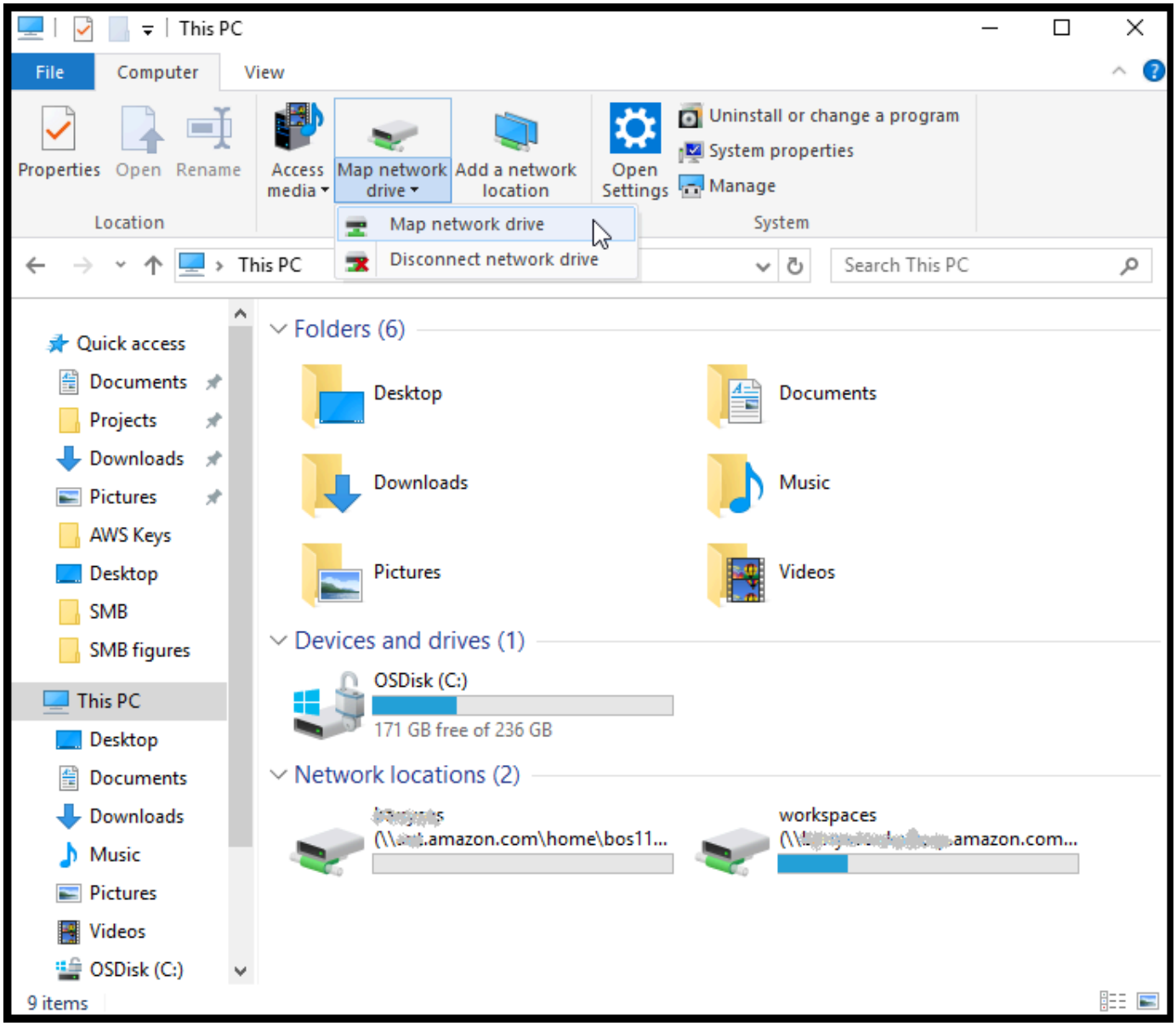
1. Pressione a tecla Windows e digite**cmd**Para visualizar o item de menu de prompt de comando.
2. Abra o menu de contexto (clique com o botão direito do mousePrompt de comandoe escolhaExecutar como administrador.
3. Digite o comando

   ```
   C:\>cmdkey /add:[Gateway VM IP address] /user:[DomainName]\[UserName] /pass:[Password]
   ```

> **Note**
>
> Ao montar compartilhamentos de arquivos, talvez seja necessário montar novamente o compartilhamento de arquivos após reinicializar seu cliente.

Para montar um compartilhamento de arquivos SMB usando Windows File Explorer

1. Pressione a tecla Windows e digite**File Explorer**noJanelas de pesquisacaixa ou pressione**Win+E**.
2. No painel de navegação, selecioneEste PC.
3. NoComputer, escolhaUnidade de rede de mapase, depois, escolhaUnidade de rede de mapasNovamente, como mostrado na captura de tela a seguir.



4. NoUnidade de rede de mapas, escolha uma letra de unidade paraDrive.
5. para oPasta, insira***[File Gateway IP]**[SMB File Share Name]***, ou escolhaNavegarPara selecionar o compartilhamento de arquivos SMB na caixa de diálogo.
6. (Opcional) Selecione Reconectar ao entrar se quiser que seu ponto de montagem persista após reinicializações.
7. (Opcional) Selecione Connect using different credentials (Conectar usando credenciais diferentes) se você deseja que um usuário insira o logon do Active Directory ou uma conta de usuário e senha de convidado.
8. Escolha Finalizar para concluir o ponto de montagem.

Teste seu arquivo FSx

Você pode copiar arquivos e diretórios para sua unidade mapeada. Os arquivos são carregados automaticamente para o sistema de arquivos FSx for Windows File Server.

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

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 nome do seu sistema de arquivos.
2. Copie arquivos ou um diretório para a unidade.

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

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 na sua 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, selecioneAWSServiçospeloCategoria 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 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 seus recursos do Amazon FSx File Gateway

As seções a seguir fornecem informações sobre como gerenciar seus recursos do Amazon FSx File Gateway (FSx File), incluindo anexar e desanexar sistemas de arquivos do Amazon FSx e definir configurações do Microsoft Active Directory.

Tópicos

Anexar um sistema de arquivos do Amazon FSx

É necessário ter um sistema de arquivos do Windows File Server para anexá-lo a um sistema de arquivos do FSx for Windows File Server. Se não tiver um sistema de arquivos, você deverá criar um. Para obter instruções, consulteEtapa 1: Criar seu sistema de arquivosnoGuia do usuário do Amazon FSx for Windows File Server.

O próximo passo é ativar um Arquivo FSx e configurar seu gateway para ingressar em um domínio do Active Directory. Para obter instruções, consulte Faça as configurações do Active Directory.

> **Note**
>
> Quando o gateway ingressou em um domínio, você não precisa configurá-lo para ingressar no domínio novamente.

Cada gateway pode oferecer suporte a até cinco sistemas de arquivos conectados. Para obter instruções sobre como anexar um sistema de arquivos, consulteAnexar um sistema de arquivos do Amazon FSx for Windows File Server.

Configurando o Active Directory para seu arquivo FSx

Para usar o Arquivo FSx, você precisa configurar seu gateway para ingressar em um domínio do Active Directory. Para obter instruções, consulte Faça as configurações do Active Directory.

Definir configurações do Active Directory

Depois de configurar o gateway para ingressar em um domínio do Active Directory, você poderá editar as configurações do Active Directory.

Para editar as configurações do Active Directory

1. Abra o console do Storage Gateway emhttps://console.aws.amazon.com/storagegateway/home.
2. No painel de navegação, selecioneGateways doEm seguida, escolha o gateway cujas configurações do Active Directory você deseja editar.
3. para oAções, escolhaEditar configurações SMBE, depois, escolhaConfigurações do Active Directory.
4. Forneça as informações solicitadas na seção Active Directory settings (configurações do Active Directory) e escolhaSalve as alterações.

Editando as configurações do arquivo FSx

Depois que o gateway for ativado, você poderá editar as configurações do gateway.

Para editar as configurações do gateway

1. Abra o console do Storage Gateway emhttps://console.aws.amazon.com/storagegateway/home.
2. No painel de navegação, selecioneGateways doEm seguida, escolha o gateway cujas configurações você deseja editar.
3. para oAções, escolhaEditar informações do gateway.
4. para oNome do gateway, edite o nome do gateway selecionado.
5. para oFuso horário do gateway, escolha um fuso horário.
6. para oGrupo de logs de integridade do gateway, escolha uma das opções para monitorar seu gateway usando grupos de log do Amazon CloudWatch.

   Se escolherUsar um grupo de logs existenteEscolha um grupo de logs noLista de grupos de logs existentesE, depois, escolhaSalve as alterações.

Edição das configurações do sistema de arquivos do Amazon FSx for Windows File Server

Depois de criar um sistema de arquivos do Amazon FSx for Windows File Server, você pode editar as configurações do sistema de arquivos.

Para editar as configurações do sistema de arquivos Amazon FSx

1. Abra o console do Storage Gateway emhttps://console.aws.amazon.com/storagegateway/home.
2. No painel de navegação, selecioneSistema de arquivosEscolha o sistema de arquivos cujas configurações você deseja editar.
3. para oAções, escolhaEditar configurações do sistema de arquivos.
4. Na seção de configurações do sistema de arquivos, verifique o gateway, a localização do Amazon FSx e as informações de endereço IP.

   > **Note**
   >
   > Você não pode editar o endereço IP de um sistema de arquivos depois que ele for anexado a um gateway. Para alterar o endereço IP, você deve desanexar e reconectar o sistema de arquivos.

5. NoLogs de auditoria, escolha uma opção para usar grupos de log do CloudWatch para monitorar o acesso aos sistemas de arquivos Amazon FSx. É possível usar um grupo de logs existente.
6. para oConfigurações automatizadas de atualização de cacheEscolha uma opção. Se escolherDefinir intervalo de atualização, defina a hora em dias, horas e minutos para atualizar o cache do sistema de arquivos usando Time To Live (TTL).

   TTL é o período de tempo desde a última atualização. Quando o diretório é acessado após esse período de tempo, o gateway de arquivos atualiza o conteúdo desse diretório a partir do sistema de arquivos Amazon FSx.

   > **Note**
   >
   > Os valores de intervalo de atualização válidos estão entre 5 minutos e 30 dias.

7. NoConfigurações da conta de serviço - opcionalSeção, insira um nome de usuário e umPassword. Essas credenciais são para um usuário que tem a função Administrador de Backup do serviço Active Directory associado aos seus sistemas de arquivos Amazon FSx.
8. Escolha Save changes (Salvar alterações).

Desanexar um sistema de arquivos do Amazon FSx

A desanexação de um sistema de arquivos não exclui seus dados no FSx for Windows File Server. Os dados gravados nos compartilhamentos de arquivos nesses sistemas de arquivos antes de excluir o sistema de arquivos ainda serão carregados para o FSx for Windows File Server.

Para desanexar um sistema de arquivos Amazon FSx

1. Abra o console do Storage Gateway emhttps://console.aws.amazon.com/storagegateway/home.
2. No painel de navegação à esquerda, selecioneSistema de arquivosEm seguida, escolha o sistema de arquivos que você deseja desanexar. Você pode excluir vários sistemas de arquivos.
3. para oAções, escolhaDesanexar sistema de arquivos.
4. Digite**`detach`**na caixa para confirmar e escolherDesconectar.

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 sistema de arquivos do Amazon FSx. É possível configurar o grupo quando estiver ativando o gateway ou depois que o gateway estiver ativado e em execução. Para obter informações sobre como configurar um grupo de logs do CloudWatch ao ativar um gateway, consulteConfigurar o Amazon FSx 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.

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, selecione, selecione oGateways 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 do. Ou, noDetalhesguia, emRegistros de HealtheNão foi habilitado, escolhaConfigurar grupo de logspara abrir oEditeCustomerGateWayNameCaixa de diálogo.
4. para oGrupo de logs de integridade do gateway, escolha uma das seguinte 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.

- Use 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 visualizar os logs de integridade do seu gateway, faça o seguinte:

   1. No painel de navegação, selecione, selecione oGateways 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 do. Ou, noDetalhesguia, ao lado deRegistro em log, emNão foi habilitado, escolhaConfigurar grupo de logspara abrir oEdição das informações do gateway doCaixa de diálogo.
4. para oGrupo de logs de gateway do, escolhaUse um grupo de logs existenteE 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 você 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, em seguida, escolha oDetalhesGuia.

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

Usar métricas do Amazon CloudWatch

Você pode 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 que você usar para trabalhar com métricas, deverá especificar as seguintes informações:

- A dimensão da métrica com a qual trabalhará. Uma dimensão é um par nome/valor, que ajuda a identificar com exclusividade uma métrica. As dimensões do Storage Gateway 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

Noções básicas de métricas de gateway

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

Você sempre deve especificar se deseja trabalhar com um gateway ou um sistema de arquivos ao trabalhar com uma métrica específica. Especificamente, ao trabalhar com métricas do gateway, você deve especificar o`Gateway  Name`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 FSxs.

Métrica	Descrição
`AvailabilityNotifications`	Essa métrica relata o número de notificações de integridade relacionadas à disponibilidade geradas pelo gateway no período do relatório. Unidades: Contagem
`CacheDirectorySize`	Essa métrica controla o tamanho das pastas no cache do gateway. O tamanho da pasta é determinado pelo número de arquivos e subpastas em seu primeiro nível, isso não conta recursivamente em subpastas.

Métrica	Descrição
	Use essa métrica com o`Average`estatística para medir o tamanho médio de uma pasta no cache do gateway. Use essa métrica com o`Max`estatística para medir o tamanho máximo de uma pasta no cache do gateway. Unidades: Contagem
`CacheFileSize`	Essa métrica controla o tamanho dos arquivos no cache do gateway. 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 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

Métrica	Descrição
`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
`CacheUsed`	Essa métrica informa o 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/s aída por segundo (IOPS). Unidades: Bytes
`CloudBytesUploaded`	O número total de bytes que o gateway baixou doAWSdurante 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

Métrica	Descrição
`FilesFailingUpload`	Essa métrica rastreia o número de arquivos que não são carregados noAWS. Esses arquivos gerarão notificações de integrida de 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
`FileShares`	Essa métrica informa o o número de compartil hamentos de arquivos no gateway. Unidades: Contagem
`FileSystem-ERROR`	Essa métrica fornece o número de associações de sistemas de arquivos nesses gateways que estão no estado ERROR. Se essa métrica relatar que alguma associaçã o de sistema de arquivos está no estado ERROR, 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
`HealthNotifications`	Essa métrica relata o número de notificações de integridade geradas por esse gateway no período do relatório. Unidades: Contagem

Métrica	Descrição
IoWaitPercent	Essa métrica relata o percentual de tempo em 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
MemUsedBytes	Essa métrica relata a quantidade de memória usada no gateway. Unidades: Bytes
RootDiskFreeBytes	Essa métrica informa o 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
SmbV2Sessions	Essa métrica informa o o número de sessões do SMBv2 que estão ativas no gateway. Unidades: Contagem
SmbV3Sessions	Essa métrica informa o o número de sessões do SMBv3 que estão ativas no gateway. Unidades: Contagem
TotalCacheSize	Essa métrica informa o tamanho total do cache. Unidades: Bytes

Métrica	Descrição
`UserCpuPercent`	Essa métrica relata a porcentagem de tempo gasto no processamento do gateway. Unidades: Percentual

Compreendendo métricas do sistema 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

Métrica	Descrição
`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 cache do gateway de armazenamento. 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
`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

Métrica	Descrição
`CloudBytesDownloaded`	O número total de bytes que o gateway baixou doAWSdurante 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 FSx File Gateway (FSx File Gateway) fornecem detalhes sobre o acesso do usuário a arquivos e pastas em uma associação de sistemas de arquivos. É possível usar logs de auditoria para monitorar as atividades do usuário e tomar medidas se forem identificados padrões de atividade inadequados. Os logs são formatados de forma semelhante aos eventos de

log de segurança do Windows Server, para oferecer suporte à compatibilidade com ferramentas de processamento de log existentes para eventos de segurança do Windows.

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 os atributos de acesso ao arquivo de log de auditoria do FSx File Gateway.

Atributo	Definição
`securityDescriptor`	Mostra a lista de controle de acesso discricio nário (DACL) definida em um objeto, no formato SDDL.
`sourceAddress`	O endereço IP da máquina cliente de compartil hamento de arquivos.
`SubjectDomainName`	O domínio do Active Directory (AD) ao qual pertence a conta do cliente.

Atributo	Definição
`SubjectUserName`	O nome de usuário do Active Directory do cliente.
`source`	O ID do Storage Gateway`FileSyste mAssociation` que está sendo auditado.
`mtime`	A hora em que o conteúdo do objeto foi modificado, definida pelo cliente.
`version`	A versão do formato do log de auditoria.
`ObjectType`	Define se o objeto é um arquivo ou uma pasta.
`locationDnsName`	O nome DNS do sistema FSx File Gateway.
`objectName`	O caminho completo para o objeto.
`ctime`	A hora em que o conteúdo ou os metadados do objeto foram modificados, definida pelo cliente.
`shareName`	O nome do compartilhamento que está sendo acessado.
`operation`	O nome da operação de acesso ao objeto.
`newObjectName`	O caminho completo para o novo objeto depois que ele foi renomeado.
`gateway`	O ID do Storage Gateway.
`status`	O status da operação. Somente o êxito é registrado (as falhas são registradas, com a exceção das falhas decorrentes de permissões negadas).
`fileSizeInBytes`	O tamanho do arquivo em bytes, definido pelo cliente no momento da criação do arquivo.

Atributos registrados por operação

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

	Ler dados	Gravar dados	Criar pasta	Criar arquivo	Renomea arquivo/ pasta	Excluir arquivo/ pasta	Atributos de gravação (alterar ACL)	Atributos de gravação (chown)	Atributos de gravação (chmod)	Atributos de gravação (chgrp)
securi escrip							X			
source ress	X	X	X	X	X	X	X	X	X	X
Subjec mainNa	X	X	X	X	X	X	X	X	X	X
Subjec erName	X	X	X	X	X	X	X	X	X	X
source	X	X	X	X	X	X	X	X	X	X
mtime			X	X						
versio	X	X	X	X	X	X	X	X	X	X
object e	X	X	X	X	X	X	X	X	X	X
locati nsName	X	X	X	X	X	X	X	X	X	X
object e	X	X	X	X	X	X	X	X	X	X
ctime			X	X						

	Ler dados	Gravar dados	Criar pasta	Criar arquivo	Renomea arquivo/ pasta	Excluir arquivo/ pasta	Atributos de gravação (alterar ACL)	Atributos de gravação (chown)	Atributos de gravação (chmod)	Atributos de gravação (chgrp)
shareN	X	X	X	X	X	X	X	X	X	X
operat	X	X	X	X	X	X	X	X	X	X
newObj Name					X					
gatewa	X	X	X	X	X	X	X	X	X	X
status	X	X	X	X	X	X	X	X	X	X
fileSi nBytes				X						

Como manter seu gateway

A manutenção de seu gateway inclui tarefas como configuração de armazenamento em cache e espaço do buffer de upload e manutenção geral do desempenho de seu gateway. Essas tarefas são comuns a todos os tipos de gateway.

Tópicos

Desligar a VM do 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 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 sistema de arquivos pendente para o Amazon S3 ou o 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. Um 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 o armazenamento em cache.

Determinando o tamanho do armazenamento em cache a ser alocado

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 ao gateway sem interromper as atividades 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 eles 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 para o gateway.

Para adicionar e configurar ou armazenar 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 do 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.

O FSx File Gateway não suporta armazenamento efêmero.

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 com uma mensagem no console do Storage Gateway e noAWS 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 sua conexão de gateway FSx File Gateway com endpoints de 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 do 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. Após fazer isso, o Storage Gateway roteia todos osAWSO 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	

Para	Faça o seguinte
	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.

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 inicialme nte 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 sua conexão de gateway FSx File Gateway com endpoints de gateway

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

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. O 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. O Storage Gateway exibe uma mensagem que descreve os resultados da verificação de recursos.

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

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. 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

Para	Faça o seguinte
	hipervisor e o gateway não recebem atualizaç ões de horário. Neste caso, o horário da VM do gateway será diferente do horário real. Quando há um desvio de horário, ocorre uma discrepân cia 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 hiperviso r 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 informaçõ es, 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.
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 no 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

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 sua conexão de gateway FSx File Gateway com endpoints de 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

Você pode se conectar à sua Instância do Amazon EC2 usando um cliente Secure Shell (SSH). Para obter informações detalhadas, consulteConecte-se à sua instâncianoGuia 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 EC2noGuia 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 - ConfiguraçãoMenu principal, como mostrado na seguinte captura de tela.

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
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. Após fazer isso, o Storage Gateway roteia todos osAWSO 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**. 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**. 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 selecionarTestar a conectividade de rede.

   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. O 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. O Storage Gateway exibe uma mensagem que descreve os resultados da verificação de recursos.

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

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
- Acesso ao console local do gateway com o VMware ESXi
- Acessar o console local do gateway com o Microsoft Hyper-V

Acessar o console local do gateway com o Linux KVM

Existem diferentes maneiras de configurar máquinas virtuais em execução na KVM, dependendo da distribuição do Linux que estiver sendo usada. Siga as instruções para acessar as opções de configuração da KVM na linha de comando. As instruções podem variar dependendo da sua implementação da KVM.

Como acessar o console local do gateway com a KVM

1. Use o comando a seguir para listar as VMs que estão atualmente disponíveis na KVM.

   ```
   # virsh list
   ```

   É possível escolher VMs disponíveis por `Id`.

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

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 escolha 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 do 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 oAWSIsso ajuda a evitar despesas de uso não intencionais.

Como remover recursos de 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 anexados à instância, se tiver objetivo de usá-los novamente. Para obter mais informações, consulteLimpar a instância e o volumenoGuia do usuário do Amazon EC2 para instâncias do Linux.

Performance

Nesta seção, você encontra informações sobre o desempenho do Storage Gateway.

Tópicos

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 adicionais 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 suporta o 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 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: 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 da 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 disso muitas vezes dentro da janela de tempo 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 Gateway, consulteAWSServiços do 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 Storage Gateway ou outroAWSserviços usando o console, a API,AWS CLI, ouAWSSDKs do. 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 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 ServiceChaves mestras de cliente (CMKs) (SSE-KMS).

> **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 do Storage Gateway para criptografar dados gravados em um compartilhamento de arquivos, consulte.CreateNFSFileSharenoAWS Storage GatewayReferência de API do.

Criptografar um sistema de arquivos

Para obter mais informações, consulte,Criptografia 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, consulteUso de 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 para 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 seções a seguir 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 solicitações. No entanto, a menos que tenha permissões, você não pode 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
- Como especificar elementos de política do: Ações, efeitos, recursos e diretores principais
- Especificar condições em uma política

Recursos e operações do Storage Gateway

No Storage Gateway, o recurso principal é umGateway do. O Storage Gateway também oferece suporte para os seguintes tipos de recursos adicionais: 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 do sistema de arquivos	`arn:aws:fsx:` *`region`*`:`*`account-id`* `:file-system/` *`filesystem-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 ver uma tabela com todas as ações de API do Storage Gateway e os recursos aos quais elas se aplicam, consulte.Permissões 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 do 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, esse 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 em sua conta da Amazon Web Services com permissões para ativar um gateway, qualquer pessoa que puder assumir a 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 IAM é onoGuia do usuário do IAM.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 da— 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 políticas baseadas em identidade com o Storage Gateway, consulte.Usar 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.

Como especificar elementos de política do: Ações, efeitos, recursos e diretores 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 declaração permite `questoragegateway:ActivateGatewaystoragegateway:ListGatewaysações` em qualquer gateway. O caractere curinga é usado aqui porque não é possível saber qual é 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**
  >
  > ARNs identificam exclusivamente oAWSrecursos 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) exigem 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 API 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 aos quais elas se aplicam, consultePermissões 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 peloAWS. 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 sobreAWSPolíticas gerenciadas do, consulteAWSpolíticas gerenciadas pelanoIAM User Guide.

Os seguintes exemplos deAWSAs políticas gerenciadas pela, que podem ser anexadas 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
- Exemplo 2: Permitir acesso somente leitura a um gateway
- Exemplo 3: Permitir acesso a um gateway específico
- Exemplo 4: Permitir que um usuário acesse um volume específico
- Exemplo 5: Permitir todas as ações em gateways com um prefixo específico

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 API 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`Ação do Amazon EC2, que é essencial 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, é preciso conceder permissões adicionais, conforme descrito emExemplo 3: Permitir acesso a um gateway específico.

Usar tags para controlar o acesso ao 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**`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"
            }
         }
      }
   ]
}
```

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 lista 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 usar oAWSAs chaves de condição em toda a nas 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 cada 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, consulte.Recursos 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 outroAWSServiços 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 uma 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 às funções vinculadas a serviços, o Storage Gateway criou a função AWSServiceRoleForStorageGateway em 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 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 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 para 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, haverá falha na operação de exclusão.

> **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 do 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 ao 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 usando funções vinculadas a serviços em todas as regiões em que o serviço está disponível. Você pode usar a função AWSServiceRoleForStorageGateWay nas seguintes regiões.

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
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

Nome da região	Identidade da região	Support no Storage Gateway
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, função ou umAWSserviço no Storage Gateway. O CloudTrail captura todas as chamadas de API para 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 para 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 ao Storage Gateway, o endereço IP do qual a solicitação foi feita, quem a fez e quando ela foi feita, além de 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 emHistórico 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 do arquivo 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 terceirizados avaliam a segurança e a conformidade doAWSStorage Gateway como parte de váriosAWSProgramas de conformidade. Eles incluem SOC, PCI, ISO, FedRAMP, HIPAA, HIPAA, MTCS, C5, K-ISMS, 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 doAWSA 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 o 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 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 de gateway de arquivos do Amazon S3. 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 de 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 habilitarSuportePara ajudar a solucionar problemas do gateway do.

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.

Problema	Medida a ser tomada
	• 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 roteador 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.

Problema	Medida a ser tomada
A ativação do gateway falha quando você clica noProssiga para a 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 sua conexão de gateway FSx File Gateway com endpoints de 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 ação de horário de hosts e VMs de hipervisor, consulte Configura r 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 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 de.
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 e oAWS. 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 o 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 GatewayGatewayA guia deve corresponder aos endereços IP de seu gateway, que determina dos 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 sua conexão de gateway FSx File Gateway com endpoints de 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.
	
	Você pode 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.

Problema	Medida a ser tomada
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.
Você recebe uma mensagem que diz: “Os dados que foram gravados no volume do seu gateway não estão 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 contatoSuporte.

HabilitarSuportepara 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 ativação doSuportePara acessar o gateway para ajudá-lo a solucionar problemas de gateway. Por padrão,SuporteO acesso ao seu gateway está desativado. Esse acesso é ativado por meio do console local do host. Para darSuportePara acessar o gateway, primeiro faça login no console local do host, navegue até o console do gateway de armazenamento e conecte-se ao servidor de suporte.

Para habilitar oSuporteAcesso 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 oSuporteConsole 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 para oSuporteentãoSuportepode 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 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 mensagem de erro: “Falha na importação. Unable to find virtual machine import file under location...".	Esse erro pode ocorrer pelos seguintes motivos: • 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.
Você tenta importar um gateway e recebe a mensagem de erro: “Falha na importação. 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.
Você tenta importar um gateway e recebe uma mensagem de erro: “Falha na importação. Import failed because the virtual machine must have a new	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.

Problema	Medida a ser tomada
identifier. Select a new identifier and try the import again".	
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 de.
Você tenta iniciar uma VM do 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 de.
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 para o Microsoft Hyper-V Storage Gateway 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.

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 querSuportepara 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. Uma instância baseada na AMI do Storage Gateway deve 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 querSuportepara 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 ativação doSuportePara acessar o gateway para ajudá-lo a solucionar problemas de gateway. Por padrão,SuporteO 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 grupos de segurança e como adicionar regras a eles, consulteGrupos de segurança do Amazon EC2noGuia do usuário do Amazon EC2.

Para deixarSuporteConecte-se ao seu gateway, primeiro faça login no console local da Instância do EC2 do Amazon, navegue até o console do gateway de armazenamento e ofereça acesso.

Para habilitar oSuporteAcesso 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 instânciaanoGuia 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.

2. No prompt, insira**6 - Command Prompt**para abrir oSuporteConsole 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 para oSuporteentãoSuportepode 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 encerrar sessão na instância do Storage Gateway.

Como solucionar problemas do dispositivo de hardware

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 em seu dispositivo, entre em contato com a equipe do Storage Gateway Hardware Appliance para obter Support, 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, você deve alterar 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 oHardwareNo console Storage Gateway, conforme mostrado a seguir.

Onde obter suporte ao equipamento de hardware

Para contatar o suporte do Storage Gateway Hardware Appliance,Suporte.

OSuporteA 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 paraSuporte.

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. É possível 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

: ERROR ObjectMissing

Você pode obter um`ObjectMissing`Erro quando um gravador diferente do gateway de arquivos determinado exclui o arquivo especificado do Amazon FSx. Todos os uploads subsequentes no Amazon FSx ou as recuperações do Amazon FSx para o objeto falharão.

Para resolver um erro ObjectMissing

1. Salve a cópia mais recente do arquivo no sistema de arquivos local do cliente SMB (você precisa dessa cópia de arquivo na etapa 3).
2. Exclua o arquivo do gateway de arquivos usando o cliente SMB.
3. Copie a versão mais recente do arquivo que você salvou na etapa 1 do Amazon FSx usando o cliente SMB. 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 contatoSuporte.

: 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.

: ERROR 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 emAWScontas 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
- Seu gateway não está respondendo
- Você não vê arquivos em seu sistema de arquivos Amazon FSx
- Seu gateway está transferindo dados lentamente para o Amazon FSx
- Seu trabalho de backup do gateway falha ou há erros ao gravar no gateway

Seu gateway reage lentamente ao navegar em diretórios

Se o gateway de arquivos reage lentamente ao executar olscomandos ou navegar diretórios, verifique o`IndexFetch`e`IndexEviction`Metrics (CloudWatch):

- Se o`IndexFetch`métrica é maior que 0 quando você executa um`ls`Comando ou navegar por diretórios, o gateway de arquivos começou sem informações sobre o conteúdo do diretório afetado e precisava acessar o Amazon S3. Os esforços subsequentes para listar o conteúdo desse diretório deverão ocorrer com mais rapidez.
- Se o`IndexEviction`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 contatoSuporte.

Discutir comSuporteO conteúdo do sistema de arquivos do Amazon FSx 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 está 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.

Você não vê arquivos em seu sistema de arquivos Amazon FSx

Se você perceber que os arquivos no gateway não são refletidos no sistema de arquivos Amazon FSx, 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 gateway está transferindo dados lentamente para o Amazon FSx

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, significará que 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 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.

Seu trabalho de backup do gateway falha ou há erros ao gravar no gateway

Se o trabalho de backup do gateway de arquivos falhar ou se houver erros ao gravar no gateway de arquivos, faça o seguinte:

- Se o`CachePercentDirty`A métrica é 90% ou acima, o gateway de arquivos não consegue aceitar novas gravações em disco porque não há espaço disponível suficiente no disco de cache. Para ver a velocidade em que o gateway de arquivos está fazendo upload para o Amazon FSx ou o 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 for 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.

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 contatoSuporte.

: 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 Amazon Machine Image (AMI) do Amazon EC2. Se a VM do gateway apresentar problemas, ative um novo gateway e recupere seus dados para esse gateway usando as instruções a seguir.

Tópicos

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 sua conexão de gateway FSx File Gateway com endpoints de 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 do Amazon EC2. Se você não tiver acesso a outro datacenter, recomendamos criar o gateway em uma instância do Amazon EC2. As etapas que você segue dependem do tipo de gateway cujos dados você está cobrindo.

Para recuperar dados de um gateway de 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.

Recursos adicionais Storage Gateway

Nesta seção, você encontra informações sobre oAWSE 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

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 melhores práticasNo 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 do Storage GatewayMenu principal, insira**4**peloGerenciamento do tempo 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 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 instânciaEscolha a configuração de hardware da instância do. O Storage Gateway tem suporte para 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 for0. 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, escolhaAdicionar 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 segurança, adicione regras de firewall para um tráfego específico alcançar a 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, escolhaExecutar.

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 Managerrepositório 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 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 no atualAWSRegião :

   ```
   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_FSX/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 à API 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. Usando oAWS 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 como oAWS 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 aoAWS 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.

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 básicas sobre recursos e IDs de recurso do gateway

No Storage Gateway, o principal recurso 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 também oferece suporte ao 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 Storage Gateway aparecem em maiúscula Entretanto, 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.

> **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 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 de linha de comando (CLI) Storage Gateway. Os procedimentos a seguir mostram como adicionar, editar e excluir uma tag no console.

Para adicionar uma tag

1. Abra o console 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 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 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 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 noAWS 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 no Linux Kernel-based Virtual Machine (KVM):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 Amazon FSx File Gateway

Várias ferramentas e licenças de terceiros são usadas para fornecer a funcionalidade Amazon FSx File Gateway (FSx File Gateway).

Use os links a seguir para baixar o código-fonte de determinados componentes de software de código aberto incluídos com o software FSx File Gateway:

- Para o Amazon FSx File Gateway 2021-07-07:sgw-file-fsx-smb-open-source.tgz
- Para o Amazon FSx File Gateway 2021-04-06 Versão:sgw-file-fsx-smb-20210406-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, consulte os seguintes links:

- Para o Amazon FSx File Gateway 2021-07-07: Licença de terceiros.

- Para o Amazon FSx File Gateway 2021-04-06 Versão: Licença de terceiros.

Cotas

Cotas para sistemas de arquivos do

A tabela a seguir relaciona as cotas para sistemas de arquivos.

Recurso	Limite por sistema de arquivos
Número máximo de tags	50
Período de retenção máximo para backups automatizados	90 dias
Número máximo de solicitações de cópia de backup em andamento para uma única região de destino por conta.	5
Capacidade mínima de armazenamento, sistemas de arquivos SSD	32 GiB
Capacidade mínima de armazenamento, sistemas de arquivos HDD	2.000 GiB
Capacidade máxima de armazenamento, SSD e HDD	64 TiB
Capacidade mínima de transferência	8 MBps
Capacidade máxima de transferência	2.048 MBps
Número máximo de compartilhamentos de arquivos	100.000

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
Gateway de arquivos FSx	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 eles tenham sido alocados anteriormente como cache.

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 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 nora 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 recalcula a assinatura usando a mesma função de hash e a entrada que você usou para assinar a solicitação. Se a assinatura resultante corresponde à assinatura na solicitação, o Storage Gateway processa a 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 de 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. VerificarAWSChave 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 de 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 possível encontrar a associação do sistema de arquivos especificada.	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 obter uma lista das operações do Storage Gateway, consulte oAçõesnoAWS Storage GatewayReferência de API do.

Histórico do documento para o Guia do usuário do Amazon FSx File Gateway

- Versão da API: 30/06/2013
- Atualização de documentação mais recente: 07 de julho de 2021

A tabela a seguir descreve as versões da documentação do Amazon FSx File Gateway. Para receber notificações sobre atualizações dessa documentação, você pode se inscrever em um feed RSS.

update-history-change	update-history-description	update-history-date
Suporte do sistema de arquivos múltiplos	O Amazon FSx File Gateway agora oferece suporte a até cinco sistemas de arquivos Amazon FSx conectados. Para obter mais informações, consulteAnexar um sistema de arquivos do Amazon FSx for Windows File Server.	7 de julho de 2021
Suporte à cota de armazenamento flexível do Amazon FSx	O Amazon FSx File Gateway agora oferece suporte a cotas de armazenamento flexível (que avisam quando os usuários ultrapassam seus limites de dados) ao gravar em sistemas de arquivos Amazon FSx conectados onde as cotas de armazenamento estão configuradas. Cotas rígidas (que impõem limites de dados negando acesso de gravação) não são suportadas. As cotas flexíveis funcionam para todos os usuários, exceto o usuário	7 de julho de 2021

	administrador do Amazon FSx. Para obter mais informaçõ es sobre a configuração de cotas de armazenamento, consulteCotas de armazenam entonoGuia do usuário do Amazon FSx for Windows File Server.	
Novo guia	Além do gateway de arquivos original (agora conhecido como Amazon S3 File Gateway), o Storage Gateway fornece o Amazon FSx File Gateway (FSx File). O FSx File fornece baixa latência e acesso eficiente a compartil hamentos de arquivos do FSx for Windows File Server na nuvem a partir de sua instalação local. Para obter mais informações, consulteO que é o Amazon FSx File Gateway?	27 de abril de 2021

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.